

IIBF ADDA

Certificate Examination

in

CAIIB –IT

2019

Compiled by

Srinivas Kante B.Tech, CAIIB

About Certificate Examination in

CAIIB Elective Subject – Information Technology

The CAIIB holders are allowed to take the Certificate Examinations in 11 elective subjects in order to enhance their knowledge and skill in specialised areas as a part of Continuing Development Program.

Candidates must have completed CAIIB or PART-II of the Associate Examination, and their membership subscription should not be in arrears. Since the examination of all elective papers will be conducted in a single day, candidates can apply for only one elective paper at a time.

1. Corporate Banking 7. Human Resources Management
2. Rural Banking 8. Information Technology
3. International Banking 9. Risk Management
4. Retail Banking 10. Central Banking
5. Co-operative Banking 11. Treasury Management
6. Financial advising

Candidates may choose the elective in the area they are currently working or in the area they would like to work in future. It is suggested that the candidates may choose the elective in the area they are currently working and later move to other elective as this will enable appropriate skills / build up for handling different banking verticals.

MEDIUM OF EXAMINATION

PATTERN OF EXAMINATION

Candidates are allowed to attempt the examination either in Hindi or English, and should clearly fill in their choice of medium in the Examination Application Form. In any case change of medium will not be allowed at a later stage

(i) Each Question Paper will contain approximately 100 objective type multiple choice questions, carrying 100 marks including questions based on case study / case lets. The Institute may, however, vary the number of questions to be asked for a subject. There will NOT be negative marking for wrong answers.

(ii) Examination will be conducted under online mode only on a Sunday.

Questions for the examination will be asked for :

- (i) Knowledge testing

- (ii) Conceptual grasp
- (iii) Analytical / logical exposition
- (iv) Problem solving
- (v) Case analysis

Further, questions based on current developments in banking and finance may be asked.

Candidates are advised to refer to financial news papers / periodicals more particularly "IIBF VISION" and "BANK QUEST" published by the Institute.

DURATION OF EXAMINATION

PERIODICITY AND EXAMINATION CENTRES

PASSING CRITERIA

PROCEDURE FOR APPLYING FOR EXAMINATION

STUDY MATERIAL / WORKBOOK

TUTORIAL / CONTACT PROGRAMMES

SYLLABUS

The duration of the examination will be of 2 hours.

(i) The examination will be conducted normally twice a year in May / June and November / December on Sundays. The schedule of the examination will be announced by the Institute at least 3 months before the examination.

(ii) A list of Examination Centres will be available in the online examination Application Form.

i) Pass : Minimum marks for pass in every subject - 50 out of 100 marks.

Application for examination should be made online from the Institute's website www.iibf.org.in.

No physical form will be accepted by the Institute with effect from 1st January, 2013.

The Institute has published courseware to facilitate study and they will be available at outlets / showrooms / distributors of M/s. Macmillan India Pvt. Ltd. (Please visit iibf web-site www.iibf.org.in for details).

Tutorial / Contact programmes will be organized by the Institute at various centres. For details in this regard candidates may get in touch with Zonal Office or logon to the Institute's website www.iibf.org.in.

INFORMATION TECHNOLOGY

Module - A : Introduction to Information Technology

Impact of IT on Banking : Changing Financial Environment and IT as a Strategic Responses

Hardware (H / W) - Software : (S / W)

System Software :

Operating Systems (Desktop OS / Server OS) Windows (Desktop / Server) / UNIX (H. P. Unix, Sun Solaris, Linux, IBM AIX)

Computer Languages - 1st Generation Languages (Assembly), 2nd Generation (Fortran, Algol, Cobol), 3rd Generation (C, C++, C# and JAVA etc.) and 4th Generation Languages (Clipper, Power Builder, SQL etc.) and 5th Generation Languages (Logic Programming Languages)

Database Management System and Relational Database Management Systems (Oracle10g, MS SQL-2005, MySQL)

Application Servers (Oracle 10AS, BeWeblogic, WebSheare)

Web Servers (IIS, Apachi etc.)

Web Browsers (IE 7.0, Firefox etc.)

Application Software : Packaged Software, Custom built Software etc.

Computer Networks, Equipment & Data Communication:

Computer Networks : Network Layers, Topologies, Protocols, IP Address Mechanisms, LAN, WAN, VLAN, Intranet, Extranet, Interne

Network Equipments : Cables (BNC, Twisted Pair, Fibre Optics), Connectors, I/Os, Patch Panel, Jack Panels, Network Racks.

Data Communication : CLL, Leased Lines, MPLS, VPNS, ISDN, Satellite Links, Wi Fi, Wi Max.,

Network / Security Equipments: Modems, Hubs, Switches, Bridges, Routers, Firewalls, NIDS, HIDS, IPS

Module - B : Systems and Design

Systems Design & Analysis(Data modeling, Entity Relationships, Generic Data

Modeling, Semantic Data modeling Normalization(from 1st to 3rd and BCNF, 4th & 5th level of normalization)

Software Development Life Cycle (SDLC) - Various phases of SDLC, In-house / Outsourcing,

Software Project Management, Computer Aided Software Engineering (CASE)

Tools.

System Architecture : Clients (Hardware / Software), Servers (Hardware / Software). Client
Server Architecture, 3 Tier Architecture, N-Tier Architecture etc.

Data Warehousing - Data Mining tools

MIS and Organization Support Systems - DSS, EIS, GDSS, Groupware and Multimedia

Business Intelligence - Expert Systems, Artificial Neural Networks (ANN)

Grid Computing, Virtualization and Consolidation.

Module - C : Applications in Banking

Centralized Banking System / Core Banking System / System Administration, Database
Administration, Application Server and Application Administration, Network Administration,
Domains, ISPS, Hosting, Data Downloads / Uploads, Band widths, Data Centre, Data
Storage Devices, Data Backups / Restoration, Disaster Recovery Centre

Delivery Channels - ATM, EFTPOS, Phone Banking, Internet Banking, SMS Banking, Mobile
Banking, Credit / Debit Cards, Smart Cards

E-Mails, SMS alerts

E-Commerce - Secure Electronic Transfer (SET), Payment Gateways (Credit card / Debit
cards), Authentication of payments etc.

PKI - CCA, CA, RA, Digital Certificate, Digital Signature, Non-repudiation of Origin, Nonrepudiation
of Receipt.

Service - Level Agreement

Module - D : Security, Controls and Guidelines

Threats to Information System : i) Physical (Insiders / outsiders) ii) Viruses, Worms,
Trojan horse, Malwares, Software bombs, Phishing, Spoofing, Spamming, denial of service
attacks etc.

Information System Security Measures, Policy, controls, ISO, 17799, BS7799,
IS4477, IS Audit, BCP / DRP, IT Act 2000, Basel guidelines for E-banking, Various
RBI Committee Reports on Information Systems.

IT Service Delivery & Support : Service level management practices, Operations
management - work load scheduling, network services management, Preventive
maintenance, Systems performance monitoring process tools, techniques, Functionality
of hardware, software, data base. Drafting of RFP, system specifications, SLAs, Capacity
planning & monitoring, Change management processes / scheduled, emergency in
configuration of production systems, application of patches, releases etc., Incident &
problem management practices, System resiliency tools and techniques - fault tolerance,
elimination of single point of failure, clustering

Questions asked in Morning Shift:

1. SDLC phase and definition
 2. Normalization definition
 3. Threats and attacks in network.
 4. Routers/Switch/Firewall
 5. Honey Pot
 6. Biometrics.
 7. Disaster avoidance.
 8. Phases of CMM.
 9. SQL query commands.
 10. DDL/DML
 11. NEFT/RTGS/FEDWIRE
 12. SLA Negotiation
 13. Purging of data.
 14. Artificial Intelligence
 15. Spamming/Eavesdropping/Phishing
 16. Digital Signature
 17. IDEA encryption
 18. RAID
 19. Generalized Audit Software
 20. Virtual Classroom concept
 21. Web SAFARI
 22. Strategic Information
 23. Fibre Optic cables.
 24. Blooms Taxonomy
 25. OLAP
 26. Deferred Payment System
 27. SFMS
 28. Floor Limit ??
 29. Software Escrow Management?
 30. Types of cards?
 31. Call Centre Benchmarks?
-

32. Hash Function used in Digital Signature?

33. SCORM benefit?

34. Characteristics of BHIM ?

35. Rupay Cards used in ?

Introduction to Information Technology

Introduction With information technology (IT) going mobile, thanks to the deployment of faster and more reliable broadband networks, we are experiencing yet another technology driven transition. Technology (-based) businesses can be referred to as businesses that engage in technology related products, processes and services. They may be low-, medium- or high technology. One area of the economy which has seen significant growth is that focused on new technology-based products and services and the high-technology sectors are perceived as major sources of future economic prosperity and employment growth. However, IT includes the management information systems (computers, hardware, software, networks) used to automate and support business tasks and decision-making. IT is used to automate simple, routine tasks such as word processing and advanced processes such as production, scheduling and logistics. In this manner, information technology enables businesses to operate efficiently and profitably. Technological advances in the past few decades have greatly increased the competitive nature of the economic business world. Companies have used software, computers and the Internet to transform their businesses from local places of business to national and global market competitors. Many companies have responded to these changes by automating their business processes and capturing industry-related information and using it to their advantage. Technology has also forced businesses to remain flexible, adapting their operations to newer and better technological advances. Business owners once had very few tools at their disposal: little more than a basic adding machine and paper records. Today's business owners can complete their duties much more effectively than their predecessors with an array of technological tools at their disposal. By using these techtools,

companies and employees enjoy a number of business-related benefits. We know that the business sector produces products and services for profit. Information technology describes any technology used to create, process and disseminate information that is critical to business performance. Information technology is important to the business sector as a management tool to optimize the processing of information to produce goods and services for profit. Automation improvements achieved by deploying

information technology usually decrease the number of personnel required. Economies of scale gained through the deployment of information technology reduce the overall cost for businesses to produce products and services. This has an overwhelmingly positive effect on the financial goals of a business. Quality assurance entails systematic testing to ensure that a business is producing quality goods and services for its customers. Rigorous quality standards help business outputs meet the required specifications. Quality assurance can be used within processes such as marketing, customer support and accounting, as well as product testing. The effective and efficient processing of information related to achieving quality assurance goals is key to the delivery of quality goods and services to business customers. Investments in information technology can help make a firm's operational processes substantially more efficient, and its managerial processes much more effective. By making such improvements to its business processes a firm may be able to:

1. Dramatically cut costs
2. Improve the quality and customer service
3. Develop innovative products for new markets

Investments in information systems technology can result in the development of new products, services, and processes. This can:

1. Create new business opportunities
2. Enable a firm to enter new markets
3. Enable a firm to enter into new market segments of existing markets.

About strategic, competitive advantage plays a fundamental role in the success of a given business within its sector. Information technology has become fundamental to acquiring competitive advantage. The combination of process improvements, cost reductions, communications and quality assurance all contribute to the competitive advantage of a business unit. However, the constant identification and analysis of new risks and opportunities are critical to the ongoing success of a business. Evolving Internet aggregation technologies, including social networks, blogs and subscription databases, are becoming important tools needed to achieve and maintain advantages within the business sector. The transfer of information is a significant impact of information technology in business. Companies gather information from both internal and external sources with more efficiently than in previous years. Email is now a common form of business communication that results in near-instant messages that deliver important information.

2. The Role of Information Technology

2.1 Importance of Information Technology in business relationships

The social interaction of a business relationship can be discussed in terms of how often people from the companies meet, or how well the parties know each other. It is argued that depending on the extent of the use of information technology for different exchanges, the impact on the social interaction patterns that are carried out without information technology may be influenced. One argument that could be raised in the theorizing on the effect of use of information technology in business relationships is that the number of meetings, or need for meetings will decrease, as the use of the technology handles a great deal of information exchanges, i.e. replaces some of the personal exchange of information. The question is if the need for personal meetings decreases when the levels of information technology use increase. That would suggest increased efficiency of meetings, as the use of information technology then replaces other means of interaction for some types of exchanges. On the other hand, the use of information technology may require additional meetings, if the technology is difficult use or the purpose of its employment is another than making the information exchange more efficient by decreasing the need for meetings. The reasons why the use of information technology in business relationships would decrease or increase the need for personal meetings can only be speculated on.

The social interaction of a business relationship can be discussed in terms of how often people from the companies meet, or how well the parties know each other. It is argued that depending on the extent of the use of information technology for different exchanges, the impact on the social interaction patterns that are carried out without information technology may be influenced. One argument that could be raised in the theorizing on the effect of use of information technology in business relationships is that the number of meetings, or need for meetings will decrease, as the use of

exchanges, i.e. replaces some of the personal exchange of information. The question is if the need for personal meetings decreases when the levels of information technology use increase. That would suggest increased efficiency of meetings, as the use of information technology then replaces other means of interaction for some types of exchanges. On the other hand, the use of information technology may require additional meetings, if the technology is difficult use or the purpose of its employment is another than making the information exchange more efficient by decreasing the need for meetings. The reasons why the use of information technology in business relationships would decrease or increase the need for personal meetings can only be speculated on. This paper analyses the extent to which the need for personal meetings has decreased or increased in the investigated business relationships as a result of the use of information technology, as well as to the extent which such a change is related to levels of

lower and higher of information technology. If the use of information technology affects the need for personal meetings, and that effect is related to when the use is lower or higher, it is interesting to analyze why and how the need for personal meetings is affected by the use of information technology. Now, most organizations in all sectors of industry, commerce and government are fundamentally dependent on their information technologies. The information revolution is sweeping through our economy. No company can escape its effects. Dramatic reduction in the cost of achieving, processing, and transmitting information is changing the mode by which we do business. This article moves towards the explaining and distinguishing impact IT has on internal and corporate strategies in small and medium enterprises. The information revolution is sweeping through information is changing the mode by which we do business. Many companies in most our economy; no company can escape its effects. Dramatic reduction in the cost of achieving, processing, and transmitting industries have little choice but to implement some form of information technology in order to remain both innovative and on the cutting edge of competitive advantage.

2.2 View of Information Technology's Relationship to Business

There are two basic concepts or principles that can be effectively executed and applied within an organization to help the organization succeed when it comes to Information Technology [1].

- Link Information Technology Solutions to Overall Business Strategy
- Keep IT Simple

Maintaining focus on the overall goals and mission of an organization while looking at Information Technology enables management to make appropriate investments, reduce cost, and provide value. We recommend a top-down approach and have found the seven layer OSI (Open Systems Interconnection) Model an excellent tool to help think about Information Technology needs. OSI is an international standard to help implementers, developers, technicians, and service providers ensure software and hardware properly work with one another and communication can occur within the network and with end-users. We found the same approach can be used when thinking about your Information Technology needs. By looking at the "big picture", it is possible to align your business processes and Information Technology needs with the overall strategy and goals of your organisation. Strategy, Goals, Mission and Culture drive Business Processes. Business Processes determine necessary tasks (who, what, why, where and how). The tasks define the Information Technology requirements (software and hardware) to be investigated, decided upon, and implemented. The challenge occurs when discussing the tasks and

Information Technology requirements. The communication channel tends to break down. This is known by many as the “IT Divide”. Both sides have their own jargon, abbreviations, and unique experiences. Neither is able to explain, in terms understandable by the other, the necessary requirements, limitations, gaps, and potential solutions that are an acceptable fit. Executives, Managers and Technologists each go their own way out of frustration with one another. And the alignment of business processes and strategy with Information Technology goes by the wayside. Information Technology success comes from having a common understanding. Everyone on the team needs to take a look at the total picture and approach the solution with the same view and goal. If this occurs it is possible to align business processes and Information Technology needs with the overall strategy and goals of an organization. The result is motivated employees, satisfied customers, and reduced costs.

2.3 Keep “IT” Simple

We have found many organizations have a tendency to complicate their Information Technology environment. It is our belief that Information Technology should not and does not need to be complicated. We believe organizations should focus on keeping “IT” simple. By simplifying and consolidating an organization’s Information Technology there is [2]:

- Reduced or lowered costs,
- Improved efficiency and increased consistency,
- Easier overall administration,
- Ability to respond quicker to change, and
- Better use resources (hardware, software and people).

Some Keep “IT” Simple” recommendations are:

- Standardize on hardware and software,
- Develop and follow policies and procedures,
- Document your network infrastructure,
- Purchase and use proven products from well known and reliable vendors,
- Select and integrate application systems prudently, and
- Limit business workstation use to business use only.

It is our experience that the more complex the environment, the more complicated it becomes as well as inflexible. This results in additional time and effort needed to maintain and/or change the environment increasing operational and maintenance costs. By keeping IT simple we have found funds can be reallocated from maintenance and routine operational activities to spending on strategic information technology and/or operational needs that support the overall organizational objectives and goals. How can the preceding competitive strategy concepts be applied to the strategic role of information systems? Information technology can be used to implement a variety of competitive strategies. These include the five basic competitive strategies (differentiation, cost, innovation, growth, alliance), as well as other ways that companies can use information systems strategically to gain a competitive edge. For example:

- 1) Lower Costs
- 2) Differentiate
- 3) Innovate
- 4) Promote Growth
- 5) Develop Alliances
- 6) Improve quality and efficiency
- 7) Build an IT platform
- 8) Other strategies • use interorganizational information systems to create switching costs that lock in customers and suppliers.
 - use investments in IT to build barriers to entry against industry outsiders.
 - use IT components to make substitution of competing products unattractive.

3. Reengineering Business Processes

One of the most popular competitive strategies today is business process reengineering (BPR), most often simply called reengineering. Reengineering is the fundamental rethinking and radical redesign of business processes to achieve dramatic improvements in cost, quality, speed, and service. BPR combines a strategy of promoting business innovation with a strategy of making major improvements to business processes so that a company can become a much stronger and more successful competitor in the marketplace. **3.1 How To Implement Business Process Reengineering In Your Business?** The following steps (Davenport, 1992) can help BPR realize its core principles of customer satisfaction, reduced costs of business and increased competitiveness [3]. Business vision and objectives: Any BPR activity needs to begin with a clearly defined and measurable objectives. Whether the goal is reducing

costs, improving quality of product, or increasing efficiency, the framework for what needs to be achieved has to be decided upon at the outset, in line with the company's vision and mission.

Identification and slacking processes: Once a clear goal is in mind, all processes need to be studied and those seen as 'slacking' or that can be improved need to be identified.

Among these, those processes with direct impact on the company's output or those that clash with the company's mission become part of the 'red' list. This clear identification makes the difference between BPR success and failure. **Understand and measure the 'red' processes:** With a list of slacking processes in hand, it is imperative to identify how they were identified as such. Are they taking too much time to complete? Is the quality of the outcome being compromised? Whatever the issue, each process must be judged objectively either against industry standards or ethically obtained competitor best practices. **Information system and technology capabilities:** An efficient and relevant IT system is an essential BPR enabler. Without such a system, it is not possible to keep a check on all factors affecting the change. Before setting out on a radical BPR activity, it is vital to set in place information systems that can deal with the magnitude of the change. Design, build and test the new prototype: Before any new product is launched, a prototype is tested out. A failure at a testing stage should never be implemented at a larger scale. BPR projects fail more often than not for a variety of reasons but a basic reason is the inability to identify and accept any limitations at the testing stage. Among other factors, both the management's attitude towards the new way of work and the employees' outlook towards the change should be carefully assessed. Adapting the organization: Managing change brought about by BPR activities is the final effort towards a successful project. Providing updated documentation, organizational structures, governance models as well as updated charts of authority and responsibility leave little room for confusion and allow a smooth transition into the new way of work. Business process reengineering is a radical change activity that cannot be repeated if it goes wrong the first time. It is often a high risk activity that involves monetary investment and a risk of demotivated employees. It is essential to have buy in all the way from top management down and it should have a broad functional scope. It is Important To Acknowledge and understand that BPR is not a foolproof method of success. As with all activities it runs the risk of failure [4]. **A BPR program can be successful if:**

- Customer needs are made the priority and this vision is used to appropriately direct business practices.
- There are cost advantages to be achieved that help the organization become more competitive in its industry
- A strategic view of all operational processes is taken with relevant questions being asked about the established way of work and how it can be developed over the long term into more efficient business practices.

- There is a willingness to look beyond tasks and traditional functional boundaries with a focus outcomes.
- Through

this, entire processes can be eliminated or amalgamated into fewer but more relevant and powerful processes throughout the organization.

- There is a real desire to simplify the way of work by objectively assessing all activities and tasks and eliminating any that add less value and more complexity.

A BPR program will fail if:

- It is seen as a way to make minor adjustments and improvements to existing processes. If there is no clear willingness to put all existing process onto the chopping block, there is no chance of success.
- It is seen as a one-time cost cutting exercise. In reality, cost reductions are often a handy by product of the activity but not the primary concern. It is also not a one-time activity but an ongoing change in mindset
- There is no success in gaining dedicated long term commitment from management and the employees. Bringing people onboard is a difficult task and many BPR initiatives never take off because enough effort is not put into securing support
- There is less effort to redesign and more to automate.
- One department is prioritized at the expense of the process. There needs to be an openness towards studying every single process in detail and a willingness to change whatever is needed to achieve overall efficiency.
- There is too much internal focus and not enough of an eye on the industry and what competitor best practices can be used as benchmarks.

4. Information Technology And Competitive Advantage

Although the objective of any Information IT business unit is the enhancement of modern firm's performance - through the improvement of the quality of managerial decisions - in the absence of an adequate alignment between IT and Business objectives, the attainment of the firm's agility status is jeopardized, and consequently, the chances of achieving the IT-Business competitive advantage are reduced. The strategic role of information systems involves using information technology to develop

products, services, and capabilities that give a company strategic advantages over the competitive forces it faces in the global marketplace. This creates strategic information systems, information systems that support or shape the competitive position and strategies of an enterprise. So a strategic information system can be any kind of information system (TPS, MIS, DSS, etc.) that helps an organization:

- 1) Gain a competitive advantage
- 2) Reduce a competitive disadvantage
- 3) Meet other strategic enterprise objectives

Information technology emerges as an essential asset of modern firms' competitive advantage, because it connects all business functions and supports managerial decision processes - both essential conditions for the attainment of the organization agility level.

Conclusion

Information technology can change the way businesses compete. For this reason, you should view information systems strategically, that is, as vital competitive networks, as a means of organizational renewal, and as a necessary investment in technologies that help an enterprise achieve its strategic objectives.

The evidence also suggests that turning investment in ICT into higher productivity is not straightforward. It typically requires complementary investments and changes, e.g. in human capital, organizational change and innovation. Moreover, ICT-related changes are part of a process of search and experimentation, where some firms succeed and grow and others fail and disappear. Countries with a business environment that enables this process of creative destruction may be better able to seize benefits from ICT than countries where such changes are more difficult and slow to occur. As a result, small businesses are investing in information and communication technologies to expand information systems applications to support their business strategy and thereby establish a competitive advantage based on the unique capability created in their markets. Consequently alignment between an organization's business strategy and its information systems strategy positively affects business performance.

THE ROLE OF TECHNOLOGY IN BANKING INDUSTRY

The banking sector has embraced the use of technology to serve its client's faster and also to do more with less. Emerging technologies have changed the banking industry from paper and branch based banks to "digitized and networked banking services. Unlike before, broadband internet is cheap and it makes the transfer of data easy and first. Technology has changed the accounting and management system of all banks. And it is now changing the way how banks are delivering services to their customers. However this technology comes at a cost, implementing all this technology has been expensive but the rewards are limitless. Below I have listed some of the roles of technology in the banking industry.

- **E-banking:** This enables the bank to deliver its services easily to its high end customers. To make the system user friendly to all clients, banks have used a Graphical User Interface (GUI) , with this software , customers can access their bank details on their own computers, make money transfers from one account to another, print bank statements and inquire about their financial transactions. Another technology used by banks to exchange data between the bank and clients is called Electronic Data Interchange (EDI); this software can be used to transmit business transaction in a computer-readable form. So the client on the other end will be in position to read the information clearly.
- **NRI Banking Services:** This technology has been embraced in countries like India, USA, UAE, just to mention but a few. Since many people go abroad to work, they have a need of supporting their families. So technology has made it simple for them to send money to their loved ones easily.

- **RURAL Banking:** Unlike in the past when banking was centralized in urban areas, now day's technology has made it simple to set up banking facilities in rural areas. For example: In Africa, they have introduced Mobile money banking facilities. In this case a user in a rural area will have an account with a mobile company which is opened for free. They can then deposit money on that account via a near by mobile money operating center. This money can be withdrawn at any time any were in that area and they can also receive or send money using the same system.



- **Plastic money:** Credit cards or smart cards like "VISA ELECTRON" have made the banking industry more flexible than before. With a credit card , a customer can borrow a specific amount of money from the bank to purchase any thing and the bank bills them later. In this case, they don't have to go through the hassle of borrowing small money. Then with "Smart Cards" like visa electron , a customer can pay for any thing using that card and that money is deducted from their bank accounts automatically, they can also use the same card to deposit or withdraw money from their accounts using an ATM machine.
- **Self-inquiry facility:** Instead of customers lining up or going to the help desk, banks have provided simple self inquiry systems on all branches. A customer can use their ATM card to know their account balance, or to get their bank statement. This saves time on both sides.
- **Remote banking:** Banks have installed ATM machines in various areas; this means a customer does not have to go to the main branch to make transactions. This facility has also enabled anytime banking, because customers can use ATM machines to deposit money on their accounts. Remote banking has helped people in rural areas improve on their culture of saving money.
- **Centralized Information results to quick services:** This enables banks to transfer information from one branch to another at ease. For example, if a customer registered their account with a rural branch, they can still get details of their account while at the main bran in an urban area.
- **Signature retrieval facilities:** Technology has played a big role in reducing fraud in banks which protects its clients. For example, banks use a technology which verifies signatures before a customers withdraws large sums of money on a specific account and this reduces on the errors or risks which might arise due to forgery.

The New Era

The 21st century will bring about an all-embracing convergence of computing, communications, information and knowledge. This will radically change the way we live, work, and think. The growth of high speed networks, coupled with the falling cost of computing power, is making possible applications undreamed of in the past. Voice, data, images, and video may now be transferred around the world in micro-seconds. This explosion of technology is changing the banking industry from paper and branch banks to digitized and networked banking services. It has already changed the internal accounting and management systems of banks. It is now fundamentally changing the delivery systems banks use to interact with their customers. All over the world, banks are still struggling to find a technological solution to meet the challenges of a rapidly-changing environment. It is clear that this new technology is changing the banking industry forever. Banks with the ability to invest and integrate information technology will become dominate in the highly competitive global market. Bankers are convinced that investing in IT is critical. Its potential and consequences on the banking industry future is enormous.

Technology and Banks Transformation

Computers are getting more sophisticated. They have given banks a potential they could only dream about and have given bank customers high expectations. The changes that new technologies have brought to banking are enormous in their impact on officers, employees, and customers of banks. Advances in technology are allowing for delivery of banking products and services more conveniently and effectively than ever before - thus creating new bases of competition. Rapid access to critical information and the ability to act quickly and effectively will distinguish the successful banks of the future. The bank gains a vital competitive advantage by having a direct marketing and accountable customer service environment and new, streamlined business processes. Consistent management and decision support systems provide the bank that competitive edge to forge ahead in the banking marketplace.

Major applications. The advantages accruing from computerization are three-directional - to the customer, to the bank and to the employee.

For the customer. Banks are aware of customer's need for new services and plan to make them available. IT has increased the level of competition and forced them to integrate the new technologies in order to satisfy their customers. They have already developed and implemented a certain number of solutions among them:

- *Self-inquiry facility:* Facility for logging into specified self-inquiry terminals at the branch to inquire and view the transactions in the account.
- *Remote banking:* Remote terminals at the customer site connected to the respective branch through a modem, enabling the customer to make inquiries regarding his accounts, on-line, without having to move from his office.
- *Anytime banking- Anywhere banking:* Installation of ATMs which offer non-stop cash withdrawal, remittances and inquiry facilities. Networking of computerized branches inter-city and intra-city, will permit customers of these branches, when interconnected, to transact from any of these branches.
- *Telebanking:* A 24-hour service through which inquiries regarding balances and transactions in the account can be made over the phone.
- *Electronic Banking:* This enables the bank to provide corporate or high value customers with a Graphical User Interface (GUI) software on a PC, to inquire about their financial transactions and accounts, cash transfers, cheque book issue and inquiry on rates without visiting the bank. Moreover, LC text and details on bills can be sent by the customer, and the bank can download the same. The technology used to provide this service is called electronic data interchange (EDI). It is used to transmit business transactions in computer-readable form between organizations and individuals in a standard format.
- As information is centralized and updates are available simultaneously at all places, single-window service becomes possible, leading to effective reduction in waiting time.

For the bank. During the last decade, banks applied IT to a wide range of back and front office tasks in addition to a great number of new products. The major advantages for the bank to implement IT are:

- Availability of a wide range of inquiry facilities, assisting the bank in business development and follow-up.
- Immediate replies to customer queries without reference to ledger-keeper as terminals are provided to Managers and Chief Managers.

- Automatic and prompt carrying out of standing instructions on due date and generation of reports.
- Generation of various MIS reports and periodical returns on due dates.
- Fast and up-to-date information transfer enabling speedier decisions, by interconnecting computerized branches and controlling offices.

For the employees. IT has increased their productivity through the followings:

- Accurate computing of cumbersome and time-consuming jobs such as balancing and interest calculations on due dates.
- Automatic printing of covering schedules, deposit receipts, pass book / pass sheet, freeing the staff from performing these time-consuming jobs, and enabling them to give more attention to the needs of the customer.
- Signature retrieval facility, assisting in verification of transactions, sitting at their own terminal.
- Avoidance of duplication of entries due to existence of single-point data entry.

A search of the banking literature reveals that banks are moving rapidly to take advantage of recent and new customer service and cost reduction opportunities that new technologies offer. A sampling is in the table below:

Technology	Current Use	Use in Next 3 Years.
------------	-------------	----------------------

Infrastructure

PC Networks: Tellers	48%	80%
Sales Tracking Software	44%	80%
Relational Data Base	36%	76%
Automate Credit Scoring	8%	48%
E-mail	60%	95%
Equipment Management Software	33%	57%
Imaging Checks / Statements	12%	72%
Imaging Documents	7%	45%

Delivery Systems

Internet Banking Home Page	3%	25%
Internet Electronic Office	1%	15%
Telebanking	56%	88%
Smart Cards Debit Cards	35%	70%

Internet: Riding the tiger. The Internet is rapidly becoming the information superhighway of a global electronic marketplace. The rising commercial interests in the Internet are especially evident in "frontend" applications such as electronic catalogs, yellow pages, storefronts, malls, and customer support centers. All these applications are based on the World Wide Web (WWW) -- the fastest growing segment of the Internet. Although "back-end" applications such as electronic data interchange (EDI) are equally important, their adoption has not been as rapid. One major concern is security: the Internet is generally perceived as not secure enough for transmitting sensitive data such as payments. Upon a closer look, however, this view is not warranted, since technologies such as public key encryption and firewalls address essential security concerns. Moreover, such technologies are already available. The only remaining barrier is the lack of real world users of those technologies.

The pilot project between Bank of America (BoFA) and one of its large corporate customers involves transporting financial EDI transactions over the Internet. If successful, BoFA expects that this new EDI option will lead to a reduction in telecommunications costs, an improved position with respect to its value-added network (VAN), and valuable learning experience with the Internet environment, which is becoming increasingly important to the bank. The project is also significant beyond BoFA: because it is one of the first large-scale, real-world trials, its outcome will help dispel many uncertainties surrounding Internet-based EDI, and encourage more companies to move in this direction.

Investing in technology. According to a survey conducted by the American Bankers Association, US banks expenditure on information technology grown.

How to survive. The key to survival is customer service. Customer loyalty will be determined by convenient and innovative delivery of products and personalized services. In the '70's and '80's, banks were marketing to a generation raised on old style banking: personal interaction at a banking office. That generation was disdainful of "impersonal" service and afraid of computers. Convenience was having a "branch" in one's neighbourhood. Today, personal service and convenience are still the critical factors in the banking relationship, but they are defined differently. Consumers still want to bank with a financial institution they "know," and one who "knows" them, but they do not necessarily want to go to the bank. They are not afraid of computers and technology; they embrace them. Convenience is doing their banking when they want, and where they want. They are now comfortable with personal computers and other

electronic devices. They expect fast, efficient, and accurate service And the only way to cost effectively provide the instant, quality service that customers demand, and that the competition provides, is through intensive use of the most advanced information technologies and through good people trained in the use of these technologies. For all these reasons, the banks delivery systems are completely changing.

The new Delivery Systems. The increasing cost of building brick-and-mortar branches, decreasing cost of computers, high delivery costs and slow revenue growth force a relook at the conventional delivery systems. Moreover, growing comfort of technology usage by the customer is rapidly fostering usage of non-branch channels for routine transactions.

The new strategy changes the focus of the branch from being a high cost transaction center to a provider of a wide range of services like telebanking, customer service kiosks, ATMs, and remote electronic banking.

New Marketing Opportunities. As the new technology is so expensive banks need to use the new systems to do more than deliver information and basic services. Banks need the ability to also sell insurance and investment products to get a better return on this investment. Telephone banking can bring financial services to the home or office, especially if they are affordable screen phones. By noticing how much interest the customer expresses, the bank can market stock quotes and insurance quotes. Interactive videos are new technology that banks can make available to the customer to maintain personal contact while still lowering the expense of delivery service. With an interactive video an expert employee is not needed in each branch. Complex life insurance products, open brokerage accounts, customized product illustrations can be widely available where needed. The interactive videos will be cost effective expertise. The internet is a medium to allow banks to offer products to customers outside the normal customer base of a branch. Banks are aware of the customer's need for these services and plan to make them available before other sources do.

Drawbacks. Early experiences with electronic commerce in the banking industry, which has been a pioneer in the use of electronic systems, can be used to learn of some potential dangers and issues to be taken into account. The use of Automated Teller Machines and electronic home banking systems has increasingly allowed customers to bank outside of traditional bank facilities, for most of their usual transactions. This was consistent with the cost-savings strategy of most banks, which discovered that electronic transactions were about seven times less costly compared to the manual handling of these transactions by a bank teller. Nevertheless, the fact that customers' only contact with their banks was through (rather unsophisticated) electronic interfaces, and the major difficulties in integrating the legacy

systems of a typical bank, prevented banks in many cases from selling additional products to customers (cross-selling). In some European markets, the insurance companies took opportunity of that to grab business from banks, selling savings products to customers through their extensive distribution network. Similarly, the decrease in human interaction with customers could also lead to a less sophisticated understanding of their needs, as they're not always able to express comments, criticisms or requests for new products while interacting with machines. This should lead to a design of electronic commerce systems which incorporate capabilities for customer understanding and for proactive selling of new products. Electronic business transactions can only be successful if financial exchanges between buyers and sellers can occur in a simple, universally accepted, safe and cheap way. Various systems have been proposed, some of them based on traditional mechanisms (e.g. credit cards accounts) while others rely on new designs, such as electronic money. The key here will be to find a few widely accepted mechanisms, which can be used by most actors. The recent agreement between Mastercard and Visa on one security standard for credit card transactions over the Internet, and its backing by most major software vendors is one step in the right direction. This doesn't diminish the need for more specialized systems, for instance to allow microtransactions, the exchange of very small amounts of money (a few cents) in exchange for information or services. These new payment mechanisms will in turn enable new business models such as pay-per-article newspapers.



Technology Adoption. The vast majority of the Lebanese banks have set very high standards of excellence for themselves in terms of technology, state-of-the-art facilities, customer service and customer orientation with all facets of operations totally computerized. The banks also make extensive use of communication technology to provide off-site banking facilities including ATMs.

Their ambition is to position themselves as technology-driven banks offering superior services to both their clientele classes - the corporate customer and the retail customer. The corporate customer typically requires quick disposal of loan applications and maximum returns from the cash balance. The needs of the corporate customer are functions of the speed of response. Technologically the answer to this is a reliable network connecting branches that run on-line. Incompatibility of the old systems with the strategic necessity of integrating new technologies like ATMs, telebanking, etc. in order to provide the high quality services to the customers and competing on an equal foot with the foreign banks.

The competition. The banks are also planning to offer the entire range of services like telebanking, ATMs, etc. They also respond very actively in the marketplace in introducing new products and services. Arab Bank was the pioneer in introducing ATMs in Lebanon. Arab bank started to install ATM machines in 1993. Other banks followed, by establishing in 1994 a network called Link Network, using Link cards. About 25 banks have joined this network and are sharing now its almost 60 machines located in the major cities of Lebanon. The central bank is expecting that about 700 ATM machines will be installed in Lebanon by the year 2000.

Banks are also introducing remote banking services. Arab bank was also the first bank in Lebanon to offer this service. Early in 1994, Arab bank installed an interactive voice response system, called Phone Banking. At the same time, it introduced the computer based remote banking service which is called Corporate banking. Four other banks, Allied Business Bank, BLOM, Universal Bank, and the British Bank of the Middle East followed and introduced their telephone based remote banking. However these services are providing only inquiry facilities because they are off-line systems.

Technology Assessment. The diffusion and successful implementation of IT in Lebanese banks is not an easy process. Lebanese banks are facing enormous challenges in mastering the new tools provided by IT. An important constraint to the diffusion and success of IT implementation is the telecommunications infrastructure, another obstacle is managerial practices and organizational weaknesses. In the following section, I will analyse and discuss these obstacles. In evaluating banks' use of technology, we look at both the technology in place to serve today's customer and the plans for serving tomorrow's. The first objective is to examine the bank's deployment of technology relative to what is available, tested, and proven to enhance bank performance. The second is to examine the bank's preparation for the future. We want to answer the following questions: The most important issues to be analysed are :

To what degree is the bank using proven technologies to enhance performance?

Are there any technologies not deployed that would have a significant, positive effect on performance?

What level of specialized training has been received by the officers and employees assigned to selecting, deploying, and managing technology?

What level of systems training has been provided to other officers and employees?

How effective are the systems that are being used?

Is Management monitoring the evolution of banking technologies and planning for the future?

Telecommunication infrastructure. The greatest obstacle to real time electronic banking in Lebanon is the telecommunications infrastructure. Telecommunications in the banking sector is a major factor to the success or failure of any application or service. The Lebanese telecommunications infrastructure was devastated by the civil war. The process of rehabilitation and modernization of this infrastructure started in 1993. According to the recovery plan developed by CDR the telecommunications rehabilitation plan will be completed by the year 1998. This means that banks will not be able to rely on the public network until 1998. The result of such situation is a delay in implementing new services and products like remote banking, electronic funds transfer, real time bank information systems. This has also an effect on the reliability of the services already implemented like ATMs. In order to face this challenge, banks began studying the feasibility of installing a private telecommunications network. Four banks, Bank Audi, Arab Bank, Byblos Bank, and BLOM, started in the early 1996 considering the installation of a private network to connect their branches and thus conduct real time banking operations. This network will also be used to connect the ATMs machines which will thus function on-line. However three problems are delaying the implementation of such network:

- Obtaining a license from the Ministry of Post and telecommunications.
- The high cost of the equipment 0 The lack of coordination between the members of the Lebanese Banks Association.

Human Resources Problems. Banking industry is heavily depending upon information technology that needs professionals for development, implementation and support. Despite the programs performed by many banks to develop their local expertise in IT, there is still a real shortage of qualified personnel. According to a recent survey (T. Abdul Reda and M. Dayya, Banking IT: a look at Lebanon, AUB, 1996) the following problems were identified:

- almost half of the Lebanese banks do not have one engineer among their staff.
- lack of professional training programs. Financial institutions in Lebanon offer a wide range of training programs to their employees. However, with respect to their technical IT staff the

percentage of training programs is much less, because IT staff are considered to be trained, highly qualified and hence do not need extended training sessions. The consequence of such policy is a reduction of the capability of IT staff to be up to date in the most recent advances .

- High turnover rate of technical staff. The turnover rate of the technical staff in some 40% percent the Lebanese banks is around 20%. The low salaries and better opportunities in other industries are the main reasons for this high rate.
- Resistance to change. Resistance to change and the absorption capacity is often neglected once the automation system is adopted. However, this human factor is a critical factor in the success of any banking application of information technology. The only way to solve this problem is to design adequate training programs and increase the awareness of the employees. Most Lebanese banks have realized this fact and some of them have established a training centre.

These are the major obstacles for implementing IT in Lebanese banks. Another point that should be mentioned is the necessity of planning very carefully the development of any new application. A computerization plan is the basis for implementing successful information technology solutions. To be relevant, these plans have to be linked closely to organizational strategies, objectives, priorities and processes.

Strategy for the future

Banks face a serious challenge. The basic structure of the bank is increasingly in conflict with the changing product, delivery, and service needs of the customers. The future belongs to financial service providers not traditional banks. The vast majority of large banks, will create value networks. Doing so presents tremendous challenges. Banks will have to first develop a comprehensive distribution system that will enable customers to touch them at multiple points. Banks must also create performance measurement systems to assure the mix products and services they offer are beneficial to both the customer and the bank. They must determine whether to deploy new technologies themselves or with other service providers. Nevertheless, technology alone will not solve issues or create advantages. This technology needs to be integrated in an organization, with the change management issues linked to people resisting new concepts and ideas. It also needs to support a clearly defined and well communicated business strategy

Internet of Things (IoT)

If you own a Smartphone and wear a Fitbit, then the Internet of Things (IoT) phenomenon is already impacting your daily life, and probably more than you think. In today's world, the Internet of Things, or IoT as it is also called, has grown beyond simply laptops, smartphones and tablets and includes everything from fitness trackers to even fridges, air conditioning unit at your home or office.

The IoT has a significant ability to impact the future of mankind. We are entering a world where everything has the potential to be connected. In fact, [there is an estimate](#) that by 2020, the installed base for the IoT will be as high as 212 billion, including 30 billion "connected things." This is a large market and will have a great impact on the daily life of the average person. There is already talk of connected and self-driving cars, "smart" homes and even connected healthcare is in the works, indicating the huge potential impact of the Internet of Things.

The Internet of Things has a financial impact as well, with the projected value expected to be close to \$30 billion by 2020. This is going to become a major factor in the global economy as connectivity becomes the norm in the next few years. IoT is in fact termed by some as 'bigger than industrial revolution' in the world economy. One of the most important challenges associated with IoT is security, which needs to be addressed with priority as IoT is evolving with tremendous speed.

Initiatives by Government of India for Propagating e-Banking

For growth and development and to promote e-banking in India the Indian government and RBI have been taken several initiatives.

The Government of India enacted the IT Act, 2000 with effect from October 17, 2000 which provided legal recognition to electronic transactions and other means of electronic commerce.

The Reserve Bank monitors and reviews the legal requirements of e-banking on a continuous basis to ensure that challenges related to e-banking may not pose any threat to financial stability of the nation

Dr. K.C. Chakrabarty Committee including members from IIM, IDRBT, IIT and Reserve Bank prepared the IT Vision Document- 2011-17, which provides an indicative road map i.e. guidelines to enhance the usage of IT in the banking sector.

The Reserve Bank is striving to make the payment systems more secure and efficient. It has advised banks and other stakeholders to strengthen the security aspects in internet banking by adopting certain security measures in a timely manner. RBI believes that the growing popularity of these alternate channels of payments (such as: Internet Banking, Mobile Banking, ATM etc.) brings an additional responsibility on banks to ensure safe and secure transactions through these channels.

National Payments Corporation of India (NPCI) was permitted by the RBI to enhance the number of mobile banking services and widen the IMPS (Immediate Payment Service) channels like ATMs, internet, mobile etc. Along with this, NPCI is also working to bring more mobile network operators which can provide mobile banking services through a common platform.

There has been a dramatic surge in the volume and value of mobile transactions in the recent past. MoM increase in no. of transactions from Dec14 to Dec 15 was 135% and Dec 15 to Dec 16 was 182%. MoM increase in value of transactions from Dec 14 to Dec 15 was 330% and Dec 15 to Dec 16 was 178%.

The future:

In the backdrop of demonetization- a colloquial term for the withdrawal of 86 percent of the value of India's currency in circulation by the Government of India since 8th November 2016 followed by digital

push for 'less cash' economy, a dramatic multi-fold rise in e-banking transactions and especially mobile banking transactions, is expected in the near future.

Interactive Technology for Banks

With the launch of sbiINTOUCH on 1st July, 2014, State Bank of India was the first Bank in India to introduce the concept of "Digital Banking". State of the art technology like Debit Card Printing Kiosks, Interactive Smart Tables, Interactive Digital Screens, Remote Experts through video call etc were introduced to providing a completely different experience through online self-service mode.

The key feature of these branches is that one can open one's savings bank account - Account Opening Kiosk (AOK) within 15 minutes. Besides that you can have access to a vast array of Banking related activities and products.

India's first banking robot Lakshmi made her debut in November 2016 by City Union Bank, the artificial intelligence powered robot will be the first on-site bank helper. Lakshmi, which took more than six months to develop, can answer intelligently on more than 125 subjects. Top private lender HDFC Bank, which is also experimenting with robots to answer customer queries, is testing its humanoid at its innovation lab.

INTRODUCTION TO COMPUTING

COMPUTER

INTRODUCTION

An amazing machine! We are living in the computer age today and most of our day to day activities cannot be accomplished without using computers. Sometimes knowingly and sometimes unknowingly we use computers. Computer has become an indispensable and multipurpose tool. We are breathing in the computer age and gradually computer has become such a desire necessity of life that it is difficult to imagine life without it.

DEFINITION

For most of the people, computer is a machine used for a calculation or a computation, but actually it is much more than that.

Precisely, "Computer is an electronic device for performing arithmetic and logical operation." Or "Computer is a device or a flexible machine to process data and converts it into information."

To know about the complete process that how computer works, we will have to come across the various terms such as Data, Processing and Information. First of all we will have to understand these terms in true sense.

DATA

"Data" is nothing but a mere collection of basic facts and figure without any sequence. When the data is collected as facts and figure, it has no meaning at that time, for example, name of student, names of employees etc.

PROCESSING

'Processing' is the set of instruction given by the user or the related data to output the meaningful information. Which can be used by the user? The work of processing may be the calculation, comparisons or the decision taken by the computer.

INFORMATION

'Information' is the end point or the final output of any processed work. When the output data is meaning it is called information

DEVELOPMENT OF COMPUTER

Actually speaking electronic data processing does not go back more than just half a century i.e. they are in existence merely from early 1940's. In early days when our ancestor used to reside in cave the counting was a problem. Still it is stated becoming difficult.

When they started using stone to count their animals or the possession they never knew that this day will lead to a computer of today. People today started following a set of procedure to perform calculation with these stones, which later led to creation of a digital counting device, which was the predecessor the first calculating device invented, was known as ABACUS.

THE ABACUS

Abacus is known to be the first mechanical calculating device. Which was used to be performed addition and subtraction easily and speedily? This device was first developed by the Egyptians in the 10th century B.C, but it was given its final shape in the 12th century A.D. by the Chinese educationists.

Abacus is made up of wooden frame in which rod were fitted across with round beads sliding on the rod. It is divided into two parts called 'Heaven' and 'Earth'. Heaven was the upper part and Earth was the lower one. Thus any no. can be represented by placing the beads at proper place.

NAPIER'S BONES

As the necessity demanded, scientist started inventing better calculating device. In this process John Napier's of Scotland invented a calculating device, in the year 1617 called the Napier Bones.

In the device, Napier's used the bone rods of the counting purpose where some no. is printed on these rods. These rods that one can do addition, subtraction, multiplication and division easily.

PASCAL'S CALCULATOR

In the year 1642, Blaise Pascal a French scientist invented an adding machine called Pascal's calculator, which represents the position of digit with the help of gears in it.

LEIBNZ CALCULATOR

In the year 1671, a German mathematician, Gottfried Leibniz modified the Pascal calculator and he developed a machine which could perform various calculation based on multiplication and division as well.

ANALYTICAL ENGINE

In the year 1833, a scientist from England known to be Charles Babbage invented such a machine. Which could keep our data safely? This device was called Analytical engine and it deemed the first mechanical computer.

It included such feature which is used in today's computer language. For this great invention of the computer, Sir Charles Babbage is also known as the father of the computer.

GENERATION OF COMPUTER

As the time passed, the device of more suitable and reliable machine was needed which could perform our work more quickly. During this time, in the year 1946, the first successful electronic computer called ENIAC was developed and it was the starting point of the current generation of computer.

First Generation: Vacuum Tubes (1940-1956)

The first computer systems used vacuum tubes for circuitry and magnetic drums for memory, and were often enormous, taking up entire rooms. These computers were very expensive to operate and in addition to using a great deal of electricity, the first computers generated a lot of heat, which was often the cause of malfunctions.

First generation computers relied on machine language, the lowest-level programming language understood by computers, to perform operations, and they could only solve one problem at a time. It would take operators days or even weeks to set-up a new problem. Input was based on punched cards and paper tape, and output was displayed on printouts.

The UNIVAC and ENIAC computers are examples of first-generation computing devices. The UNIVAC was the first commercial computer delivered to a business client, the U.S. Census Bureau in 1951.



A UNIVAC computer at the Census Bureau.

Second Generation: Transistors (1956-1963)

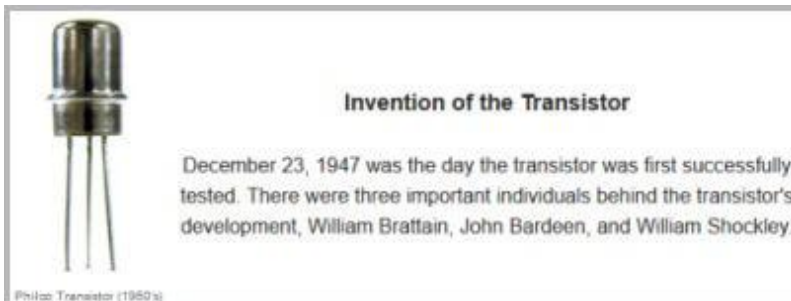
The world would see transistors replace vacuum tubes in the second generation of computers. The transistor was invented at Bell Labs in 1947 but did not see widespread use in computers until the late 1950s.

The transistor was far superior to the vacuum tube, allowing computers to become smaller, faster, cheaper, more energy-efficient and more reliable than their first-generation predecessors. Though the transistor still generated a great deal of heat that subjected the computer to damage, it was a vast improvement over the vacuum tube. Second-generation computers still relied on punched cards for input and printouts for output.

From Binary to Assembly

Second-generation computers moved from cryptic binary machine language to symbolic, or assembly, languages, which allowed programmers to specify instructions in words. High-level programming languages were also being developed at this time, such as early versions of COBOL and FORTRAN. These were also the first computers that stored their instructions in their memory, which moved from a magnetic drum to magnetic core technology.

The first computers of this generation were developed for the atomic energy industry.



An early Philco Transistor (1950's)

Third Generation: Integrated Circuits (1964-1971)

The development of the integrated circuit was the hallmark of the third generation of computers.

Transistors were miniaturized and placed on silicon chips, called semiconductors, which drastically increased the speed and efficiency of computers.

Instead of punched cards and printouts, users interacted with third generation computers through keyboards and monitors and interfaced with an operating system, which allowed the device to run many different applications at one time with a central program that monitored the memory. Computers for the first time became accessible to a mass audience because they were smaller and cheaper than their predecessors.

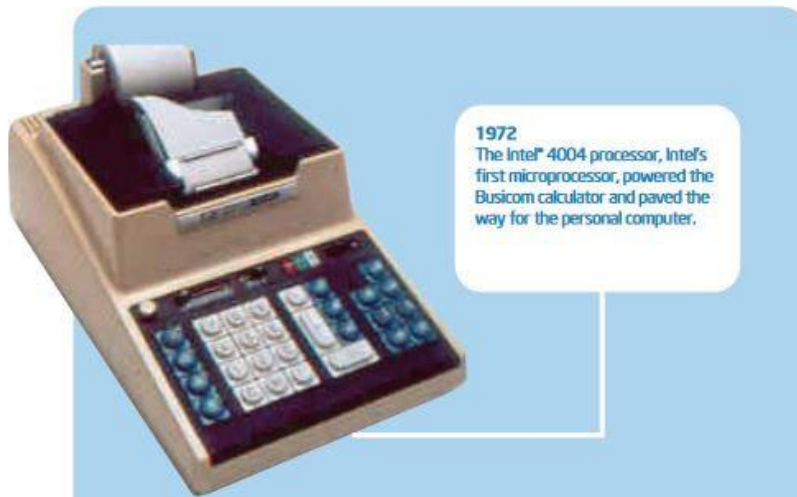
Did You Know... ? An integrated circuit (IC) is a small electronic device made out of a semiconductor material. The first integrated circuit was developed in the 1950s by Jack Kilby of Texas Instruments and Robert Noyce of Fairchild Semiconductor.

Fourth Generation: Microprocessors (1971-Present)

The microprocessor brought the fourth generation of computers, as thousands of integrated circuits were built onto a single silicon chip. What in the first generation filled an entire room could now fit in the palm of the hand. The Intel 4004 chip, developed in 1971, located all the components of the computer—from the central processing unit and memory to input/output controls—on a single chip.

In 1981 IBM introduced its first computer for the home user, and in 1984 Apple introduced the Macintosh. Microprocessors also moved out of the realm of desktop computers and into many areas of life as more and more everyday products began to use microprocessors.

As these small computers became more powerful, they could be linked together to form networks, which eventually led to the development of the Internet. Fourth generation computers also saw the development of GUIs, the mouse and handheld devices.



Intel's first microprocessor, the 4004, was conceived by Ted Hoff and Stanley Mazor.

Fifth Generation: Artificial Intelligence (Present and Beyond)

Fifth generation computing devices, based on artificial intelligence, are still in development, though there are some applications, such as voice recognition, that are being used today. The use of parallel processing and superconductors is helping to make artificial intelligence a reality. Quantum computation and molecular and nanotechnology will radically change the face of computers in years to come. The goal of fifth-generation computing is to develop devices that respond to natural language input and are capable of learning and self-organization.

SCOPE OF COMPUTER

Certain characteristics of computer interaction can make computers well suited for distance learning. The features listed below the prospect of the computer use look more promising:

- Access to expert and respected peers.
 - One to One and much communication.
 - Active learner participation.
 - Linking of new learning to concrete on the job problems.
 - Follow up, feedback and implementation support from peers or experts.
-

- Self direction control over stop or start, time, pace and place of learning or communication activity.

USES OF A COMPUTER

A computer is used in all human life. It has revolutionized all phases of human activities. The most important have been given as follows:

Routine job handling

the routine classical and stenotype jobs calculating and formality bits, salaries, updating stocks, tax return, reservation records and information.

Traffic control

Controlling traffic, traffic lights. Television cameras are used to maintain traffic light routine.

Electronic money

Automatic tellers machine (ATM) is very common in banks. You can deposit and withdraw money with the ATM.

Electronic office

All type information are stored, manipulated and utilized in the electronic form. A document is sent to different place with FAX, internet and e-mail.

Industrial Application

It plays an important role in production control. It is bringing efficiency it trade and industry.

Telephones

With help computerized telephone through satellites STD and IST services have been introduced. It maintains the record of calls and does the billing for you.

Trade

Every type of trade computer is used successfully. It is used in Banks, stock exchanges to control stocks and accounts.

Scientific research

In every science, the research work becomes economical from time, energy, money point of new. A large data is analyzed very quickly.

Medicine

There is wide use in medical science e. g. ECG, CAT scan, Ultra sound. The proper and accounts diagnosis is done with the help of computer. The medical apparatus are controlling computerized.

Space Science

The satellite controlling the space with the help of computer. The information's are collected by using the computer from the space satellite.

Publication

The composing work is done speedily and economical with the help of computer. The designing work is also done by computer. The quality is maintained is publication by computer.

Communications

The computer is used for sending message example printer, FAX, e-mail, Internet. The import and export work is done on internet.

Film industry

It had influenced film industry such as animation; titling etc. The multimedia approach is used in film production with the help of computer. The cartoon films are developed by computers.

Education

The computer is widely used in the field of education and independent study field of computer science has developed which is popular these days. At every stage computer is compulsory. The distance education is using computer for instructional purpose as multimedia approach. The computer makes teacher learning process effecting by involving audio and visual sense of learners.

LANGUAGES OF COMPUTER

A language is defined as the medium of expression of thoughts . All the human beings in this world communicate with each other by a language. Similarly, computer also needs some expression medium to communicate with others

A computer follows the instructions given by the programmer to perform a specific job. To perform a particular task, programmer prepares a sequence of instructions, know as programmed. A program written for a computer is known as Software. The programmed is stored in RAM. The CPU takes one instruction of the programmed at a time from RAM and executes it. The instructions are executed one by one in sequence and finally produce the desired result.

The Journey of computer software machine language to high level languages to modern 4GL / 5GL languages is an interesting one. Let us talk about this in detail.

FIRST GENERATION LANGUAGES 1GLs (Machine language)

When the human being started programming the computer the instruction were given to it in a language that it could easily understand. And that language was machine language. The binary language a

language, a language of 1s and 0s is known as Machine language. Any instruction in this language is given in the form of string of 1s and 0s. Where the symbol 1 stands for the presence of electrical pulse and 0 stands for the absence of electric pulse. A set of 1s and 0s as 11101101 has a specific meaning to a computer even though it appears as binary number to us.

The writing of programmer in machine language is very cumbersome and complicated and this was accomplished by experts only. All the instructions and input data are fed to the computer in numeric form, specifically a binary form.

SECOND GENERATION LANGUAGES 2GLs (Assembly Language)

Lots of efforts are made during last 50 years to obviate the difficulties faced for using the machine language. The first language similar to English was developed in 1950 which was known as Assembly Language or Symbolic Programming Languages. After 1960, the High Level Languages were developed which brought the common man very close to the computer. And this was the main reason for tremendous growth in computer industry. The high level languages are also known as Procedure Oriented Languages.

THIRD GENERATION LANGUAGES (3GLs) (High Level Languages)

The assembly language was easier to use compared with machine language as it relieved the programmer from a burden of remembering the operation – codes and addresses of memory location. Even though the assembly languages proved to be great help to the programmer, a search was continued for still better languages nearer to the conventional English language. The languages developed which were nearer to the English language, for the use of writing the programmer in 1960 were known as High Level languages.

The different high level languages which can be used by the common user are FORTRAN, COBOL, BASIC, PASCAL, PL-1 and many others. Each high level language was developed to fulfill some basic requirements for particular type of problems. But further developments are made in each language to widen its utility for different purposes.

FOURTH GENERATION LANGUAGES (4GLs)

The 3GLs are procedural in nature i.e., HOW of the problem gets coded i.e., the procedures require the knowledge of how the problem will be solved. Contrary to them, 4GLs are non procedural. That is only WHAT of the problem is coded i.e., only 'What is required' is to be specified and rest gets done on its own.

Thus a big program of a 3GLs may get replaced by a single statement of a 4GLs. The main aim of 4GLs is to be cut down on development and maintenance time and making it easier for users.

GUI BASED LANGUAGES

With the invention and popularity of GUI based interfaces. GUI based languages include:

1. TCL/Tk
2. Visual basic
3. Visual C++
4. C# (Pronounced as C sharp)
5. Visual basic.NET
6. Visual basic 2005

ANATOMY OF A COMPUTER

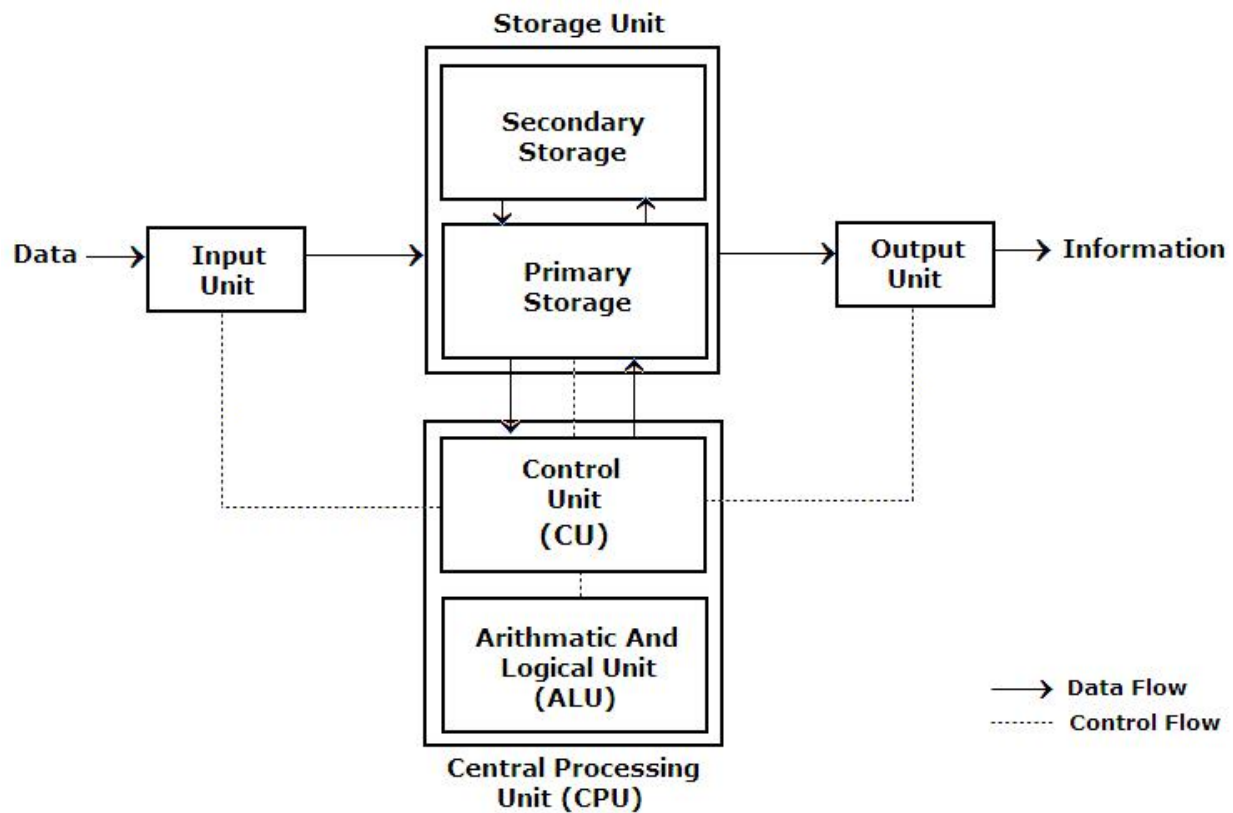
The internal design of computers differs from one model to another. But the basic components of computer remain the same for all models. To function properly, a computer needs both hardware and software. Hardware consists of the mechanical and electronic devices which we can see and touch. Key Board, Monitor, DVD are some examples for Computer Hardware. The software consists of programs, the operating systems and the data that reside in the memory and storage devices. JAVA, Microsoft Office, Open Office are some examples for Computer Software.

A computer mainly performs the following four functions.

1. **Receive input** – accept information from outside through various input devices like keyboard, mouse etc.
2. **Process information** – perform arithmetic or logical operations on the information.
3. **Produce output** – communicate information to the outside world through output devices like monitor, printer etc.
4. **Store information** – store the information in storage devices like hard disk, compact disk etc.

A computer has the following three main components.

- a. Input/ Output Unit
- b. Central Processing Unit
- c. Memory Unit



a) Input/ Output Unit: Computer is a machine that processes the input data according to a given set of instructions and gives the output. The unit used for getting the data and instructions into the computer and displaying or printing output is known as input/ output unit. Keyboard is the main input device while the monitor is the main output device.

b) Central Processing Unit: Central processing Unit (CPU) is the main component or 'brain' of the computer which performs all the processing of input data. In micro computers, the CPU is built on a single chip or Integrated Circuit (IC) and is called Microprocessor. The CPU consists of the following distinct parts:

- i. Arithmetic Logic Unit (ALU)
- ii. Control Unit (CU)
- iii. Registers

- iv. Buses
- v. Clock

(i) **Arithmetic Logic Unit:** The arithmetic logic unit is responsible for all arithmetic operations like addition, subtraction, multiplication and divisions as well as logical operations such as less than, equal to and greater than.

(ii) **Control Unit:** The control unit is responsible for controlling the transfer of data and instructions among other units of a computer. It is considered as the 'Central Nervous System' of computer as it manages and coordinates all the units of the computer. It obtains the instructions from the memory, interprets them and directs the operation of the computer.

(iii) **Registers:** Registers are small high speed circuits which are used to store data, instructions and memory addresses, when ALU performs arithmetic and logical operations. Depending on the processor's capability, the number and type of registers vary from one CPU to another.

(iv) **Buses:** Data is stored as a unit of eight bits in a register. Each bit is transferred from one register to another by means of a separate wire. This group of eight wires which is used as a common way to transfer data between registers is known as a bus. Bus is a connection between two components to transmit signal between them. Bus is of three major types namely data bus, control bus and address bus.

(v) **Clock:** Clock is an important component of CPU which measures and allocates a fixed time slot for processing each and every micro-operation. CPU executes the instructions in synchronization with the clock pulse. The clock speed of CPU is measured in terms of Mega Hertz or millions of cycles per second. The clock speed of CPU varies from one model to another.

c) **Memory Unit:** Memory unit is used to store the data, instructions and information before, during and after the processing by ALU. It is actually a work area (physically a collection of integrated circuits) within the computer where the CPU stores the data and instructions. Memory is of two types:

- i. Read Only Memory (ROM)
- ii. Random Access Memory (RAM)

(i) **Read Only Memory:** Read Only Memory is an essential component of the memory unit. The memory which has essential instructions is known as Read Only Memory. This memory is permanent and is not

erased when the system is switched off. The memory capacity of ROM varies from 64 KB to 256 KB depending on the model of computer.

(ii) **Random Access Memory:** Random Access Memory is used to store data and instructions during the execution of programs. Contrary to ROM, RAM is temporary and is erased when the computer is switched off. RAM is a read/ write type of memory and thus can be read and written by the user. As it is possible to randomly use any location of this memory, it is known as random access memory. The memory capacity of RAM varies from 640 KB to several mega bytes with different models of computer.

Hardware and software are two broad categories of computer components. Hardware refers to physical component while software to the programs required to operate computers.

-

2.4 INPUT DEVICES

An input device is any machine that feeds data, information and instructions into a computer. We may classify input devices into the following two broad categories.

- i. Basic input devices
- ii. Special input devices

Basic Input Devices: The input devices which are essential to operate a PC are called basic input devices. These devices are always required for basic input operations. These devices include keyboard and mouse.

Special Input Devices: The input devices which are not essential to operate a PC are called special input devices. These devices are used for various special purposes and are generally required for basic input operations. These devices include Trackball, Light Pen, Touch Screen, Joystick, Digitizer, Scanner, Optical Mark Reader (OMR), Bar Code Reader (BCR), Optical Character Reader (OCR), Magnetic Ink Character Recognition (MICR) and Voice-Input Devices.

2.4.1 Keyboard

Keyboard is the most common input device used for manual data entry. Computer keyboards are similar to electric-typewriter keyboards but contain additional keys. Keyboard has been standardized for use in

all types of computers such as a PC, a workstation or a notebook computer. The keys on computer keyboards are classified as follows:

1. **Letter Keys:** These are the 26 letters of English alphabet arranged as in a typewriter.
2. **Digit Keys:** There are two sets of digit keys; one on the second row from the top of the keys just as in a typewriter and the other is a numeric key pad at the bottom right which allows quick entry of numbers with the fingers of one hand.
3. **Special character keys:** These are characters such as <, >, ?, /, {, }, [,], (,), ., ", @, #, \$, %, &, *, etc
4. **Non-printable control keys:** These are used for backspacing, going to the next line, tabulation, moving the cursor up or down, insert, delete characters etc. There is also a space bar at the bottom for leaving a space.
5. **Function keys:** These are labeled F1, F2 up to F15 and when pressed invoke programs stored in the computer.



You can understand the function of each and every key actually by working on a PC. When any key is pressed, an electric signal is produced. This signal is detected by a keyboard encoder that sends a binary code corresponding to the key pressed to the CPU. There are many types of keyboards but 101 keys board is the most popular one.

2.4.2 Mouse

Mouse is a device that controls the movement of the cursor on the display screen. It is a small object you can roll along a hard, flat surface. Its name is derived from its shape which looks like a mouse. As you move the mouse, the pointer on the display screen moves in the same direction. Mice contain at least one button and sometimes as many as three which have different functions depending on what program is running. There are three basic types of mice. They are mechanical, opto mechanical and optical. Wireless mice are also being manufactured. They transmit the motion of the mouse to the computer wirelessly and is convenient to use. Recently touch panel displays are manufactured which do not need a mouse as a locator. An appropriate icon on the screen may be touched either by finger or a pointing device such as a ballpoint pen to invoke the corresponding program.

2.4.3 Other Input Devices

Trackball:

Trackball is an input device which is mostly used in notebook or laptop computer instead of a mouse. This is a ball which is half inserted and moving fingers on the ball, pointer can be moved. Trackball is considered better than mouse because it requires little arm movement and less desktop space.

Light Pen:

Light pen is a pointing device which is similar to a pen. It is used to select a displayed menu item or draw pictures on the monitor screen. It consists of a photocell and an optical system placed in a small tube. When the tip of a light pen is pressed, its photocell sensing element detects the screen location and sends the corresponding signal to the CPU.

Touch Screen:

Some special VDU devices have touch sensitive screens. These screens are sensitive to human fingers and act as tactile devices. Using touch screen, the user can point to a selection on the screen instead of pressing keys. Touch screen helps the user in getting the information quickly.

Joystick:



Joystick is a pointing device which is used to move cursor position on a monitor screen. Joystick is a stick having a spherical ball at its both lower and upper ends. The lower spherical ball moves in a socket. Joystick can be moved in all four directions. The function of joystick is similar to that of a mouse. It is mainly used in Computer Aided Designing (CAD) and playing computer games.

Digitizer:



Digitizer is an input device which converts analog information into digital form. Digitizer can convert a signal from the television or camera into a series of numbers that could be stored in a computer. They can be used by the computer to create a picture of whatever the camera had been pointed at. Digitizer is also known as Tablet or Graphics Tablet because it converts graphics and pictorial data into binary inputs. A graphic tablet as digitizer is used for doing fine works of drawing.

Scanner:

Scanner works more like a photocopy machine. It is used when some information is available on a paper and it is to be transferred to the hard disk of the computer for further manipulation. Scanner captures images from the source which are then converted into the digital form that can be stored on the disc. These images can be edited before they are printed.

Optical Mark Reader (OMR):



OMR is a special type of optical scanner used to recognize the type of mark made by pen or pencil. It is used where one out of a few alternatives is to be selected and marked. It is specially used for checking the answer sheets of examinations having multiple choice questions.

Bar Code Reader (BCR):



BCR is an optical scanner used for reading bar-coded data (data in the form of light and dark lines). Bar-coded data is generally used in labeling goods, numbering of books etc. Bar Code Reader scans a bar code image, converts it into an alphanumeric value which is then fed to the computer to which the Bar Code Reader is connected.

Optical Character Reader (OCR):

OCR is an optical scanner used to read a printed text. OCR scans text optically character by character, converts them into a machine-readable code and stores the text on the system memory. It is used for reading of passenger tickets, computer-printed bills of credit card companies and reading of ZIP codes in postal services.

Magnetic Ink Character Reader (MICR):

MICR is generally used in banks because of a large number of cheques to be processed every day. The bank's code number and cheque number are printed on the cheques with a special type of ink that contains particles of magnetic material that are machine readable. This reading process is called Magnetic Ink Character Recognition.

Voice-Input Devices:



Voice-input devices are the latest input devices that can recognize the human voice. Microphone is a voice input device to input sound which is then stored in digital form. It is used for various applications like adding sound to a multimedia presentation or for mixing music.

Data Processing Methods

The carrying out of various operations on data from a software to retrieve, transform, or classify information is what you call "data processing".

Mostly, data processing happens on software programs where a set of inputs produces a defined set of outputs.

There are two common types of data processing, namely Batch Processing and Real-Time Processing. The determination on whether to use one over the other will depend on the following:

- The type and volume of data
- The time that the data needs to be processed and
- Which process is really suited to a certain business.

The two data processing types help businesses handle information seamlessly. However, like most things, both have advantages and disadvantages.

- Batch Data Processing

This is an efficient way of processing high/large volumes of data where a group of transactions is collected over a certain period of time. In batch data processing, information is collected, entered, processed and then the batch outputs are produced. This data process requires separate programs for input, process and output. Examples of software programs that use this kind of data processing are payroll and billing systems.

Advantages:

- o Ideal for processing large volumes of data/transaction for it increases efficiency rather than processing each individually.
- o Can be done or processed independently during less-busy times or at a desired designated time.
- o It offers cost efficiency for the organization by carrying out the process (data reconciliation for the master file) when needed.
- o It allows good audit trail.

Disadvantages:

- o The very disadvantage of batch processing is the time delay between the collection of data (transaction receiving) and getting the result (output in master file) after the batch process.
- o The Master File (The organizations big data) is not always kept up to date.
- o The One time process can be very slow.

- Real-Time Processing

In contrast with batch data processing, real time data processing involves continuous input, process and output of data. Thus, data are processed in a short period of time. Few examples of programs that use such data processing type are bank ATMs, customer services, radar systems, and Point of Sale (POS)

Systems. POS uses this data process to update the inventory, provide inventory history, and sales of a particular item – allowing business to handle payments in real time.

With this kind of data process, every transaction is directly reflected to the master file so that it will always be updated.

Advantages:

- o No significant delay in response.
- o Information is always up to date thus giving the organization the ability to take immediate action when responding to an event, issue or scenario in the shortest possible span of time.
- o It could also give the organization the ability to gain insights from the updated data to detect patterns for possible identification of either opportunities or threats to the organization's business.

Disadvantages:

- o This type of processing is more expensive and complex.
- o Real-time processing is a bit tedious and more difficult for auditing.
- o Daily data backups (depends on transaction frequency) should be implemented and necessary to ensure the retention of the most recent data transaction.

The decision to select the best data processing system will greatly depend on the current system in your business. So, choose the one that best suit your business system.

Computing

Computing is any goal-oriented activity requiring, benefiting from, or creating computers. Computing includes designing, developing and building hardware and software systems; designing a mathematical sequence of steps known as an algorithm; processing, structuring, and managing various kinds of information; doing scientific research on and with computers; making computer systems behave intelligently; and creating and using communications and entertainment media. The field of computing includes computer engineering, software engineering, computer science, information systems, and information technology.

Cloud Computing – Cloud computing is a computing paradigm shift where computing is moved away from personal computers or an individual application server to a “cloud” of computers. Users of the cloud only need to be concerned with the computing service being asked for, as the underlying details of how it is achieved are hidden. This method of distributed computing is done through pooling all computer resources together and being managed by software rather than a human.

- The services being requested of a cloud are not limited to using web applications, but can also be IT management tasks such as requesting of systems, a software stack or a specific web appliance.

Grid Computing Multiple independent computing clusters which act like a “grid” because they are composed of resource nodes not located within a single administrative domain. (formal)

- Offering online computation or storage as a metered commercial service, known as utility computing, computing on demand, or cloud computing.
- The creation of a “virtual supercomputer” by using spare computing resources within an organization.

Utility Computing –

- Conventional Internet hosting services have the capability to quickly arrange for the rental of individual servers, for example to provision a bank of web servers to accommodate a sudden surge in traffic to a web site.
 - “Utility computing” usually envisions some form of virtualization so that the amount of storage or computing power available is considerably larger than that of a single time-sharing computer. Multiple
-

servers are used on the “back end” to make this possible. These might be a dedicated computer cluster specifically built for the purpose of being rented out, or even an under-utilized supercomputer. The technique of running a single calculation on multiple computers is known as distributed computing.

Distributed Computing – A method of computer processing in which different parts of a program are run simultaneously on two or more computers that are communicating with each other over a network. Distributed computing is a type of segmented or parallel computing, but the latter term is most commonly used to refer to processing in which different parts of a program run simultaneously on two or more processors that are part of the same computer. While both types of processing require that a program be segmented—divided into sections that can run simultaneously, distributed computing also requires that the division of the program take into account the different environments on which the different sections of the program will be running. For example, two computers are likely to have different file systems and different hardware components.

Cluster Computing – A computer cluster is a group of linked computers, working together closely so that in many respects they form a single computer. The components of a cluster are commonly, but not always, connected to each other through fast local area networks. Clusters are usually deployed to improve performance and/or availability over that provided by a single computer, while typically being much more cost-effective than single computers of comparable speed or availability.

Additional Cloud Topics

- Actor model
- Cluster manager
- Communication as a service
- Grid computing
- Online Office
- Parallel computing
- Parallel processing

- Redundant Array of Inexpensive Servers
- Software as a service
- Utility computing
- Virtual Private Cloud
- Web operating system
- Web Services

Grid Computing Concepts and related technology

- Distributed computing
- List of distributed computing projects
- High-performance computing
- Network Agility
- Render farm
- Semantic grid
- Supercomputer
- Computer cluster
- Computon
- Grid FileSystem
- Edge computing
- Metacomputing

- Cloud Computing
- Space based architecture (SBA)

Farm Computing:

- Link farm
- Blade server
- Data center
- Render farm
- Comparison of wiki farms
- Server room

Types of cloud computing

Cloud computing is typically classified in two ways:

1. Location of the cloud computing
2. Type of services offered

1. Location of the cloud

Cloud computing is typically classified in the following three ways:

Public cloud: In Public cloud the computing infrastructure is hosted by the cloud vendor at the vendor's premises. The customer has no visibility and control over where the computing infrastructure is hosted. The computing infrastructure is shared between any organizations.

Private cloud: The computing infrastructure is dedicated to a particular organization and not shared with other organizations. Some experts consider that private clouds are not real examples of cloud computing. Private clouds are more expensive and more secure when compared to public clouds.

Private clouds are of two types: On-premise private clouds and externally hosted private clouds. Externally hosted private clouds are also exclusively used by one organization, but are hosted by a third party specializing in cloud infrastructure. Externally hosted private clouds are cheaper than On-premise private clouds.

Hybrid cloud: Organizations may host critical applications on private clouds and applications with relatively less security concerns on the public cloud. The usage of both private and public clouds together is called hybrid cloud.

Community cloud involves sharing of computing infrastructure in between organizations of the same community. For example all Government organizations within the state of California may share computing infrastructure on the cloud to manage data related to citizens residing in California.

2. Classification based upon service provided

Based upon the services offered, clouds are classified in the following ways:

Infrastructure as a service (IaaS) involves offering hardware related services using the principles of cloud computing. These could include some kind of storage services (database or disk storage) or virtual servers. Leading vendors that provide Infrastructure as a service are Amazon EC2, Amazon S3, Rackspace Cloud Servers and Flexiscale.

Platform as a Service (PaaS) involves offering a development platform on the cloud. Platforms provided by different vendors are typically not compatible. Typical players in PaaS are Google's Application Engine, Microsoft's Azure and Salesforce.com's force.com .

Software as a service (SaaS) includes a complete software offering on the cloud. Users can access

a software application hosted by the cloud vendor on pay-per-use basis. This is a well-established sector. The pioneer in this field has been Salesforce.com's offering in the online Customer Relationship Management (CRM) space. Other examples are online email providers like Google's gmail and Microsoft's hotmail, Google docs and Microsoft's online version of office called BPOS (Business Productivity Online Standard Suite).

Challenges of cloud computing

Cloud computing challenges have always been there. Companies are increasingly aware of the business value that cloud computing brings and are taking steps towards transition to the cloud. Some of the most important challenges are as follows.

Security and Privacy: The main challenge to cloud computing is how it addresses the security and privacy concerns of businesses thinking of adopting it. The fact that the valuable enterprise data

will reside outside the corporate firewall raises serious concerns. Hacking and various attacks to cloud infrastructure would affect multiple clients even if only one site is attacked. These risks can be mitigated by using security applications, encrypted file systems, data loss software, and buying security hardware to track unusual behavior across servers.

Availability & Scalability: It is difficult to assess the costs involved due to the on-demand nature of the services. Budgeting and assessment of the cost will be very difficult unless the provider has some good and comparable benchmarks to offer. The service-level agreements (SLAs) of the provider are not adequate to guarantee the availability and scalability. Businesses will be reluctant to switch to cloud without a strong service quality guarantee.

Interoperability and Portability: Businesses should have the leverage of migrating in and out of the cloud and switching providers whenever they want, and there should be no lock-in period. Cloud computing services should have the capability to integrate smoothly with the on-premise IT.

Reliability and Availability: Cloud providers still lack round-the-clock service; this results in frequent outages. It is important to monitor the service being provided using internal or third-party tools. It is vital to have plans to supervise usage, SLAs, performance, robustness, and business dependency of these services.

Performance and Bandwidth Cost: Businesses can save money on hardware but they have to spend more for the bandwidth. This can be a low cost for smaller applications but can be significantly high for the data-intensive applications. Delivering intensive and complex data over the network requires sufficient bandwidth. Because of this, many businesses are waiting for a reduced cost before switching to the cloud.

All these challenges should not be considered as road blocks in the pursuit of cloud computing. It is rather important to give serious consideration to these issues and the possible ways out before adopting the technology.

Future of cloud technology in India

In February 2017, US tech giant Oracle predicted that as enterprise cloud is expected to become the most secure place for IT processing with nearly 60 per cent IT organisations to move their systems management to the cloud in 2017, India will be among top beneficiaries from cloud computing.

Increased government spending on digital technologies, coupled with heightened demand from the private sector, continues to be a great boost for the cloud industry. Not only the large firms, cloud will empower small business innovation in 2017 and Artificial Intelligence (AI) will become a reality, Oracle said. Gartner has predicted that in India alone, the cloud market will reach over \$3 billion by 2017—an almost five-fold increase from 2012.

India Inc has pledged R4.5 lakh crore for Digital India, which can create employment for some 18 lakh people. A good number of them will be in cloud computing. With the launch of 100 Smart Cities, 500 rejuvenated cities and numerous projects to create industrial hubs, a strong virtual backbone, which is possible with cloud technology, is a critical necessity to take the development process to the next level.

Latest Trends in Virtualization

Network and Storage Virtualization

The virtualization of storage and virtual storage area networks (VSANs) is another trend that's gaining ground. Like server virtualization, VSANs offer greater ease of use, security, flexibility and scalability, since businesses do not need to buy more hardware or invest in updating it while scaling up. This also reduces hardware redundancy, in addition to investment costs.

Updated Physical Resources

The computing and storage equipment that IT departments use, as well as physical network parts like routers and switches, have undergone a sea change in recent times. Newer kinds of hardware available today are designed to run and configure VLANs (virtual LANs) as well as support virtual network design and implementation, and companies are investing in these to avoid virtualization issues. We shall discuss VLANs in more detail in the chapter on 'Networking Systems'.

New Players in Virtualization

While VMware has been the main player in virtualization technology so far, there are many new ones joining the race. Some of these deal with specific solutions and activities like VMware monitoring while others like Citrix, IBM and HP are gaining ground with alternative software and systems, especially targeting companies who have faced VMware problems in the past.

Mobile phone operating systems

There are also mobile phone operating systems that have gained tremendous importance recently. In the mobile world mostly it is the operating system that rules the mobile phone market. Some of the most popular mobile operating systems are Android, iOS (iPhones), BlackBerry and Windows. Each mobile OS

has numerous versions. Android OS is the unquestioned king of mobile market followed far behind by iOS as of date.

Microsoft Windows operating systems

Microsoft Windows is a family of proprietary operating systems designed by Microsoft Corporation and primarily targeted to Intel architecture based computers, with an estimated 89 percent total usage share on Web connected computers. In 2011, Windows 7 overtook Windows XP as most common version in use. The latest version is Windows 10.

Microsoft Windows was first released in 1985, as an operating environment running on top of MS-DOS, which was the standard operating system shipped on most Intel architecture personal computers at the time. In 1995, Windows 95 was released which only used MS-DOS as a bootstrap. Later to 2000 all versions have been based on the Windows NT kernel. Windows NT (New Technology) is an operating system that supports preemptive multitasking. There are actually two versions of Windows NT: Windows NT Server, designed to act as a server in networks, and Windows NT Workstation for stand-alone or client workstations.

Server editions of Windows are widely used. In recent years, Microsoft has expended significant capital in an effort to promote the use of Windows as a server operating system. However, Windows' usage on servers is not as widespread as on personal computers as Windows competes against Linux and BSD for server market share. The share of Windows server operating systems may range between 20-30%, whereas the Unix and Unix-like OS cuts the major chunk.

As per the latest statistics, in very high-end systems like super computers, the share of Windows OS is reduced to almost nil whereas the Unix and Unix-like operating systems are used in more than 99% of systems.

Unix and Unix-like operating systems

Unix was originally written in assembly language. Ken Thompson wrote B, mainly based on BCPL, based on his experience in the MULTICS project. B was replaced by C, and Unix, rewritten in C, developed into a large, complex family of inter-related operating systems which have been influential in every modern operating system.

The Unix-like family is a diverse group of operating systems, with several major sub-categories including System V, BSD, and Linux. The name "UNIX" is a trademark of The Open Group which licenses it for use with any operating system that has been shown to conform to their definitions. "UNIX-like" is commonly used to refer to the large set of operating systems which resemble the original UNIX.

Unix-like systems run on a wide variety of computer architectures. They are used heavily for servers in business, as well as workstations in academic and engineering

environments. Free UNIX variants, such as Linux and BSD, are popular in these areas.

Four operating systems are certified by The Open Group (holder of the Unix trademark) as Unix. HP's HP-UX and IBM's AIX are both descendants of the original System V Unix and are designed to run only

on their respective vendor's hardware. In contrast, Sun Microsystems's Solaris can run on multiple types of hardware, including x86 and Sparc servers, and PCs.

Apple's macOS, a replacement for Apple's earlier (non-Unix) Mac OS, is a hybrid kernel-based BSD variant.

Fourth Generation programming languages:

Fourth generation languages are also known as very high level languages. They are non-procedural languages, so named because they allow programmers and users to specify what the computer is supposed to do without having to specify how the computer is supposed to do it. Consequently, fourth generation languages need approximately one tenth the number of statements that a high level languages needs to achieve the same results.

A fourth-generation programming language (4GL) is a computer programming language envisioned as a refinement of the style of languages classified as third-generation

programming language (3GL). Languages claimed to be 4GL may include support for database management, report generation, mathematical optimization, GUI development,

or web development. Depending on the language, the sophistication of fourth generation languages varies widely. These languages are usually used in conjunction with a database and its data dictionary.

Basic types of language tools fall into the fourth generation language category are Query languages, Report generators, Applications generators and Decision support systems and financial planning languages.

Examples: Oracle Forms, Oracle Designer, PL/SQL, Clipper, Power Builder, SAS, SPSS, SQL

Fifth Generation programming languages:

While 4GL are designed to build specific programs, 5GL are designed to make the computer solve a given problem without the programmer. This way, the programmer only needs to worry about what problems need to be solved and what conditions need to be met, without worrying about how to implement a routine or algorithm to solve them.

Natural Languages represent the next step in the development of programming languages, i-e fifth generation languages. The text of a natural language statement very closely resembles human speech. In fact, one could word a statement in several ways perhaps even misspelling some words or changing the order of the words and get the same result. These languages are also designed to make the computer “smarter”. Natural languages already available for microcomputers include Clout, Q&A, and Savvy Retriever (for use with databases) and HAL (Human Access Language). Other examples of 5GL are Prolog, OPS5 and Mercury.

The use of natural language touches on expert systems, computerized collection of the knowledge of many human experts in a given field, and artificial intelligence, independently smart computer systems.

Widely used open-source software: Open source software projects are built and maintained by a network of volunteer programmers and are widely used in free as well as commercial products. Prime examples of

open-source products are the Apache HTTP Server, the e-commerce platform osCommerce, internet browsers Mozilla Firefox and Chromium (the project where the vast majority of development of the freeware Google Chrome is done) and the full office suite LibreOffice. One of the most successful open-source products is the GNU/Linux operating system, an open-source Unix-like operating system, and its derivative Android, an operating system for mobile devices. In some industries, open source software is the norm.

WEB BROWSERS

A web browser is a software application that lets us visit web pages on the Internet. Although browsers are primarily intended to use the World Wide Web, they can also be used to access information provided by web servers in private networks or files in file systems. Web browsers consist of a user interface, layout engine, rendering engine, JavaScript interpreter, UI backend, networking component and data persistence component. These components achieve different functionalities of a web browser and together provide all capabilities of a web browser.

The most popular web browsers that are used today are Google Chrome, Mozilla Firefox, Microsoft Internet Explorer, Apple Safari and the Opera browser. Internet Explorer was deprecated in Windows 10, with Microsoft Edge replacing it as the default web browser. As per the statistics available in 2017, Google Chrome has a market share of 64% followed by Mozilla Firefox and Internet Explorer with 15% and 10% respectively.

Operating System Compatibility: Both Firefox and Opera have compatible versions for all kinds of operating systems covering Windows, macOS, Linux, BSD, Android, iOS and Other Unix based operating systems. Google Chrome too supports all these operating systems except BSD & other UNIX based OS. Safari supports only macOS and iOS and IE only Windows as of date.

Functioning of a Web browser

The primary purpose of a web browser is to bring information resources to the user ("retrieval" or "fetching"), allowing them to view the information ("display", "rendering"), and then access other information ("navigation", "following links").

This process begins when the user inputs a Uniform Resource Locator (URL), for example <http://en.wikipedia.org/>, into the browser. The prefix of the URL, the Uniform Resource Identifier or URI, determines how the URL will be interpreted. The most commonly used kind of URI starts with `http:` and identifies a resource to be retrieved over the Hypertext Transfer Protocol (HTTP). Many browsers also support a variety of other prefixes, such as `https:` for HTTPS, `ftp:` for the File Transfer Protocol, and `file:` for local files. Prefixes that the web browser cannot directly handle are often handed off to another application entirely. For example, `mailto:` URIs are usually passed to the user's default e-mail application, and `news:` URIs are passed to the user's default newsgroup reader.

In the case of `http`, `https`, `file`, and others, once the resource has been retrieved the web browser will display it. HTML and associated content (image files, formatting information such as CSS, etc.) is passed to the browser's layout engine to be transformed from markup to an interactive document, a process known as "rendering". Aside from HTML, web browsers can generally display any kind of content that can be part of a web page. Most browsers can display images, audio, video, and XML files, and often have plug-ins to support Flash applications and Java applets. Upon encountering a file of an unsupported type or a file that is set up to be downloaded rather than displayed, the browser prompts the user to save the file to disk.

Information resources may contain hyperlinks to other information resources. Each link contains the URI of a resource to go to. When a link is clicked, the browser navigates to the resource indicated by the link's target URI, and the process of bringing content to the user begins again.

Replacement of Dial-up by broadband

Broadband internet access via cable, digital subscriber line, satellite and FTTx has been replacing dial-up access in many parts of the world. Broadband connections typically offer speeds of 700 kbit/s or higher for two-thirds more than the price of dial-up on average. In addition broadband connections are always on, thus avoiding the need to connect and disconnect at the start and end of each session. Finally, unlike dial-up, broadband does not require exclusive use of a phone line and so one can access the Internet and at the same time make and receive voice phone calls without having a second phone line.

Dial-up Internet access has undergone a precipitous fall in usage, and potentially approaches extinction as modern users turn towards broadband. In contrast to the year 2000 when about 34% of Internet users used dial-up, this dropped to 1% in 2016.

Extranet

The term Extranet is linked with Intranet. Extranet is an external of computer network that allows the outside users to access the Intranet of organization. On the other hand, Internet is a global network system and is available to all while Intranet and Extranet are available to the inside users and users of selectively linked outside organization respectively. For instance, whereas your organization's LAN or WAN network represents an Intranet, the external trusted networks such as RBI, NPCI and IDRBT, which are connected to your Intranet for limited access or flow of data may be called Extranet networks with respect to your WAN, i.e., your Intranet. Generally Extranets are connected to Intranet through Routers as well as network security devices such as Firewalls for securing Intranet from the users of Extranet.

Network Switches and Routers

There are three main devices that work to connect one computer to another computer. A network hub, switch, and router can all perform this function. It can sometimes be confusing when trying to figure out what device is currently being used on a computer network, without knowing what each device does. Routers and switches are both computer networking devices that allow one or more computers to be connected to other computers, networked devices, or to other networks. The functions of a router, switch and hub and are all different, even if at times they are integrated into a single device.

Switches are used to connect multiple devices on the same network within a building or campus. For example, a switch can connect your computers, printers, and servers, creating a network of shared resources. The switch, one aspect of your networking basics, would serve as a controller, allowing the various devices to share information and talk to each other. Through information sharing and resource allocation, switches save you money and increase productivity.

There are two basic types of switches to choose from as part of your networking basics: managed and unmanaged. An unmanaged switch works out of the box and does not allow you to make changes. Home networking equipment typically includes unmanaged switches. A managed switch can be accessed and programmed. This capability provides greater network flexibility because the switch can be monitored and adjusted locally or remotely. With a managed switch, you have control over network traffic and network access.

Routers, the second valuable component of your networking basics, are used to connect multiple networks together. For example, you would use a router to connect your networked computers to the Internet and thereby share an Internet connection among many users. The router will act as a dispatcher, choosing the best route for your information to travel so that you receive it quickly. Routers analyze the data being sent over a network, change how it is packaged, and send it to another network or to a different type of network. They connect your business to the outside world,

protect your information from security threats, and can even decide which computers get priority over others. Depending on your business and your networking plans, you can choose from routers that include different capabilities. These can include networking basics such as:

Firewall: Specialized software that examines incoming data and protects your business network against attacks.

Virtual private network (VPN): A way to allow remote employees to safely access your network.

IP phone network: Combines your company's computer and telephone network, using voice and conferencing technology, to simplify and unify your communications.

Patch Panel vs Switch: A patch panel performs no other function except for acting as a connector. A network switch connects clients within a network to enable them to access the internet, share data and perform other functions

Introduction to Software

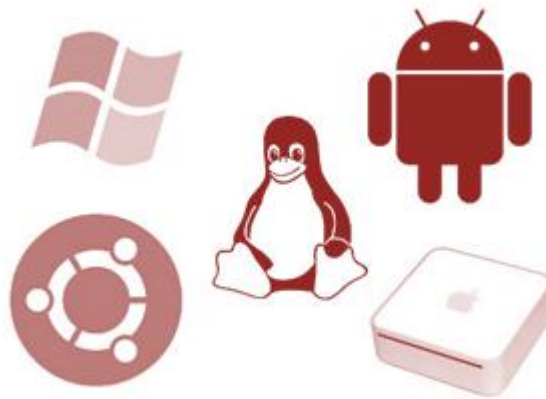
COMPUTER SOFTWARE-MEANING AND TYPES

Software could be considered as the language of a computer. It is the combination of programmes/commands used by products containing processors. That is, software is a set of programmes/commands designed to perform a well-defined task. You have already learnt about the components of a computer, whether it is desktop/laptop/palmtop; which has both hardware and software. The tangible part is the hardware and the instructions that can make the processors to work is the software. As we know computers do not think for themselves, so they need software, which is made to manipulate its hardware in such a way that you, the user, can understand. In short, Software is the set of instructions that tell a computer what it needs to do or the non-physical part of a computer; programs and documentation that play a part in a computer system's operation. JAVA, C++, Microsoft Office, Open Office etc. are examples for computer software.



(Picture Source:
https://upload.wikimedia.org/wikipedia/commons/thumb/e/e1/Operating_system_placement.svg/200px-Operating_system_placement.svg.png)

Software can be classified into different types such as *system software*, *application software*, *proprietary software*, *open software*, *shareware* and *freeware*, which will be discussed in the following sections.



System Software

Now, we know that software is the language in which the user can interact with the computer. The basic interaction of the user with the computer is through input devices (you have already learnt different input devices in earlier chapter). For example if you use a key board to input, there are only some key strokes going into the computer, with which we would like to get the task done. This is possible when there is an interface which converts our inputs to be meaningful to the system, which is called *system software*.

System software is a collection of programmes or commands designed to operate, control, and extend the processing capabilities of the computer. Examples of system software are *Operating system*, *Compilers*, *Interpreter*, and *Assemblers*.

One needs to have a thorough knowledge about the grammar which the system can understand. The syntax and semantics are very important. The system software is found to be bit tough and complex for a common man and is dealt with by technically qualified persons.

Systems software are further subdivided into operating systems and utilities. The operating system is the program that actually makes the computer operates. Utilities are programs which either improves the functioning of the operating system or supply missing or additional functionality.

An Operating System (OS) is system software that manages computer hardware and software resources and provides common services for computer programs. The operating system is a component of the system software in a computer system. Application programs usually require an operating system for them to function. Examples include: Microsoft Windows (XP, Vista, or 7), any flavor of Linux, and Mac OS X (An apple version of UNIX).

The following is a list of some of the functions of the operating system:

- boot-up the computer
- control the hard drives: this includes such features as formatting as well as saving files to and retrieving files from disk
- control the input/output ports
- control input devices such as keyboard, mouse and scanner
- control output devices such as the video display and printer
- provide the functionality for computers to be linked in a network
- provide the foundation for application software to be launched
- enable application software to access and use the hardware

A compiler is a computer program (or a set of programs) that transforms source code written in a programming language (the source language) into another computer language (the target language), with the latter often having a binary form known as object code.

An interpreter is a computer program that directly executes, i.e. performs, instructions written in a programming or scripting language, without previously compiling them into a machine language program.

An assembler is a program that takes basic computer instructions and converts them into a pattern of bits that the computer's processor can use to perform its basic operations. Some people call these instructions assembler language and others use the term assembly language.

Utilities are programs that manage, repair, and optimize data on a computer. A basic set of utilities is provided with every OS.

Application Software



Application Software is designed to run a particular application such as word processing, presentation, drawing, communicating etc. It may be single software or a combination in order to perform a particular application. Examples include payroll software, reservation software, Microsoft Word, Libre Office Writer etc. Ease of use, ease in manipulating and interactivity are some of the benefits of such software.

Application software does the specific things you want the computer to do, whereas the Operating System gives general instructions to the computer for controlling the hardware.

Table below gives the list of different type application software, brand and functions:

Application	Brand Name	Function
Word Processor	Open Office.org writer Libre Office writer Microsoft Word	Create, store, format and edit documents, letters and articles. Word processors are used where the emphasis is on manipulation of text.
Spreadsheet	Open Office.org Calc Libre office Calc Microsoft Excel	Create financial statements, balance sheets, perform statistical and numerical analysis of data and make forecasts based on numeric data. Spreadsheets are used where the emphasis is on arithmetic.
Presentation	Open Office.org Libre Office Impress Microsoft PowerPoint	Create slide show, lecture, seminar and other types of presentation.
Data Base	Sybase MySQL Microsoft ACCESS	Store and convert data into information. Databases are particularly useful in working with large quantities of data.
Web Browser	Mozilla Chrome	Surf the Internet and view web sites.

	Netscape	
	Internet Explorer	
Desktop Publishing (DTP)	Page Maker Microsoft Publisher	DTP is similar to word processing except that there is more emphasis on page layout and the integration of diagrams.
Graphics and Imaging	Adobe Photoshop GIMP	Create and manipulate graphics images and store images in a variety of formats.

Proprietary Software



Pro

proprietary software is software that is owned by an individual or a company (usually the one that developed it). There are almost always major restrictions on its use, and its source code is almost always kept secret

(source code is the version of the software as it is originally written by a developer in a plain text, readable in plain or alphanumeric characters). Sometimes these are called 'closed code software' which means, the source code is not for open access. Most software is covered by copyright which, along with contract law, patents, and trade secrets, provides legal basis for its owner to establish exclusive rights.

The owner of proprietary software exercises certain exclusive rights over the software. The owner can restrict use, inspection of source code, modification of source code, and redistribution. Proprietary software may also have licensing terms that limit the usage of that software to a specific set of hardware.

Apple has such a licensing model for Mac OS X, an operating system which is limited to Apple hardware, both by licensing and various design decisions. Examples of proprietary software include Microsoft Windows, Adobe Flash Player, PS3 OS, iTunes, Adobe Photoshop, Google Earth, Mac OS X, Skype, WinRAR, Oracle's version of Java and some versions of UNIX.

Open Source Software



The term "open source" refers to something that can be modified and shared because its design is publicly accessible. Open source software is software whose source code is available for modification or enhancement by anyone. Open source software is different. Its authors make its source code available to others who would like to view that code, copy it, learn from it, alter it, or share it. Libre Office and the GNU Image Manipulation Program are examples of open source software. As they do with proprietary software, users must accept the terms of a license when they use open source software—but the legal terms of open source licenses differ dramatically from those of proprietary licenses. Open source software licenses promote collaboration and sharing because they allow other people to make modifications to source code and incorporate those changes into their own projects. Some open source licenses ensure that anyone

who alters and then shares a program with others must also share that program's source code without charging a licensing fee for it.

Shareware

Shareware is software, generally downloaded from the Internet, which can be freely used and distributed. However, it does require that if users would like to continue using it, they pay the developer a fee. This is nearly always done by means of a credit card transfer across the Internet. When payment is received, users get a serial number with which they can continue to use the software.

Shareware is not a totally free software but you usually get a certain days trial depending on the software or the company. After you have passed those days the software expires and works no more. If the user would like to continue using that software they have to pay a certain fee to get the original product.

Shareware is not free software, or even semi free. There are two reasons it is not:

- For most shareware, source code is not available; thus, you cannot modify the program at all.
- Shareware does not come with permission to make a copy and install it without paying a license fee, not even for individuals engaging in nonprofit activity. (In practice, people often disregard the distribution terms and do this anyway, but the terms don't permit it.)

Shareware is inexpensive because it is usually produced by a single programmer and is offered directly to customers. Thus, there is practically no packaging or advertising expenses. Those Sharewares can be shared in any website as long as they are for trial purposes or to attract customers.

Freeware

Freeware is software which can be freely copied and distributed. Usually there are certain restrictions such as it may not be resold or its source should be acknowledged. Examples of free ware include PDF edit (Software that allows you to edit PDF files), YouTube Downloader (Downloads & converts videos from YouTube), 3.GOM media player (Play video files of multiple video formats)

FREE OPEN SOURCE SOFTWARE(FOSS)

We have discussed about different software. The software developer has all the rights to decide whether the source code needs to be shared or not. This decision makes the change that the software is free or

proprietary. The paradigm shift in the intellectual property and knowledge management paves the roots for democratization of knowledge. This results in free and open movement and also *copy left* movement (as against copy right). These basically focus on the freedom of the user to access, modify, and redistribute the software.

Concept

Free and Open-Source Software (FOSS) is computer software that can be classified as both free software and open-source software. That is, anyone is freely licensed to use, copy, study, and change the software in any way, and the source code is openly shared so that people are encouraged to voluntarily improve the design of the software. This is in contrast to proprietary software, where the software is under restrictive copyright and the source code is usually hidden from the users.

The first known use of the phrase *free open-source software* on Usenet was in a posting on 18 March 1998. The primary license difference between free software and [open source](#) is one of philosophy. According to the Free Software Foundation, "Nearly all open source software is free software. The two terms describe almost the same category of software, but they stand for views based on fundamentally different values" (Richard Stallman).

"Free software" means software that respects users' freedom and community. Roughly, it means that **the users have the freedom to run, copy, distribute, study, change and improve the software**. Thus, "free software" is a matter of liberty, not price. To understand the concept, you should think of "free" as in "free speech," not as in "free beer"

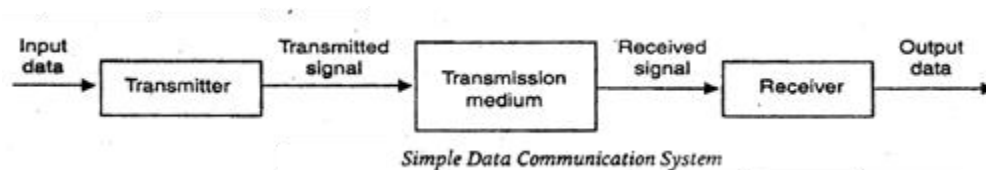


Networking Systems

Data communication refers to the exchange of data between a source and a receiver via form of transmission media such as a wire cable. Data communication is said to be local if communicating devices are in the same building or a similarly restricted geographical area.

The meanings of source and receiver are very simple. The device that transmits the data is known as source and the device that receives the transmitted data is known as receiver. Data communication aims at the transfer of data and maintenance of the data during the process but not the actual generation of the [information](#) at the source and receiver.

Datum mean the facts information statistics or the like derived by calculation or experimentation. The facts and information so gathered are processed in accordance with defined systems of procedure. Data can exist in a variety of forms such as numbers, text, bits and bytes. The Figure is an illustration of a simple data communication system.



The term data used to describe information, under whatever form of words you will be using.

A data communication system may collect data from remote locations through data transmission circuits, and then outputs processed results to remote locations. Figure provides a broader view of data communication networks. The different data communication techniques which are presently in widespread use evolved gradually either to improve the data communication techniques already existing or to replace the same with better options and features. Then, there are data communication jargons to contend with such as baud rate, modems, routers, LAN, WAN, TCP/IP, ISDN, during the selection of communication systems. Hence, it becomes necessary to review and understand these terms and gradual development of data communication methods

Components of data communication system

A Communication system has following components:

1. **Message:** It is the information or data to be communicated. It can consist of text, numbers, pictures, sound or video or any combination of these.
 2. **Sender:** It is the device/[computer](#) that generates and sends that message.
-

3. **Receiver:** It is the device or computer that receives the message. The location of receiver computer is generally different from the sender computer. The distance between sender and receiver depends upon the types of network used in between.

4. **Medium:** It is the channel or physical path through which the message is carried from sender to the receiver. The medium can be wired like twisted pair wire, coaxial cable, fiber-optic cable or wireless like laser, radio waves, and microwaves.

5. **Protocol:** It is a set of rules that govern the communication between the devices. Both sender and receiver follow same [protocols](#) to communicate with each other.

A protocol performs the following functions:

1. **Data sequencing.** It refers to breaking a long message into smaller packets of fixed size. Data sequencing rules define the method of numbering packets to detect loss or duplication of packets, and to correctly identify packets, which belong to same message.

2. **Data routing.** Data routing defines the most efficient path between the source and destination.

3. **Data formatting.** Data formatting rules define which group of bits or characters within packet constitute data, control, addressing, or other information.

4. **Flow control.** A communication protocol also prevents a fast sender from overwhelming a slow receiver. It ensures resource sharing and protection against traffic congestion by regulating the flow of data on communication lines.

5. **Error control.** These rules are designed to detect errors in messages and to ensure transmission of correct messages. The most common method is to retransmit erroneous message block. In such a case, a block having error is discarded by the receiver and is retransmitted by the sender.

6. **Precedence and order of transmission.** These rules ensure that all the nodes get a chance to use the communication lines and other resources of the network based on the priorities assigned to them.

7. **Connection establishment and termination.** These rules define how connections are established, maintained and terminated when two nodes of a network want to communicate with each other.

8. **Data security.** Providing data security and privacy is also built into most communication software packages. It prevents access of data by unauthorized users.

9. **Log information.** Several communication software are designed to develop log information, which consists of all jobs and data communications tasks that have taken place. Such information may be used for charging the users of the network based on their usage of the network resources.

The effectiveness depends on four fundamental characteristics of data communications

1. **Delivery:** The data must be deliver in correct order with correct destination.
2. **Accuracy:** The data must be deliver accurately.
3. **Timeliness:** The data must be deliver in a timely manner.late delivered Data useless.
4. **Jitter:** It is the uneven delay in the packet arrival time that cause uneven quality.

Network

A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

Two very common types of networks include:

- Local Area Network (LAN)
- Wide Area Network (WAN)

You may also see references to a Metropolitan Area Networks (MAN), a Wireless LAN (WLAN), or a Wireless WAN (WWAN).

Local Area Network

A Local Area Network (LAN) is a network that is confined to a relatively small area. It is generally limited to a geographic area such as a writing lab, school, or building.

Computers connected to a network are broadly categorized as servers or workstations. Servers are generally not used by humans directly, but rather run continuously to provide "services" to the other computers (and their human users) on the network. Services provided can include printing and faxing, software hosting, file storage and sharing, messaging, data storage and retrieval, complete access control (security) for the network's resources, and many others.

Workstations are called such because they typically do have a human user which interacts with the network through them. Workstations were traditionally considered a desktop, consisting of a computer, keyboard, display, and mouse, or a laptop, with with integrated keyboard, display, and touchpad. With the advent of the tablet computer, and the touch screen devices such as iPad and iPhone, our definition of

workstation is quickly evolving to include those devices, because of their ability to interact with the network and utilize network services.

Servers tend to be more powerful than workstations, although configurations are guided by needs. For example, a group of servers might be located in a secure area, away from humans, and only accessed through the network. In such cases, it would be common for the servers to operate without a dedicated display or keyboard. However, the size and speed of the server's processor(s), hard drive, and main memory might add dramatically to the cost of the system. On the other hand, a workstation might not need as much storage or working memory, but might require an expensive display to accommodate the needs of its user. Every computer on a network should be appropriately configured for its use.

On a single LAN, computers and servers may be connected by cables or wirelessly. Wireless access to a wired network is made possible by wireless access points (WAPs). These WAP devices provide a bridge between computers and networks. A typical WAP might have the theoretical capacity to connect hundreds or even thousands of wireless users to a network, although practical capacity might be far less.

Nearly always servers will be connected by cables to the network, because the cable connections remain the fastest. Workstations which are stationary (desktops) are also usually connected by a cable to the network, although the cost of wireless adapters has dropped to the point that, when installing workstations in an existing facility with inadequate wiring, it can be easier and less expensive to use wireless for a desktop.

See the [Topology](#), [Cabling](#), and [Hardware](#) sections of this tutorial for more information on the configuration of a LAN.

Wide Area Network

Wide Area Networks (WANs) connect networks in larger geographic areas. Dedicated transoceanic cabling or satellite uplinks may be used to connect this type of global network.

A WAN or Wide Area Network is a group of widely dispersed computers that are connected together. These could be across the same town or across a country or even across the world. Apart from distance, the other feature that distinguishes a WAN from a LAN is that the WAN would make use of a range of communication technologies such as telephone, microwave and satellite links. Much of the problems

faced by LAN connections can be solved by WAN. Most WANs are made from several LANs connected together.

Media

Guided and Unguided media::

Telecommunication links can broadly be classified into two categories, namely, guided media (wired) and unguided media(wireless). Both media are used for short distance (LANs, MANs) and long distance (WANs) communication.

Guided Media or Wired links:



Examples of Wired Media

As the name indicates, in guided media

- Electrical/Optical signals are passed through a solid medium (different types of cables/wires)
- As the path traversed by the signals is guided by the size, shape and length of the wire, this type of media is called guided media. Also, in guided media, the signals are confined within the wire and do not propagate outside of the wire/media.
- E.g., Copper Unshielded Twisted Pair (UTP), Copper Shielded Twisted Pair (STP), Copper Coaxial cables, Fiber Optic Cables.

Twisted Pair Copper:

- It is the most widely deployed media type across the world, as the last mile telephone link connecting every home with the local telephone exchange is made of twisted pair copper. These telephone lines are reused as last mile DSL access links to access the internet from home.
 - They are also used in Ethernet LAN cables within homes and offices.
 - They support low to High Data Rates (in order of Giga bits)
- However, they are effective only upto a maximum distance of a few kilometres/miles, as the signal strength is lost significantly beyond this distance.

- They come in two variants, namely UTP (unshielded twisted pair) and STP (shielded twisted pair). Within each variant, there are multiple sub-variants, based on the thickness of the material (like UTP-3, UTP-5, UTP-7 etc.)

- E.g. DSL, 10/100/1000Mbps Ethernet cables

Copper Co-axial Cables

- Co-axial copper cables have an inner copper conductor and an outer copper shield, separated by a di-electric insulating material, to prevent signal losses.
- It is primarily used in cable TV networks and as trunk lines between telecommunication equipments.
 - It serves as an internet access line from the home.
 - It supports medium to High Data Rates
- It has much better immunity to noise and hence signal strength is retained for longer distances than in copper twisted pair media.

Fiber Optic Cables

- Here, information is transmitted by propagation of optical signals (light) through fiber optic cables and not through electrical/electromagnetic signals. Due to this, fiber optics communication supports longer distances as there is no electrical interference.
- As the name indicates, fiber optic cables are made of very thin strands of glass (silica).
- As they support very high data rates, fiber optic lines are used as WAN backbone and trunk lines between data exchange equipments.
- They are also used for accessing internet from home through FTTH (Fiber-To-The-Home) lines.
- Additionally, they are used even for LAN environment with different LAN technologies like Fast Ethernet, Gigabit Ethernet etc. using optical links at the physical layer.

•

OC-48, OC-192, FTTC, HFC are examples of Fiber Optical links.

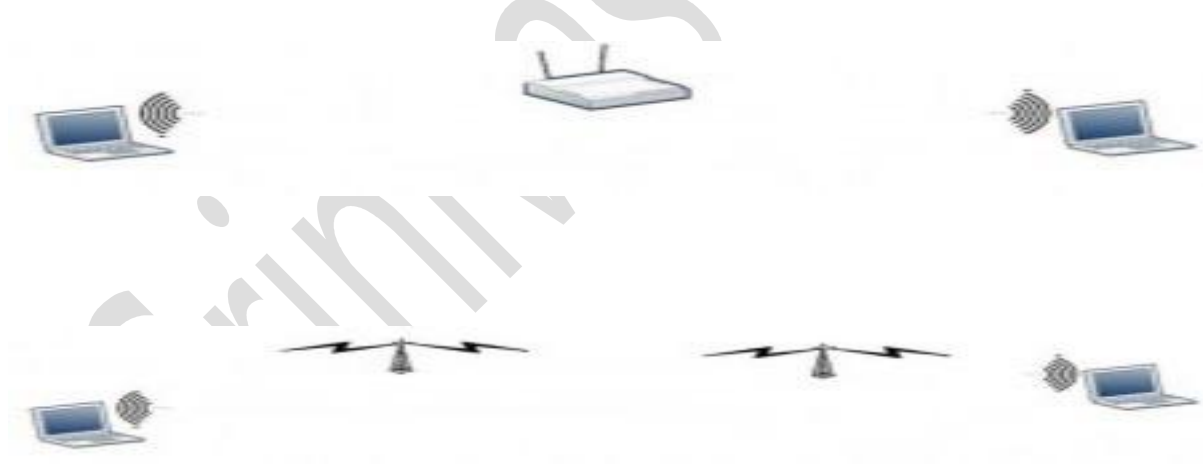
Unguided Wireless Media:

Here information is transmitted by sending electromagnetic signals through free space and hence the name unguided media, as the signals are not guided in any specific direction or inside any specific medium.

All unguided media transmission are classified as wireless transmission.

Wireless transmission can be used as the medium in both LAN and WAN environments, as illustrated in the diagrams below:

Two laptops communicating within a LAN using a wireless Access Points



Two laptops communicating via. a long distance WAN using a WiMax Wireless transmission network

Different forms of wireless communication used in the internet vary mainly based on the following attributes:

- Distance separating the end stations
- Frequency spectrum used by the electromagnetic signals

- Line Encoding technique used

Based on these attributes, a wide variety of wireless PHYs and different types of antennae are used in wireless communication.

The diagram given below illustrates different types of antennae typically used in wireless communication

Different Types of Antennae Used in wireless communication



As illustrated in the diagram, antennae can be of many sizes and shapes. Some of them are point to point antennae while others are omni-directional antennae. Even satellites act as giant antennae in the sky, by receiving and transmitting signals generated from the earth.

Wi-Fi, Wi-Max, 3G are example wireless networks used for internet communication

Network Controls

Network security is an over-arching term that describes that the policies and procedures implemented by a network administrator to avoid and keep track of unauthorized access, exploitation, modification, or denial of the network and network resources.

This means that a well-implemented network security blocks viruses, malware, hackers, etc. from accessing or altering secure information.

The first layer of network security is enforced through a username/password mechanism, which only allows access to authenticated users with customized privileges. When a user is authenticated and granted specific system access, the configured firewall enforces network policies, that is, accessible user services.

However, firewalls do not always detect and stop viruses or harmful malware, which may lead to data loss. An anti-virus software or an intrusion prevention system (IPS) is implemented to prevent the virus and/or harmful malware from entering the network.

Network security is sometimes confused with information security, which has a different scope and relates to data integrity of all forms, print or electronic

Some of the most commonly used network devices are

Modem

A modem is a network device that both modulates and demodulates analog carrier signals (called sine waves) for encoding and decoding digital information for processing. Modems accomplish both of these tasks simultaneously and, for this reason, the term modem is a combination of "modulate" and "demodulate."

Repeater

A repeater is a network device that retransmits a received signal with more power and to an extended geographical or topological network boundary than what would be capable with the original signal.

Switch

A switch, in the context of networking is a high-speed device that receives incoming data packets and redirects them to their destination on a local area network (LAN). A LAN switch operates at the data link layer (Layer 2) or the network layer of the OSI Model and, as such it can support all types of packet protocols.

Hub

A hub, also called a network hub, is a common connection point for devices in a network. Hubs are devices commonly used to connect segments of a LAN. The hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets

Gateway

In computer networking and telecommunications, a gateway is a component that is part of two networks, which use different protocols. The gateway will translate one protocol into the other. A router is a special case of a gateway.

Gateways, also called protocol converters, can operate at any network layer. The activities of a gateway are more complex than that of the router or switch as it communicates using more than one protocol.

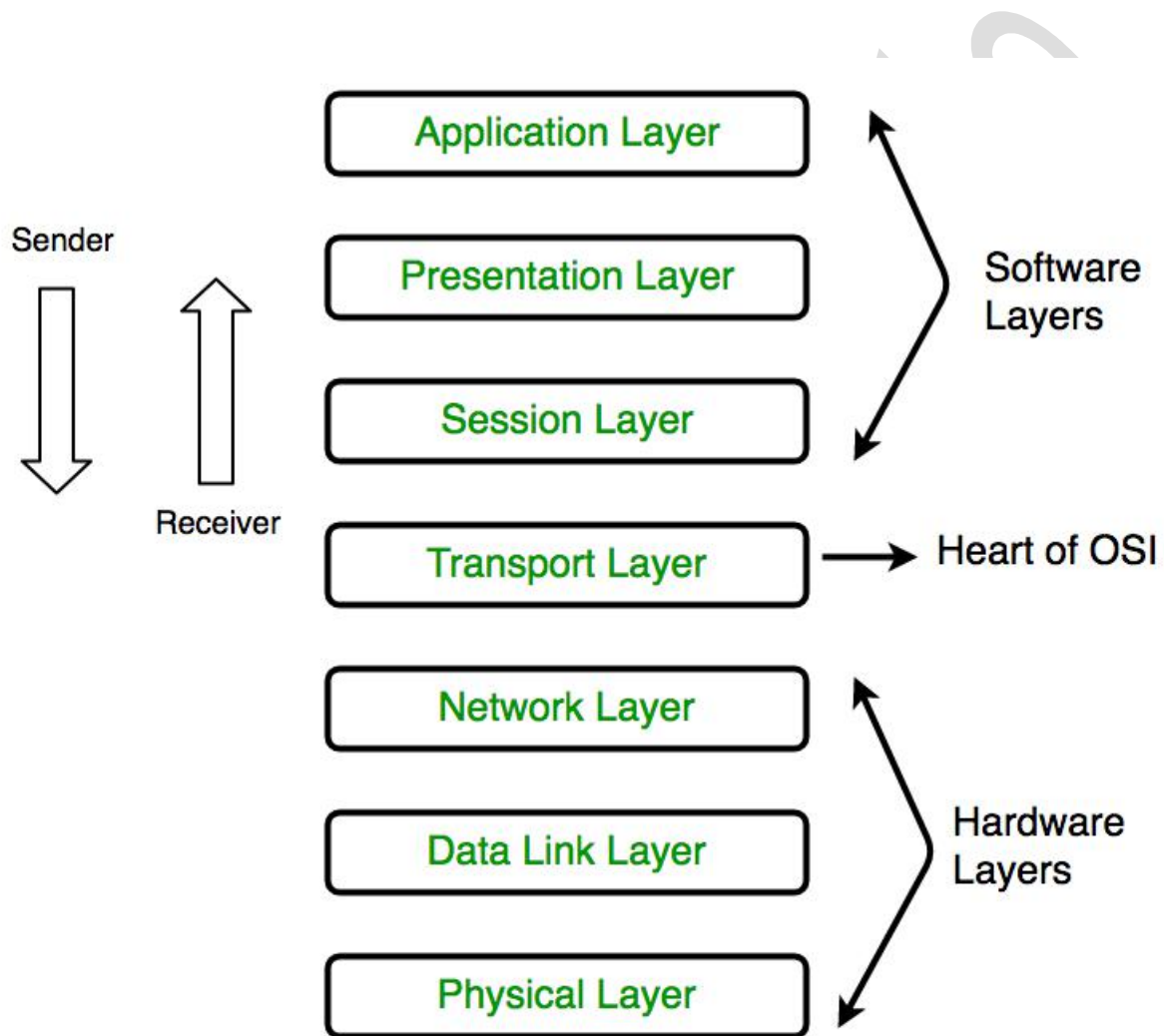
Both the computers of internet users and the computers that serve pages to users are *host nodes*. The nodes that connect the networks in between are *gateways*. These are gateway nodes:

- the computers that control traffic between company networks
- the computers used by internet service providers (ISPs) to connect users to the internet
-

Computer Network | Layers of OSI Model

OSI stands for **Open Systems Interconnection**. It has been developed by ISO – '**International Organization of Standardization**', in the year 1974. It is a 7 layer architecture with each layer having

specific functionality to performed. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.



1. Physical Layer (Layer 1) :

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits. It is responsible for the actual physical connection between the devices. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.

The functions of the physical layer are :

1. Bit synchronization: The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.
2. Bit rate control: The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
3. Physical topologies: Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topology.
4. Transmission mode: Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full-duplex.

* Hub, Repeater, Modem, Cables are Physical Layer devices.

** Network Layer, Data Link Layer and Physical Layer are also known as Lower Layers or Hardware Layers.

2. Data Link Layer (DLL) (Layer 2) :

The data link layer is responsible for the node to node delivery of the message. The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.

Data Link Layer is divided into two sub layers :

1. Logical Link Control (LLC)
2. Media Access Control (MAC)

Packet received from Network layer is further divided into frames depending on the frame size of NIC(Network Interface Card). DLL also encapsulates Sender and Receiver's MAC address in the header.

The Receiver's MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking "Who has that IP address?" and the destination host will reply with its MAC address.

The functions of the data Link layer are :

1. Framing: Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
2. Physical addressing: After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.
3. Error control: Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
4. Flow Control: The data rate must be constant on both sides else the data may get corrupted thus , flow control coordinates that amount of data that can be sent before receiving acknowledgement.
5. Access control: When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.

* Packet in Data Link layer is referred as Frame.

** Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.

*** Switch & Bridge are Data Link Layer devices.

3. Network Layer (Layer 3) :

Network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP address are placed in the header by network layer.

The functions of the Network layer are :

1. Routing: The network layer protocols determine which route is suitable from source to destination.

This function of network layer is known as routing.

2. Logical Addressing: In order to identify each device on internetwork uniquely, network layer defines an addressing scheme. The sender & receiver's IP address are placed in the header by network layer. Such an address distinguishes each device uniquely and universally.

* Segment in Network layer is referred as Packet.

** Network layer is implemented by networking devices such as routers.

4. Transport Layer (Layer 4) :

Transport layer provides services to application layer and takes services from network layer. The data in the transport layer is referred to as Segments. It is responsible for the End to End delivery of the complete message. Transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if error is found.

- At sender's side:

Transport layer receives the formatted data from the upper layers, performs Segmentation and also implements Flow & Error control to ensure proper data transmission. It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.

Note: The sender need to know the port number associated with the receiver's application.

Generally this destination port number is configured, either by default or manually. For example, when a web application makes a request to a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default port assigned.

- At receiver's side:

Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.

The functions of the transport layer are :

1. Segmentation and Reassembly: This layer accepts the message from the (session) layer , breaks the message into smaller units . Each of the segment produced has a header associated with it. The transport layer at the destination station reassembles the message.
2. Service Point Addressing: In order to deliver the message to correct process, transport layer header includes a type of address called service point address or port address. Thus by specifying this address, transport layer makes sure that the message is delivered to the correct process.

The services provided by transport layer :

1. Connection Oriented Service: It is a three phase process which include
 - Connection Establishment
 - Data Transfer
 - Termination / disconnection

In this type of transmission the receiving device sends an acknowledgment, back to the source after a packet or group of packet is received. This type of transmission is reliable and secure.

2. Connection less service: It is a one phase process and includes Data Transfer. In this type of transmission the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection oriented Service is more reliable than connection less Service.

* Data in the Transport Layer is called as Segments.

** Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.

Transport Layer is called as Heart of OSI model.

5. Session Layer (Layer 5) :

This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.

The functions of the session layer are :

1. Session establishment, maintenance and termination: The layer allows the two processes to establish, use and terminate a connection.
2. Synchronization : This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
3. Dialog Controller : The session layer determines which device will communicate first and the amount of data that will be sent.

**All the above 3 layers are integrated as a single layer in TCP/IP model as "Application Layer".

**Implementation of above 3 layers is done by the network application itself. These are also known as Upper Layers or Software Layers.

SCENARIO:

Let's consider a scenario where a user wants to send a message through some Messenger application running in his browser. The "Messenger" here acts as the application layer which provides the user with an interface to create the data. This message or so called Data is compressed, encrypted (if any secure data) and converted into bits (0's and 1's) so that it can be transmitted.

6. Presentation Layer (Layer 6) :

Presentation layer is also called the Translation layer. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

The functions of the presentation layer are :

1. Translation : For example, ASCII to EBCDIC.
2. Encryption/ Decryption : Data encryption translates the data into another form or code. The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
3. Compression: Reduces the number of bits that need to be transmitted on the network.

7. Application Layer (Layer 7) :

At the very top of the OSI Reference Model stack of layers, we find Application layer which is implemented by the network applications. These applications produce the data, which has to be

transferred over the network. This layer also serves as window for the application services to access the network and for displaying the received information to the user.

Ex: Application – Browsers, Skype Messenger etc.

**Application Layer is also called as Desktop Layer.

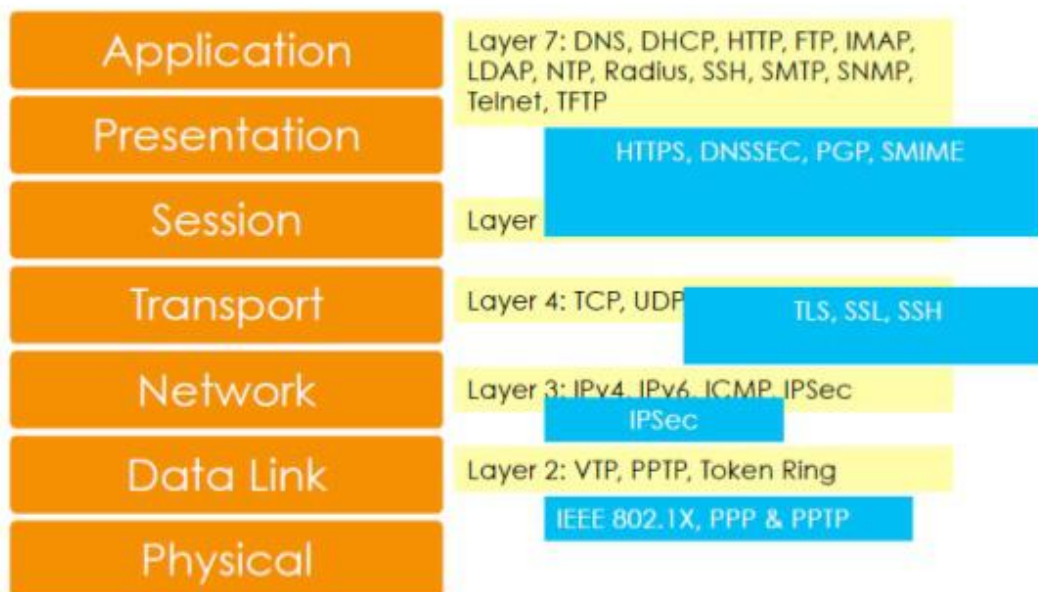
The functions of the Application layer are :

1. Network Virtual Terminal
2. FTAM-File transfer access and management
3. Mail Services
4. Directory Services

OSI model acts as a reference model and is not implemented in Internet because of its late invention.

Current model being used is the TCP/IP model.

Security on Different Layers



Internet Protocol Security (IPsec)

Internet protocol security (IPsec) is a set of protocols that provides security for Internet Protocol. It can use cryptography to provide security. IPsec can be used for the setting up of virtual private networks (VPNs) in a secure manner.

Also known as IP Security.

IPsec involves two security services:

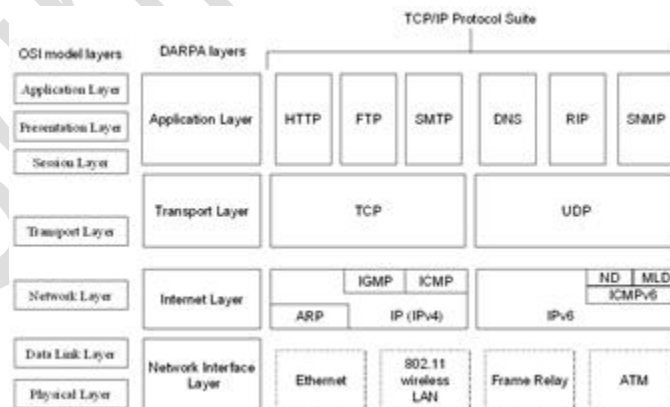
- Authentication Header (AH): This authenticates the sender and it discovers any changes in data during transmission.

- Encapsulating Security Payload (ESP): This not only performs authentication for the sender but also encrypts the data being sent.

There are two modes of IPsec:

- Tunnel Mode: This will take the whole IP packet to form secure communication between two places, or gateways.
- Transport Mode: This only encapsulates the IP payload (not the entire IP packet as in tunnel mode) to ensure a secure channel of communication

Architectural Overview of the TCP/IP Protocol Suite



The TCP/IP Protocol Suite

The TCP/IP protocol suite maps to a four-layer conceptual model known as the DARPA model, which was named after the U.S. government agency that initially developed TCP/IP. The four layers of the DARPA model are: Application, Transport, Internet, and Network Interface. Each layer in the DARPA model corresponds to one or more layers of the seven-layer OSI model.

Figure 2-1 shows the architecture of the TCP/IP protocol suite.

Bb726993.caop0201(en-us,TechNet.10).gif

Figure 2-1 The architecture of the TCP/IP protocol suite

The TCP/IP protocol suite has two sets of protocols at the Internet layer:

IPv4, also known as IP, is the Internet layer in common use today on private intranets and the Internet.

IPv6 is the new Internet layer that will eventually replace the existing IPv4 Internet layer.

Network Interface Layer

The Network Interface layer (also called the Network Access layer) sends TCP/IP packets on the network medium and receives TCP/IP packets off the network medium. TCP/IP was designed to be independent of the network access method, frame format, and medium. Therefore, you can use TCP/IP to communicate across differing network types that use LAN technologies—such as Ethernet and 802.11 wireless LAN—and WAN technologies—such as Frame Relay and Asynchronous Transfer Mode (ATM). By being independent of any specific network technology, TCP/IP can be adapted to new technologies.

The Network Interface layer of the DARPA model encompasses the Data Link and Physical layers of the OSI model. The Internet layer of the DARPA model does not take advantage of sequencing and acknowledgment services that might be present in the Data Link layer of the OSI model. The Internet layer assumes an unreliable Network Interface layer and that reliable communications through session establishment and the sequencing and acknowledgment of packets is the responsibility of either the Transport layer or the Application layer.

Internet Layer

The Internet layer responsibilities include addressing, packaging, and routing functions. The Internet layer is analogous to the Network layer of the OSI model.

The core protocols for the IPv4 Internet layer consist of the following:

The Address Resolution Protocol (ARP) resolves the Internet layer address to a Network Interface layer address such as a hardware address.

The Internet Protocol (IP) is a routable protocol that addresses, routes, fragments, and reassembles packets.

The Internet Control Message Protocol (ICMP) reports errors and other information to help you diagnose unsuccessful packet delivery.

The Internet Group Management Protocol (IGMP) manages IP multicast groups.

For more information about the core protocols for the IPv4 Internet layer, see "IPv4 Internet Layer" later in this chapter.

The core protocols for the IPv6 Internet layer consist of the following:

IPv6 is a routable protocol that addresses and routes packets.

The Internet Control Message Protocol for IPv6 (ICMPv6) reports errors and other information to help you diagnose unsuccessful packet delivery.

The Neighbor Discovery (ND) protocol manages the interactions between neighboring IPv6 nodes.

The Multicast Listener Discovery (MLD) protocol manages IPv6 multicast groups.

For more information about the core protocols for the IPv6 Internet layer, see "IPv6 Internet Layer" later in this chapter.

Transport Layer

The Transport layer (also known as the Host-to-Host Transport layer) provides the Application layer with session and datagram communication services. The Transport layer encompasses the responsibilities of the OSI Transport layer. The core protocols of the Transport layer are TCP and UDP.

TCP provides a one-to-one, connection-oriented, reliable communications service. TCP establishes connections, sequences and acknowledges packets sent, and recovers packets lost during transmission.

In contrast to TCP, UDP provides a one-to-one or one-to-many, connectionless, unreliable communications service. UDP is used when the amount of data to be transferred is small (such as the data that would fit into a single packet), when an application developer does not want the overhead associated with TCP connections, or when the applications or upper-layer protocols provide reliable delivery.

TCP and UDP operate over both IPv4 and IPv6 Internet layers.

Note The Internet Protocol (TCP/IP) component of Windows contains separate versions of the TCP and UDP protocols than the Microsoft TCP/IP Version 6 component does. The versions in the Microsoft TCP/IP Version 6 component are functionally equivalent to those provided with the Microsoft Windows NT® 4.0 operating systems and contain all the most recent security updates. The existence of separate protocol components with their own versions of TCP and UDP is known as a dual stack architecture. The ideal architecture is known as a dual IP layer, in which the same versions of TCP and UDP operate over both IPv4 and IPv6 (as Figure 2-1 shows). Windows Vista has a dual IP layer architecture for the TCP/IP protocol components.

Application Layer

The Application layer allows applications to access the services of the other layers, and it defines the protocols that applications use to exchange data. The Application layer contains many protocols, and more are always being developed.

The most widely known Application layer protocols help users exchange information:

The Hypertext Transfer Protocol (HTTP) transfers files that make up pages on the World Wide Web.

The File Transfer Protocol (FTP) transfers individual files, typically for an interactive user session.

The Simple Mail Transfer Protocol (SMTP) transfers mail messages and attachments.

Additionally, the following Application layer protocols help you use and manage TCP/IP networks:

The Domain Name System (DNS) protocol resolves a host name, such as www.microsoft.com, to an IP address and copies name information between DNS servers.

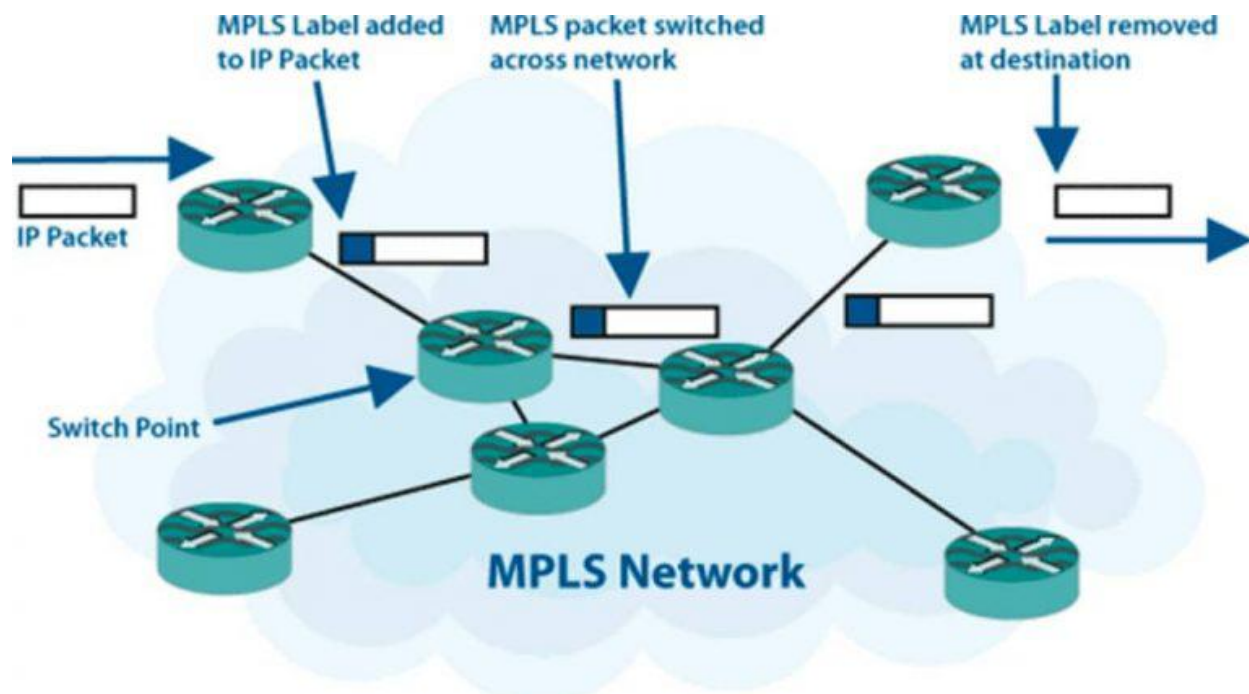
The Routing Information Protocol (RIP) is a protocol that routers use to exchange routing information on an IP network.

The Simple Network Management Protocol (SNMP) collects and exchanges network management information between a network management console and network devices such as routers, bridges, and servers.

Multiprotocol Label Switching (MPLS)

Multiprotocol label switching (MPLS) is a mechanism used within computer network infrastructures to speed up the time it takes a data packet to flow from one node to another. It enables computer networks to be faster and easier to manage by using short path labels instead of long network addresses for routing network packets.

MPLS primarily implements and uses labels for making routing decisions. The label-based switching mechanism enables the network packets to flow on any protocol. MPLS operates by assigning a unique label or identifier to each network packet. The label consists of the routing table information, such as the destination IP address, bandwidth and other factors as well as source IP and socket information. The router can refer only to the label to make the routing decision rather than looking into the packet. MPLS supports IP, Asynchronous Transfer Mode (ATM), frame relay, Synchronous Optical Networking (SONET) and Ethernet-based networks. MPLS is designed to be used on both packet-switched networks and circuit-switched networks.



IDS

Stands for "Intrusion Detection System." An IDS monitors network traffic for suspicious activity. It may be comprised of hardware, software, or a combination of the two. IDSes are similar to firewalls, but are designed to monitor traffic that has entered a network, rather than preventing access to a network entirely. This allows IDSes to detect attacks that originate from within a network.

An intruder detection systems can be configured for either a network or a specific device. A network intrusion detection system (NIDS) monitors inbound and outbound traffic, as well as data transfers between systems within a network. NIDSes are often spread out across several different points in a network to make sure there a no loopholes where traffic may be unmonitored.

An IDS configured for a single device is called a host intrusion detection system, or HIDS. It monitors a single host for abnormal traffic patterns. For example, it may look for known viruses or malware in both inbound and outbound traffic. Some HIDSes even check packets for important system files to make sure they are not modified or deleted.

Both network and host IDSes are designed to detect intrusions and sound an alert. This alert may be sent to a network administrator or may be processed by an automated system. A system that automatically handles intrusion alerts is called a reactive IDS or an intrusion prevention system (IPS).

Firewall

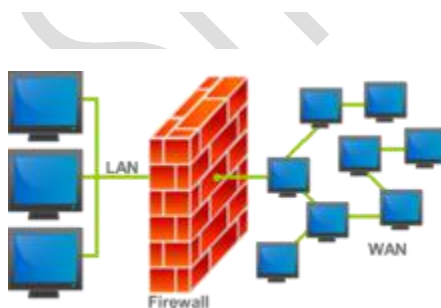
A firewall is software used to maintain the security of a private network. Firewalls block unauthorized access to or from private networks and are often employed to prevent unauthorized Web users or illicit software from gaining access to private networks connected to the Internet. A firewall may be implemented using hardware, software, or a combination of both.

A firewall is recognized as the first line of defense in securing sensitive information. For better safety, the data can be encrypted.

Firewalls generally use two or more of the following methods:

- Packet Filtering: Firewalls filter packets that attempt to enter or leave a network and either accept or reject them depending on the predefined set of filter rules.
- Application Gateway: The application gateway technique employs security methods applied to certain applications such as Telnet and File Transfer Protocol servers.

-



- Circuit-Level Gateway: A circuit-level gateway applies these methods when a connection such as Transmission Control Protocol is established and packets start to move.

- **Proxy Servers:** Proxy servers can mask real network addresses and intercept every message that enters or leaves a network.

Stateful Inspection or Dynamic Packet Filtering: This method compares not just the header information, but also a packet's most important inbound and outbound data parts.

Network Security Equipment - Firewalls, NIDS, HIDS, IPS

Firewalls:

A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices which is configured to permit or deny computer based application upon a set of rules and other criteria.

Firewalls can be implemented in either hardware or software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

There are different types of firewalls which serve nearly same purpose but for different audiences.

The two most common types are:

- 1) **Network level firewalls:** These are standalone boxes & are much more sophisticated with loads of features. To mention a few, SPI[Stateful Packet Inspection], Deep Packet Inspection, Logging Capabilities etc. They usually run on proprietary Operating system such as the Cisco series, they run on the Cisco IOS[Internetwork Operating System].

- 2) **Application level firewalls:** Software firewalls, application level proxies come under this category. Apart from the regular huff & puff they offer a few nifty features such as content filtering, blocking unwanted hosts.

Generally, firewalls are configured to protect against unauthenticated interactive logins from the outside world. This helps prevent [hackers](#) from logging into machines on your network. [More sophisticated firewalls](#) block traffic from the outside to the inside, but permit users on the inside to communicate a little more freely with the outside.

IDS (Network Intrusion Detection System) & HIDS (Host Intrusion Detection System):

An [intrusion detection system](#) (IDS) is designed to monitor all inbound and outbound network activity and identify any suspicious patterns that may indicate a [network](#) or [system](#) attack from someone attempting to break into or compromise a system. IDS is considered to be a passive-monitoring system, since the main function of an IDS product is to warn you of suspicious activity taking place – not prevent them. An IDS essentially reviews your network [traffic](#) and [data](#) and will identify probes, attacks, exploits and other vulnerabilities. IDSs can respond to the suspicious event in one of several ways, which includes displaying an alert, [logging](#) the event or even paging an administrator. In some cases the IDS may be prompted to reconfigure the network to reduce the effects of the suspicious intrusion.

An IDS specifically looks for suspicious activity and events that might be the result of a [virus](#), [worm](#) or [hacker](#). This is done by looking for known [intrusion signatures](#) or attack

signatures that characterize different worms or viruses and by tracking general variances which differ from regular system activity. The IDS is able to provide notification of only known attacks.

Network-based vs. Host-based IDS:

Intrusion detection systems are network or host based solutions. Network-based IDS systems ([NIDS](#)) are often standalone hardware appliances that include network intrusion detection capabilities. It will usually consist of hardware sensors located at various points along the network or software that is installed to system computers connected to your network, which analyzes data packets entering and leaving the network.

Host-based IDS systems (HIDS) do not offer true real-time detection, but if configured correctly are close to true real-time. Host-based IDS systems consist of software agents installed on individual computers within the system. HIDS analyze the traffic to and from the specific computer on which the intrusion detection software is installed on. HIDS systems often provide features you can't get with network-based IDS. For example, HIDS are able to monitor activities that only an [administrator](#) should be able to implement. It is also able to monitor changes to key system [files](#) and any attempt to overwrite these files. Attempts to install [Trojans](#) or [backdoors](#) can also be monitored by a HIDS and stopped. These specific intrusion events are not always seen by a NIDS.

While it depends on the size of the network and the number of individual computers which require intrusion detection system, NIDS are usually a cheaper solution to implement and it requires less administration and training – but it is not as versatile as a HID.

IPS (Intrusion Prevention System):

IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) both increase the security level of networks, monitoring traffic and inspecting and scanning packets for suspicious data. Detection in both systems is mainly based on signatures already detected and recognized.

The main difference between one system and the other is the action they take when an attack is detected in its initial phases (network scanning and port scanning).

- a) The Intrusion Detection System (IDS) provides the network with a level of detective and alertive security against any suspicious activity. The IDS achieves this objective

through early warnings aimed at systems administrators. However, unlike IPS, it is not designed to block attacks.

- b) An Intrusion Prevention System (IPS) is a device that controls access to IT networks in order to protect systems from attack and abuse. It is designed to inspect attack data and take the corresponding action, blocking it as it is developing and before it succeeds.

While many in the security industry believe IPS is the way of the future and that IPS will take over IDS, it is somewhat of an apples and oranges comparison. The two solutions are different in that one is a passive detection monitoring system and the other is an active prevention system.

False Positive and Negatives:

The term [false positive](#) itself refers to security systems incorrectly seeing legitimate requests as spam or security breaches. Basically, the IDS will detect something it is not supposed to. Alternatively, IDS is prone to false negatives where the system fails to detect something it should. Both of these problems are associated with IDS and even IPS, It is a topic worth consideration when looking at different IDS solutions.

Pre-implementation configuration of an IDS or IPS plays a great role in reducing false positives/false negatives to negligible levels.

Emerging Trends in VSAT Technology

Advances in technology have dramatically improved the price–performance ratio of fixed satellite service (FSS) over the past five years. New VSAT systems are coming online using Ka band technology that promise higher data rates for lower costs.

FSS systems currently in orbit have a huge capacity with a relatively low price structure. FSS systems provide various applications for subscribers, including: telephony, fax, television, high-speed data communication services, Internet access, satellite news gathering (SNG), Digital Audio Broadcasting (DAB) and others. These systems provide high-quality service because they create efficient communication systems for both residential and business users. Modern VSAT systems are a prime example of convergence, and hence require skills from both the RF (Radio Frequency) and IP (Internet Protocol) domains.

MPLS

What is a computer networking protocol?

The term 'protocol' is used extensively in computer networking language. Also for understanding the concept of MPLS, we need to have a fair idea about what a 'protocol' means.

In simple terms, protocols are a set of rules that govern a computer network. Protocols enable communication between two devices or even two different networks. A protocol is a kind of communication that is universally accepted to be used within a framework of pre-defined set of rules.

Network protocols are formal standards and policies comprised of rules, procedures and formats that define communication between two or more devices over a network. Network protocols govern the end-to-end processes of timely, secure and managed data or network communication.

There are several broad types of networking protocols, including:

- a) Network communication protocols: These are basic data communication protocols such as TCP/IP and HTTP;
- b) Network security protocols: Implement security over network communications and include HTTPS, SSL and SFTP and ;
- c) Network management protocols: Provide network governance and maintenance and include SNMP and ICMP.

Now coming back to MPLS, Multiprotocol Label Switching (MPLS) is a type of data-carrying technique for high-performance telecommunications networks that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table.

The most prominent advantage of MPLS cloud technology is its better **resilience** with respect to the erstwhile point-to-point (P2P) leased line connectivity. Mainly for this reason, most of the Banks and other major financial institutions in India have switched to MPLS cloud technology for connecting their domestic as well as overseas establishments as of date.

India Post, which is a mammoth organization with respect to its widely distributed outlets across the country, is now transforming them to service centers while retaining the post and logistics. They plan to foray into Banking, Insurance & enabler for E-governance. They are now partnering with Sify for their backbone MPLS networking

VLAN (Virtual LAN)

Computer networks can be segmented into local area networks (LAN) and wide area networks (WAN). Network devices such as switches, hubs, bridges, workstations and servers connected to each other in the same network at a specific location are generally known as LANs. An LAN is also considered a broadcast domain.

A VLAN (virtual LAN) as the name indicates, allows several networks to work virtually as one LAN. One of the most beneficial elements of a VLAN is that it removes latency (reduction in speed) in the network, which saves network resources and increases network efficiency. In addition, VLANs are created to provide segmentation and assist in issues like security, network management and scalability. Traffic patterns can also easily be controlled by using VLANs. VLANs can quickly adapt to change in network requirements and relocation of workstations and server nodes.

Key benefits of implementing VLANs include:

- Allowing network administrators to apply additional security to network communication

- Making expansion and relocation of a network or a network device easier

- Providing flexibility because administrators are able to configure in a centralized environment while the devices might be located in different geographical locations

- Decreasing the latency and traffic load on the network and the network devices, offering increased performance

VLANs also have some disadvantages and limitations as listed below:

High risk of virus issues because one infected system may spread a virus through the whole logical network

More effective at controlling latency than a WAN but less efficient than a LAN

Wireless Networks

A wireless local-area network (LAN) uses radio waves to connect devices such as laptops to the Internet and to the business network and its applications. When one connects a laptop to a WiFi hotspot at a cafe, hotel, airport lounge, or other public place, one is connecting to that business's wireless network. On the contrary, a wired network connects devices to the Internet or other network using cables.

In the past, some believed wired networks were faster and more secure than wireless networks. But continual enhancements to wireless networking standards and technologies have eroded those speed and security differences.

Many network routers today act as wireless networking access points. They let anyone connect multiple computers to a single wireless network. And they connect the local network to the Internet.

One can extend wireless networking throughout one's office, store, or campus by placing additional wireless access points in various locations. The additional access points extend the wireless signal's range and strength over a wider geographical area, so that it's available in more places, such as conference rooms.

The signal generated from each wireless access point or router extends up to approximately 300 feet. Walls, metal (such as in elevator shafts) and floors can negatively affect range. And the wireless signal's strength weakens the longer it has to travel. For best results, we need to space out the access points and position them in central areas. Access points can provide stronger signals when installed on or near ceilings.

For best results, better not share any single wireless access point with more than 20 users. Typically, the more users sharing an access point, the slower the wireless network can become. If the business network supports a voice over Internet Protocol (VoIP) or Unified Communications system, we need to limit each access point to 8-12 users. This will prevent potential degradation in voice quality.

Security is vital to wireless networking. Some security methods to consider for the network include:

Data encryption, so only authorized users can access information over the wireless network

User authentication, which identifies computers trying to access the network

Secure access for visitors and guests

Control systems, which protect the laptops and other devices that use the network.

A **radio frequency (RF)** signal refers to a wireless electromagnetic signal used as a form of communication, if one is discussing wireless electronics. Radio waves are a form of electromagnetic radiation with identified radio frequencies that range from 3Hz to 300 GHz.

Apart from RF, **wireless 3G** connectivity under GSM technology is also being actively considered by many organizations for their network designs owing their low cost and questionably higher reliability. Security is one of the most important considerations in these solutions of wireless connectivity, which needs to be addressed, mostly by way of strong encryption of data under transmission, before implementation.

IPv6 addresses

The rapid exhaustion of IPv4 address space prompted the [Internet Engineering Task Force](#) (IETF) to explore new technologies to expand the addressing capability in the Internet. The permanent solution was deemed to be a redesign of the Internet Protocol itself. This new generation of the Internet Protocol was eventually named [Internet Protocol Version 6](#) (IPv6) in 1995. The address size was increased from 32 to 128 [bits](#) (16 [octets](#)), thus providing up to 2^{128} (approximately 3.403×10^{38}) addresses. This is deemed sufficient for the foreseeable future.

The intent of the new design was not to provide just a sufficient quantity of addresses, but also redesign routing in the Internet by more efficient aggregation of subnetwork routing prefixes. This resulted in slower growth of routing tables in routers. The smallest possible individual allocation is a subnet for 264 hosts, which is the square of the size of the entire IPv4 Internet. The following table depicts the major differences between IPv4 and IPv6 addressing schemes.

IPv4	IPv6
The size of an address in IPv4 is 32 bits	The size of an address in IPv6 is 128 bits
Address Shortages: IPv4 supports 4.3×10^9 (4.3 billion) addresses, which is inadequate to give one (or more if they possess more than one device) to every living person.	Larger address space: <u>IPv6 supports 3.4×10^{38} addresses, or 5×10^{28} (50 octillion) for each of the roughly 6.5 billion people alive today.^{33(*)}</u>
IPv4 header has 20 bytes	IPv6 header is the double, it has 40 bytes
IPv4 header has many fields (13 fields)	IPv6 header has fewer fields, it has 8 fields.
IPv4 is subdivided into classes <A-E>.	IPv6 is classless. IPv6 uses a prefix and an Identifier ID

	known as IPv4 network
IPv4 address uses a subnet mask.	IPv6 uses a prefix length.
IPv4 has no built-in security. Encryption and authentication are optional	IPv6 has a built-in strong security - Encryption - Authentication
ISP have IPv4 connectivity or have both IPv4 and IPv6 Non equal geographical distribution (>50% USA)	Many ISP don't have IPv6 connectivity No geographic limitation

The large number of IPv6 addresses allows large blocks to be assigned for specific purposes and, where appropriate, to be aggregated for efficient routing. With a large address space, there is no need to have complex address conservation methods as used in CIDR.

All modern desktop and enterprise server operating systems include native support for the IPv6 protocol, but it is not yet widely deployed in other devices, such as residential networking routers, [voice over IP](#) (VoIP) and multimedia equipment, and network peripherals.

Bitcoin Crypto-currency & Block-chain Technology

Now, most people have heard about [Bitcoin](#), the cryptocurrency. The technology behind Bitcoin and what makes it so potentially disruptive at so many levels is called [block-chain](#), or also a distributed ledger.

Block-chain, thus; is essentially a distributed database. Many of the Banks, nationally and internationally, have started taking steps towards adopting block-chain technology for their cross-border payment systems, to start with.

Today, there are several banks pursuing individual block-chain strategies. These individual initiatives will be meaningful when they are used by all the banks. For instance, a payment system such as NEFT cannot be successful if it is adopted by only one bank. Block-chain, the technology behind cyber currency Bitcoin, follows the concept of a centralized registry that can be accessed by all members, and every event is registered as an unalterable 'block'. Being the largest bank in India, SBI has taken the lead in initiating block-chain. Other banks in the country are following suit gradually.

All the subsequent events related to the loan can be put on the “block” so that members can take informed decisions. Another business where block-chain can be used as a tool is in trade finance where there's a risk of fraud with the merchant going to multiple banks with the same invoice to get the bill discounted. If documents are put on the block-chain, everyone will know which invoices have been discounted by Bank X and this could prevent multiple discounting frauds.

SOME CONCEPTS

BLOCKCHAIN: It is a code—a digital ledger software code. A ledger is a collection of financial transactions which records the exchange between parties. It shows what comes in and to whom and what goes out and to whom. Blockchain collects all this information in digital form. It is a decentralised system that can be created and updated anywhere. As the name suggest, every block of data is connected to another block in a chain format. Blockchain doesn't mean digitisation of a physical ledger, but it is another way to record a ledger.

Blockchain is the technology underlying the use of bitcoins. It is an architecture on which you can build applications for different needs.

At present, for any transaction, a reconciliation is required to ensure that the transaction is genuine. Blockchain built applications don't need reconciliation of any transactions because all information will be readily available and verified for anyone to see if he is part of a particular blockchain ecosystem. Across the world, telecom companies, financial institutions, information technology companies and startups are testing how to use blockchain in various sectors. In the banking sector, banks and IT companies are exploring ways to use blockchain in payments, remittance and security. There are companies that are trying to build applications on top of blockchain for other sectors as well such as property, precious metals and airlines.

BITCOIN : Bitcoin is digital currency which was founded in 2008. It is designed for secure financial transactions that require no central authority, no banks and no government regulators. Bitcoin would let transacting parties remain anonymous, keep transactions very secure, and eliminate middlemen fees. What does it hope to achieve? What drove its initial development was its purely digital existence, away from the control of government regulators. The values of other currencies can rise and fall when a central bank decides to print more paper money. But since Bitcoin is digital and there is a limited number of them, the expectation is that it won't be prone to such devaluation.

How safe is Bitcoin? Speculators and money launderers have already found much to like about the anonymous digital currency, and that has forced the government to play catch-up. While Bitcoin users need a secret, numerical key to unlock their accounts, the anonymity of the system is vulnerable when the virtual currency is exchanged for dollars. Speculators have hoarded Bitcoin just because there is a limited number of them. And when banks around the world decided to shun the currency, its value took a tumble. The people and businesses that make transactions using Bitcoin, therefore, have dealt with their share of disruption.

What is the controversy surrounding this currency? Since the founding of the cryptocurrency, Bitcoin's inventor or inventors have been shrouded in mystery. It is believed that it was first introduced by a Japanese programmer who went by the name of Satoshi Nakamoto. On May 2, 2016, Australian tech entrepreneur Craig Wright claimed that he was the founder of the virtual currency, ending years of mystery. As Bitcoins require no central authority, banks, or government regulators they become attractive to off-the-grid activities, those who want to evade tax authorities, and criminals. Hence governments and central banks have been vocal about the risks involved in dealing with virtual currencies.

BITCOIN:

Latest development : Mr.Craig Steven Wright, an Australian entrepreneur and self-declared cyber security expert, revealed his identity as Satoshi Nakamoto, the inventor of Bitcoin alternative currency and blockchain technology. Though it is not clear if his claim is indeed true, the story has shifted at cyberspeed from bitcoins to blockchain technology.

How has Bitcoin evolved in India? In April this year, an IT company in Mysuru became the target of a 'denial-of-service' attack, the attackers demanded Bitcoins in return for sharing the key to restore the company's computer systems. India's biggest Bitcoin trading platform, BuySellBitCo.in, recently suspended its operations, citing a recent Reserve Bank of India public advisory that highlighted the risks involved in dealing with virtual currencies. Bitcoin and other virtual currencies have begun to gain widespread acceptance in India, despite poor Internet penetration and a natural scepticism of assets not backed by tangible entities such as land. The central bank had issued a notice on the risks involved and added that it could be used for money laundering and funding terrorism activities. It stopped short, however, of issuing a ban or any other restrictions.

CRYPTO – CURRENCY: Crypto currency is a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.

CLOUD COMPUTING is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. Cloud computing is comparable to grid computing, a type of computing where unused processing cycles of all computers in a network are harnesses to solve problems too intensive for any stand-alone machine.

In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for "the internet," so the phrase cloud computing means " a type of Internet-based computing," where different services – such as servers, storage and applications – are delivered to an organization's computers and devices through the internet.

The goal of cloud computing is to apply traditional super computing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive online computer games.

To do this cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

CRYPTOGRAPHY:

Public key cryptography or asymmetric cryptography, is any cryptographic system that uses two kinds of keys. Public keys may be disseminated widely, while private keys are known to the owner only.

In public key encryption system, any person can encrypt a message using the public key (better imagined as a lock) of the receiver and leave it on a public server or transmit it on a public network. Such a message can be decrypted only with the receiver's private key.

Public key infrastructure (PKI) is a set of roles, policies and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.

A Typical PKI consists of hardware, software, policies and standards to manage the creation, administration, distribution and revocation of keys and digital certificates are the heart of PKI, as they affirm the identity of the certificate subject and bind that identity to the public key contained in the certificate.

RSA – Relatively slow algorithm is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called PKC, because one of the keys can be given to everyone.

A typical PKI includes the following elements.

A trusted party, called a certificate authority (CA), acts as root of the trust and provides services that authenticate the identity of individuals, computers and other entities. CA issues the digital certificates to individuals and entities. It signs these certificates using its private keys. Its public key is made available to all interested parties.

A registration authority (RA) often called a subordinate CA, certified by a root of CA to issue certificates for specific uses permitted by the root.

A Certificate database which stores certificate requests and issues and revokes certificates.

A certificate store, which resides on a local computer as a place to store issued certificates and private keys.

Digital signature (not to be confused with the digital certificate) are the public key primitives of message authentication. In the physical world, it is common to use handwritten signature on handwritten or printed message. They are used to bind the signatory to the message. Similarly, a digital signature is a technique that binds a person/entity to the digital data.

It is also a mathematical technique used to validate the authenticity and integrity of a message, software or digital document.

Digital certificates are a means by which consumers and business can utilize the security application of PKI. PKI comprises of the technology to enable secure e-commerce and internet based communication. It is also referred to as public key certificate.

Introduction to Information systems

Information System (IS) :

An information system can be defined as a set of interrelated components that collect (or retrieve), process, store, and distribute information to support decision making and control in an organization. In addition to supporting decision making, coordination, and control, information systems may also help managers and workers analyse problems, visualize complex subjects, and create new products.

Components of Information System:

- (1) People Resource: People are considered part of the system because without them, systems would not operate correctly. In Information system there are two kinds of people resource –
 - (i) End User: also called users or clients, are people who actually use the information system or its products. Eg. Customers, salesperson, engineers, clerks, managers
 - (ii) IS Specialist: also called IS developers, are people who develop the information system and its components. Eg. System Analysts (who design IS based on requirements of end users), Software developers (create computer programs based on specifications of analysts), System Operator (who help monitor and operate large computer system and networks) and

other Managerial, Technical, Clerical IS personnel.

(2) Hardware Resource: All physical and tangible devices or material used in information processing. e.g.

(i) Computer Systems: It consists of the central processing units and interconnect peripheral devices. Eg. Handheld devices, laptops, desktops, large mainframes computers

(ii) Computer Peripherals: input and output devices such as keyboard, mouse, printer, monitor, disk drive, etc.

(3) Software Resource: It includes set of operating instructions called programs, which direct and control computer hardware and set of information processing instructions called procedures that people need.

Hardware resources need programs and procedures in order to properly collect, process and disseminate information to their users.

Examples:

(i) System Software: such as an operating system. It controls and supports the operations of a computer system.

(ii) Application Software: which are programs that directly processing for a particular use of computers by end users. e.g. Sales analysis programs, a payroll program, a word program, etc.

(iii) Procedures: Instructions for people who will use the IS. Eg. instructions for filling out a paper form.

(4) Data Resource: Data resources include data (which is raw material of information systems) and database. Data can take many forms, including traditional alphanumeric data, composed of numbers and alphabetical and other characters that describe business transactions and other events and entities. Text data, consisting of sentences and paragraphs used in written communications; image data, such as graphic shapes and figures; and audio data, the human voice and other sounds, are also important forms of data.

Data resources must meet the following criteria:

Comprehensiveness: It means that all the data about the subject are actually present in the database.

Non-redundancy: It means that each individual piece of data exists only once in the database.

Appropriate structure: It means that the data are stored in such a way as to minimize the cost of expected processing and storage.

The data resources of IS are typically organized into:

Processed and organized data – Databases

Knowledge in a variety of forms such as facts, rules, and case examples about successful business practices

(5) Network Resources: Telecommunications networks like the Internet, intranets, and extranets have become essential to the successful operations of all types of organizations and their computer-based information systems. Telecommunications networks consist of computers, communications processors, and other devices interconnected by communications media and controlled by communications software. The concept of Network Resources emphasizes that communications networks are a fundamental resource component of all information systems.

Network resources include:

Communications media: such as twisted pair wire, coaxial cable, fiberoptic cable, microwave systems, and communication satellite systems.

Network support/infrastructure: This generic category includes all of the people, hardware, software, and data resources that directly support the operation and use of a communications network. Examples include communications control software such as network operating systems and Internet packages.

Types of Information System:

(1) Management Support System – When Information Systems's focus on providing information and support for effective decision making by managers it is called a Management Support System.

Types of Management Support System:-

(i) Management Information System (MIS): It provides information in form of reports and displays to managers and other business professionals.

Example, Sales Manager may use this computer to instantaneously display

sales result of their product and access their corporate intranet for daily sales analysis report that evaluate sales made by each sales person.

(ii) Decision Support System (DSS): It gives direct support to managers during decision making process. It tests alternative solutions and selects the better option. Example, A product manager may use DSS to decide how much product to manufacture based on expected sales associated with future promotion and availability of raw material.

Uses: Logistics, Financial Planning, Group decision support

(iii) Executive Information System (EIS): It provides critical information from wide variety of internal and external sources in easy-to-use form to executives and managers. They measure Critical Success Indicators (CSI)

and Key Performance Indicators (KPI) associated with the problem to provide valuable information.

(2) Operations Support System – The Role of OSS is to efficiently process business transactions, control industrial processes, support enterprise communications and collaborations, and updates corporate databases.

Types of Operational Support System:-

(i) Transaction Processing System: It records and process data resulting from business transactions. It processes transactions in two ways –

a.) Batch Processing – transactions are accumulated over a period of time and processed periodically.

b.) Real Time – transaction is processed immediately after a transaction occurs.

Uses: Sales software at many retail stores, Order Processing, Payroll Management etc.

(ii) Process Control System: It monitors and controls physical processes.

It tells the user about change in variables related to a process for effective performance evaluation and decision making. Example, petroleum refinery uses electronic sensors linked to computers to continuously monitor and control chemical processes.

Uses: Sensors, Auto-inventory reorder

(iii) Enterprise Collaboration System: These help to enhance team and workgroup communications and productivity in an organization. It includes applications that are sometimes called office automation systems.

Example, video conference of a product design team (virtual team).

Uses: Communicating ideas, Share resources and Coordinate corporate work efforts

Tiers of Redundancy of a Data centre

A single point of failure (SPOF) is a part of a system that, if it fails, will stop the entire system from working. Some examples of SPOFs are database and application servers, network, power and storage systems. SPOFs are undesirable and redundancy needs to be maintained for all SPOFs in a DC. A Tier III data center is concurrently maintainable, allowing for any planned maintenance activity of power and cooling systems to take place without disrupting the operation of computer hardware located in the data center. In terms of redundancy, Tier III offers [N+1 availability](#). Any unplanned activity such as operational errors or spontaneous failures of infrastructure components can still cause an outage. In other words, Tier III isn't completely fault tolerant. A Tier 4 data center is fault-tolerant, allowing for the occurrence of any unplanned activity while still maintaining operations. Tier 4 facilities have no single points of failure. Because of heavy cost constraints, most of the banks in India have adopted Tier III level redundancy. As the criticality has been increasing on account of 24x7 banking services being extended, the Indian banks have gradually started moving towards Tier-IV Data Centres.

Disaster Recovery Site (DRS) for Data Centre

As the entire data of a bank resides at one place, viz. the Data Centre (DC), there is a concentration risk. In the event of something happening at the DC, or it getting isolated, the entire working of a bank will

come to a stand-still. Therefore, another similar DC called the Disaster Recovery site (DR site) is setup in different seismic zone. The branches are linked to both DC & DR through a web of communication lines. Redundancy is provided at every stage in the form of a dial-up ISDN lines as a backup for a leased lines, the city Network Aggregation Point (NAP) being connected to both DC & DR. The idea is to ensure that in the event of failure of one; the other can take over, thus ensuring continuity of business and services.

While designing DCs for banks, redundancy needs to be maintained for all SPOFs (single point of failures) in a Data Centre. Even a replica of DC, which is called DRS (disaster recovery site) is established in a different seismic zone for business continuity purposes in case of any eventuality.

Acquisition projects

Acquisition projects are similar to development projects because management approves project requests, defines functional, security, and system requirements, and appropriately tests and implements products. Organizations often employ structured acquisition methodologies similar to the SDLC when acquiring significant hardware and software products. However, organizations replace the SDLC design and development phases with a bid solicitation process that involves developing detailed lists of functional, security, and system requirements and distributing them to third parties.

Acquisition standards should also ensure managers complete appropriate vendor, contract, and licensing reviews and acquire products compatible with existing systems. Key tools in managing acquisition projects include invitations-to-tender and request-for-proposals. Invitations-to-tender involve soliciting bids from vendors when acquiring hardware or integrated systems of hardware and software. Request-for-proposals involve soliciting bids when acquiring off-the-shelf or third-party developed software. However, the terms are sometimes used interchangeably.

The risks associated with using general business purpose, off-the-shelf software, such as a word processing application, are typically lower than those associated with using financial applications. Therefore, the acquisition of general business purpose, off-the-shelf software typically requires less stringent evaluation procedures than acquiring hardware or software specifically designed for financial purposes.

CASE Tools & SDLC

Computer-aided software engineering (CASE) is the domain of software tools used to design and implement applications. CASE tools are similar to and were partly inspired by computer-aided design (CAD) tools used for designing hardware products. The scope of CASE and CASE tools goes throughout SDLC. We shall discuss various types of CASE tools as follows.

CASE Tools

CASE tools are set of software application programs, which are used to automate SDLC activities. CASE tools are used by software project managers, analysts and engineers to develop software system. There are number of CASE tools available to simplify various stages of Software Development Life Cycle such as Analysis tools, Design tools, Project management tools, Database Management tools, Documentation tools are to name a few. Use of CASE tools accelerates the development of project to produce desired result and helps to uncover flaws before moving ahead with next stage in software development.

Components of CASE Tools

CASE tools can be broadly divided into the following parts based on their use at a particular SDLC stage:

Central Repository - CASE tools require a central repository, which can serve as a source of common, integrated and consistent information. Central repository is a central place of storage where product

specifications, requirement documents, related reports and diagrams, other useful information regarding management is stored. Central repository also serves as data dictionary.

1. Upper Case Tools - Upper CASE tools are used in planning, analysis and design stages of SDLC.
2. Lower Case Tools - Lower CASE tools are used in implementation, testing and maintenance.
3. Integrated Case Tools - Integrated CASE tools are helpful in all the stages of SDLC, from Requirement gathering to Testing and documentation.

CASE tools can be grouped together if they have similar functionality, process activities and capability of getting integrated with other tools.

We now briefly go through various CASE tools and their applications:

Diagram tools - These tools are used to represent system components, data and control flow among various software components and system structure in a graphical form. For example, Flow Chart Maker tool for creating state-of-the-art flowcharts.

Process Modeling Tools - Process modeling is method to create software process model, which is used to develop the software. Process modeling tools help the managers to choose a process model or modify it as per the requirement of software product. For example, EPF Composer

Project Management Tools - These tools are used for project planning, cost and effort estimation, project scheduling and resource planning. Managers have to strictly comply project execution with every mentioned step in software project management. Project management tools help in storing and sharing project information in real-time throughout the organization. For example, Creative Pro Office, Trac Project, Basecamp.

Documentation Tools - Documentation in a software project starts prior to the software process, goes throughout all phases of SDLC and after the completion of the project. Documentation tools generate documents for technical users and end users. Technical users are mostly in-house professionals of the development team who refer to system manual, reference manual, training manual, installation manuals etc. The end user documents describe the functioning and how-to of the system such as user manual. For example, Doxygen, DrExplain, Adobe RoboHelp for documentation.

Analysis Tools - These tools help to gather requirements, automatically check for any inconsistency, inaccuracy in the diagrams, data redundancies or erroneous omissions. For example, Accept 360, Accompa, CaseComplete for requirement analysis, Visible Analyst for total analysis.

Design Tools - These tools help software designers to design the block structure of the software, which may further be broken down in smaller modules using refinement techniques. These tools provides detailing of each module and interconnections among modules. For example, Animated Software Design

Configuration Management Tools - An instance of software is released under one version. Configuration Management tools deal with –

1. Version and revision management
2. Baseline configuration management
3. Change control management

CASE tools help in this by automatic tracking, version management and release management. For example, Fossil, Git, Accu REV.

Change Control Tools - These tools are considered as a part of configuration management tools. They deal with changes made to the software after its baseline is fixed or when the software is first released.

CASE tools automate change tracking, file management, code management and more. It also helps in enforcing change policy of the organization.

Programming Tools - These tools consist of programming environments like IDE (Integrated Development Environment), in-built modules library and simulation tools. These tools provide comprehensive aid in building software product and include features for simulation and testing. For example, Cscope to search code in C, Eclipse.

Prototyping Tools - Software prototype is simulated version of the intended software product.

Prototype provides initial look and feel of the product and simulates few aspect of actual product.

Prototyping CASE tools essentially come with graphical libraries. They can create hardware independent user interfaces and design. These tools help us to build rapid prototypes based on existing information. In addition, they provide simulation of software prototype. For example, Serena prototype composer, Mockup Builder.

Web Development Tools - These tools assist in designing web pages with all allied elements like forms, text, and script, graphic and so on. Web tools also provide live preview of what is being developed and how will it look after completion. For example, Fontello, Adobe Edge Inspect, Foundation 3, Brackets.

Quality Assurance Tools - Quality assurance in a software organization is monitoring the engineering process and methods adopted to develop the software product in order to ensure conformance of quality as per organization standards. QA tools consist of configuration and change control tools and software testing tools. For example, SoapTest, AppsWatch, JMeter.

Maintenance Tools - Software maintenance includes modifications in the software product after it is delivered. Automatic logging and error reporting techniques, automatic error ticket generation and root

cause Analysis are few CASE tools, which help software organization in maintenance phase of SDLC. For example, Bugzilla for defect tracking, HP Quality Center.

Database management system (DBMS)

A database management system (DBMS) is system software for creating and managing databases. The DBMS provides users and programmers with a systematic way to create, retrieve, update and manage data.

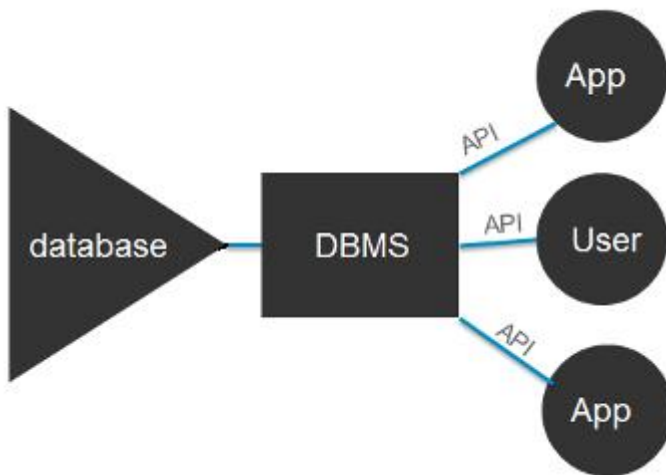
A DBMS makes it possible for end users to create, read, update and delete data in a database. The DBMS essentially serves as an interface between the database and end users or application programs, ensuring that data is consistently organized and remains easily accessible.

The DBMS manages three important things: the data, the database engine that allows data to be accessed, locked and modified -- and the database schema, which defines the database's logical structure. These three foundational elements help provide concurrency, security, data integrity and uniform administration procedures. Typical database administration tasks supported by the DBMS include change management, performance monitoring/tuning and backup and recovery. Many database management systems are also responsible for automated rollbacks, restarts and recovery as well as the logging and auditing of activity.

The DBMS is perhaps most useful for providing a centralized view of data that can be accessed by multiple users, from multiple locations, in a controlled manner. A DBMS can limit what data the end user sees, as well as how that end user can view the data, providing many views of a single database schema. End users and software programs are free from having to understand where the data is physically located or on what type of storage media it resides because the DBMS handles all requests.

The DBMS can offer both logical and physical data independence. That means it can protect users and applications from needing to know where data is stored or having to be concerned about changes to the physical structure of data (storage and hardware). As long as programs use the application programming interface (API) for the database that is provided by the DBMS, developers won't have to modify programs just because changes have been made to the database.

With relational DBMSs (RDBMSs), this API is SQL, a standard programming language for defining, protecting and accessing data in a RDBMS.



Popular types of DBMSes

Popular database models and their management systems include:

Relational database management system (RDMS) - adaptable to most use cases, but RDBMS Tier-1 products can be quite expensive.

NoSQL DBMS - well-suited for loosely defined data structures that may evolve over time.

In-memory database management system (IMDBMS) - provides faster response times and better performance.

Columnar database management system (CDBMS) - well-suited for data warehouses that have a large number of similar data items.

Cloud-based data management system - the cloud service provider is responsible for providing and maintaining the DBMS.

Advantages of a DBMS

Using a DBMS to store and manage data comes with advantages, but also overhead. One of the biggest advantages of using a DBMS is that it lets end users and application programmers access and use the same data while managing data integrity. Data is better protected and maintained when it can be shared using a DBMS instead of creating new iterations of the same data stored in new files for every new application. The DBMS provides a central store of data that can be accessed by multiple users in a controlled manner.

Central storage and management of data within the DBMS provides:

- Data abstraction and independence
- Data security
- A locking mechanism for concurrent access
- An efficient handler to balance the needs of multiple applications using the same data
- The ability to swiftly recover from crashes and errors, including restartability and recoverability
- Robust data integrity capabilities
- Logging and auditing of activity
- Simple access using a standard application programming interface (API)
- Uniform administration procedures for data

Another advantage of a DBMS is that it can be used to impose a logical, structured organization on the data. A DBMS delivers economy of scale for processing large amounts of data because it is optimized for such operations.

A DBMS can also provide many views of a single database schema. A view defines what data the user sees and how that user sees the data. The DBMS provides a level of abstraction between the conceptual schema that defines the logical structure of the database and the physical schema that describes the files,

indexes and other physical mechanisms used by the database. When a DBMS is used, systems can be modified much more easily when business requirements change. New categories of data can be added to the database without disrupting the existing system and applications can be insulated from how data is structured and stored.

Of course, a DBMS must perform additional work to provide these advantages, thereby bringing with it the overhead. A DBMS will use more memory and CPU than a simple file storage system. And, of course, different types of DBMSes will require different types and levels of system resources.

RDBMS (Relational database management system)

A relational database management system (RDBMS) is a collection of programs and capabilities that enable IT teams and others to create, update, administer and otherwise interact with a relational database. Most commercial RDBMSes use Structured Query Language (SQL) to access the database, although SQL was invented after the initial development of the relational model and is not necessary for its use.

RDBMS vs. DBMS

In general, databases store sets of data that can be queried for use in other applications. A database management system supports the development, administration and use of database platforms.

An RDBMS is a type of DBMS with a row-based table structure that connects related data elements and includes functions that maintain the security, accuracy, integrity and consistency of the data.

Functions of relational database management systems

Elements of the relational database management system that overarch the basic relational database are so intrinsic to operations that it is hard to dissociate the two in practice.

The most basic RDBMS functions are related to create, read, update and delete operations, collectively known as CRUD. They form the foundation of a well-organized system that promotes consistent treatment of data.

The RDBMS typically provides data dictionaries and metadata collections useful in data handling. These programmatically support well-defined data structures and relationships. Data storage management is a common capability of the RDBMS, and this has come to be defined by data objects that range from binary large object (blob) strings to stored procedures. Data objects like this extend the scope of basic relational database operations and can be handled in a variety of ways in different RDBMSes.

The most common means of data access for the RDBMS is via SQL. Its main language components comprise data manipulation language (DML) and data definition language (DDL) statements. Extensions are available for development efforts that pair SQL use with common programming languages, such as COBOL (Common Business-Oriented Language), Java and .NET.

RDBMSes use complex algorithms that support multiple concurrent user access to the database, while maintaining data integrity. Security management, which enforces policy-based access, is yet another overlay service that the RDBMS provides for the basic database as it is used in enterprise settings.

RDBMSes support the work of database administrators (DBAs) who must manage and monitor database activity. Utilities help automate data loading and database backup. RDBMSes manage log files that track system performance based on selected operational parameters. This enables measurement of database usage, capacity and performance, particularly query performance. RDBMSes provide graphical interfaces that help DBAs visualize database activity.

While not limited solely to the RDBMS, ACID compliance is an attribute of relational technology that has proved important in enterprise computing. Standing for *atomicity, consistency, isolation* and *durability*, these capabilities have particularly suited RDBMSes for handling business transactions.

Relational database management systems are central to key applications, such as banking ledgers, travel reservation systems and online retailing. As RDBMSes have matured, they have achieved increasingly

higher levels of query optimization, and they have become key parts of reporting, analytics and data warehousing applications for businesses as well. RDBMSes are intrinsic to operations of a variety of enterprise applications and are at the center of most master data management (MDM) systems.



Data warehouse

A data warehouse is a federated repository for all the data that an enterprise's various business systems collect. The repository may be physical or logical.

Data warehousing emphasizes the capture of data from diverse sources for useful analysis and access, but does not generally start from the point-of-view of the end user who may need access to specialized, sometimes local databases. The latter idea is known as the data mart.

There are two approaches to data warehousing, top down and bottom up. The top down approach spins off data marts for specific groups of users after the complete data warehouse has been created. The bottom up approach builds the data marts first and then combines them into a single, all-encompassing data warehouse.

Typically, a data warehouse is housed on an enterprise mainframe server or increasingly, in the cloud. Data from various online transaction processing (OLTP) applications and other sources is selectively extracted for use by analytical applications and user queries.

The term data warehouse was coined by William H. Inmon, who is known as the Father of Data Warehousing. Inmon described a data warehouse as being a subject-oriented, integrated, time-variant and nonvolatile collection of data that supports management's decision-making process.

Characteristics of Data warehouse

A data warehouse has following characteristics:

- Subject-Oriented
- Integrated
- Time-variant
- Non-volatile

Subject-Oriented

A data warehouse is subject oriented as it offers information regarding a theme instead of companies' ongoing operations. These subjects can be sales, marketing, distributions, etc.

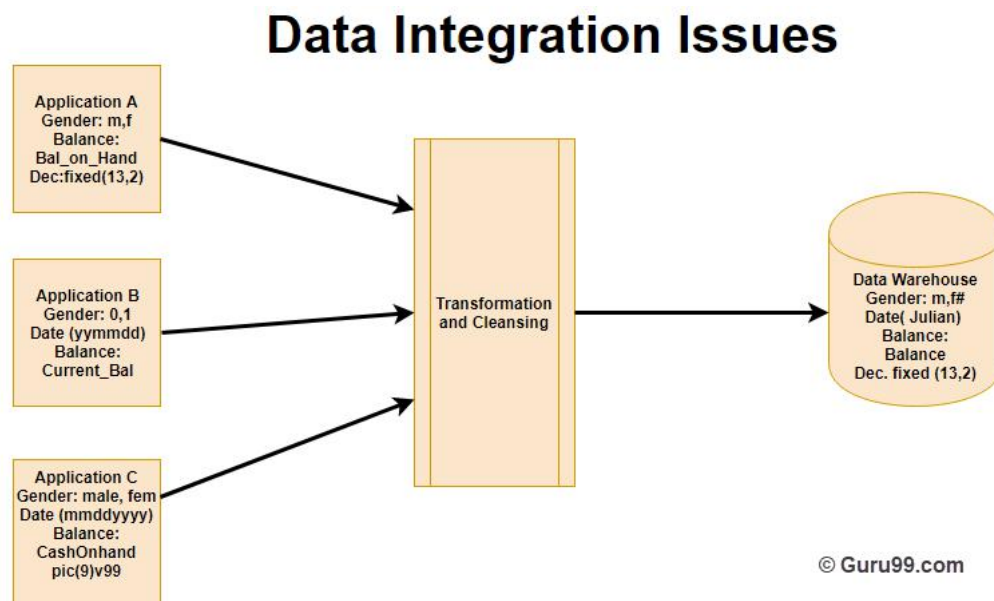
A data warehouse never focuses on the ongoing operations. Instead, it put emphasis on modeling and analysis of data for **decision making**. It also provides a simple and concise view around the specific subject by excluding data which not helpful to support the decision process.

Integrated

In Data Warehouse, integration means the establishment of a common unit of measure for all similar data from the dissimilar database. The data also needs to be stored in the Datawarehouse in common and universally acceptable manner.

A data warehouse is developed by integrating data from varied sources like a mainframe, relational databases, flat files, etc. Moreover, it must keep consistent naming conventions, format, and coding.

This integration helps in effective analysis of data. Consistency in naming conventions, attribute measures, encoding structure etc. have to be ensured. Consider the following example:



In the above example, there are three different application labeled A, B and C. Information stored in these applications are Gender, Date, and Balance. However, each application's data is stored different way.

- In Application A gender field store logical values like M or F
- In Application B gender field is a numerical value,
- In Application C application, gender field stored in the form of a character value.
- Same is the case with Date and balance

However, after transformation and cleaning process all this data is stored in common format in the Data Warehouse.

Time-Variant

The time horizon for data warehouse is quite extensive compared with operational systems. The data collected in a data warehouse is recognized with a particular period and offers information from the historical point of view. It contains an element of time, explicitly or implicitly.

One such place where Datawarehouse data display time variance is in in the structure of the record key. Every primary key contained with the DW should have either implicitly or explicitly an element of time. Like the day, week month, etc.

Another aspect of time variance is that once data is inserted in the warehouse, it can't be updated or changed.

Non-volatile

Data warehouse is also non-volatile means the previous data is not erased when new data is entered in it.

Data is read-only and periodically refreshed. This also helps to analyze historical data and understand what & when happened. It does not require transaction process, recovery and concurrency control mechanisms.

Activities like delete, update, and insert which are performed in an operational application environment are omitted in Data warehouse environment. Only two types of data operations performed in the Data Warehousing are

1. Data loading
2. Data access

Here, are some major differences between Application and Data Warehouse

Operational Application	Data Warehouse
Complex program must be coded to make sure that data upgrade processes maintain high integrity of the final product.	This kind of issues does not happen because data update is not performed.
Data is placed in a normalized form to ensure minimal redundancy.	Data is not stored in normalized form.
Technology needed to support issues of transactions, data recovery, rollback, and resolution as its deadlock is quite complex.	It offers relative simplicity in technology.

Data Warehouse Architectures

There are mainly three types of Datawarehouse Architectures

Single-tier architecture

The objective of a single layer is to minimize the amount of data stored. This goal is to remove data redundancy. This architecture is not frequently used in practice.

Two-tier architecture

Two-layer architecture separates physically available sources and data warehouse. This architecture is not expandable and also not supporting a large number of end-users. It also has connectivity problems because of network limitations.

Three-tier architecture

This is the most widely used architecture.

It consists of the Top, Middle and Bottom Tier.

1. Bottom Tier: The database of the Datawarehouse servers as the bottom tier. It is usually a relational database system. Data is cleansed, transformed, and loaded into this layer using back-end tools.
2. Middle Tier: The middle tier in Data warehouse is an OLAP server which is implemented using either ROLAP or MOLAP model. For a user, this application tier presents an abstracted view of the database. This layer also acts as a mediator between the end-user and the database.
3. Top-Tier: The top tier is a front-end client layer. Top tier is the tools and API that you connect and get data out from the data warehouse. It could be Query tools, reporting tools, managed query tools, Analysis tools and Data mining tools.

Datawarehouse Components

The data warehouse is based on an RDBMS server which is a central information repository that is surrounded by some key components to make the entire environment functional, manageable and accessible

There are mainly five components of Data Warehouse:

Data Warehouse Database

The central database is the foundation of the data warehousing environment. This database is implemented on the RDBMS technology. Although, this kind of implementation is constrained by the fact

that traditional RDBMS system is optimized for transactional database processing and not for data warehousing. For instance, ad-hoc query, multi-table joins, aggregates are resource intensive and slow down performance.

Hence, alternative approaches to Database are used as listed below-

- In a datawarehouse, relational databases are deployed in parallel to allow for scalability. Parallel relational databases also allow shared memory or shared nothing model on various multiprocessor configurations or massively parallel processors.
- New index structures are used to bypass relational table scan and improve speed.
- Use of multidimensional database (MDDBs) to overcome any limitations which are placed because of the relational data model. Example: Essbase from Oracle.

Sourcing, Acquisition, Clean-up and Transformation Tools (ETL)

The data sourcing, transformation, and migration tools are used for performing all the conversions, summarizations, and all the changes needed to transform data into a unified format in the datawarehouse.

They are also called Extract, Transform and Load (ETL) Tools.

Their functionality includes:

- Anonymize data as per regulatory stipulations.
- Eliminating unwanted data in operational databases from loading into Data warehouse.
- Search and replace common names and definitions for data arriving from different sources.
 - Calculating summaries and derived data
 - In case of missing data, populate them with defaults.
- De-duplicated repeated data arriving from multiple datasources.

These Extract, Transform, and Load tools may generate cron jobs, background jobs, Cobol programs, shell scripts, etc. that regularly update data in datawarehouse. These tools are also helpful to maintain the Metadata.

These ETL Tools have to deal with challenges of Database & Data heterogeneity.

Metadata

The name Meta Data suggests some high- level technological concept. However, it is quite simple. Metadata is data about data which defines the data warehouse. It is used for building, maintaining and managing the data warehouse.

In the Data Warehouse Architecture, meta-data plays an important role as it specifies the source, usage, values, and features of data warehouse data. It also defines how data can be changed and processed. It is closely connected to the data warehouse.

For example, a line in sales database may contain:

4030 KJ732 299.90

This is a meaningless data until we consult the Meta that tell us it was

- Model number: 4030
- Sales Agent ID: KJ732
- Total sales amount of \$2999.90

Therefore, Meta Data are essential ingredients in the transformation of data into knowledge.

Metadata helps to answer the following questions

- What tables, attributes, and keys does the Data Warehouse contain?
 - Where did the data come from?
 - How many times do data get reloaded?

- What transformations were applied with cleansing?

Metadata can be classified into following categories:

1. Technical Meta Data: This kind of Metadata contains information about warehouse which is used by Data warehouse designers and administrators.
2. Business Meta Data: This kind of Metadata contains detail that gives end-users a way easy to understand information stored in the data warehouse.

Query Tools

One of the primary objects of data warehousing is to provide information to businesses to make strategic decisions. Query tools allow users to interact with the data warehouse system.

These tools fall into four different categories:

1. Query and reporting tools
2. Application Development tools
3. Data mining tools
4. OLAP tools

1. Query and reporting tools:

Query and reporting tools can be further divided into

- Reporting tools
- Managed query tools

Reporting tools: Reporting tools can be further divided into production reporting tools and desktop report writer.

1. Report writers: This kind of reporting tool are tools designed for end-users for their analysis.

2. Production reporting: This kind of tools allows organizations to generate regular operational reports. It also supports high volume batch jobs like printing and calculating. Some popular reporting tools are Brio, Business Objects, Oracle, PowerSoft, SAS Institute.

Managed query tools:

This kind of access tools helps end users to resolve snags in database and SQL and database structure by inserting meta-layer between users and database.

2. Application development tools:

Sometimes built-in graphical and analytical tools do not satisfy the analytical needs of an organization. In such cases, custom reports are developed using Application development tools.

3. Data mining tools:

Data mining is a process of discovering meaningful new correlation, patterns, and trends by mining large amount data. Data mining tools are used to make this process automatic.

4. OLAP tools:

These tools are based on concepts of a multidimensional database. It allows users to analyse the data using elaborate and complex multidimensional views.

Data warehouse Bus Architecture

Data warehouse Bus determines the flow of data in your warehouse. The data flow in a data warehouse can be categorized as Inflow, Upflow, Downflow, Outflow and Meta flow.

While designing a Data Bus, one needs to consider the shared dimensions, facts across data marts.

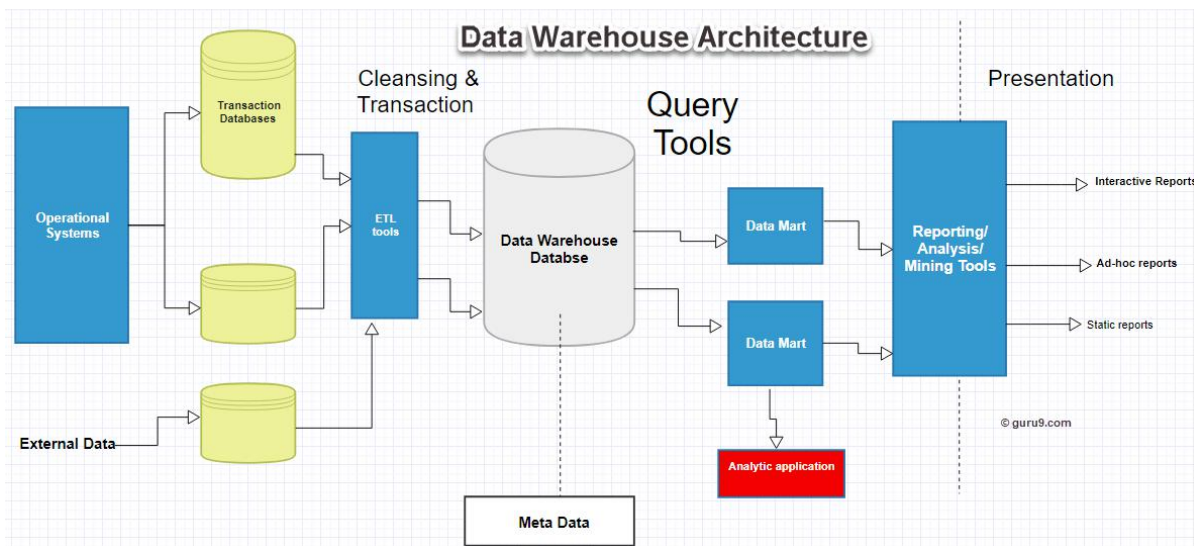
Data Marts

A data mart is an access layer which is used to get data out to the users. It is presented as an option for large size data warehouse as it takes less time and money to build. However, there is no standard definition of a data mart is differing from person to person.

In a simple word Data mart is a subsidiary of a data warehouse. The data mart is used for partition of data which is created for the specific group of users.

Data marts could be created in the same database as the Datawarehouse or a physically separate Database.

Data warehouse Architecture Best Practices



To design Data Warehouse Architecture, you need to follow below given best practices:

- Use a data model which is optimized for information retrieval which can be the dimensional mode, denormalized or hybrid approach.
- Need to assure that Data is processed quickly and accurately. At the same time, you should take an approach which consolidates data into a single version of the truth.
- Carefully design the data acquisition and cleansing process for Data warehouse.
- Design a MetaData architecture which allows sharing of metadata between components of Data Warehouse

- Consider implementing an ODS model when information retrieval need is near the bottom of the data abstraction pyramid or when there are multiple operational sources required to be accessed.
- One should make sure that the data model is integrated and not just consolidated. In that case, you should consider 3NF data model. It is also ideal for acquiring ETL and Data cleansing tools

Summary:

- Data warehouse is an information system that contains historical and commutative data from single or multiple sources.
- A data warehouse is subject oriented as it offers information regarding subject instead of organization's ongoing operations.
- In Data Warehouse, integration means the establishment of a common unit of measure for all similar data from the different databases
- Data warehouse is also non-volatile means the previous data is not erased when new data is entered in it.
 - A Datawarehouse is Time-variant as the data in a DW has high shelf life.
- There are 5 main components of a Datawarehouse. 1) Database 2) ETL Tools 3) Meta Data 4) Query Tools 5) DataMarts
- These are four main categories of query tools 1. Query and reporting, tools 2. Application Development tools, 3. Data mining tools 4. OLAP tools
- The data sourcing, transformation, and migration tools are used for performing all the conversions and summarizations.
- In the Data Warehouse Architecture, meta-data plays an important role as it specifies the source, usage, values, and features of data warehouse data.

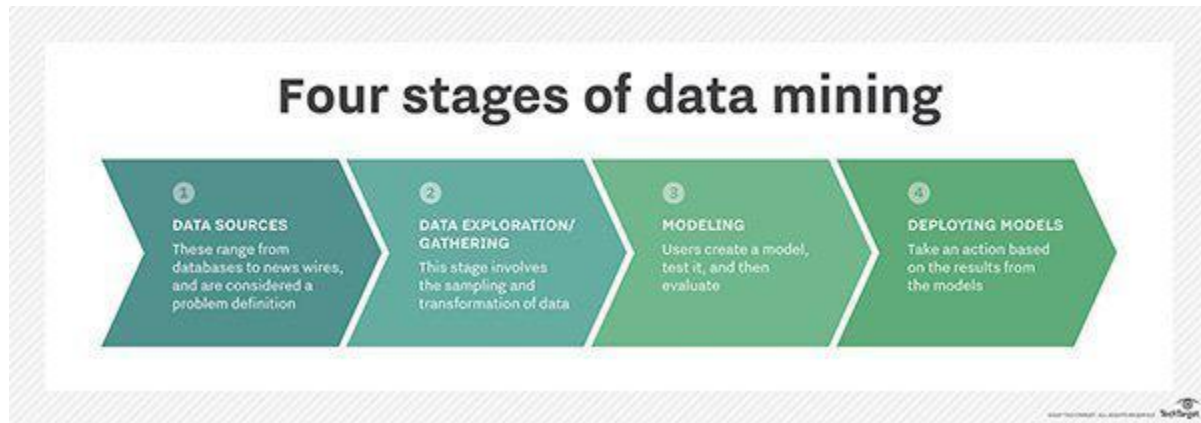
Data Mining

Data mining is the process of sorting through large [data sets](#) to identify patterns and establish relationships to solve problems through data analysis. Data mining tools allow enterprises to predict future trends.

Data mining parameters

In data mining, [association rules](#) are created by analyzing data for frequent if/then patterns, then using the support and confidence criteria to locate the most important relationships within the data. Support is how frequently the items appear in the [database](#), while confidence is the number of times if/then statements are accurate.

Other data mining [parameters](#) include Sequence or Path Analysis, [Classification](#), [Clustering](#) and Forecasting. Sequence or Path Analysis parameters look for patterns where one event leads to another later event. A Sequence is an ordered list of sets of items, and it is a common type of data structure found in many databases. A Classification parameter looks for new patterns, and might result in a change in the way the data is organized. Classification [algorithms](#) predict variables based on other factors within the database.



Clustering parameters find and visually document groups of facts that were previously unknown.

Clustering groups a set of objects and aggregates them based on how similar they are to each other.

There are different ways a user can implement the cluster, which differentiate between each clustering model. Fostering parameters within data mining can discover patterns in data that can lead to reasonable predictions about the future, also known as predictive analysis.

Data mining tools and techniques

Data mining techniques are used in many research areas, including mathematics, cybernetics, genetics and marketing. While data mining techniques are a means to drive efficiencies and predict customer behavior, if used correctly, a business can set itself apart from its competition through the use of predictive analysis.

Data Mining 101

Web mining, a type of data mining used in customer relationship management, integrates information gathered by traditional data mining methods and techniques over the web. Web mining aims to understand customer behavior and to evaluate how effective a particular website is.

Other data mining techniques include network approaches based on multitask learning for classifying patterns, ensuring parallel and scalable execution of data mining algorithms, the mining of large databases, the handling of relational and complex data types, and machine learning. Machine learning is a type of data mining tool that designs specific algorithms from which to learn and predict.

Benefits of data mining

In general, the benefits of data mining come from the ability to uncover hidden patterns and relationships in data that can be used to make predictions that impact businesses.

Specific data mining benefits vary depending on the goal and the industry. Sales and marketing departments can mine customer data to improve lead conversion rates or to create one-to-one marketing campaigns. Data mining information on historical sales patterns and customer behaviors can be used to build prediction models for future sales, new products and services.

Companies in the financial industry use data mining tools to build risk models and detect fraud. The manufacturing industry uses data mining tools to improve product safety, identify quality issues, manage the supply chain and improve operations.



DBMS vs Relational DBMS

Relational software uses the concept of database normalization and the constraints of primary and foreign keys to establish relationships between rows of data in different database tables. That eliminates the need to redundantly store related data in multiple tables, which reduces data storage requirements,

streamlines database maintenance and enables faster querying of databases. Normalization is a concept that applies to relational databases only.

Another notable difference between DBMS and RDBMS architectures, leaving the latter category out of the broad DBMS classification, is relational technology's support for referential integrity and other integrity checks designed to help keep data accurate and prevent inconsistent information from being entered in database tables. That's part of an adherence to the [ACID properties](#) -- atomicity, consistency, isolation and durability -- for ensuring that database transactions are processed in a reliable way. That isn't necessarily the case with other DBMS types -- for example, many NoSQL databases guarantee a more limited form of ACID compliance, called eventual consistency.

While these RDBMS concepts and features provide reliable, stable and relatively robust processing of structured transaction data, relational technology does have some limitations -- in particular, its requirement that databases include a rigid schema that's difficult for DBAs to modify on the fly. That has helped create an opening for NoSQL software and, to a greater extent, [file-based Hadoop clusters](#) in big data environments, although relational databases are still at the center of most IT architectures.

ACID properties (Atomicity, Consistency, Isolation & Durability)

Atomicity: Atomicity requires that each transaction be "all or nothing": if one part of the transaction fails, then the entire transaction fails, and the database state is left unchanged. An atomic system must guarantee atomicity in each and every situation, including power failures, errors and crashes. To the outside world, a committed transaction appears (by its effects on the database) to be indivisible ("atomic"), and an aborted transaction does not happen.

Consistency: The consistency property ensures that any transaction will bring the database from one valid state to another. Any data written to the database must be valid according to all defined rules

including constraints, cascades, triggers, and any combination thereof. This does not guarantee correctness of the transaction in all ways the application programmer might have wanted

Srinivas Kante

(that is the responsibility of application-level code), but merely that any programming errors cannot result in the violation of any defined rules.

Isolation: The isolation property ensures that the concurrent execution of transactions results in a system state that would be obtained if transactions were executed sequentially, i.e., one after the other. Providing isolation is the main goal of concurrency control. Depending on the concurrency control method (i.e., if it uses strict - as opposed to relaxed - serializability), the effects of an incomplete transaction might not even be visible to another transaction.

Durability: The durability property ensures that once a transaction has been committed, it will remain so, even in the event of power loss, crashes, or errors. In a relational database, for instance, once a group of SQL statements execute, the results need to be stored permanently (even if the database crashes immediately thereafter). To defend against power loss, transactions (or their effects) must be recorded in a non-volatile memory.

NORMALIZATION OF A DATABASE

Normalization is a process of organizing the data in database to avoid data redundancy, insertion anomaly, update anomaly & deletion anomaly. Normalization divides larger tables to smaller tables and link them using relationships.

Let's discuss anomalies first then we will discuss normal forms with examples.

Anomalies in DBMS

There are three types of anomalies that occur when the database is not normalized. These are – Insertion, update and deletion anomaly. Let's take an example to understand this.

Example: Suppose a manufacturing company stores the employee details in a table named

employee that has four attributes: emp_id for storing employee's id, emp_name for storing employee's name, emp_address for storing employee's address and emp_dept for storing the department details in which the employee works. At some point of time the table looks like this:

emp_id	emp_name	emp_address	emp_dept
101	Krish	Delhi	D001
101	Krish	Delhi	D002
123	Malini	Agra	D890
166	Navin	Chennai	D900
166	Navin	Chennai	D004

The above table is not normalized. We will see the problems that we face when a table is not normalized.

Update anomaly: In the above table we have two rows for employee Krish as he belongs to two departments of the company. If we want to update the address of Krish then we have to update the same in two rows or the data will become inconsistent. If somehow, the correct address gets

updated in one department but not in other then as per the database, Krish would be having two different addresses, which is not correct and would lead to inconsistent data.

Insert anomaly: Suppose a new employee joins the company, who is under training and currently not assigned to any department then we would not be able to insert the data into the table if emp_dept field doesn't allow nulls.

Delete anomaly: Suppose, if at a point of time the company closes the department D890 then deleting the rows that are having emp_dept as D890 would also delete the information of employee Malini since she is assigned only to this department.

To overcome these anomalies we need to normalize the data. In the next section we will discuss normalization.

Normalization

The inventor of the relational model Edgar Codd proposed the theory of normalization with the introduction of First Normal Form and he continued to extend theory with Second and Third Normal Form. Later he joined with Raymond F. Boyce to develop the theory of Boyce-Codd Normal Form (BCNF).

Theory of Data Normalization in SQL is still being developed further. For example there are discussions even on 6th Normal Form. **But in most practical applications normalization achieves its best in 3rd Normal Form (3NF).** The evolution of Normalization theories is illustrated below-

We need to understand the basic concepts of primary key, foreign key, candidate key and super key in a relational database, before we proceed further to understand the evolution of normal forms.

Super, Candidate, Primary & Foreign keys

A Super Key is the combination of fields by which the row is uniquely identified and the Candidate Key is the minimal Super Key. Basically, a Candidate Key is a Super Key from which no more Attribute can be pruned. A Super Key identifies uniquely rows/tuples in a table/relation of a database.

A Primary Key uniquely identify a record in the table. A Foreign Key is a field in the table that is Primary Key in another table. By default, Primary Key is clustered index and data in the database table is physically organized in the sequence of clustered index. We can have only one Primary Key in a table.

As discussed above, a Candidate Key can be any column or a combination of columns that can qualify as unique key in a database. There can be multiple Candidate Keys in one table. On the other hand, a Primary Key is a column or a combination of columns that uniquely identify a record. Thus each Candidate Key can qualify as Primary Key. However, as there may be multiple Candidate Keys in a table, a Primary Key can be only one for a given table.

The above terms are freely used in the following discussion on normal forms. You may notice that as the normalization process upgrades from 1NF to 2NF and then to 3NF and so on, the number of tables and reference keys keep increasing.

A DATA WAREHOUSE ARCHITECTURE

Different data warehousing systems have different structures. Some may have an ODS (operational data store), while some may have multiple data marts. In general a Data Warehouse is used on an enterprise level, while **Data Mart** is used on a business division/department level. Some may have a small number of data sources, while some may have dozens of data sources. In view of this, it is far more reasonable to present the different layers of a data warehouse architecture rather than discussing the specifics of any one system.

Layers in a Data Warehouse

In general, all data warehouse systems have the following layers:

Data Source Layer

Data Extraction Layer
Staging Area

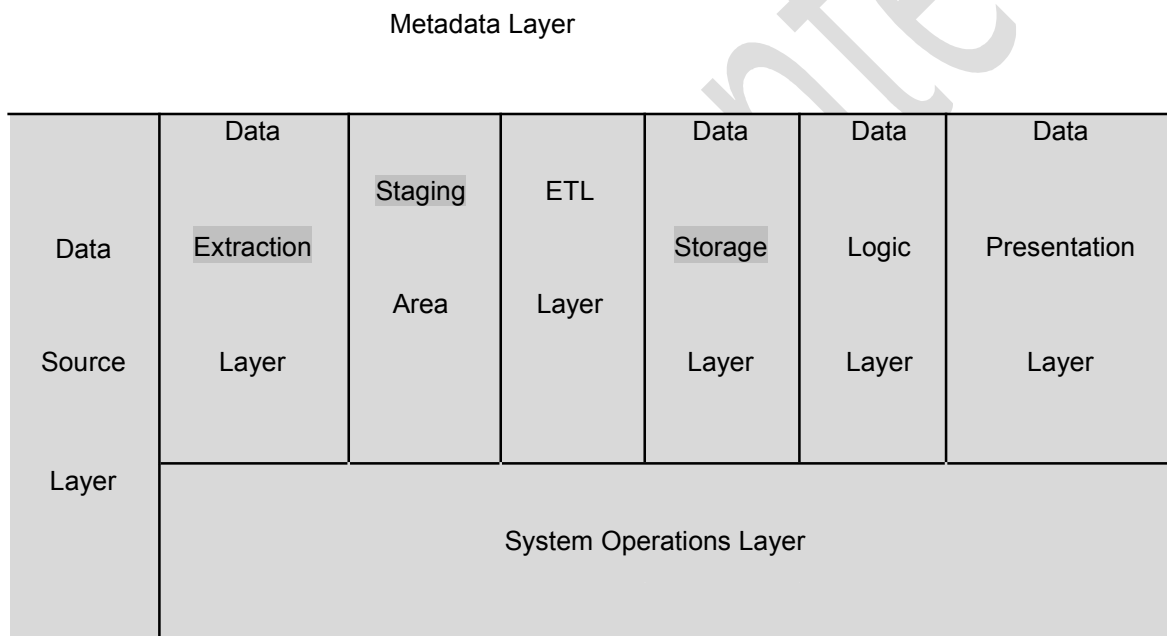
ETL Layer

Data Storage Layer
Data Logic Layer

Data Presentation Layer
Metadata Layer

System Operations Layer

The picture below shows the relationships among the different components of the data warehouse architecture:



Each component is discussed individually below:

Data Source Layer

This represents the different data sources that feed data into the data warehouse. The data source can be of any format -- plain text file, relational database, other types of database, Excel file, etc., can all act as a data source.

Srinivas Kante

Many different types of data can be a data source:

Operations -- such as sales data, HR data, product data, inventory data, marketing data, systems data.

Web server logs with user browsing data.

Internal market research data.

Third-party data, such as census data, demographics data, or survey data.

All these data sources together form the Data Source Layer.

Clearly, the goal of data warehousing is to free the information that is locked up in the operational databases and to mix it with information from other, often external, sources of data. Increasingly, large organizations are acquiring additional data from outside databases. This information includes demographic, econometric, competitive and purchasing trends.

Data Extraction Layer

Data gets pulled from the data source into the data warehouse system. There is likely some minimal data cleansing, but there is unlikely any major data transformation.

Staging Area: This is where data sits prior to being scrubbed and transformed into a data warehouse / data mart. Having one common area makes it easier for subsequent data processing / integration.

ETL Layer

ETL stands for “Extract, Transform and Load”. This is where data gains its "intelligence", as logic is applied to transform the data from a transactional nature to an analytical nature. This layer is also where data cleansing happens. The [ETL design phase](#) is often the most time-consuming phase in a data warehousing project, and an [ETL tool](#) is often used in this layer.

Data Storage Layer

This is where the transformed and cleansed data sit. Based on scope and functionality, 3 types of entities can be found here: data warehouse, data mart, and operational data store (ODS). In any given system, you may have just one of the three, two of the three, or all three types.

Data Logic Layer

This is where business rules are stored. Business rules stored here do not affect the underlying data transformation rules, but do affect what the report looks like.

Data Presentation Layer

This refers to the information that reaches the users. This can be in a form of a tabular / graphical report in a browser, an emailed report that gets automatically generated and sent every day, or an alert that warns users of exceptions, among others. Usually an [OLAP tool](#) and/or a [reporting tool](#) is used in this layer.

Metadata Layer

This is where information about the data stored in the data warehouse system is stored. Metadata is data about data. A logical data model would be an example of something that's in the metadata layer. A [metadata tool](#) is often used to manage metadata. Data warehouse contains huge amount of data. The metadata component contains the information like: (1) description of data warehouse;

(2) rules to map, translate and transform data sources to warehouse elements; (3) the navigation paths and rules for browsing in the data warehouse; (4) the data dictionary; (5) the list of pre-designed and built-in queries available to the users etc. Record descriptions in a COBOL program DIMENSION statements in a FORTRAN program, or SQL Create statement fields are examples of metadata.

In order to have a fully functional warehouse, it is necessary to have a variety of meta-data available, data about the end-user views of data and data about the operational databases. Ideally, end-users should be able to access data from the data warehouse (or from the operational databases) without having to know where that data resides or the form in which it is stored.

System Operations Layer

This layer includes information on how the data warehouse system operates, such as ETL job status, system performance, and user access history.

BUSINESS INTELLIGENCE–EXPERT SYSTEMS & ARTIFICIAL NEURAL NETWORKS

Business intelligence (BI)

Business Intelligence includes several types of applications and technologies for acquiring, storing, analyzing, and providing access to information to help users make more sound business decisions. BI applications include decision support systems (DSS), query and reporting, online analytical processing

(OLAP), statistical analysis, and data mining. We have discussed in detail the concepts of DSS, Group DSS in the foregoing Chapter 5.

Often BI applications use data gathered from a [data warehouse](#) (DW) or from a [data mart](#), and the concepts of BI and DW sometimes combine as "BI/DW" or as "BIDW". A data warehouse contains a copy of analytical data that facilitates decision support.

Artificial Neural Networks & Expert Systems

Artificial neural networks (ANNs) are inspired by the information processing model of the mind/brain. The human brain consists of billions of neurons that link with one another in an intricate pattern. Every neuron receives information from many other neurons, processes it, gets excited or not, and passes its state information to other neurons.

Just like the brain is a multipurpose system, so also the ANNs are very versatile systems. They can be used for many kinds of pattern recognition and prediction.

In artificial intelligence, an Expert System (ES) is a computer system that emulates the decision-making ability of a human expert. Expert systems are designed to solve complex problems by reasoning about knowledge, represented mainly as if-then rules rather than through conventional procedural code. An expert system is divided into two subsystems: the [inference engine](#) and the [knowledge base](#). The knowledge base represents facts and rules. The inference engine applies

the rules to the known facts to deduce new facts. Inference engines can also include explanation and debugging abilities

An expert system is made up of three parts: A user interface - This is the system that allows a non-expert user to query (question) the expert system, and to receive advice. The user-interface is designed to be as simple to use as possible. A knowledge base - This is a collection of facts and rules. A rule-based system is a set of "if-then" statements that uses a set of assertions, to which rules on how to act upon those assertions are created. In software development, rule-based systems can be used to create software that will provide an answer to a problem in place of a human expert.

Applications of ANN

Artificial Neural Networks or ANN has a multitude of real world applications in the business domain which have been classified as follows:

Accounting · Identifying tax fraud · Enhancing auditing by finding irregularities Finance · Signature and bank note verification · Mortgage underwriting · Foreign exchange rate forecasting

· Country risk rating · Predicting stock initial public offerings · Bankruptcy prediction · Customer credit scoring · Credit card approval and fraud detection · Stock and commodity selection and trading 3 · Forecasting economic turning points · Bond rating and trading · Loan approvals ·

Economic and financial forecasting · Risk management Human resources · Predicting employee's performance and behaviour · Determining personnel resource requirements Marketing · Classification of consumer spending patterns · New product analysis · Identification of customer characteristics · Sale forecasts · Targeted marketing.

Artificial Intelligence (AI), which is gaining popularity at a great pace today, is a much superior cousin of Artificial Neural Network (ANN) which has been discussed in the previous section. Artificial intelligence (AI)

involves the study of cognitive phenomena in machines. One of the practical goals of AI is to implement aspects of human intelligence in computers. Computers are also widely used as a tool with which to study cognitive phenomena. Cognitive computing (CC) describes technology platforms that are based on the scientific disciplines of artificial intelligence (AI) and signal processing. These platforms encompass machine learning, reasoning, natural language processing, speech recognition and vision (object recognition), human–computer interaction, dialog and narrative generation, among other technologies.

The intelligence emerges from a business point of view when machines – based on information – are able to make decisions, which maximizes the chances of success in a given topic. By the use of Machine Learning, Artificial Intelligence is able to use learning from a data set to solve problems and give relevant recommendations. For example, we can use the learning about the correlation between weather, local events and sales numbers to create a fully automated system that decides upon the daily supply shipped to a given store.

Machine learning is a field of [computer science](#) that uses statistical techniques to give [computer systems](#) the ability to learn, i.e., progressively improve performance on a specific task, with [data](#), without being explicitly programmed. Machine Learning is algorithms that learn from data and create foresights based on this data. A simple example of how it can be used: Building a model, that can predict customer demand by understanding the correlation between sales numbers from a store correlated with historical weather data and local events happening in the area.

Machine learning is employed in a range of computing tasks where designing and programming explicit algorithms with good performance is difficult or infeasible; example applications include email filtering, detection of network intruders or malicious insiders working towards a data breach, optical character recognition (OCR), learning to rank, and computer vision.

Cognitive analytics is a cognitive computing technology platform typically specialize in the processing and analysis of large, unstructured datasets. Generally, word processing documents, emails, videos,

images, audio files, presentations, webpages, social media and many other data formats often need to be manually tagged with metadata before they can be fed to a computer for analysis and insight generation. The principal benefit of utilizing cognitive analytics over traditional big data analytics is that such datasets do not need to be pre-tagged.

Cognitive analytics systems can use machine learning to adapt to different contexts with minimal human supervision. Cognitive analytics systems can be equipped with a chatbot or search assistant that understands queries, explains data insights and interacts with humans in natural language.

E-Learning Environment

E-learning is defined by many people, in many ways, since the term e-learning is used inconsistently, in order to gain a clear understanding of what e-learning is, here are a few definitions of e-learning. The letter "e" in e-learning stands for the word "electronic", e-learning would incorporate all educational activities that are carried out by individuals or groups working online or offline via networked or standalone computers and other electronic devices.

- Brandon Hall defines E-learning as: "...instruction that is delivered electronically, in part or wholly via a Web browser, through the Internet or an intranet, or through multimedia platforms such as CD-ROM or DVD."
- Rosenberg: "E-learning refers to the use of Internet technologies to deliver a broad array of solutions that enhance knowledge and performance." Rosenberg claims that e-learning is based on three fundamental criteria:

Characteristics of E- learning

- **E-learning is Learner-Centric Learning:** The learner centric e-learning model makes an array of resources available to the learner, who is free to choose when, where and how to learn.

- **E-learning for lifelong learning:** With increasing access to technologies and its ever increasing sophistication this approach to learning facilitates lifelong learning among various stake holders.
- **E-learning is Flexible Learning:** E-learning has historically been linked with distance education and flexible learning. In distance education, various technologies can be used to link learners, instructors and resources that are removed in time or space. The hallmark of flexible learning, as its name suggests, is its adaptability to learners' needs and circumstances.
- **E-learning is Social:** E-learning seeks to foster collaboration and peers interaction. Various e-learning technologies facilitate various types of collaboration among learners and teachers.
- **E-learning Involves Learning Objects:** E-learning uses reusable learning objects. This RLO permits one to create e-learning course with ease.
- **E-learning is Personalized:** Usually e-learning system permits its users to personalize the learning by tailoring its offerings to their learning style, job requirements, career goals, current knowledge and personal preferences.
- **E-learning Involves Effective Communication:** The effectiveness of e-learning also depends on establishing two-way communication between teachers and learners, and among learners themselves. There are many standalone tools as well as learner management system integrated tools to foster interactive and collaborative engagement.

LEARNING TOOLS AND TECHNOLOGIES

E-learning is a flexible learning environment which serves a number of individual and organizational purposes by making use of a number of technologies. There are many tools and technologies essential for e-learning and many of these tools come in handy as a standalone to deliver learning using variety of approaches to e-learning. In addition we also have many Learning Management Systems which integrate many of the individual tools into a single platform to develop and deliver online learning. A comprehensive list of e-learning tools and technologies are provided in the following table.

E-learning Tools and Technologies

Content creation tools <ul style="list-style-type: none"> ○ Tools for creating avatars (virtual characters) ○ Course and lesson authoring tools ○ E-book tools ○ Graphics and animation tools ○ Image galleries and sound effects libraries ○ Assessment tools ○ Pdf tools ○ Video and simulation tools ○ Web page authoring tools ○ Survey and polling tools Delivery and distribution tools <ul style="list-style-type: none"> ○ Podcasting tools ○ RSS tools ○ Web casting and streaming tools ○ Presentation tools ○ Mobile learning tools User Tools <ul style="list-style-type: none"> ○ Operating system ○ Browsers ○ Media players ○ Plug ins ○ Pdf reader ○ Word processor 	Communication and Collaboration Tools <ul style="list-style-type: none"> ○ Discussion boards and forum tools ○ E-mail tools ○ Live support tools ○ Meeting and teleconferencing tools ○ Instant messaging and chat tools ○ Social networking tools ○ Social book marking and file sharing tools ○ Wiki tools E-learning Systems <ul style="list-style-type: none"> ○ Content management systems ○ Learning management systems ○ Course management systems Hardware Tools <ul style="list-style-type: none"> ○ PC/laptop/ net book ○ Smart phones/ palmtop computer ○ Printer / scanner/ speaker ○ Microphone /speaker/ web ca7
---	--

Content Creation Tools/Authoring tools

An e-learning content authoring tool is a software package which developers use to create and package e-learning content deliverable to end users. According to Wikipedia.org, “a content authoring tool is a software application used to create multimedia content typically for delivery on the World Wide Web. Content-authoring tools may also create content in other file formats so the training can be delivered on a CD (Compact Disc) or in other formats for various different uses. The category of content-authoring tools includes HTML, Flash, and various types of e-learning authoring tools.”

Thus, e-learning authoring tools are a class of products designed for people who need to create online educational or training courses that are deployed from a standard, cloud-based learning management system. Many programs can be considered authoring tools, including Flash, and PowerPoint. However, only a small group of programs specifically include support for e-learning content standards such as SCORM (Shareable Content Object Reference Model).

There are many proprietary as well as open source authoring tools available currently in the market. Some of the most famous proprietary authoring tools are Elucidate, Lectora, Easygenerator, Smart Builder, Adobe Presenter, Camtasia, Articulate, Captivate and Udutu. There are also many open source authoring tools which have many features. They are Learner Activity Management System (LAMS), Adapt, Xerte, and eXeLearning.

In addition to these SCORM compatible authoring tools there are many specific applications necessary for creating content such as image editing, video editing, audio editing and animation tools to create multimedia e-content. Currently most of the LMS have its own inbuilt authoring tools to create e-content due to the convergence of the software features.

Short descriptions of the popular open source authoring tools are given in the following section.



Adapt: The Adapt authoring tool is an application to allow you to quickly build responsive e-learning content. It's accessed through a web browser. You can create an account, log in, create courses and add assets, components and extensions. You can preview and publish your e-learning content from the authoring tool.



LAMS: Learner Activity Management System (LAMS) is a revolutionary new tool for designing, managing, and delivering online collaborative learning activities. It provides teachers with highly intuitive visual authoring environment for creating sequence of learning activities.





Xerte: Xerte is a fully-featured e-learning development environment for creating rich interactivity. Xerte is aimed at developers of interactive content who will create sophisticated content with some scripting, and Xerte can be used to extend the capabilities of Xerte Online Toolkits with new tools for content authors. Xerte Online Toolkits is a server-based suite of tools for content authors. E-learning materials can be authored quickly and easily using browser-based tools, with no programming required. Xerte Online Toolkits is aimed at content authors, who will assemble content using simple wizards. Content authors can easily collaborate on projects. Xerte Online Toolkits can be extended by developers using Xerte.



eXeLearning: The eXe project developed a freely available Open Source authoring application to assist teachers and academics in the publishing of web content without the need to become proficient in HTML or XML markup. Resources authored in eXe can be exported in IMS Content Package, SCORM 1.2, or IMS Common Cartridge formats or as simple self-contained web pages.

LEARNING MANAGEMENT SYSTEM (LMS)

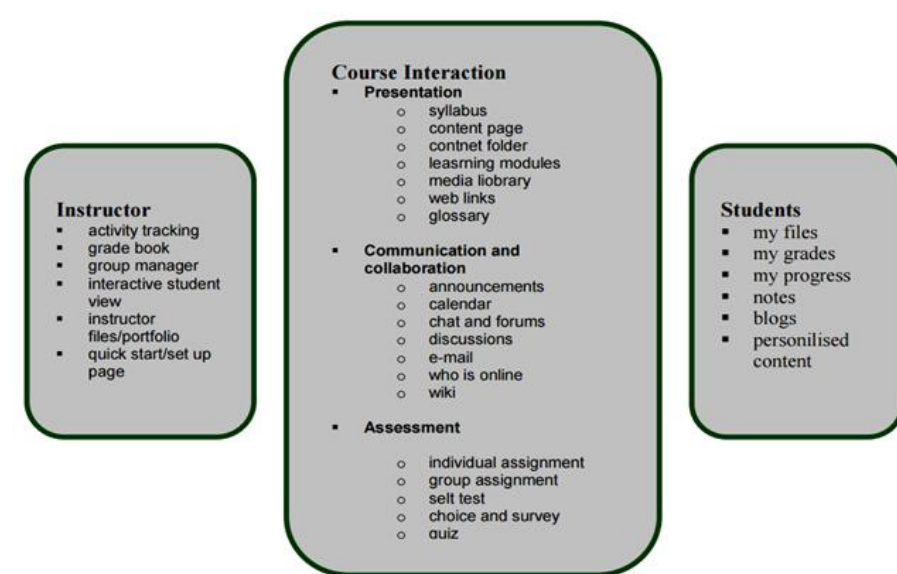
After so many years of technology use in education, it is felt that educators today need a web-enabled relational database that links curriculum, instructional resources, assessment strategies, student data, and staff proficiencies all on a single platform. This is possible by adopting a comprehensive and systemic integration of a multi-dimensional system called Learning Management System (LMS). LMS provide an infrastructure platform through which learning content is delivered and the learning and learners are managed. It provides a combination of software tools that perform a variety of functions related to online and offline training administration and performance management. Typically, an LMS is internet-based software that deploys, manages, tracks, reports on the interaction between the learner and the content, and the learner and the instructor. Administratively, an LMS makes it easy to enter, track, manage, and report on learning activities and competencies. An LMS is not limited to e-learning and can also manage other forms of instruction. In essence, an LMS primarily focuses on competencies, learning

activities, and the logistics of delivering learning activities. An LMS does not focus on creation, reusability, management, or improvement of content itself. Tasks of the LMS:

- Manage learners taking whole courses
- Manage the curriculum
- Manage courses in various curriculums
- Present options depending on learner profiles
- Track learner needs and preferences
- Track course completions and scores

Features of LMS: LMS has specific features meant for instructor, course interaction, and students.

Listings of all these features are given below:



LMS and Learning Content Management System (LCMS)

LMS	LCMS
The focus of an LMS is to deliver online courses or training to learners, while managing students and keeping track of their progress and performance across all types of training activities. An LMS is not used to create course content.	LCMS is a related software technology that provides a multi-user environment where developers, authors, instructional designers, and subject matter experts may create, store, reuse, manage, and deliver digital educational technology (also known as e-learning) content from a central object repository. LCMS focuses on the development, management

LMS	LCMS
	and publishing of the content that will typically be delivered via an LMS. Users can both create and re-use content and reduce duplicated development efforts.
LMS Functionality	LCMS Functionality
<ul style="list-style-type: none"> • Course Content Delivery • Student Registration and Administration • Training Event Management (i.e., scheduling, tracking) • Curriculum and Certification Management • Skills and Competencies Management • Skill Gap Analysis • Individual Development Plan (IDP) • Assessing • Reporting • Training Record Management • Courseware Authoring • Resource Management • Performance Management System <ul style="list-style-type: none"> ○ Template-driven, Collaborative Content Development ○ Facilitated Content Management (i.e., indexing and reuse) ○ Publishing ○ Workflow Integration ○ Automated Interface with an LMS 	<p>The components of an LCMS include:</p> <ul style="list-style-type: none"> ○ An authoring application ○ A learning object repository, ○ A dynamic delivery interface ○ Administration tools. <p>An LCMS may provide course to an LMS that tracks and manages the learner and learning.</p>

While LMS and LCMS have different strengths and weaknesses, and despite their distinction mentioned in the above table, the term LMS is often used to refer to both an LMS and an LCMS, although the LCMS is actually a complementary solution to an LMS. Either as separate platforms or as a merged product, LCMSs work together with LMSs to develop and deliver course content to students. Due to lack of industry standardization as well as being a young industry, products that combine LCMS and LMS attributes may be referred to as course management systems (CMS), learning management systems (LMS) and LMS/LCMS.

ADVANTAGES AND POTENTIAL DRAWBACKS OF E-LEARNING

Advantages of e-Learning to the Trainer or Organization

- **Reduced overall cost** is the single most influential factor in adopting e-learning. The elimination of costs associated with instructor's salaries, meeting room rentals, and student travel, lodging, and meals are directly quantifiable.
- **Increased retention** and application
- **Consistent delivery** of content is possible with asynchronous, self-paced e-learning.
- **Expert knowledge** is communicated, but more importantly captured, with good e-learning and knowledge management systems.
- **Proof of completion and certification**, essential elements of training initiatives, can be automated.

Advantages to the Learner

- **On-demand availability** enables students to complete training conveniently at off-hours or from home.
- **Self-pacing** for slow or quick learners reduces stress and increases satisfaction.
- **Interactivity** engages users, pushing them rather than pulling them through training.
- **Confidence** that refresher or quick reference materials are available reduces burden of responsibility of mastery.

Potential drawbacks

Technology dependent: Learners will need access to a machine of minimum specification as dictated by the e-learning supplier or access to a service with a high bandwidth to transfer the course materials in a timely way.

Material Incompatibility: Some materials designed for one particular system will not function properly on another (for example, the Apple Macintosh and the Windows PC). Standards will help in the area.

Unsuitable for Certain Types of Training: Any skill that relies heavily on inter-personal contact although these courses could be supplemented by e-learning.

Unsuitable for Certain Types of Learners: e-learning requires a high-level of self-discipline and personal time management. E-Learners need to be highly self-motivated to take full advantage of the

medium as often the online learning experience can be impersonal. Working through 'packaged' programmes can be irritating.

Reliant of the Quality of the Content: It is too easy for some institutions to defer the photocopying costs onto the learner by placing all lecture notes and course handouts online. Such practices often mean that the course materials are in an inappropriate format for online learning. Course providers need to develop new technical skills and course design skills to suit the new medium.

Expensive: Start-up cost of an e-learning service is expensive and the cost of production of online training materials is very high. Teachers must be confident that the extra costs are balanced with the benefits of delivering a course online. Significant time needs to be invested in course set-up and in ongoing maintenance (checking links, updating course content etc.).

Reliant on Human Support: E-learning is still dependent on help on either the course materials or the software.

Social/economic disadvantage: It can limit or prevent access by some student groups (for example, cost of equipment, online access and printing).

No Match for Face-to-Face Teaching: Electronic communication does not necessarily provide a good match for face-to-face communication and is more linear than face-to-face discussion.

Too Reliant on IT Skills: Learners may have limited IT skills, or be uncomfortable with electronic communication and need to learn how to use the medium effectively.

Disabilities: Students with visual or physical impairments may be disadvantaged.

Inflexible: Flexibility may be lost as adjustments to the course in response to student reaction are not easy to make once the course is underway.

Pedagogically Unsound: The electronic environment does not per se offer a pedagogically enhancing learning environment.

Virtual Class room

A virtual classroom is a teaching and learning environment where participants can interact, communicate, view and discuss presentations, and engage with learning resources while working in groups, all in an

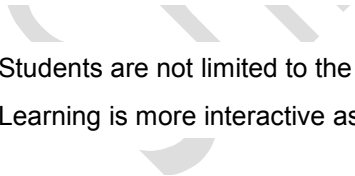
online setting. The medium is often through a video conferencing application that allows multiple users to be connected at the same time through the Internet, which allows users from virtually anywhere to participate.

A virtual classroom is also known as a virtual learning environment (VLE).

There is no concrete definition of what a virtual classroom is, but the most logical one is simply that it is an online classroom environment facilitated via specialized video conferencing applications. The participants, of course, include one or multiple instructors and students. However, a classroom or class does not always need an active instructor to supervise students; in this setting, they can proceed at their own pace, with the instructor only around to evaluate the students; sometimes there is no instructor at all. This type of virtual classroom is called an unsupervised virtual classroom, which is characterized by ready-made learning materials that students can follow without the aid of an instructor, essentially a self-paced tutorial course where the exams can be automated after every activity. This is the most common form of virtual classroom, where students just read a PowerPoint presentation or watch a video tutorial. This makes YouTube, by association, the most widely used virtual classroom thus far (even if it is not considered as one).

The second type of virtual classroom is the supervised or instructor-led classroom. This conforms more to a traditional classroom definition. There is at least one active instructor present and the lesson is carried out in real time at a specific time and date, with the students being in attendance virtually through a video conferencing application. Here, students and teachers can truly interact and actively participate in class.

A virtual classroom has the following advantages:

- 
- Students are not limited to the courses available in their geography.
 - Learning is more interactive as its nature forces the student's attention.

It has the following disadvantages, however:

- In the case of supervised classes, the schedule may be an issue to some students.
- It is limited by the technological capacity of the student; those with slower hardware or Internet speeds are at a disadvantage.

LET US SUM UP

E-learning is: "...instruction that is delivered electronically, in part or wholly via a Web browser, through the Internet or an intranet, or through multimedia platforms such as CD-ROM or DVD".(Brandon Hall)

- E-learning methods can be classified into Synchronous, Asynchronous and Blended Learning Methods.
- Modern Technology provides us with a plethora of options for communicating. The most common Communication tools used in E-learning include, e-mail, Instant Messaging and Blogging.
- Some of the popular collaboration tools of e-learning include Chat, forum, wiki, online groups, audio/video conferencing, social bookmarking and social networking.
- Some of the Content Creation Tools/Authoring tools are Course and lesson authoring tools, E-book tools, Graphics and animation tools, Assessment tools, Video and simulation tools, Survey and polling tools.
- There are many proprietary as well as open source authoring tools available currently in the market. Some of the famous proprietary authoring tools are Elucidate, Lectora, Easygenerator, Smart Builder, Adobe Presenter, Camtasia, Articulate, Captivate and Udutu. There are also many open source authoring tools which have many features. They are Learner Activity Management System (LAMS), Adapt, Xerte, and eXeLearning.
- Some of the delivery and distribution e-learning tools include SCORM, e-pub, audio/video streaming and Podcasting.
- A learning management system provides students with the ability to use interactive features such as threaded discussions, video conferencing, and discussion forums.
- LMS is the framework that handles all aspects of the learning process.
- LCMS focuses on the development, management and publishing of the content that will typically be delivered via an LMS. Users can both create and re-use content and reduce duplicated development efforts.
- MOODLE is a popular open source LMS.
- There are several organizations working toward standards and to make sure learning content is 'interoperable' with various learning management technologies. The e-learning standards support- Interoperability, durability, manageability, re-usability, and accessibility. These standards focus on content metadata, content packaging, and run-time communication to support tracking of student activities.

Banking Software

Core Banking Solution (CBS)

Core Banking Solution (CBS) is networking of bank branches, which allows customers to manage their accounts, and use various banking facilities from any part of the world. In simple terms, there is no need to visit your own branch to do banking transactions. You can do it from any location, any time. You can enjoy banking services from any branch of the bank which is on CBS network regardless of branch you have opened your account. For the bank which implements CBS, the customer becomes the bank's customer instead of customer of particular branch.

Execution of Core banking system across all branches helps to speed up most of the common transactions of bank and customer. In Core banking, the all branches access banking applications from centralized server which is hosted in secured Data Centre. Banking software/application performs basic operations like maintaining transactions, balance of withdrawal & payment, interest calculations on deposits & loans etc. This banking applications are deployed on centralized server & can be accessed using internet from any location.

Need for [Core Banking Technology](#)

Nowadays, the use of Information Technology (IT) is must for the survival & growth of any organization and same applicable to banking industry also. By using IT in any industry, banks can minimize the operation cost; also banks can offer products & services to customers at competitive rates.

CBS is required;

To meet the dynamically changing market & customer needs.

To improve & simplify banking processes so that bank staff can focus on sales & marketing stuff.

Convenience to customer as well as bank.

To speed up the banking transactions.

To expand presence in rural & remote areas.

Basic elements of CBS that helps customers are:

Internet Banking

Mobile Banking

ATM

POS & kiosk systems

Fund Transfers – NEFT, RTGS, IMPS etc.

Benefits of Core banking –

Core banking solutions are beneficial to both banks as well as customers.

A. Benefits for Customers

Quicker services at the bank counters for routine transactions like cash deposits, withdrawal, passbooks, statement of accounts, demand drafts etc.

Anywhere banking by eliminating branch banking.

Provision of banking services 24 X 7.

Fast payment processing through Internet banking, mobile banking.

Anytime anywhere banking through ATMs.

All branches access applications from central servers/datacentre, so deposits made in any branch reflects immediately and customer can withdraw money from any other branch throughout the world.

CBS is very helpful to people living in rural areas. The farmers can receive e-payments towards subsidy etc. in his account directly. Transfer of funds from the cities to the villages and vice versa will be done easily.

B. Benefits for Banks

Process standardization within bank & branches.

Retention of customers through better customer service.

Accuracy in transactions & minimization of errors.

Improved management of documentation & records – having centralized databases results in quick gathering of data & MIS reports.

Ease in submission of various reports to the Government & Regulatory boards like RBI.

Convenience in opening accounts, processing cash, servicing loans, calculating interest,

implementing change in policies like changing interest rates etc.

To cope up with the growing needs of customers; RRBs and Co-operative banks were needed to implement core banking solutions. To face the challenges of dynamic market, UCBs needed to take help of IT their operations. Considering the importance of the matter, the Reserve Bank of India (RBI) mandated a deadline for Urban Co-operative Banks (UCBs) and advised to implement the core banking solutions (CBS) by December 31, 2013, which has been met by all RRBs and UCBs.

Srinivas Kante

Web Server

A Web server is a program that uses HTTP (Hypertext Transfer Protocol) to serve the files that form Web pages to users, in response to their requests, which are forwarded by their computers' HTTP clients. Dedicated computers and appliances may be referred to as Web servers as well.

The process is an example of the [client/server](#) model. All computers that host Web sites must have Web server programs. Leading Web servers include [Apache](#) (the most widely-installed Web server), Microsoft's Internet Information Server ([IIS](#)) and nginx (pronounced engine X) from NGNIX.

a) Apache Web Server

Apache is the most popular web server in the world developed by the Apache Software Foundation. Apache is an open source software and can be installed on almost all operating systems including Linux, Unix, Windows, FreeBSD, Mac OS X and more. About 60% of machines run on Apache Web Server.

An Apache server can be customized easily as it contains a modular structure. It is also an open source which means that you can add your own modules to the server when to require and make modifications that suit your specific needs. It is more stable than any other web servers and is easier to solve administrative issues. It can be install on multiple platforms successfully. Recent Apache releases provide you the feasibility of handling more requests when you compare to its earlier versions.

b) IIS Web Server

IIS is a Microsoft product. IIS server has all the features just like Apache. But it is not an open source and more over personal modules cannot be added easily and modification becomes a

little difficult job. Microsoft developed, maintains it, and thus it works with all the Windows operating system platforms. Also, they had good customer support if it had any issues.

c) Nginx Web Server

Nginx is another free open source web server, it includes IMAP/POP3 proxy server. Nginx is known for its high performance, stability, simple configuration and low resource usage. This web server doesn't use threads to handle requests rather a much more scalable event-driven architecture which uses small and predictable amounts of memory under load. It is getting popular in the recent times and it is hosting about 7.5% of all domains worldwide.

Most of the web hosting companies select web server based on clients requirement, the number of clients on a single server, the applications/software clients use and the amount of traffic they generate that could handle by a web server. Web servers often come as part of a larger package of Internet- and intranet-related programs for serving email, downloading requests for File Transfer Protocol ([FTP](#)) files, and building and publishing Web pages. Considerations in choosing a Web server include how well it works with the operating system and other servers, its ability to handle server-side programming, security characteristics, and the particular publishing, search engine and site building tools that come with it.

Application Server

The application server is the middleman between browser-based front-ends and back-end databases and legacy systems.

This is the server on which the organization's created applications which are utilizing our database, web service, etc. This application server will host business layer (wrapped with web services), scheduled jobs, windows services, etc. This is a middle-tier business logic application or set of applications, possibly on a local area network or intranet server. Also called an app server, an application server is a program that handles all application operations between users and an organization's backend business applications or databases.

An application server is typically used for complex transaction-based applications. To support high-end needs, an application server has to have built-in redundancy, monitor for high-availability, high-performance distributed application services and support for complex database access. In many usages, the application server combines or works with a Web (Hypertext Transfer Protocol) server and is called a Web application server. The Web browser supports an easy-to-create HTML-based front-end for the user.

The Web server provides several different ways to forward a request to an application server and to forward back a modified or new Web page to the user. These approaches include the [Common Gateway Interface](#) (CGI), [FastCGI](#), Microsoft's [Active Server Page](#), and the [Java Server Page](#). In some cases, the Web application servers also support request "brokering" interfaces such as [CORBA](#) Internet Inter-ORB Protocol ([IIOP](#)).

Example of Application Servers are:

JBoss: Open-source server from JBoss community.

Sun Glassfish: Provided by Sun Microsystems. Now acquired by Oracle.

Oracle Weblogic: Provided by Oracle. It more secured.

IBM Websphere: Provided by IBM.

Database Server

[Legacy application](#) databases and transaction management applications are part of the back end or third tier. See figure 9.3. The database is generally installed on a different server which is called a Database server. A third-tier, [back-end](#), database and transaction server, sometimes on a mainframe or large server. Database server will have your one or more database hosted such as Oracle, SQL Server, MySql, etc.

Network Domain

A domain, in the context of networking, refers to a group of [computers](#) and [devices](#) on a [network](#) that are administered as a unit with common rules and procedures. Within the [Internet](#), domains

are defined by the [IP address](#). All devices sharing a common part of the IP address are said to be in the same domain. There are also many types of subdomains.

A domain has a domain controller that governs all basic domain functions and manages network security. Thus, a domain is used to manage all user functions, including username/password and shared system resource authentication and access. A domain is also used to assign specific resource privileges, such as user accounts.

In a simple network domain, many computers and/or workgroups are directly connected. A domain is comprised of combined systems, servers and workgroups. Multiple server types may exist in one domain - such as Web, database and print - and depend on network requirements.

On the other hand, domain names are used to identify one or more IP addresses. For example, the domain name microsoft.com represents about a dozen IP addresses. Domain names are used in URLs to identify particular Web pages

Windows Domain

A Windows domain is a form of a [computer network](#) in which all [user accounts](#), computers, printers and other [security principals](#), are registered with a central database located on one or more clusters of central computers known as [domain controllers](#). Authentication takes place on domain controllers. Each person who uses computers within a domain receives a unique user account that can then be assigned access to resources within the domain. Starting with [Windows 2000, Active Directory](#) is the Windows component in charge of maintaining that central database. The concept of Windows domain is in contrast with that of a [workgroup](#) in which each computer maintains its own database of security principals.

Computers can connect to a domain via [LAN, WAN](#) or using a [VPN](#) connection. Users of a domain are able to use enhanced security for their VPN connection due to the support for a [certification authority](#) which is gained when a domain is added to a network, and as a result [smart cards](#) and [digital certificates](#) can be used to confirm identities and protect stored information.

In a Windows domain, the directory resides on computers that are configured as "[domain controllers](#)." A domain controller is a Windows or [Samba](#) server that manages all security-related aspects between user and domain interactions, centralizing security and administration. A domain controller is generally suited for businesses and/or organizations when more than 10 PCs are in use. A domain does not refer to a single location or specific type of network configuration. The computers in a domain can share physical proximity on a small [LAN](#) or they can be located in different parts of the world. As long as they can communicate, their physical position is irrelevant.

Where [PCs](#) running a Windows operating system must be integrated into a domain that includes non-Windows PCs, the free [open source](#) package [Samba](#) is a suitable alternative. Whichever package is used to control it, the database contains the user accounts and security information for the resources in that domain.

Data Storage Devices

Alternatively referred to as digital storage, storage, storage media, or storage medium, a storage device is any [hardware](#) capable of holding information either temporarily or permanently.

There are two types of storage devices used with computers: a [primary storage](#) device, such as [RAM](#), and a [secondary storage](#) device, like a [hard drive](#). Secondary storage can be [removable](#), [internal](#), [external](#) or network storage. Some examples of data storage devices are discussed as below:

Magnetic storage devices

Today, [magnetic storage](#) is one of the most common types of storage used with computers and is the technology that many computer hard drives use. Examples are [Floppy diskette](#), [Hard drive](#), [Magnetic strip](#), [SuperDisk](#), [Tape cassette](#) and [Zip diskette](#).

Optical storage devices

Another common storage is [optical storage](#), which uses lasers and lights as its method of reading and writing data. Examples are [Blu-ray disc](#), [CD-ROM disc](#), [CD-R and CD-RW disc](#), [DVD-R](#), [DVD+R](#), [DVD-RW and DVD+RW disc](#).

Flash memory devices

[Flash memory](#) has started to replace magnetic media as it becomes cheaper as it is the more efficient and reliable solution. e.g., [Jump drive or flash drive](#), [Memory card](#), [Memory stick](#), and SSD (Solid State Drive).

Online and cloud

Storing data online and in cloud storage is becoming popular as people need to access their data from more than one device. Examples are [Cloud storage](#) and Network media such as NAS (Network Attached Storage) & SAN (Storage Area Network).

Paper storage

Early computers had no method of using any of the above technologies for storing information and had to rely on paper. Today, these forms of storage are rarely used or found. In the picture to the right is an example of a woman entering data to a punch card using a punch card machine. Examples are OMR and Punch Card.

Most of the storage device examples mentioned are no longer used with today's computers which primarily use a hard disk drive or SSD to store information and have the options for USB flash drives and access to cloud storage. Desktop computers with disc drives typically use a disc drive that is capable of reading CD's and DVD's and writing CD-R and other recordable discs.

For most computers, the largest storage device is the [hard drive](#) or [SSD](#). However, networked computers may also have access to even larger storage with large [tape drives](#), [cloud computing](#), [NAS](#) or SAN storage devices. Below is a list of storage devices from the smallest capacity to the largest capacity.

Desired Features of Mobile Banking

Apps are fast becoming the primary way to interact with consumers - When banks first launched apps, they were convenient tools to check your balance and keep on top of your spending. However, consumers are expecting - and banks are delivering - ever more functionality. Particularly with younger consumers, apps are becoming critical to attracting and retaining consumers. The benchmarks for ranking a mobile banking are;

- range of touchpoints,
- enrollment and login,
- account information,

- transactional functionality,
- service features,

- cross channel guidance, and
- marketing and sales.

Some of the important desired features in a mobile banking app across the world and India are as follows:

Download apps for a range of smartphone operating systems. This is one of the greatest challenges -to make the app work across operating systems with various versions of each. Downloadable smartphone apps let digital banking teams use device-specific features to create a smoother and more intuitive experience for mobile banking customers. Although some operating systems are more important in some countries than others, the major four operating systems are - Android, BlackBerry OS, iOS, and Windows Phone.

Easily complete banking tasks via a mobile website. Many customers use the browser on their mobile device to access their bank account information, pay bills on the run, or make other mobile transactions — and today they expect to perform these tasks without the hassle of pinching and zooming their way through a mobile-unfriendly web experience.

Interact with the bank via SMS. Most banks report falling use of SMS text messaging relative to other mobile banking touchpoints. Yet some consumers — especially those who do not have a smartphone — continue to use text banking.

Enroll in mobile banking directly from their smartphone. As younger generations start opening their first bank accounts, the proportion of customers who are mobile-first and mobile-only will rise. Digital banking teams need to enable customers to register for digital banking directly from their mobile devices — rather than forcing them to sign up for online banking first.

Understand how to use mobile banking. As content and functionality become more extensive, with leading banks offering regular mobile updates, it's important that digital banking teams communicate these improvements and guide new users through how to use mobile banking.

Easily access security and privacy content. Many customers who are just starting to use mobile banking worry about privacy and security, while others might want to be reassured in specific situations. This area still remains a weak spot for many retail banks.

Get valuable content and account information pre-login. Digital banking teams have recognized that customers don't need to be logged in for every banking task and that many like the convenience of accessing simple information without needing to enter a password. Log in

easily. Banks must make the mobile banking login process as painless as possible, without compromising security. Leading banks do this by using multifactor authentication the first time customers use the app, then letting them use a simplified login subsequently. Many banks offer convenient features, such as a “remember this device” option and the ability to save user names, and they let users opt into an abbreviated login process using a simple PIN code rather than entering a full alphanumeric password.

Log in easily. Banks must make the mobile banking login process as painless as possible, without compromising security. Leading banks do this by using multifactor authentication the first time customers use the app, then letting them use a simplified login subsequently. Many banks offer convenient features, such as a “remember this device” option and the ability to save user names, and they let users opt into an abbreviated login process using a simple PIN code rather than entering a full alphanumeric password.

Quickly work out how to achieve their mobile banking goals. The mobile screen customers land on immediately after logging in is a crucial part of their mobile banking experience. Digital banking teams must design screens that make it easy for customers to complete the tasks they logged into mobile banking to do. Most leading banks display prominent one-click links to the most common tasks directly on the home screen.

Quickly and conveniently find transactions. Different customers will search their transaction history with different search tools, according to personal preferences: Many banks are expanding the transaction history tools available via mobile. See an accurate forecast for their spending. A growing number of banks provide customers with a “future view” of their upcoming payments and transfers. And some are even using predictive tools to include transactions the customer hasn't yet set up.

Better understand their financial lives with embedded money management tools. Digital money management will ultimately be embedded at the heart of digital banking. Not all money management features make sense for mobile touchpoints, but digital teams should offer simple, integrated, and

contextual tools that help customers quickly and easily get the information they want or take the action they need.

Move money without hassles. Overall, the banks offer strong and easy mobile money movement functionality such as account-to-account and P2P money transfers.

Send money to other people without sensitive personal details- This is one of the important desired features in most of the countries.

Buy items in stores without plastic. It is observed that digital wallets integrating offers, coupons, point-of-sale (POS) payments, and loyalty rewards are poised to transform the way consumers shop and make payments.

Solve account issues within the mobile app. Self-service features let a customer initiate or complete a request without having to interact with a bank employee. Functionality that lets a customer dispute a card transaction, report fraud, or order a new debit card is not widely available on banks' mobile banking apps.

Set up, receive, and manage alerts. Alerts continue to offer great value to customers. Just a few years ago, customers were content to set up and manage alerts via the bank's secure website and receive the alerts via SMS or email. But behavior is changing with the mobile mind shift, and an

increasing number of banks are differentiating themselves by offering alerts delivery and management within the mobile banking app.

Find branches and ATMs. Most of the banks evaluated make it easy for customers to find nearby branches and ATMs, including key information such as hours of operation and providing step-by-step directions.

Easily apply for a new product, account, or service. Application abandonment has been an issue for digital sales teams at banks for years, and the physical limitations of mobile devices can amplify the problem. Someone trying to open a new account is more likely to give up if he or she needs to pinch and zoom through the task flow while also entering information into dozens of data entry fields. So cross-selling effectively means making buying as easy and quick as possible for a customer. For example, mBank has developed simplified product applications with two-step task flows and embedded them within mobile banking.

INTERNET SERVICE PROVIDERS / HOSTING / BANDWIDTH / DATA DOWNLOAD & UPLOAD

In a typical world scenario, we come across Internet Service Providers (ISPs) advertising about “high speed internet”. But when we look at our own internet connections, the download speeds seems to be far below compared to what has been advertised. So what did your ISP actually mean by “Connection Speed”? Is “Connection Speed” totally different from “Download Speed”?

Connection Speeds and Download Speeds

People often confuse connection speed with downloading speed. Though both of these terms refer fairly to the same thing, their interpretation is slightly different from one another.

Connection speed (or Internet Bandwidth) refers to the raw data transfer rate of the connection provided by your ISP. This is the property that is usually advertised and can vary largely among different providers and data plans. Nowadays, this figure is usually expressed in terms of Kbps (Kilobit per Second) or Mbps (Megabit per Second).

On the other hand, when we download files from the internet, the same data transfer rate is interpreted as Download Speed. Download speed is usually measured in KBps (Kilobyte per second).

A Typical Scenario

Say you have a 1 Mbps Internet connection. With such a connection speed, you might expect to download files at a rate of around 1 MB per second, but when you actually download a file, the download speed only reaches up to 100 – 120 KB per second.

Where's the catch? If connection speed and download speed are fairly one and the same, as we mentioned earlier, then we should be ideally getting the same speed for connection and download. So what's missing here?

Actually, connection and download speeds are measured in two different units, so even though these measurements refer to the same thing, their interpreted values turn out to be quite different.

Connection v/s Download (Units)

Unit used for Connection Speed: Kbps (Kilobit per Second), Mbps (Megabit per Second), Gbps (Gigabit per Second) and so on...

Unit used for Download Speed: KBps (Kilobyte per Second), MBps (Megabyte per Second) and so on.

Relation between bit and byte

1 byte = 8 bit
1 kilobyte (KB) = 8 kilobit (Kb)

Why different units are used for measuring connection and download speed?

A Bit is the most fundamental unit of representing data. That is why it was adopted as a standard for measuring the raw data transfer rate, which refers to the connection speed. Hence, connection speeds are measured in Megabit per second (Mbps).

But a bit in itself is quite meaningless. The data in your computer is stored in the form of 8 bit blocks, known as a byte. So when you download any file from the internet, it is generally represented in Byte. Hence, download speed is usually measured in Kilobyte per second (KBps).

The noteworthy point here is the difference between bit and byte as used in the two units. Connection speed is represented with a (small) 'b' for bit while download speed takes a (capital) 'B' for Byte. Let us have a deeper look at the two units.

1 Megabyte (MB) = 8 Megabit (Mb)

1 Megabyte (MB) = 1024 Kilobyte (KB)

8 Megabit (Mb) = 1024 Kilobyte (KB)

Therefore, 1 Megabit (Mb) = $[1024/8 =]$ 128 Kilobyte (KB)

So, in a 1 Mbps connection, your maximum download speed would be 128 KBps (=1Mbps). And this convention kind of suits the ISPs too, as it helps them to lure consumers into visually greater figures.

Factors affecting Download Speeds

So, we should get a maximum download speed of 128 KBps on a 1 Mbps connection. But practically, we would only be able to download files at 80 KBps – 120 KBps on average. The fall in the download rate can be attributed to several external and internal factors.

External factors affecting download speeds

Your downloading speed is affected by several server-side factors:

Packet delivery method: The data that you download from the internet are received by your device in the form of packets. Each of these packets contain additional information, like sender and receiver address, etc. These information, referred to as message headers, make up a considerable

part of the data that is downloaded; but is discarded once it reaches the client. The size of each packet and the size of the header information it contains, varies among different hosts.

Server capacity: File downloading speed also depends on the host's network speed. The server you are downloading from should be able to serve the file at a greater speed than your own connection speed. Otherwise, your download speed will be limited to the maximum speed at which the server can serve.

Server load: Capacity is not the only factor affecting the server's serving speed. Sometimes, a server which is serving too many parallel requests might throttle connections and regulate the bandwidth utilized by each connection. In that case, the server limits the maximum bandwidth available for you to download a particular file. More the load on the server, more would be the number of parallel requests it is processing, hence less will be the maximum bandwidth available for you to download.

Routing: A download request can reach the destination server in multiple ways. Generally, the shortest possible route is selected. But the maximum available download bandwidth will be fairly dependent on the distance between the server's location and the client's location. If you are downloading from a server near you, more bandwidth will be available for downloading. But if the server is far from your location, available bandwidth would be reduced as some of it is consumed by the routing process.

Internal factors affecting download speeds

Download speed may also depend on several internal / device factors:

Network Interface Controller (NIC): Network adapters vary in specifications from manufacturer to manufacturer. If the network adapter in your device cannot fully utilize the connection speed, you won't be able to achieve the maximum download speed provided by your ISP.

Operating System (OS): Your device's operating system runs a few background services that is used to establish and maintain the connection related activities. These OS level services consume some bandwidth to run their operations. However, the amount of bandwidth consumed by these services vary from OS to OS.

Disk Read/Write Speed: This is not usually a crucial factor unless you're on a very high speed internet connection or using a hard drive with very low R/W speed. But if your device is not able to write the data to the disk fast enough, a faster connection won't be useful. In other words, the connection speed should be less than you disk speed.

Bandwidth limitation in file hosting sites

A lot of file hosting websites and services (for ex. RapidShare) offer file downloads at two different schemes. A free regular download, where your download speed, bandwidth, number of parallel connection, auto resume capability, etc. are limited, and some paid Premium plans which remove these limitations. The same server may be capable of handling both types of requests. Here, the server controls the speed and bandwidth for individual connections.

If the connections are from paid users, speed / bandwidth caps are lifted and they get to utilize full server resources. Other users, however, only get to use a small portion of these resources for a

limited amount of time. Sometimes, parallel connections from the same IP is also restricted. In that case, even your download manager won't be able to download any faster than your regular speed.

Premium plans in these kind of file hosting services allow you to utilize their full bandwidth. However, it does not mean that you will get more speed and bandwidth than your local ISP can provide. So, even though a particular server allows you to download, say at 2000 KBps; on a 2Mbps connection, you can only utilize up to 256 KBps.

Downloading via Download Managers

Regular downloaders that are integrated with web browsers download files through a single connection. To enhance downloading speeds, third party download manager applications (For example; IDM, DAP, Orbit Downloader, etc.) are available which are able to set up multiple connections in parallel to download a file. Of course, this feature can be primarily controlled by server restrictions. However, if allowed, download managers can simultaneously download several parts of the file and hence improve the overall downloading speed.

Downloading from Torrents

Torrent downloads work in a different way than regular downloads. Instead of the conventional client-server model, this technology is based on a peer-to-peer model (P2P). In this model, data can flow universally among number of connected users, known as peers. A file being shared on P2P is distributed across the entire network.

There are two types of Peer –Seeder and Leecher. Seeders are users uploading data in the network, and leechers are those who are downloading it. In a torrent network, if there are more number of leechers than seeders, downloading speed might decrease as there are more nodes downloading the data than

those who are uploading. On the other hand, if there are more number of seeders, downloading speed might be higher.

Torrent downloads can, in fact, be faster than regular downloads, since there are numerous active parallel connections to download parts of the data. Nodes can connect to a torrent network via BitTorrent clients. Once peers complete download, they can also seed it for other leechers to download from.

You can find out your own connection speed by performing an online test. Speedtest.net is a good web application to rate your connection in terms of Download and Upload speed.

Connection speed and download speed are fairly the same thing, only measured in different units. So, to get download speed (in KBps) from connection speed (in Mbps), first multiply the connection speed by 1024 to convert from Megabit (Mb) to Kilobit (Kb), and then divide by 8 to convert it from Kilobit (Kb) to Kilobyte (KB).

Cheque Truncation System (CTS) or Image-based Clearing System (ICS), in India, is a project of the Reserve Bank of India (RBI), commencing in 2010, for faster clearing of cheques. CTS is based on a cheque truncation or online image-based cheque clearing system where cheque images and magnetic ink character recognition (MICR) data are captured at the collecting bank branch and transmitted electronically.

Cheque truncation means stopping the flow of the physical cheques issued by a drawer to the drawee branch. The physical instrument is truncated at some point en-route to the drawee branch and an electronic image of the cheque is sent to the drawee branch along with the relevant information like the MICR fields, date of presentation, presenting banks etc. This would eliminate the need to move the physical instruments across branches, except in exceptional circumstances, resulting in an effective reduction in the time required for payment of cheques, the associated cost of transit and delays in processing, etc., thus speeding up the process of collection or realization of cheques.

CTS has been implemented in New Delhi, Chennai and Mumbai with effect from February 1, 2008, September 24, 2011 and April 27, 2013 respectively. After migration of the entire cheque volume from MICR system to CTS, the traditional MICR-based cheque processing has been discontinued across the country. The CTS-2010 compliant cheques are both image friendly and have enhanced security features. All banks providing cheque facility to their customers have been advised to issue only 'CTS-2010' standard cheques. Cheques not complying with CTS-2010 standards would be cleared at less frequent intervals i.e. weekly once from November 1, 2014 onwards.

Banks derive multiple benefits through the implementation of CTS, like a faster clearing cycle meaning technically possible realization of proceeds of a cheque within the same day. It offers better reconciliation/ verification, better customer service and enhanced customer window. Operational efficiency provides a direct boost to bottom lines of banks as clearing of local cheques is a high cost low revenue activity. Besides, it reduces operational risk by securing the transmission route. Centralized image archival systems ensure that data storage and retrieval is easy. Reduction of manual tasks leads to reduction of errors. Real-time tracking and visibility of the cheques, less frauds with secured transfer of images to the RBI are other benefits that banks derive from this solution.

NG RTGS-Next Generation RTGS

NG-RTGS has been introduced in India since October 2013. With its advanced liquidity and queue management features, the new RTGS system is expected to significantly improve the efficiency of financial markets. He hoped the new RTGS system would be such a driver for India's financial system.

Reportedly the first in the world to be built on ISO 20022 messaging standards, the new RTGS system is highly scalable and will have several new functionalities. These include advance liquidity features, including gridlock resolution mechanism and hybrid settlement facility, facility to accept future value dated transactions, options to process multi-currency transactions, etc. These functionalities, as and when made available for use, will be notified to the participants.

The new ISO 20022 compliant RTGS system provides three access options to participants thick-client, Web-API (through INFINET or any other approved network) and Payment Originator module. The participants can decide the mode of participation in the system based on the volume of transactions and the cost of setting up the infrastructure.

The RTGS infrastructure in India is critical in facilitating the orderly settlement of payment obligations. The role of central banks as operators of large-value payment systems is important in the context of the broader role of the central bank in a nation's financial system insofar as it offers safety net attributes by providing final settlement in central bank money.

RTGS is a critical Financial market Infrastructure (FMI) operated by the Reserve Bank of India and it will be assessed against the Committee on Payment and Settlement Systems and the International Organisation of Securities Commissions (CPSS-IOSCO) Principles for Financial Market Infrastructures applicable to FMIs.

With implementation of the new RTGS system, the existing RTGS system will cease to be operational. Further, the RTGS System Regulations 2013 would replace the RTGS (Membership) Business Operating Guidelines, 2004 and RTGS (Membership) Regulations, 2004.

National Electronic Fund Transfer (NEFT)

National Electronic Funds Transfer (NEFT) is a nation-wide payment system maintained by Reserve Bank of India (RBI), facilitating one-to-one funds transfer. Under this Scheme, individuals, firms and corporates can electronically transfer funds from any bank branch to any individual, firm or corporate having an account with any other bank branch in the country participating in the Scheme. Against the principle of RTGS which is a Real-Time as well as Gross Settlement system, NEFT settlement happens in batches.

For being part of the NEFT funds transfer network, a bank branch has to be NEFT- enabled. The list of bank-wise branches which are participating in NEFT is provided in the website of Reserve Bank of India.

Individuals, firms or corporates maintaining accounts with a bank branch can transfer funds using NEFT. Even such individuals who do not have a bank account (walk-in customers) can also deposit cash at the NEFT-enabled branches with instructions to transfer funds using NEFT. However, such cash remittances will be restricted to a maximum of Rs.50,000/- per transaction. Such customers have to furnish full details including complete address, telephone number, etc. NEFT, thus, facilitates originators or remitters to initiate funds transfer transactions even without having a bank account.

Individuals, firms or corporates maintaining accounts with a bank branch can receive funds through the NEFT system. It is, therefore, necessary for the beneficiary to have an account with the NEFT enabled destination bank branch in the country.

The NEFT system also facilitates one-way cross-border transfer of funds from India to Nepal. This is known as the Indo-Nepal Remittance Facility Scheme. A remitter can transfer funds from any of the NEFT-enabled branches in to Nepal, irrespective of whether the beneficiary in Nepal maintains an account with a bank branch in Nepal or not. The beneficiary would receive funds in Nepalese Rupees.

Limit on the amount that could be transferred using NEFT – No. There is no limit – either minimum or maximum – on the amount of funds that could be transferred using NEFT. However, maximum amount per transaction is limited to Rs.50,000/- for cash-based remittances within India and also for remittances to Nepal under the Indo-Nepal Remittance Facility Scheme.

Operating hours of NEFT - Unlike Real-time gross settlement (RTGS), fund transfers through the NEFT system do not occur in real-time basis. NEFT settles fund transfers in half-hourly

batches with 23 settlements occurring between 8:00 AM and 7:00 PM on week days. Transfers initiated outside this time period are settled at the next available window. No settlements are made on the second and fourth Saturday of the month or on Sundays.

Process of NEFT system - An individual / firm / corporate intending to originate transfer of funds through NEFT has to fill an application form providing details of the beneficiary (like name of the beneficiary, name of the bank branch where the beneficiary has an account, IFSC of the beneficiary bank branch, account type and account number) and the amount to be remitted. Customers enjoying net banking facility offered by their bankers can also initiate the funds transfer request online. Some banks offer the NEFT facility even through the ATMs.

The originating bank branch prepares a message and sends the message to its pooling centre (also called the NEFT Service Centre). The pooling centre forwards the message to the NEFT Clearing Centre (operated by National Clearing Cell, Reserve Bank of India, Mumbai) to be included for the next available batch.

The Clearing Centre sorts the funds transfer transactions destination bank-wise and prepares accounting entries to receive funds from the originating banks (debit) and give the funds to the destination banks (credit). Thereafter, bank-wise remittance messages are forwarded to the destination banks through their pooling centre (NEFT Service Centre).

Finally, the destination banks receive the inward remittance messages from the Clearing Centre and pass on the credit to the beneficiary customers' accounts.

IFSC- IFSC or Indian Financial System Code is an alpha-numeric code that uniquely identifies a bank-branch participating in the NEFT system. This is an 11 digit code with the first 4 alpha characters

representing the bank, and the last 6 characters representing the branch. The 5th character is 0 (zero). IFSC is used by the NEFT system to identify the originating / destination banks / branches and also to route the messages appropriately to the concerned banks / branches.

Acknowledgement by SMS - In case of successful credit to the beneficiary's account, the bank which had originated the transaction is expected to send a confirmation to the originating customer (through SMS or e-mail) advising of the credit as also mentioning the date and time of credit. For the purpose, remitters need to provide their mobile number / e-mail-id to the branch at the time of originating the transaction.

Tracking an NEFT transaction - The remitter can track the NEFT transaction through the originating bank branch or its CFC using the unique transaction reference number provided at the time of initiating the funds transfer. It is possible for the originating bank branch to keep track and be aware of the status of the NEFT transaction at all times.

Benefits of using NEFT:

NEFT offers many advantages over the other modes of funds transfer:

The remitter need not send the physical cheque or Demand Draft to the beneficiary. 41

The beneficiary need not visit his / her bank for depositing the paper instruments.

The beneficiary need not be apprehensive of loss / theft of physical instruments or the likelihood of fraudulent encashment thereof.

Cost effective.

Credit confirmation of the remittances sent by SMS or email.

Remitter can initiate the remittances from his home / place of work using the internet banking also.

Near real time transfer of the funds to the beneficiary account in a secure manner.

NEFT has gained popularity due to its saving on time and the ease with which the transactions can be concluded. Introduction of Immediate Payment Services (IMPS) by National Payments Corporation of India (NPCI), which is gaining popularity reduces the burden on NEFT systems at RBI.

National Payments Corporation of India (NPCI) – Its Products & Services

National Payments Corporation of India (NPCI), is the umbrella organisation for all retail payment systems in India, which aims to allow all Indian citizens to have unrestricted access to e-payment services.

Founded in 2008, NPCI is a not-for-profit organisation registered under section 8 of the Companies Act 2013. The organisation is owned by a consortium of major banks,^[3] and has been promoted by the country's central bank, the Reserve Bank of India. Its recent work of developing Unified Payments Interface aims to move India to a cashless society with only digital transactions.

It has successfully completed the development of a domestic card payment network called RuPay, reducing the dependency on international card schemes. The RuPay card is now accepted at all the

ATMs, Point-of-Sale terminals and most of the online merchants in the country. More than 300 cooperative banks and the Regional Rural Banks (RRBs) in the country have also issued RuPay ATM cards.

More than 250 million cards have been issued by various banks, and it is growing at a rate of about

3 million per month. A variant of the card called 'Kisan Card' is now being issued by all the Public

Sector Banks in addition to the mainstream debit card which has been issued by 43 banks. RuPay cards are also issued under the Jan Dhan Yojana scheme.

NPCI has taken over NFS (National Financial Switch) operations from 14 December 2009 from IDRBT. Membership regulations and rules are being framed for enrolling all banks in the country as members so that when the nationwide payment systems are launched, all would get included on a standardized platform.

The key products of NPCI are:

National Financial Switch (NFS) which connects 1, 98, 953 ATMs of 449 banks (91 Member Banks, 358 Sub- Member). Immediate Payment Service (IMPS) provided to 84 member banks, with more than 8.49 crore MMID (Mobile Money Identifier) issued, and crossed 10 million transactions.

National Automated Clearing House (NACH) - has close to 400 banks on board. Aadhaar Payments Bridge System (APBS) has more than 358 banks. Cheque Truncation System (CTS)

has fully migrated in 3 grids - southern, western & northern grids from MICR centres. Aadhaar-enabled payment system (AEPS) - has 36 member banks. RuPay – Domestic Card Scheme- has issued over 20 crore cards and enabled 10, 70, 000 PoS terminals in the country. The newest and most advanced addition to the NPCI revolution is the Unified Payments Interface (UPI) which has been launched on 11 April 2016.

RuPay PaySecure - Over 20 banks now offer this authentication mechanism to their RuPay cardholders. The new transaction flow of Card + OTP has infused more simplicity to cardholders. More than 70,000 merchants accept Rupay cards online. RuPay PaySecure is live on 10 acquiring banks which includes Union Bank of India, Kotak Mahindra Bank, Citi Bank, ICICI Bank, HDFC Bank, State Bank of India, IDBI Bank, IndusInd Bank, Bank of Baroda and Bank of India.

NPCI service portfolio now and in the near future include:

National Financial Switch (NFS) - network of shared automated teller machines in India. Unified Payment Interface (UPI) - Single mobile application for accessing different bank accounts

BHIM App - Smartphone app built using UPI interface.

Immediate Payment Service (IMPS) - Real time payment with mobile number. *99# - mobile banking using USSD

National Automated Clearing House (NACH)-

Cheque Truncation System -online image-based cheque clearing system
Aadhaar Payments Bridge System (APBS) -

Bharat Bill Payment System (BBPS) - integrated bill payment system

IMPS (Immediate Payment Services)

Immediate Payment Service (IMPS) is an instant real-time inter-bank [electronic funds transfer](#) system in [India](#). IMPS offers an inter-bank electronic fund transfer service through mobile phones. Unlike [NEFT](#) and [RTGS](#), the service is available 24/7 throughout the year including bank holidays. When one initiates a fund transfer via IMPS, the initiator bank sends a message to IMPS, which debits the money and sends it to the receiving account. All this happens within 5-10 seconds.

IMPS is an innovative real time payment service that is available round the clock. This service is offered by National Payments Corporation of India (NPCI) that empowers customers to transfer money instantly through banks and RBI authorized Prepaid Payment Instrument Issuers (PPI) across India.

Benefits of IMPS

Instant

Available 24 x7 (functional even on holidays) Safe and secure, easily accessible and cost effective

Channel Independent can be initiated from Mobile/ Internet / ATM channels

- ☐ Debit & Credit Confirmation by SMS to both sender and receiver

National Unified USSD Platform (NUUP):

NUUP (National Unified USSD Platform) is a USSD based mobile banking service from NPCI that brings together all the Banks and Telecom Service Providers. In NUUP, a customer can access banking services by just pressing *99# from his/her mobile phones. This service works across all GSM mobile handsets.

IMPS transactions can be sent and received 24X7, (round the clock), including on holidays. Both sender & receiver get SMS confirmation.

For using IMPS on mobile phones, a customer will have to register for mobile banking with his/her individual bank. However, for initiating IMPS using Bank branch, Internet banking and ATM channels, no prior Mobile banking registration is required. Both banked as well as un-banked customer can avail IMPS. However, unbanked customer can initiate IMPS transaction using the services of Pre-Paid Payments instrument issuer (PPI). MMID - Mobile Money Identifier is a 7 digit number, issued by banks. MMID is one of the input which when clubbed with mobile number facilitates fund transfer. Combination of Mobile no. & MMID is uniquely linked with an Account number and helps in identifying the beneficiary details. Different MMID's can be linked to same Mobile Number. (Please contact your bank for getting the MMID issued)

Options available for a customer for doing IMPS transaction

- Using Beneficiary Mobile no. and MMID
- Using Beneficiary Account no. and IFS Code
- Using Beneficiary Aadhaar Number

Bharat Interface for Money (BHIM)

Bharat Interface for Money (BHIM) is an app that lets you make simple, easy and quick payment transactions using Unified Payments Interface (UPI). You can make instant bank-to-bank payments and Pay and collect money using just Mobile number or Virtual Payment Address (VPA).

The following are the features of BHIM:

1. Send Money: User can send money using a Virtual Payment Address (VPA), Account Number & IFSC, Aadhaar Number or QR code.
2. Request Money: User can collect money by entering Virtual Payment Address (VPA). Additionally through BHIM App, one can also transfer money using Mobile No. (Mobile No should be registered with BHIM or *99# and account should be linked)
3. Scan & Pay: User can pay by scanning the QR code through Scan & Pay & generate your QR option is also present.
4. Transactions: User can check transaction history and also pending UPI collect requests (if any) and approve or reject. User can also raise complaint for the declined transactions by clicking on Report issue in transactions.

5. Profile: User can view the static QR code and Payment addresses created or also share the QR code through various messenger applications like WhatsApp, Email etc. available on phone and download the QR code.
6. Bank Account: User can see the bank account linked with his/her BHIM App and set/change the UPI PIN. User can also change the bank account linked with BHIM App by clicking Change account provided in Menu and can also check Balance of his/her linked Bank Account by clicking "REQUEST BALANCE"
7. Language: Up to 8 regional languages (Tamil, Telugu, Bengali, Malayalam, Oriya, Gujarati, Kannada ,Hindi) available on BHIM to improve user experience.
8. Block User: Block/Spam users who are sending you collect requests from illicit sources.
9. Privacy: Allow a user to disable and enable mobilenumber@upi in the profile if a secondary VPA is created (QR for the disabled VPA is also disabled).

****BHIM APP is available in play store (for android User) and App Store (for Apple User)****

Bharat QR

In a major push for seamless cashless transactions, Govt. of India has launched Bharat QR Code, which is world's first interoperable payment platform. National Payments Corporation of India (NPCI), which is the umbrella organisation for all digital and online retail payment systems in India, has developed this platform, which is expected to inspire and encourage more digital payments, without using debit or credit card.

QR Codes are black and white two-dimensional machine readable code, which stores information about the merchant's bank accounts and URLs. With Bharat QR Code interface, merchants need to take a printout of their QR code (or have a soft copy) and show it to the consumer, who can simply scan the

code using his or her smartphone, and the payment would be made. Instantly, seamlessly and without any hassles.

We had reported last year that Govt. is considering to create a [common QR Code based payment mechanism](#), which has now been officially launched. The Retail industry is excited by its possibilities because QR code-based payments solves two major problems in a single go: a) less time consumed to make the payment, compared to debit/credit card b) no requirement to actually flash your credit/debit cards for making the payment.

Here are some interesting facts about Bharat QR Code payment system, which every debit/credit holder (who is also a bank account holder) should be aware of:

Smart Cards

The smartcards have increased data security, an active anti-fraud capabilities, multipurpose capabilities, flexibility in applications, and off-line validation. These functions are more or less inter-related but the most important of all is the high level of security provided by the smartcard compared to the other type of cards in operation. This makes it possible the use the smart cards in transactions dealing with money, property and personal data.

The Reserve Bank of India has set a target for banks to upgrade all ATMs by September 2017 with additional safety measures to process EMV chip and PIN cards in order to prevent skimming and cloning of debit and credit cards.

While the POS terminal infrastructure in the country has been enabled to accept and process EMV chip and PIN cards, the ATM infrastructure continues to process the card transactions based on data from the

magnetic stripe. As a result, the ATM card transactions remain vulnerable to skimming, cloning, etc. frauds, even though the cards are EMV chip and PIN based.

It has become necessary to mandate EMV (Europay, MasterCard, Visa) chip and PIN card acceptance and processing at ATMs also. Contact chip processing of EMV chip and PIN cards at ATMs would not only enhance the safety and security of transactions at ATMs but also facilitate preparedness of the banks for the proposed "EMV Liability Shift" for ATM transactions, as and when it comes into effect.

Further, in order to ensure uniformity in card payments ecosystem, banks should also implement the new requirements at their micro-ATMs which are enabled to handle card-based payments.

CVV OR CSC NUMBER

The CVV Number ("Card Verification Value") on credit card or debit card is a 3 digit number on VISA, MasterCard and Discover branded credit and debit cards. On American Express branded credit or debit card it is a 4 digit numeric code.

The CVV number can be located by looking on credit or debit card, as illustrated in the image below:

Providing the CVV number to an online merchant proves that one actually has the physical credit or debit card - and helps to keep one safe while reducing fraud.

CVV numbers are NOT the card's secret PIN (Personal Identification Number).

One should never enter one's PIN number when asked to provide the CVV. (PIN numbers allow one to use one's credit or debit card at an ATM or when making an in-person purchase with debit card or a cash advance with any credit card.)

CVV numbers are also known as CSC numbers ("Card Security Code"), as well as CVV2 numbers, which are the same as CVV numbers, except that they have been generated by a 2nd generation process that makes them harder to "guess".

In 2016, a new e-commerce technology called Motioncode was introduced, designed to automatically refresh the CVV code to a new one every hour or so.

ATM & POINT OF SALE (POS)

ATM (Automated Teller Machine) A typical ATM could duplicate most of the services of a live teller; deposits, withdrawals, and money transfers between accounts all could be made with relative ease. More significantly, the terminals could be located outside the bank lobby, allowing 24 hour access and greater customer convenience. For the banks ATM's became mini-branches that extended their financial territory and customer base far beyond physical buildings. As a result, many ATMs rapidly found homes inside major retail outlets, convenience stores, gas stations, and other highly trafficked locations, a situation welcomed by businesses because it provided instant cash for customers.

White label ATMs are those ATMs which do not belong to any bank but managed by a non-banking entity, e.g., Indiacash, India-1 ATM, Prism Payment Services.

However, ATM's would not be the final solution to the common electronic goal, because they still involved the use of paper money. Yet, in a second generation machine called a Point of Sale terminal (POS), the prospect of having a truly cashless society suddenly took a giant leap forward. The potential of POS for achieving a totally automated economy was enormous. It was logical to assume that if the capability existed for electronic banking to the extent of obtaining cash out of an account using a networked ATM system, then the technology also must be ripe for eliminating the need for physical money altogether. POS terminals were seen as a key ingredient in the transition to this goal.

A point of sale terminal (POS terminal) is an electronic device used to process card payments at retail locations. . Point of sale terminals are a combination of software and hardware that allows retail locations to accept card payments without updating their cash registers to read cards directly. The costs of installing POS terminals vary with the size of the business and the terms from the supplier. Small merchants may have to pay rent for the terminal, as well as pay an additional per-transaction fee.

The trend is away from the traditional use of just magnetic stripe reader as more options open up for mobile payments.

A POS terminal generally does the following:

- Reads the information off a customer's credit or debit card

- Checks whether the funds in a customer's bank account are sufficient

Transfers the funds from the customer's account to the seller's account (or at least, accounts for the transfer with the credit card network)

Records the transaction and prints a receipt

Despite the more advanced technology of a POS system as compared to a simple cash register, the POS system is still as vulnerable to employee theft through the sale window. A dishonest cashier at a retail outlet can collude with a friend who pretends to be just another customer. During checkout the cashier can bypass scanning certain items or enter a lower quantity for some items thus profiting thereby from the "free" goods.

With the launch of mobile payment particularly Android Pay and Apple Pay both in 2015, it is expected that because of its greater convenience coupled with good security features, this would eventually eclipse other types of payment services - including the use of payment terminals. However, for mobile payment to go fully mainstream, mobile devices like smartphones that are NFC-enabled must first become universal. NFC (near field communication) is the technology that allows two devices—like your phone and a payments terminal—to talk to each other when they're close together. NFC is the technology that enables contactless payments.

Electronic funds transfer at point of sale (EFTPOS) is an electronic payment system involving electronic funds transfers based on the use of payment cards, such as debit or credit cards, at payment terminals located at points of sale. EFTPOS is highly popular in Australia and New Zealand, and being used in NZ for about 60% of all retail transactions.

Latest Trends in eCommerce

A key outcome of the technology revolution in India has been connectivity, which has fuelled unprecedented access to information. Millions of people who had little means to join the national discourse can now gain new insights into the world around them. Farmers know crop prices. Consumers understand global standards of product and service quality. Rural Indians recognise the differences between the opportunities available to them and those available to their urban counterparts. And citizens have a mass forum for expressing their political opinions. The upshot of this connectivity revolution has been empowerment of Indians.

An analysis of the demographic profile of internet users further testifies that eCommerce will rise rapidly in India in coming years. Around 75% of Indian internet users are in the age group of 15 to 34 years. This category shops more than the remaining population. Peer pressure, rising aspirations with career growth, fashion and trends encourage this segment to shop more than any other category and India, therefore, clearly enjoys a demographic dividend that favours the growth of eCommerce. In coming years, as internet presence increases in rural areas, rural India will yield more eCommerce business

Mobile to be the most influential aspect of eCommerce -With mobile apps being developed by most eCommerce websites, smartphones are increasingly replacing PCs for online shopping. In 2013, only 10% of the mobile users used smartphones, and only 5% of the eCommerce transactions were made through a mobile device. This figure has more than doubled, and more than 13% of all eCommerce transactions today happen via mobile³. According to some industry players, over 50% of the orders are being placed through mobile apps, which is not only leading to substantial customer acquisition but also building customer loyalty for various brands. However, most mobile transactions so far are for entertainment, such as booking movie tickets and music downloads. This trend will change soon with more and more merchandise being ordered online.

More business coming from smaller towns - eCommerce is increasingly attracting customers from Tier 2 and 3 cities, where people have limited access to brands but have high aspirations. According to eCommerce companies, these cities have seen a 30% to 50% rise in transactions.

Enhanced shopping experience - Besides general online shopping, customers are also shopping online for weddings and festivals, thanks to wider range of products being offered and aggressive advertisements. The free and quick shipment and wider choice of products, along with the ease of

shopping online as compared to in-store shopping, is also helping eCommerce gather momentum.

Further, eCommerce companies are doing rapid business due to sales.

Exclusive partnerships with leading brands - Over the year or so, there has been a trend of exclusive tie-ups between eTailers and established boutiques, designers, and high-end lifestyle and fashion brands. For instance, Jabong added international fashion brands such as Dorothy Perkins, River Island, Blue saint and Miss Selfridge, along with local fashion brands through Jabong Boutiques. Similarly, Myntra benefited from exclusive tie-ups with brands such as Harvard Lifestyle, Desigual and WROGN from Virat Kohli.

Expanding the product basket - There is a recent trend of relatively newer products such as grocery, hygiene, and healthcare products being purchased online. Similarly, lingerie and Indian jewellery has also been in great demand among customers outside India. Export comprises 95% of cross-border eCommerce, with the US, UK, Australia, Canada and Germany being the major markets.

Innovation in online business models

To get the maximum benefit from eCommerce business, a large number of companies such as Amazon, Alibaba etc. are adopting different innovative ideas and operating models including partnering with online marketplaces or setting up their own online stores. Some key operating models include the following:

- Marketplace and pick-up & drop is a model where sellers often partner with leading marketplaces to set up a dedicated online store on the latter's website. Here sellers play a key role of managing inventory and driving sales. They leverage on high traffic on the marketplaces' website and access their distribution network. However, the sellers have limited say on pricing and customer experience.

- Self-owned inventory is a model where the eCommerce player owns the inventory. The model provides better post-purchase customer experience and fulfilment. It provides smoother operations due to ready information on the inventory, location, supply chain and shipments, effectively leading to better control over inventory. On the flipside, however, there are risks of potential mark downs and working capital getting tied up in inventory.
- Private label reflects a business where an eCommerce company sets up its own brand goods, which it sells through its own website. This model offers a wide-ranging products and pricing to its customers and competes with branded labels. Here, margins are typically higher than third-party branded goods.
- White label involves the setting up of a branded online store managed by the eCommerce player or a third party. The brand takes the responsibility of generating website traffic and providing services by partnering with payment gateways. It helps build trust, customer affinity and loyalty and provides better control of brand and product experience.

SMS BANKING & BANKING ALERTS

SMS banking is a form of mobile banking. It is a facility used by some banks or other financial institutions to send messages (also called notifications or alerts) to customers' mobile phones using SMS messaging, or a service provided by them which enables customers to perform some financial transactions using SMS.

SMS banking services may use either push and pull messages. Push messages are those that a bank sends out to a customer's mobile phone, without the customer initiating a request for the information. Typically, a push message could be a mobile marketing message or an alert of an event which happens in the customer's bank account, such as a large withdrawal of funds from an ATM or a large payment involving the customer's credit card, etc. It may also be an alert that some payment is due, or that an e-statement is ready to be downloaded.

Another type of push message is one-time password (OTPs). OTPs are the latest tool used by financial institutions to combat cyber fraud. Instead of relying on traditional memorized passwords, OTPs are sent to a customer's mobile phone via SMS, who are required to repeat the OTP to complete transactions using online or mobile banking. The OTP is valid for a relatively short period and expires once it has been used.

Bank customers can select the type of activities for which they wish to receive an alert. The selection can be done either using internet banking or by phone.

Pull messages are initiated by the customer, using a mobile phone, for obtaining information or performing a transaction in the bank account. Examples of pull messages include an account balance enquiry, or requests for current information like currency exchange rates and deposit interest rates, as published and updated by the bank. Depending on the selected extent of SMS banking transactions offered by the bank, a customer can be authorized to carry out either non-financial transactions, or both

and financial and non-financial transactions. SMS banking solutions offer customers a range of functionality, classified by push and pull services as outlined below.

Typical push services would include:

periodic account balance reporting (say at the end of month);

reporting of salary and other credits to the bank account;

successful or un-successful execution of a standing order;

successful payment of a cheque issued on the account;

insufficient funds;

large value withdrawals on an account;

large value withdrawals on the ATM or EFTPOS on a debit card;

large value payment on a credit card or out of country activity on a credit card. one-time password and authentication

an alert that some payment is due

an alert that an e-statement is ready to be downloaded.

Typical pull services would include:

Account balance enquiry;

Mini statement request;
Electronic bill payment;

Transfers between customer's own accounts, like moving money from a savings account to a current account to fund a cheque;

Stop payment instruction on a cheque;

Requesting for an ATM card or credit card to be suspended;

De-activating a credit or debit card when it is lost or the [PIN](#) is known to be compromised;

Foreign currency exchange rates enquiry;
Fixed deposit interest rates enquiry

Security concerns in SMS Banking

The lack of encryption on SMS messages is an area of concern that is often discussed. This concern sometimes arises within the group of the bank's technology personnel, due to their familiarity and past experience with encryption on the ATM and other payment channels. The lack of encryption is inherent to the SMS banking channel and several banks that use it have overcome their fears by introducing compensating controls and limiting the scope of the SMS banking application to where it offers an advantage over other channels.

Suppliers of SMS banking software solutions have found reliable means by which the security concerns can be addressed. Typically the methods employed are by pre-registration and using security tokens where the transaction risk is perceived to be high.

Most online banking platforms are owned and developed by the banks using them. There is only one open source online banking platform supporting mobile banking and SMS payments called Cyclos, which is developed to stimulate and empower local banks in development countries.

SMS & Email Alerts in Banking

This is a very useful facility that sends customer information on customer's banking transactions. The alerts are either event based or frequency based. When register for certain alerts they are sent to customer either via SMS or email, or both. Some alerts are made mandatory by regulator whereas for others they customer may choose as per his requirement. Some banks send email alerts for monthly account statements in encrypted pdf format which may be opened using a password only.

RBI's has made SMS for clearing cheque transactions mandatory- Expressing concern over the rise in cheque-related fraud cases, the Reserve Bank of India (RBI) has made SMS alerts mandatory for such transactions since November 2014. Banks now send SMS alerts to both payer and drawer in cheque transactions as soon as the instruments are received for clearing.

Bharat Bill Payment System (BBPS)

Bharat Bill Payment System (BBPS) is an integrated bill payment system in India offering interoperable and accessible bill payment service to customers online as well as through a network of agents, enabling multiple payment modes, and providing instant confirmation of payment.

National Payments Corporation of India (NPCI) will function as the authorised Bharat Bill Payment Central Unit (BBPCU), which will be responsible for setting business standards, rules and procedures for technical and business requirements for all the participants. NPCI, as the BBPCU, will also undertake clearing and settlement activities related to transactions routed through BBPS. Existing bill aggregators and banks are envisaged to work as Operating Units to provide an interoperable bill payment system irrespective of which unit has on-boarded a particular biller. Payments may be made through the BBPS using cash, transfer cheques, and electronic modes. To start with, the scope of BBPS will cover repetitive payments for everyday utility services such as electricity, water, gas, telephone and Direct-to-Home (DTH). Gradually, the scope would be expanded to include other types of repetitive payments, like school / university fees, municipal taxes etc.

Computer Security which is also at times referred to as information security is concerned with three main areas:

1. Confidentiality:- Only authorized users can access the data resources and information.
2. Integrity:- Only authorized users should be able to modify the data when needed.
3. Availability:- Data should be available to users when needed.

Each of the above three areas is critical for computer security. Confidentiality deals with prevention of data theft such as bank account information, credit card information, passwords etc. Integrity refers to prevention of unauthorized data creation, modification or deletion. Last but not the least is availability, which ensures that the users are able to access data whenever needed.

What Are ISO 27000 series standards?

The ISO 27000 series of standards are a compilation of international standards all related to information security. Every standard from the ISO 27000 series is designed with a certain focus

– if you want to build the foundations of information security in your organization, and devise its framework, you should use ISO 27001; if you want to implement controls, you should use ISO 27002, if you want to carry out risk assessment and risk treatment, you should use ISO 27005 etc.

ISO 27001 establishes requirements - if an organization wants to certify its Information Security Management System (ISMS) it needs to comply with all requirements in ISO 27001. On the other hand, ISO 27002 are best practices that are not mandatory. That means that an organization does not need to comply with ISO 27002 but can use it as inspiration to implement requirements in ISO 27001. [ISO 27002](#) was formerly known as ISO 17799, having been renamed in 2007. ISO 27002 is more complex and difficult to comply with but it is not mandatory because depending on the context and the business of the organization it could implement the control in another way. ISO 27001 establishes what you have to do but not how. ISO 27002 describes how.

Logical Security

Generally, passwords must be at least 8 characters long and include upper and lower case characters and at least one numeric character and one special character. It is amazing to note that a 'brute force' tool which may crack a 4 character password in just 4 seconds, takes about 10 years to crack an 8 character password.

Privileged identity management (PIM) is a recent concept involving a domain within [identity management](#) focused on the special requirements of powerful accounts within the IT infrastructure of an enterprise. It is frequently used as an [information security](#) and [governance](#) tool to help companies in meeting [compliance](#) regulations and to prevent internal [data breaches](#) through the use of privileged accounts, like system or database administrator. PIM, privileged identity management; PUM, privileged user management; and PAM, privileged account management OR privileged access management; all three of these acronyms revolve around the same simple concept: who can get to a server, how they can get to a server and what they can do when they get there.

Denial-of-service (DoS) attacks: Where the intruder attempts to crash a service (or the machine), overload network links, overloaded the CPU, or fill up the disk. The intruder is not trying to gain information, but to simply act as a vandal to prevent from making use of machine.

Distributed Denial of Service (DDoS) attacks: In most respects it is similar to a DoS attack but the results are much, much different. Instead of one computer and one internet connection the DDoS attack utilises many computers and many connections. The computers behind such an attack may be often distributed around the whole world and will be part of what is known as a [botnet](#). The main difference between a DDoS attack vs a DoS attack, therefore, is that the target server will be overload by hundreds or even thousands of requests in the case of the former as opposed to just one attacker in the case of the latter. Therefore it is much, much harder for a server to withstand a DDoS attack as opposed to the simpler DoS incursion.

An Intrusion Detection System (IDS) is a system for detecting such intrusions. IDS can be broken down into the following categories:

An Intrusion Prevention System (IPS) sits between the firewall and the rest of the network. That way, if an attack is detected, the IPS can stop the malicious traffic before it makes it to the rest of the network. In contrast, an IDS simply sits on top of the network rather than in front of it. Unlike IDS, IPS actively takes steps to prevent or block intrusions that are detected. These preventing steps include activities like dropping malicious packets and resetting or blocking traffic coming from malicious IP addresses. IPS can be seen as an extension of IDS, which has the additional capabilities to prevent intrusions while detecting them.

IPS is a system that actively takes steps to prevent an intrusion or an attack when it identifies one. IPS are divided into four categories. First one is the Network-based Intrusion Prevention (NIPS), which monitors the entire network for suspicious activity. The second type is the Network Behavior Analysis (NBA) systems that examine the traffic flow to detect unusual traffic flows which could be results of attack such as distributed denial of service (DDoS). The third kind is the Wireless Intrusion Prevention Systems (WIPS), which analyzes wireless networks for suspicious traffic. The fourth type is the Host-based Intrusion Prevention Systems (HIPS), where a software package is installed to monitor activities of a single host.

CRYPTOGRAPHY

There are two basic types of Encryption algorithms:

- (i) Symmetric encryption
- (ii) Asymmetric Encryption

Symmetric Encryption: In this encryption technique the sender and receiver encrypts and decrypts the message with the same key. Examples are Twofish, Serpent, AES (Rijndael), Blowfish, CAST5, Kuznyechik, RC4, 3DES, Skipjack etc.

Asymmetric encryption: In this encryption technique the sender encrypts the message with the receiver's public key and the receiver decrypts the information with recipient's private key. Hence this technique is called public key encryption. Examples are: Diffie-Hellman, RSA, ECC, ElGamal, DSA etc.

Srinivas Kante

Srinivas Kante

Among the various models of symmetric cipher analyzed the Rijndael is the best. Actually it is the role model of DES and AES. This model is adopted by different information security agencies like NSA, NIST and FIPS.

Among the various asymmetric ciphers, RSA is a moderate and most useful cipher for small data encryption like digital signature, ATM Pin etc.

But as discussed above, RSA (asymmetric technique) is much slower than Rijndael (symmetric technique) and other symmetric cipher techniques. But the scalability of asymmetric cryptosystem is far higher than the symmetric cryptosystem. Thus where the number of users is huge and required keys are very high, asymmetric cryptosystem proves to be superior.

It is scientifically predicted that the symmetric cipher like Rijndael is supposed to be secure against mathematical attacks until 2090. Thus they are very suitable for hardware level security in communicating devices.

Advanced Encryption Standard (AES): is the successor of DES (Data Encryption Standard) as standard symmetric encryption algorithm for US federal organizations. AES uses keys of 128, 192 or 256 bits, although, 128 bit keys provide sufficient strength today. It uses 128 bit blocks, and is efficient in both software and hardware implementations. It was selected through an open competition involving hundreds of cryptographers during several years.

Safe Key Length

128-bit encryption is a data/file encryption technique that uses a 128-bit key to encrypt and decrypt data or files. In today's parlance, it is considered one of the most secure encryption methods and used in most modern encryption algorithms and technologies. 128-bit encryption is considered to be logically unbreakable as of date. However, it is to be remembered that breakability is only relative considering the technology available at that time. Keeping this in view, it is also recommended by many that the cipher AES-256 be used among other places in SSL/TLS across the Internet. It's considered among the top ciphers. In theory it's not crackable since the combinations of keys is massive.

Digital Signature

In technical terms, a digital signature is the sequence of bits that is created by running an electronic message through a one-way hash function (a program). The resulting message is called Message Digest (MD). Some of the popular MD algorithms are MD5, SHA1 and SHA256. It has been shown that MD5 is less reliable with problems relating to collision (where 2 keys for different data

are the same). Besides MD5, SHA and CRC32 are other message digest algorithms. The SHA (Secure Hash Algorithm) is one of a number of cryptographic hash functions. A cryptographic hash is like a signature for a text or a data file. SHA-256 algorithm generates an almost-unique, fixed size 256-bit (32-byte) hash. Hash is a one way function – it cannot be decrypted back.

Emerging Trends in Public Key Infrastructure:

With the long-term success of PKI, it's no surprise that it has been popping up in an increasing number of situations – from the Web to identity documents to mobile devices to today's "smart" appliances, remote-controlled home systems and the entire Internet of Things (IOT). PKI's ability to combine strong protection with cost-effective management and user-friendliness is now at the core of its success. And it is expected to increase sharply as mobile devices proliferate, with more and more "smart" applications and uses.

The Growth of Mobile

PKI will continue to play a key role in the growth of mobile for trust anchoring, device identity and authentication. As more and more organizations use certificates for secure mobile connection to Wi-Fi and VPN networks, PKI meets the increased demand for safe, secure transmission of all kinds of data.

This includes a wide range of mobile apps, mobile payments, cloud services and access to physical and logical assets. Mobile certificates are also essential in identifying and securing corporate-issued devices and the growing number of Bring-Your-Own-Devices. (BYODs)

Internet of things (IOT)

Widely predicted to be a major factor in future IT infrastructure and identity, the Internet of Things will rely on PKI to play an essential role in a vast number of interconnected applications and devices. These

network-connected things already include ATMs and financial accounts, lighting systems and thermostats, home surveillance equipment, medical devices, smart meters of all varieties, electronic doggie doors, TV's, home electronics – even planes, trains and automobiles. All of these require a transparent, consistent form of certificate-based identity authentication. And having dealt with network connected devices for decades, PKI is the ideal solution to deliver and manage large numbers of certificates at high speed. Even though mobility and IoT are relatively new market drivers, their requirements are essentially the same as those of earlier network connected devices. Given the remarkable strength of PKI and its flexibility in adapting to new applications, one can expect the technology to continue for quite some time, because it does what it does really well.

In India

In India, a number of nationally important e-Governance initiatives have already been embarked upon by the Government. Large-scale adoption of Digital Signatures will be one of the key success factors in these initiatives, as they will rely on Digital Signatures for their authentication requirements. Several Training programs for different user segments have been conducted nation-wide.

Below listed are few examples of usage of digital signatures in India.

Use of PKI in Aadhaar Data Encryption: Aadhaar enrolment data packets (individual electronic file containing resident demographics and biometrics) are strongly encrypted by the Enrolment Page 2 of 16 Client software at the time of enrolment even before saving any data to any hard disk. Encryption uses highest available public key cryptography encryption (PKI-2048 and AES-256) with each data record having a built-in mechanism to detect any tampering. Even if someone attempts to decrypt, due to the use of strongest available encryption (2048-bit asymmetric encryption), even with millions of computers, it will take billions of years to break such encryption. Income Tax e-filing: A Digital Signature Certificate lets you file your Tax Returns easier and more secure. According to revised provisions under section 44AB of IT Act "E-Filing is mandatory for all the individuals/professionals having an annual gross receipt of INR 25 Lakhs and above, and for business houses with annual turnover of INR 1 Crore and above.

Ministry of Corporate Affairs (MCA): A Digital Signature Certificate helps make light work of various transactions related to the Ministry of Corporate Affairs, or Registrar of Companies. In addition to saving time, a Digital Signature Certificate also helps secure data.

eProcurement is an online tender processing system for the state government departments. More than 1000 tenders published so far. The Digital Signatures are being used both by the vendors and government officials for tender submission and processing. The vendors/traders are using it for applying tenders online, while the government officials are using it at time of opening the tenders and during finalizing of the tenders.

Voters List Preparation – The State Election Commission has issued a GO that the field data along with the photo ID will be digitized and the same will be digitally signed assuring the correctness of data.

The DSC (Digital Signature Certificate) will be used to counter verify the digitized data of voters list and the photo ID. This can be used by other applications such as eDistrict for online verification of citizen details.

Online Counseling for admission to more than 1 lakh seats of Engineering, Medical, Polytechnic

& B.Ed. courses. The Digital Signatures are being used by the Counseling In-charge for document verification, fee submission, registration & for choice locking opted by the candidates which are finally locked by the invigilators using DSC.

IRCTC: IRCTC has facilitated online ticketing for RTSA agents and IATA approved agents. With this new technology, using Digital Signature Certificates, agents registered with IRCTC will be able to issue Railway tickets from the comfort of their homes. This will ensure speedy and secure business giving it a 24X7 dimension.

DGFT: Export and Import Organizations (EXIM organizations) can apply for licenses online which means that they can also file accompanying documents electronically on the DGFT website. Since a Digital Signature Certificate ensures authenticity of the document, DGFT has mandated use of Digital Signature Certificates with all electronic documents uploaded on the DGFT site.

Since a Digital Signature Certificate is recognized by the legal system, all documents submitted using a Digital Signature Certificate is considered on par with physically signed documents, and also attract benefits endowed upon them through the Indian Information Technology Act 2000.

The Future is PKI

Looking back to the early days of public-key technology, the inherent simplicity of the most popular schemes was a concern to many. How we could we place our faith in the long-term security of such simple mathematical operations is the question. While some narrow loopholes have been discovered in some of the basic schemes, the technology itself has withstood close scrutiny by

countless experts over the past forty years. In many ways, user confidence in the effectiveness of PKI is stronger than ever – and it remains the most practical and cost-effective solution to our ever-growing security challenges.

Types of Disaster Recovery Strategies and Disaster Recovery Sites There are basically three levels of Disaster Recovery Strategies -

Cold Site Replication - This is basically an entry level solution where the recovery time may be as much as 10 days but for a medium sized bank are typically between 5-7 days.

Recovery in Days

Lowest Cost Solution

Restore data from Tape

Hardware is Optional

No Data Replicated via Communication Line

Warm Site Replication - This is a good initial level solution for a medium sized branch where the recovery time generally is between one hour and 8 hours extending sometimes to 24 hours. Systems are synchronized via a secure network connection from the primary production system to the secondary system located elsewhere. Data is periodically synchronized via a network using a choice of industry leading data synchronization and replication software.

Recovery in Hours

Medium Cost Solution

Faster Restoration

Hardware needs to be purchased or leased

Data Synchronization Over Communication Line

Hot Site Replication - This is a high end solution for businesses which cannot even stop for seconds. Systems are synchronized via a secure network connection from the primary production system to the secondary system located elsewhere. Data is frequently synchronized via a network using a choice of industry leading data synchronization and replication software. Recovery times can be as low as a minute extending to 10 minutes.

Recovery in Seconds/Minutes

Higher Cost Solution

Almost immediate Restoration

Hardware needs to be purchased or leased

Fully Redundant & Mirrored Environment

Data Mirroring and Disk Arrays: RAID 5 is the most common secure RAID level. It requires at least 3 drives. A RAID 5 array can withstand a single drive failure without losing data or access to data. If a drive fails, you still have access to all data, even while the failed drive is being replaced and the storage controller rebuilds the data on the new drive.

Srinivas Kante

BCP & DRP

Business Continuity Planning (BCP) and Disaster Recovery Plan (DRP) are used together so often that people often begin to forget that there is a difference between the two. A BCP is a plan that allows a business to plan in advance what it needs to do to ensure that its key products and services continue to be delivered (technicality: at a predefined level) in case of a disaster, while a DRP allows a business to plan what needs to be done immediately after a disaster to recover from the event. So, a BCP tells your business the steps to be taken to continue its key product and services, while a DRP tells your business the steps to be taken to recover post an incident. Some experts also opine that DRP takes care of technology side of BCP.

Your impact analysis, your business continuity strategy and business continuity plans are a part of BCP. Your incident response, emergency response, damage assessment, evacuation plans, etc. are all a part of DRP. It makes sense to divide your planning into two parts

Planning to continue your business operations (BCP) and
Planning to recover from disaster situations (DRP).

As part of the business continuity process an organisation will normally develop a series of DRPs. These are more technical plans that are developed for specific groups within an organisation to allow them to recover a particular business application. The most well-known example of a DRP is the Information Technology (IT) DRP. The typical test for a DR Plan for IT would be; "if we lost our IT services how would recover them?"

It is pertinent to note that BCP and DRP have similarities in banking industry since information processing application and business application have thin line of distinction and look like one and the same. All banking business operations and the concerned data processing operations are inseparable.

A few more kinds of attacks

Phishing: Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers. Phishing has become rampant now a days and entities worldwide have lost their sensitive data and money.

Spoofing: In the context of computer security, a spoofing attack is a situation in which one person or program successfully pretending as another by falsifying data, thereby gaining an illegitimate advantage. Spoofing is of two types. (1) Email spoofing is the creation of email messages with a forged sender address. Because the core email protocols do not have any mechanism for authentication, it is common for spam and phishing emails to use such spoofing to mislead the recipient about the origin of the message. (2) Network spoofing-in computer networking, IP address spoofing or IP spoofing is the creation of Internet Protocol (IP) packets with a false source IP address, for the purpose of hiding the identity of the sender or impersonating another computing system.

Sniffing: Sniffing is the act of intercepting and inspecting data packets using sniffers (software or hardware devices) over the network. On the other hand, Spoofing is the act of identity

impersonation. Packet sniffing allows individuals to capture data as it is transmitted over a network and is used by network professionals to diagnose network issues, and by malicious users to capture unencrypted data, like passwords and usernames.

Spamming: Electronic spamming is the use of electronic messaging systems to send an unsolicited message (spam), especially advertising, as well as sending messages repeatedly on the same site. While the most widely recognized form of spam is email spam, the term is applied to similar abuses in other media too. Spam can also be used to spread computer viruses, Trojan or other malicious software. The objective may be identity theft, or worse (e.g., advance fee fraud). Some spam attempts to capitalize on human greed, while some attempts to take advantage of the victims' inexperience with computer technology to trick them (e.g., phishing).

Ransomware: Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid. Simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse. More advanced malware encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. The ransomware may also encrypt the computer's Master File Table (MFT) or the entire hard drive. Thus, ransomware is a denial-of-access attack that prevents computer users from accessing files since it is intractable to decrypt the files without the decryption key.

Some examples of ransomware are Reveton, Cryptolocker, Cryptowall, Fusob and WannaCry. Wide-ranging attacks involving encryption-based ransomware began to increase through Trojans such as CryptoLocker, which had procured an estimated US\$3 million before it was taken down by authorities, and CryptoWall, which was estimated by the US Federal Bureau of Investigation (FBI) to have accrued over \$18m as ransom money by the attackers by June 2015.

In May 2017, the WannaCry ransomware attack spread through the Internet, using an exploit vector that Microsoft had issued a "Critical" patch for (MS17-010) two months before on March 14, 2017. The ransomware attack infected lakhs of users in over 150 countries, using 20 different languages to demand money from users.

Measures against attacks

Against Phishing attacks, obviously there cannot be an antivirus tool for checking. Only appropriate user education and generating awareness can prevent or reduce phishing menace.

Spoofing attacks which take advantage of TCP/IP suite protocols may be mitigated with the use of [firewalls](#) capable of [deep packet inspection](#) or by taking measures to verify the identity of the sender or recipient of a message

To protect against sniffing, we need to encrypt all important data we send or receive, scan our networks for any issues or dangers and use only trusted Wi-Fi networks.

To prevent spamming, most of the email services, viz., Gmail, Yahoo, Hotmail etc. provide filtering facilities and also enable users to categorize certain messages as spam.

Best measures for protection against ransomware are taking regular backups of data, applying OS patches regularly and using latest anti-malware solution.

Types of Computer Frauds

1. Sending hoax emails to scare people
2. Illegally using someone else's computer or "posing" as someone else on the internet
3. Using spyware to gather information about people
4. Emails requesting money in return for "small deposits"
5. Pyramid schemes or investment schemes via computer with the intent to take and use someone else's money
6. Emails attempting to gather personal information used to access and use credit cards or social security numbers
7. Using the computer to solicit minors into sexual alliances
8. Violating copyright laws by copying information with the intent to sell it
9. Hacking into computer systems to gather large amounts of information for illegal purposes
10. Hacking into or illegally using a computer to change information such as grades, work, reports, etc.
11. Sending computer viruses or worms with the internet to destroy or ruin someone else's computer

Precautions

Refrain from opening e-mail and e-mail attachments from individuals you do not know. Have ALL external storage devices scanned by virus-scanning software before inserted on your PC. Secure your Internet Web browsing.

Make sure you have a regular backup, in case you need to restore data. If you have high-speed (broadband) Internet access in your office, think about getting either a hardware or software firewall to

protect your computer system. If you run a “Wireless Network” you must take time to secure it and understand how it works.

Individuals should not pay attention to get rich quick schemes. If they seem too good to be true, they absolutely are. Children should be taught about safe communication on the Internet to protect them from predators. Avoid communication with strangers and never tell strangers your location.

Traps by ATM fraudsters at ATM

1. Hidden camera: Tiny, pinhole cameras may be placed on the machine or even the roof at strategic positions to capture your PIN.
2. Card skimmer: These devices are installed on the card reader slot to either copy the information from the magnetic strip of your card or steal the card itself.
3. Bulky slot: If the slot feels slightly bulky or misaligned, in all probability an additional card reader slot has been placed on top of the actual one. Loose slot: If the slot is wobbly or loose, it indicates the presence of a ‘Lebanese loop’, which is a small plastic device with a barb that holds your card back in the machine. You may think the machine has swallowed your card or it has been stuck.

4. Shoulder surfers: These are people lurking in the ATM room or outside. They will either peer over your shoulder to read your PIN or offer help if your card is stuck.
5. False front: It may be a little difficult to detect as the fake front completely covers the original machine because it is installed on top of it. This allows fraudsters to take your PIN as well as money.
6. Fake keypad: This is placed on top of the actual keypad. If the keypad feels spongy to touch or loose, don't enter your PIN.

Frauds in Online transactions

The ease of e-shopping or online bill payment is matched by the felicity with which identity theft can be carried out on computer or smartphone. This can then be used for unauthorised transactions Pharming: In this technique, fraudsters reroute you to a fake website that seems similar to the original. So even as you conduct transactions and make payment via credit or debit card, the card details can be stolen.

Keystroke logging: Here, you unintentionally download a software, which allows the fraudster to trace your key strokes and steal passwords or credit card and net banking details.

Public Wi-Fi: If you are used to carrying out transactions on your smartphone, public Wi-Fi makes for a good hacking opportunity for thieves to steal your card details.

Malware: This is a malicious software that can damage computer systems at ATMs or bank servers and allows fraudsters to access confidential card data.

Merchant or point-of-sale theft: This is perhaps the simplest and most effective form of stealth, wherein your card is taken by the salesperson for swiping and the information from the magnetic strip is copied to be used later for illegal transactions.

Phishing & vishing: While phishing involves identity theft through spam mails which seem to be from a genuine source, vishing is essentially the same through a mobile phone using messages or SMS. These trick you into revealing your password, PIN or account number.

SIM swipe fraud: Here the fraudster contacts your mobile operator with fake identity proof and gets a duplicate SIM card. The operator deactivates your original SIM and the thief generates one-time password (OTP) on the phone to conduct online transactions.

Unsafe apps: Mobile apps other than those from established stores can gain access to information on your phone like passwords, etc., and use it for unauthorised transactions.

Lost or stolen cards, interception: This is the oldest form of theft, wherein transactions are carried out using stolen cards, those intercepted from mail before they reach the owner from the card issuer, or by fishing out information like PINs and passwords from trash bins.

Cards using other documents: This is also an easy form of identity theft, where new cards are made by the fraudster using personal information that is stolen from application forms or other lost or discarded documents.

How to prevent card related frauds?

Some basic, preventive steps can ensure that you do not fall prey to credit or debit card fraud.

Here's how:

ATM safeguards

Check machine: Do not use ATMs with unusual signage, such as a command to enter your PIN twice to complete the transaction. Also watch out for machines that appear to have been altered, if the front looks crooked, loose or damaged. It could be a sign that someone has attached a skimming device.

Cover keypad: Make sure to cover the keypad with your hand while entering the PIN to escape any cameras attached nearby.

Don't take help: It is advisable to use only your own bank ATMs, particularly those attached to a bank branch and those that have security guards. Also, avoid taking the help of any person loitering outside the ATM or volunteering to assist you if you get stuck.

Online precautions

Use safe sites: Go only to well-known, established sites for e-shopping. Remember to confirm the site's legitimacy before using it and shop only on those that are Secure Sockets Layer (SSL)-certified. These can be identified through the lock symbol next to the browser's URL box. Also make sure that the website uses the 'https' protocol instead of 'http', where 's' stands for 'secure'. Additionally, make sure not to click on the option that asks for saving your card details on any site.

Anti-virus software: While banks deploy ATM network security measures, on an individual level you can safeguard transactions by installing anti-virus software on your computer and smartphone to keep out malware. You can also install identity theft detection apps on your phone from an official app store. Besides, have software on your smartphone that enables you to wipe out the data remotely in case the mobile gets stolen.

Debit card: Make sure that you do not use your debit card for e-commerce transactions. This is because if your card is compromised, the entire cash in your bank account can be wiped out instantly. The credit card, on the other hand, offers a month's grace period before the cash leaves your account, during which the investigation can possibly nail the fraud.

Hide CVV: When you enter the CVV on the site, it should be masked by asterisks. This is especially important while shopping on foreign websites where the CVV is the only point of verification. Also use a virtual keyboard to avoid keystroke logging.

Public Wi-Fi: "Customers must avoid using unsecured W-Fi networks or public Wi-Fi as these are easy targets for identity theft cases in online transactions.

Register for alerts: This is a very important step since the bank will alert you to any online card transaction or ATM withdrawals the moment these take place. Also remember to update your mobile contact number in case of a change.

Log out: Always log out from social media sites and other online accounts to ensure data security and avoid storing confidential passwords on your mobile phones as these can be used by fraudsters.

Change passwords: Keep changing your passwords from time to time to reduce the probability of identity theft.

Virtual cards: You can use this prepaid card if you are not a frequent shopper. It is a limited debit card that does not provide the primary card information to the merchant and expires after a day or 48 hours.

Offline preventive measures

Here are some additional precautions you can take to ensure your card is safe.

Don't disclose details: Never reveal your PIN, CVV or password to anyone. Make sure not to respond to e-mails or SMSes that ask for crucial personal or card-related details. No bank or credit card firm is authorised to seek card details from customers on mail or through phone.

Check statements: Regularly go through your bank or credit card statements so that you can detect any unauthorised transaction through identity theft and alert the bank immediately.

Merchants & POS: At shops or petrol pumps, make sure that the card is not taken by the salesperson to a remote location where you cannot see it as the card information can be easily copied and stolen. Also, try shopping with retailers that use chip-enabled card readers. Though not every merchant has such readers, this provision can help bring down the risk of fraudulent card activity significantly.

RBI mandate on security of card transactions

The Reserve Bank of India has asked banks to upgrade all ATMs by September 2017 with additional safety measures to process EMV chip and PIN cards in order to prevent skimming and cloning of debit and credit cards.

While the POS terminal infrastructure in the country has been enabled to accept and process EMV chip and PIN cards, the ATM infrastructure continues to process the card transactions based on data from the magnetic stripe. As a result, the ATM card transactions remain vulnerable to skimming, cloning, etc. frauds, even though the cards are EMV chip and PIN based. It has become necessary to mandate EMV (Europay, Mastercard, Visa) chip and PIN card acceptance and processing at ATMs also, RBI said. Contact chip processing of EMV chip and PIN cards at ATMs would not only enhance the safety and security of transactions at ATMs but also facilitate preparedness of the banks for the proposed "EMV Liability Shift" for ATM transactions, as and when it comes into effect.

Computer Aided Audit Tools and Techniques (CAATTs) can refer to any computer program utilized to improve the audit process. Generally, however, it is used to refer to any data extraction and analysis software. This would include programs such as data analysis and extraction tools, spreadsheets (e.g. Excel), databases (e.g. Access), statistical analysis (e.g. SAS), general audit software (e.g. ACL, Arbutus, EAS, business intelligence (e.g. Crystal Reports and Business Objects), etc.

An IT auditor uses some general tools, technical guides and other resources recommended by ISACA or any other accredited body. This is why many audit organizations will encourage their

employees to obtain relevant certifications such as CISA (Certified Information Systems Auditor) which is awarded by ISACA.

Emerging Trends in IS Audit

There are also new audits being imposed by various standard boards which are required to be performed, depending upon the audited organization, which will affect IT and ensure that IT departments are

performing certain functions and controls appropriately to be considered compliant. Examples of such audits are SSAE 16, ISAE 3402, PCI DSS and ISO27001:2013.

ISAE 3402 and SSAE 16 audits deal with internal control over financial reporting and compliance controls of an organization respectively.

A Report on Compliance (ROC) is a form that has to be filled by all Visa and MasterCard merchants undergoing a PCI DSS (Payment Card Industry Data Security Standard) audit. The ROC form is used to verify that the merchant being audited is compliant with the PCI DSS standard. Currently both Visa and MasterCard require merchants and service providers to be validated according to the PCI DSS.

ISO/IEC 27001:2013 is an information security standard that was published in September 2013. It supersedes ISO/IEC 27001:2005, and is published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the joint ISO and IEC subcommittee. It is a specification for an information security management system (ISMS). Organizations which meet the standard may be certified compliant by an independent and accredited certification body on successful completion of a formal compliance audit.

Amendment to IT Act in 2008

A major amendment to IT Act 2000 was made in 2008. It introduced the Section 66A which penalised sending of "offensive messages". It also introduced the Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource". It also introduced penalties for child porn, cyber terrorism and voyeurism. However, on 24 March 2015, the Supreme Court of India, gave the verdict that Section 66A is unconstitutional in entirety. The court said that Section 66A of IT Act 2000 is "arbitrarily, excessively and disproportionately invades the right of free speech" provided under [Article 19\(1\)](#) of the [Constitution of India](#).

Change Management

A well-defined change management procedure is a critical security measure to protect the production IT environment from any unwanted/unintended disruptions on account application of system and application patches and hardware changes. The vendor should be bound through SLA to strictly follow the laid down change management processes.

Changes in the system may be divided into two types, (a) scheduled changes and (b) emergency changes. As a rule a change cannot happen without undergoing the change management process, however, in case of emergency changes, though the change is implemented in urgency, the entire change management process should invariably be followed post implementation of change.

The change management process should be documented, and include approving and testing changes to ensure that they do not compromise security controls, performing changes and signing them off to ensure they are made correctly and securely, reviewing completed changes to ensure that no unauthorized changes have been made.

Some of the sound Change Management processes include;

1. Following a documented risk-based strategy for inventorying IT components that need to be patched, identification of patches and applying patches so as to minimize the number of vulnerable systems and the time window of vulnerability/exposure.
2. Putting in place systems and processes to identify, track, manage and monitor the status of patches to operating system and application software running at end-user devices directly

connected to the internet and in respect of Server operating Systems/Databases/Applications/Middleware, etc.

3. Changes to business applications, supporting technology, service components and facilities should be managed using robust configuration management processes, configuration baseline that ensure integrity of any changes thereto.
4. Having clearly defined roll-back methodology in place if any applied change fails in production environment.
5. As a threat mitigation strategy, identifying the root cause of any incident and apply necessary patches to plug the vulnerabilities.

18.7.2 System Resiliency, SPOF & Clustering

In the previous modules, we have discussed the concepts of Single Point of Failure (SPOF) and its mitigations to a certain extent. Clustering is one of the popular solutions to ensure system resiliency and to reduce the existence of SPOF.

System Resiliency: System resiliency is a planned part of a facility's architecture and is usually associated with other disaster planning and data center disaster-recovery considerations such as data protection. The adjective resilient means "having the ability to spring back."

Resiliency may also at times be called as fault tolerance. Fault-tolerant technology is the capability of a computer system, electronic system or network to deliver uninterrupted service, despite one or more of its components failing. Fault tolerance also resolves potential service interruptions related to software or logic errors. The purpose is to prevent catastrophic failure that could result from a single point of failure.

Data center resiliency is often achieved through the use of redundant components, subsystems, systems or facilities. When one element fails or experiences a disruption, the redundant element takes over

seamlessly and continues to support computing services to the user base. Ideally, users of a resilient system never know that a disruption has even occurred.

SPOF and clustering: In a data center or other information technology (IT) environment, a single point of failure (SPOF) can compromise the availability of workloads – or the entire data center – depending on the location and interdependencies involved in the failure.

Consider a data center where a single server runs a single application. The underlying server hardware would present a single point of failure for the application's availability. If the server

failed, the application would become unstable or crash entirely; preventing users from accessing the application, and possibly even resulting in some measure of data loss. In this situation, the use of server clustering technology would allow a duplicate copy of the application to run on a second physical server. If the first server failed, the second would take over to preserve access to the application and avoid the SPOF.

Consider another example where an array of servers is networked through a single network switch. The switch would present a single point of failure. If the switch failed (or simply disconnected from its power source), all of the servers connected to that switch would become inaccessible from the remainder of the network. For a large switch, this could render dozens of servers and their workloads inaccessible. Redundant switches and network connections can provide alternative network paths for interconnected servers if the original switch should fail, avoiding the SPOF.

It is the responsibility of the data center architect to identify and correct single points of failure that appear in the infrastructure's design. However, it's important to remember that the resiliency needed to overcome single points of failure carries a cost (e.g. the price of additional servers within a cluster or additional switches, network interfaces and cabling). Architects must weigh the need for each workload against the additional costs incurred to avoid each SPOF. In some cases, designers may determine that the cost to correct a SPOF is costlier than the benefits of the workloads at risk.

Much as a chain is only as strong as its weakest link, the effectiveness of a high availability cluster is limited by any single point of failures (SPOF) which exist within its deployment. To ensure the absolute highest levels of availability, SPOFs must be removed. There is a straightforward method for ridding the cluster of these weak links.

First, we must identify any SPOFs which exist with particular attention paid to servers, network connections and storage devices. Modern servers come with redundant and error correcting memory, data striping across hard disks and multiple CPUs which eliminates most hardware components as a SPOF.

But even configured with multi-pathing, shared storage/SANs still represent single points of failure as does the physical data center where it is located. To provide further protection, off-site replication of critical data combined with cross-site clustering must be deployed. Combined with network redundancy between sites, this optimal solution removes all SPOFs. Real-time replication ensures that an up-to-date copy of business critical data is always available; doing this off-site to a backup data center or into a cloud service also protects against primary data center outages that can result from fire, power outages, etc.

The use of application-level monitoring and auto-recovery, multi-pathing for shared storage, and data replication for off-site protection each eliminate potential Single Points of Failure within our cluster architecture. Paying attention to these components during cluster architecture and deployment will ensure the greatest possible levels of uptime

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

BANKING SOFTWARE

Core Banking Solution (CBS)

Core Banking Solution (CBS) is networking of bank branches, which allows customers to manage their accounts, and use various banking facilities from any part of the world. In simple terms, there is no need to visit your own branch to do banking transactions. You can do it from any location, any time. You can enjoy banking services from any branch of the bank which is on CBS network regardless of branch you have opened your account. For the bank which implements CBS, the customer becomes the bank's customer instead of customer of particular branch.

Execution of Core banking system across all branches helps to speed up most of the common transactions of bank and customer. In Core banking, the all branches access banking applications from centralized server which is hosted in secured Data Centre. Banking software/application performs basic operations like maintaining transactions, balance of withdrawal & payment, interest calculations on deposits & loans etc. This banking applications are deployed on centralized server & can be accessed using internet from any location.

Need for Core Banking Technology

Nowadays, the use of Information Technology (IT) is must for the survival & growth of any organization and same applicable to banking industry also. By using IT in any industry, banks can minimize the operation cost; also banks can offer products & services to customers at competitive rates.

CBS is required;

To meet the dynamically changing market & customer needs.

To improve & simplify banking processes so that bank staff can focus on sales & marketing stuff.

Convenience to customer as well as bank.
To speed up the banking transactions.

To expand presence in rural & remote areas.

Basic elements of CBS that helps customers are:

Internet
Banking
Mobile
Banking ATM

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

POS & kiosk systems

Fund Transfers – NEFT, RTGS, IMPS etc.

Benefits of Core banking –

Core banking solutions are beneficial to both banks as well as customers.

A. Benefits for Customers

Quicker services at the bank counters for routine transactions like cash deposits, withdrawal, passbooks, statement of accounts, demand drafts etc.

Anywhere banking by eliminating branch banking.
Provision of banking services 24 X 7.

Fast payment processing through Internet banking, mobile banking.
Anytime anywhere banking through ATMs.

All branches access applications from central servers/datacentre, so deposits made in any branch reflects immediately and customer can withdraw money from any other branch throughout the world.

CBS is very helpful to people living in rural areas. The farmers can receive e-payments towards subsidy etc. in his account directly. Transfer of funds from the cities to the villages and vice versa will be done easily.

B. Benefits for Banks

Process standardization within bank & branches.

Retention of customers through better customer service.
Accuracy in transactions & minimization of errors.

Improved management of documentation & records – having centralized databases results in quick gathering of data & MIS reports.

Ease in submission of various reports to the Government & Regulatory boards like RBI.
Convenience in opening accounts, processing cash, servicing loans, calculating interest,

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

implementing change in policies like changing interest rates etc.

To cope up with the growing needs of customers; RRBs and Co-operative banks were needed to implement core banking solutions. To face the challenges of dynamic market, UCBs needed to take help of IT their operations. Considering the importance of the matter, the Reserve Bank of India (RBI) mandated a deadline for Urban Co-operative Banks (UCBs) and advised to implement the core banking solutions (CBS) by December 31, 2013, which has been met by all RRBs and UCBs.

Introduction With the globalization trends world over it is difficult for any nation big or small, developed or developing, to remain isolated from what is happening around. For a country like India, which is one of the most promising emerging markets, such isolation is nearly impossible. More particularly in the area of Information technology, where India has definitely an edge over its competitors, remaining away or uniformity of the world trends is untenable. Financial sector in general and banking industry in particular is the largest spender and beneficiary from information technology. This endeavours to relate the international trends in it with the Indian banking industry. The last lot includes possibly all foreign banks and newly established Private sector banks, which have fully computerized all the operations. With these variations in the level of information technology in Indian banks, it is useful to take account of the trends in Information technology internationally as also to see the comparative position with Indian banks. The present article starts with the banks perception when they get into IT up gradation. All the trends in IT sector are then discussed to see their relevance to the status of Indian banks.

IT Considerations Since the early nineties, each Indian bank has done some IT improvement effort. The first and foremost compulsion is the fierce competition. While deciding on the required architecture for the IT consideration is given to following realities. (1.) **Meeting Internal Requirement:** The requirements of the banks are different individually depending upon their nature and volume of business; focus on a particular segment, spread of branches and a like. Many a time's banks do have the required information but it is scattered. The operating units seldom know the purpose of gathering the information by their higher authorities. (2.) **Effective in Data Handling:** As stated earlier the banks have most of the needed data but are distributed. Further the cost of collection of data and putting the same to use is prohibitively high. The accuracy and timeliness of data generation becomes the causalities in the process. Best of the intentions on computerization are wished away because there is non-visible reduction in cost /efforts/time required for the required data gathering. (3.) **Extending Customer Services:** Addressing to rising customers expectations is significant particularly in the background of increased competition. In case bank A is unable to provide the required service at a competitive price and in an accurate manner with speed.

There is always a bank IT at its next-door waiting to hire the customer. Awareness of customers about the availability of services and their pricing as also available options have brought into sharp focus the issue of customer satisfaction. (4.) **Creative Support for New Product Development:** It has become necessary for the banks to vitalize the process of product development. Marketing functionaries needs a lot of information not only from the outside sources but also from within the banks. Banks are looking to retail segment as the future market places for sales efforts. Having full-fledged information of existing customer is the key for this purpose. The emergences of data requirement and an appropriate architecture to support the same are significant issues to be handled in this regard. (5.) **End-user Development of the Non-technical Staff:** Banking being a service industry, it is the staffs at counters that deliver the products. In Indian scenario, virtual banking is likely to have a few more years to establish. The dependence on counter staff is unavoidable. The staffs are large in number and the majority is non-technical. The customer satisfaction levels at the counter determine the ultimate benefit of IT offensive. Giving due consideration to this aspect in choosing architecture is necessary.

Trends in Information Technology Certain trends have been visualized of information technology in banking sector all over the world. (1.) **Outsourcing:** Outsourcing is one of the most talked about as also a controversial issue. The drivers for getting in to outsourcing are many to

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

include gaps in IT expectations and the reality, demystification of computerization in general and IT in particulars, trend towards focusing on core competencies, increased legitimacy of outsourcing and intention of getting out of worries and sort of up gradation of hardware and software versions. Not that the practice is new as earlier it was refused to as 'buying time' or 'service bureau'. What is needed is the clear of outsourcing, beside a definite plan to be more competitive after outsourcing. It is necessary to have checks and balances to monitor vendor performance. Cost aspects merit consideration, as also a decision on the part of the process to be outsourced shall be significance. Exit route and resource on the amount of failure after outsourcing are the other issue to be looked onto. Notwithstanding these risks, outsourcing has come to say. (2.) Integration: One of the IT trend is moving from hierarchy to team approach. The purpose is to see an alternative to retooling, to react speedily and to develop capabilities rather than exploiting them. Such integration is necessary so as to address to prevalent situations:

(a) Functions needing data and not getting from others

(b) Sending data to those who do not want to require them. (c) Global data exist but do not travel to required business functions. Indian banks seem to follow this trend through the sincere redesign as described earlier. Instead of vertically divided pyramid type organizational set-ups, banks are now being to have separate group like finance, international consumer banking, industrial/commercial credit etc. (3.) From Solo to Partnership: With the development of IT, two things are taking place simultaneously. The work force as a percentage of total staff is going down and spending on IT as percentage of total spending is going up. The forms of partnership can include binding by superior service, accommodation in service sharing network, equal partnership and situations, where survival is threatened. At times, the partnership becomes necessary to get out of areas where there is no competitive advantage. Low development cost or wider geographical coverage is the aspects that create such partnership. Instances are not frequent, where joint ventures have been found with the IT vendors. (4.) Distinctive Edge: It is always said that many use but a few make use of IT. Historically, the emphasis is on using IT for large volumes like payrolls, balancing the books, the consolidation etc. That realization on having IT as matter of competitive edge has come about very lately. It is recognized that customer service is not an easy thing to provide, but IT is used as a mean. It does give value additions and erases barriers for competitors to enter. Banks understand that the cost of cultivating the new customer is 5 to 6 times of retaining the old one. Customer normally switches banks due to poor service. The appreciation of these facts has compelled the banks world over to look upon IT as an instrument to create distinctive edge over competitors. The private sector banks that were established in 1990's as a part of finance sector reforms did make good of IT to have an edge over the others. The foreign banks operating in India have also been able to market IT superiority as a distinctive edge. The public sector banks are still to make use of IT in this regard, although they are blessed with huge information base all across the country. While steps are mooted in this direction by leading public sector banks, more offensive postures are necessary.

(5.) IT as Profit Centre: In the embryonic phases, IT was looked upon a means to get rid of high processing cost and time and to convert the manual operation with high volume/low complexity in two mechanical ones. With the evolutionary the process, it was seen as the best means of generating, MIS. The same approach gave the status of DSS to IT. All along, IT has been recognized as the service function in Indian Banks. However, the new trend that is emerging is considering IT as a profit centre. The cost benefit analysis of having IT or otherwise in one part. But having IT set up to generate income for the organization is the new beginning. Getting jobs from outside the bank for processing data and the like are the current trends. The outsourcing done by others is the business, cater to by these organizations the trend of this kind is not deserved in Indian situation particularly banks. The Banks have been

able to just manage what is to consider as their responsibility as IT, within the individual banks. (6.) Prospering in Down Market: The trend suggests that when there is a down turn in the market place, Pro-active corporations take the benefit of available unutilized resources to upgrade and revisit technology issues. This is seen as the right time to establish the R & D centre for IT. There are false notions about technology and its capability. Some misconceptions include:

Best-fit possible technology is implemented.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

System solution is good enough and there is need to look into user expectations.

Innovations are generally successful.

Success is related only to novel ideas.

Technology is the sole determinant of business success, and

Measures and standards i.e. audit and inspection issues stand in the way of innovation.

The time available to debate on similar issues is ample and these false notions get clarified during the down market. Eventually, the decision makers reach a consensus that IT is not a panacea but it is an enabler that too when well supported by BRP (Business Process Re-engineering), human resources initiatives, physical infrastructure and responsive organization set up. (7.) Leading to Downsizing: The IT initiative is making the organization lean and flat. For IT functionaries downsizing means transferring computing power from mainframe to the personal computer and workstations. Downsizing is a typical issue faced with associated problems. Absence of top management commitment, lack of understanding of the prevalent IT infrastructure, doing too much and too fast and undertaking the exercise without a framework for controlling the downsizing operations are primarily the situations that create adversities in downsizing. In any case the trend of downsizing is very much existent in the IT environment. (8.) Getting Competitive Intelligence: IT is now seen as a resource for gathering and dissemination of executive information system (EIS). The purpose is to minimize that the bombarding and focusing on the relevance, accuracy and timeliness of the information particularly about the competitors such information enhances follow up and tracks early warning on competitor move and also customer expectations.

As far as Indian banks are concerned individually, they have to compete with other banking industry participants as also with other players in the financial sector. The competition from for insurance and government notes and saving, mutual funds and the like is always

forthcoming particularly because of attendant tax benefits. Collection of required information and using the same for business purpose is constrained by the availability of the information, its volume and diversity. As such it may take some time for this trend to be visible in Indian banking scenario. Recent Developments in Banking Sector (1.) Internet: Internet is a networking of computers. In this marketing message can be transferred and received worldwide. The data can be sent and received in any part of the world. In no time, internet facility can do many a job for us. It includes the following:

This net can work as electronic mailing system.

It can have access to the distant database, which may be a newspaper of foreign country.

We can exchange our ideas through Internet. We can make contact with anyone who is a linked with internet.

On internet, we can exchange letters, figures/diagrams and music recording.

Internet is a fast developing net and is of utmost important for public sector undertaking, Education Institutions, Research Organization etc. (2.) Society for Worldwide Inter-bank Financial Telecommunications (SWIFT): SWIFT, as a co-operative society was formed in May 1973 with 239 participating banks from 15 countries with its headquarters at Brussels. It started functioning in May 1977. RBI and 27 other public sector banks as well as 8 foreign banks in India have obtained the membership of the SWIFT. SWIFT provides have rapid, secure, reliable and cost effective mode of transmitting the financial messages worldwide. At present more than 3000 banks are the members of the network. To cater to the growth in messages, SWIFT was upgrade in the 80s and this version is called SWIFT-II. Banks in India are hooked to SWIFT-II system. SWIFT is a method of the sophisticated message transmission of international repute. This is highly cost effective, reliable and safe means of fund transfer.

This network also facilitates the transfer of messages relating to fixed deposit, interest payment, debit-credit statements, foreign exchange etc.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

This service is available throughout the year, 24 hours a day.

This system ensure against any loss of mutilation against transmission.

It serves almost all financial institution and selected range of other users. It is clear from the above benefit of SWIFT that it is very beneficial in effective customer service. SWIFT has extended its range to users like brokers, trust and other agents. (3.) Automated Teller Machine (ATM): ATM is an electronic machine, which is operated by the customer himself to make deposits, withdrawals and other financial transactions. ATM is a step in improvement in customer service. ATM facility is available to the customer 24 hours a day. The customer is issued an ATM card. This is a plastic card, which bears the customer's name. This card is magnetically coded and can be read by this machine. Each cardholder is provided with a secret personal identification number (PIN). When the customer wants to use the card, he has to insert his plastic card in the slot of the machine. After the card is a recognized by the machine, the customer enters his personal identification number. After establishing the authentication of the customers, the ATM follows the customer to enter the amount to be withdrawn by him. After processing that transaction and finding sufficient balances in his account, the output slot of ATM give the required cash to him. When the transaction is completed, the ATM ejects the customer's card. (4.) Cash Dispensers: Cash withdrawal is the basic service rendered by the bank branches. The cash payment is made by the cashier or teller of the cash dispenses is an alternate to time saving. The operations by this machine are cheaper than manual operations and this machine is cheaper and fast than that of ATM. The customer is provided with a plastic card, which is magnetically coated. After completing the formalities, the machine allows the machine the transactions for required amount. (5.) Electronic Clearing Service: In 1994, RBI appointed a committee to review the mechanization in the banks and also to review the electronic clearing service. The committee recommended in its report that electronic clearing service-credit clearing facility should be made available to all corporate bodies/Government institutions for making repetitive low value payment like dividend, interest, refund, salary, pension or commission, it was also recommended by the committee Electronic Clearing Service-Debit clearing may be introduced for pre-authorized debits for payments of utility bills, insurance premium and instalments to leasing and financing companies. RBI has been necessary step to introduce these schemes, initially in Chennai, Mumbai, Calcutta and New Delhi. (6.) Bank net: Bank net is a first national level network in India, which was commissioned in February 1991. It is communication network established by RBI on the basis of recommendation of the committee appointed by it under the chairmanship of the executive director T.N.A. Lyre. Bank net has two phases: Bank net-I and Bank net- II.

Areas of Operation and Application of Bank net:

The message of banking transaction can be transferred in the form of codes from the city to the other.

Quick settlement of transactions and advices.

Improvement in customer service-withdrawal of funds is possible from any member branch.

Easy transfer of data and other statements to RBI.

Useful in foreign exchange dealings.

Access to SWIFT through Bank net is easily possible.

(7.) Chip Card: The customer of the bank is provided with a special type of credit card which bears customer's name, code etc. The credit amount of the customer account is written on the card with

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

magnetic methods. The computer can read these magnetic spots. When the customer uses this card, the credit amount written on the card starts decreasing. After use of number of times, at one stage, the balance becomes nil on the card. At that juncture, the card is of no use. The customer has to deposit cash in his account for re-use of the card. Again the credit amount is written on the card by magnetic means. (8.) Phone Banking: Customers can now dial up the bank's designed telephone number and he by dialling his ID number will be able to get connectivity to bank's designated computer. The software provided in the machine interactive with the computer asking him to dial the code number of service required by him and suitably answers him. By using Automatic voice recorder (AVR) for simple queries and transactions and manned phone terminals for complicated queries and transactions, the customer can actually do entire non-cash relating banking on telephone: Anywhere, Anytime. (9.) Tele-banking: Tele banking is another innovation, which provided the facility of 24 hour banking to the customer. Tele-banking is based on the voice processing facility available on bank computers. The caller usually a customer calls the bank anytime and can enquire balance in his account or other transaction history. In this system, the computers at bank are connected to a telephone link with the help of a modem. Voice processing facility provided in the software. This software identifies the voice of caller and provides him suitable reply. Some banks also use telephonic answering machine but this is limited to some brief functions. This is only telephone answering system and now Tele-banking. Tele banking is becoming popular since queries at ATM's are now becoming too long

(10.) Internet Banking: Internet banking enables a customer to do banking transactions through the bank's website on the Internet. It is a system of accessing accounts and general information on bank products and services through a computer while sitting in its office or home. This is also called virtual banking. It is more or less bringing the bank to your computer. In traditional banking one has to approach the branch in person, to withdraw cash or deposit a cheque or request a statement of accounts etc. but internet banking has changed the way of banking. Now one can operate all these type of transactions on his computer through website of bank. All such transactions are encrypted; using sophisticated multi-layered security architecture, including firewalls and filters. One can be rest assured that one's transactions are secure and confidential. (11.) Mobile Banking: Mobile banking facility is an extension of internet banking. The bank is in association with the cellular service providers offers this service. For this service, mobile phone should either be SMS or WAP enabled. These facilities are available even to those customers with only credit card accounts with the bank.

(12.) Any where Banking: With expansion of technology, it is now possible to obtain financial details from the bank from remote locations. Basic transaction can be effected from faraway places. Automated Teller Machines are playing an important role in providing remote services to the customers. Withdrawals from other stations have been possible due to inter-station connectivity of ATM's. The Rangarajan committee had also suggested the installation of ATM at non-branch locations, airports, hotels, Railway stations, Office Computers, Remote Banking is being further extended to the customer's office and home. (13.) Voice Mail: Talking of answering systems, there are several banks mainly foreign banks now offering very advanced touch tone telephone answering service which route the customer call directly to the department concerned and allow the customer to leave a message for the concerned desk or department, if the person is not available. Challenges Ahead Important Business Challenges:

Meet customer expectations on service and facility offered by the bank.

Customer retention.

Managing the spread and sustain the operating profit.

Retaining the current market share in the industry and the improving the same.

Completion from other players in the banking industry.

Other Important Operational Challenges:

Frequent challenges in technologies used focusing up grades in hardware and software, attending to that implementation issues and timely roll out.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Managing technology, security and business risks.

System re-engineering to enable. Defined and implemented efficient processes to be able to reap benefits off technology to its fullest potential.

Upgrading the skill of work force spread across the country.

With the opening of economy, deregulation, mergers and acquisition of banks, implementation of BASLE II norms, disinvestment of government holding in banks, the competition is going to be increased from new banks and merged entities. This will also open up new opportunities for introduction of a new products and services. A definite trend is emerging as to consolidation of the banking system, sharing of ATM networks and services, tie ups with insurance companies, other billing organizations like mobile operators, electricity and telephone bills and bank for cross selling of various products and services. How to meet the challenges? At corporate level to meet the challenges, various initiated have been taken and implementation is in process beside up gradation of data centre facilities: (1.) Centralization of functions

Inward clearing data uploading and processing

Check book issues

MIS-On-Line Monitoring/Generation of statement by controlling offices

Audit from the remote location

Sending mails and statement of accounts to customers & completion of non-mandatory field in newly opened accounts.

(2.) Single Window System (3.) Revised Account opening form for capturing complete customer/Account data as per CBS requirement. (4.) Call centre for customers

(5.) Customer Relationship Management (CRM) Application. (6.) Data Warehousing. Immediate Focus To facilitate successful implementation of the above initiative, intensive efforts are to be undertaken by all of us on following issues:

Completion of correct MIS details in all accounts and SRM's.

Customer/ Account data completion/correction.

Customer-ID crystallization.

Aggressive marketing of Internet Banking & Debit Card products to increase share of delivery channels transaction.

Skill up gradation & increase in awareness of all staff member.

Strict compliance of Circular & Guidance available online (CBSINFO)/ Messages issued through scrolling ticker on login page.

Present slowdown in rollover must be put to full use to have concrete action on these fronts. Conclusion Indian public sector banks that hold around 75 % of market share do have taken initiative in the field of IT. They are moving towards the centralized database and decentralize decisions making process. They possess enviable quality manpower. Awareness and appreciation of IT are very much there. What is needed is a 'big push' the way it was given in the post nationalization period for expansionary activities. IT and India have become synonymous. Whether India becomes a destination for outsourcing or it becomes a development centre is matter of debate. As far as banking industry in India is concerned it can be said that although the Indian banks may not be as technologically

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

advanced as their counterparts in the developed world, they are following the majority of international trends on the IT front. The strength of Indian banking lie in withering storms and rising up to the expectations from all the quarters-catching up with all the global trends is a matter of time

Overview of IT operations

Introduction:

For banks in which information technology (IT) systems are used to manage information, IT Operations should support processing and storage of information, such that the required information is available in a timely, reliable, secure and resilient manner.

IT Operations are a set of specialized organizational capabilities that provide value to customers (internal or external) in form of IT services. Capabilities take the form of functions and processes for managing services over technology lifecycle. IT Operations should ensure effectiveness and efficiency in delivery and support of these services to ensure value for customers.

Scope:

Functions covered as a part of IT Operations are:

IT Service Management

Infrastructure Management

Application Lifecycle Management

IT Operations Risk Framework

The Board, Senior Management:

Roles and Responsibilities:

Bank's Board of Directors has ultimate responsibility for oversight over effective functioning of IT operational functions. Senior management should ensure the implementation of a safe IT Operation environment. Policies and procedures defined as a part of IT Operations should support bank's goals and objectives, as well as statutory requirements.

Functional areas, within the preview of these roles, are:

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Core IT Operations

Business Line-specific IT Operations

Any Affiliates-related IT Operations

Business Partners' Operations (including that of IT support vendors if any)

The Board or Senior Management should take into consideration the risk associated with existing and planned IT operations and the risk tolerance and then establish and monitor policies for risk management.

Organisational Structure:

IT Operations include business services that are available to internal or external customers using IT as a service delivery component—such as mobile or internet banking. IT Operations include components that are used to support IT Operations: service desk application, ticketing and event management tools, etc. Banks may consider including Test and Quality Assurance Environment (besides, Production Environment) within the scope of IT Operations.

Service Desk: The service desk is the primary point of contact (Single Point of Contact or SPOC) for internal and external customers. Besides handling incidents

and problems, it also provides interface to other IT operation processes, such as Request For Change (RFC), Request Fulfillment, Configuration Management, Service Level Management and Availability Management, etc. It can have the following functions:

Interacting with customers (e-mail, voice or chat): first-line customer liaison

Recording and tracking incidents and problems or requests for change

Keeping customers informed on request status and progress

Making an initial assessment of requests, attempting to resolve them via knowledge management or escalating, based on agreed service levels

Monitoring and escalation procedures relative to the appropriate SLA

Managing the request life-cycle, including closure and verification

Coordinating second-line and third-party support groups

Providing management information for service improvement

Identifying problems

Closing incidents and confirmation with the customer

Contributing to problem identification

Performing user satisfaction surveys

A structure for the Service Desk that allows optimum resource utilization would include:

Local Service Desk

Central Service Desk

Virtual Service Desk

Follow the Sun i.e. in time zones such that service desk is available for assistance and recording of incidents round the clock

Specialized Service Desk Groups

IT Operations Management

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

IT Operations management is a function which is primarily responsible for the day-to-day management and maintenance of an organisation's IT infrastructure, ensuring service delivery to the agreed level as defined by Service Level Agreement (SLA).

IT Operations management can have following functions:

Operational Control: Oversee the execution and monitoring of operational activities and events in IT infrastructure which is within the preview of IT operations. Operational control activities are normally carried out by Network Operations Centre (NOC) or Operations Bridge. Beside execution and monitoring of routine tasks operation control also involve the following activities :

Console Management

Job Scheduling

Backup and Restoration

Print and Output Management

General Maintenance Activities

Facility Management: It refers to management of physical IT environment of data centre, computers rooms and recovery sites

Operations Management Structure: For all practical reasons, application management and infrastructure management teams should be part of IT operations. As, these functions manage and execute operational activities, whereas others delegate these to dedicate IT operations function.

Application Management:

It involves handling and management of application as it goes through the entire life-cycle. The life-cycle encompasses both application development and application management activities. Sub-activities that can be defined for application management functions are:

Application Development: It is concerned with activities needed to plan, design and build an application that ultimately is used by a part of the organisation to address a business requirement. This also includes application acquisition, purchase, hosting and provisioning

Application Maintenance/Management: It focuses on activities that are involved with the deployment, operation, support and optimisation of the application

Application Management related functions may include the following:

Managing operational applications, whether vendor developed, or off-the-shelf or in-house

It acts as a custodian of technical knowledge and expertise related to managing and supporting applications. It ensures that the technical knowledge and expertise required to

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

design, develop, test, manage and improve IT services are identified, developed and refined. Therefore, it participates in IT operation management

It ensures that appropriate resources are effectively trained and deployed to deliver, build, transit, operate and improve the technology required to manage and support IT services

It defines and executes training programmes

It documents skill sets available within an organisation and skills that need to be developed to manage application management as function

It defines standards to be adapted when defining new application architecture and involvement in design and build of new services

It assesses the risk involved in an application architecture

It records feedbacks on availability and capacity management activities

It designs and performs tests for functionality, performance and manageability of IT services

It defines and manages event management tools

It participates in incident, problem, performance, change and release management, and in resource fulfillment

It provides information on the Configuration Management System

Application Management Structure: Though activities to manage applications are generic and consistent across applications; application management function, for all practical reasons, is not performed by a single department or group. It consists of technical areas as per technical skill sets and expertise. Some of these can be:

Financial application

Infrastructure applications

Messaging and collaborative applications

Web portal or web applications

Contact centre applications

Function-specific applications

Infrastructure Management

It is the function primarily responsible for providing technical expertise and overall management of the IT infrastructure. Its primary objective is to assist in plan, implement and maintenance of a stable technical infrastructure in order to support an organisation's business processes.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Infrastructure Management can have following functions:

Manage IT infrastructure components for an environment, which falls within the preview of IT operations

It acts as a custodian of technical knowledge and expertise, related to the management of IT infrastructure. It ensures that technical knowledge and expertise required to design, develop, test, manage and improve IT services are identified, developed and refined

It ensures appropriate resources are effectively trained and deployed to deliver, build, transit, operate and improve the technology required to deliver and support IT infrastructure

It helps define and execute training programmes

It helps document skill sets available within an organisation and skills needed to be developed to manage infrastructure management as function

Definition of standards to be adapted when defining new IT architecture and involvement in the design and build of new services

Risk assessment for IT infrastructure architecture

Feedbacks to availability and capacity management activities

Designing and performing tests for functionality, performance and manageability of IT services

Definition and management of event management tools

Participation in incident, problem, performance, change and release management and resource fulfillment

Infrastructure management function should provide information or manage for configuration Management System

Infrastructure Management Structure: For all practical reasons, infrastructure management function is not performed by a single department or group, it consist of technical areas as per the technical skill sets and expertise, some of these are:

Mainframe management team

Server management team

Storage management team

Network support team

Desktop support team

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Database management team

Middleware management team

Directory services team

Internet team

Messaging team

IP-based telephony team

Components of IT operations framework: a)

Risk Management

Banks should analyse their IT Operation environment, including technology, human resources and implemented processes, to identify threats and vulnerabilities. They should conduct a periodic risk assessment which should identify:

Internal and external risks

Risks associated with individual platforms, systems, or processes, as well as automated processing units

While identifying the risks, a risk assessment process should quantify the probability of a threat and vulnerability, and the financial consequences of such an event. Banks should also consider the inter-dependencies between risk elements, as threats and vulnerabilities have the potential to quickly compromise inter-connected and inter-dependent systems and processes.

Banks should implement a cost-effective and risk-focused environment. The risk control environment should provide guidance, accountability and enforceability, while mitigating risks.

Risk Categorisation: As a part of risk identification and assessment, banks should identify events or activities that could disrupt operations, or negatively affect the reputation or earnings, and assess compliance to regulatory requirements. Risks identified can be broadly categorised into following categories:

Strategic Failures: That might include improper implementation, failure of supplier, inappropriate definition of requirements, incompatibility with existing application infrastructure etc. It will also include regulatory compliance

Design Failures: It might include inadequate project management, cost and time overruns, programming errors and data migration failures among others

Transition Failures: It might include inadequate capacity planning, inappropriately defined availability requirements, SLA / OLA / Underpinning contracts not appropriately defined and information security breaches, among others

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Risk Mitigation: Once the organisation has identified, analyzed and categorized the risks, organisation should define following attributes for each risk component:

Probability of Occurrence;

Financial Impact;

Reputational Impact;

Regulatory Compliance Impact;

Legal Impact.

Beside above specified attributes, an organisation should also consider these:

Lost revenues

Loss of market share

Non-compliance of regulatory requirements

Litigation probability

Data recovery expenses

Reconstruction expenses

These, along with the business process involved, should be used to prioritise risk mitigation actions and control framework.

IT Operations Processes

IT Strategy

Processes within IT Strategy provide guidance to identify, select and prioritise services that are aligned to business requirements. IT strategy, as a framework, provides feedback to IT Operations on the services to be supported and their underlying business processes and prioritisation of these services, etc.

A well-defined IT Strategy framework will assist IT Operations in supporting IT services as required by the business and defined in OLA / SLAs.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

IT Strategy processes provide guidelines that can be used by the banks to design, develop, and implement IT Operation not only as an organisational capability but as a strategic asset.

Financial Management: It provides mechanism and techniques to IT operations to quantify in financial terms, value of IT services it supports, value of assets underlying the provisioning of these services, and qualification of operational forecasting.

Advantages of implementing Financial Management process are:

- Assists in decision-making
- Speed of changes
- Service Portfolio Management
- Financial compliance and control
- Operational control
- Value capture and creation

Service Valuation

It is the mechanism that can be considered by banks to quantify services, which are available to customers (internal or external) and supported by IT operations in financial terms. It assists IT Operation functions to showcase the involvement of function in supporting the bank's core business.

Financial Management uses Service Valuation to quantify financial terms, value of IT services supported by IT Operations. It provides a blueprint from which businesses can comprehend what is actually delivered to them from IT. Combined with Service Level Management, Service Valuation is the means to a mutual agreement with businesses, regarding what a service is, what its components are, and its cost and worth.

Service Valuation quantifies, in financial terms, funding sought by a business and IT for services delivered, based on the agreed value of those services. The activity involves identifying cost baseline for services and then quantifying the perceived valued, added by the provider's service assets in order to conclude a final service value.

Service Valuation will have two components, these being:

Provisioning Value: The actual underlying cost of IT, related to provisioning a service, including all fulfillment elements—tangible and intangible. Input comes from financial systems and consists of payment of actual resources consumed by the IT in the provisioning of services. This cost element includes items such as:

Hardware and software license cost

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Annual maintenance fees for hardware and software

Personnel resources used in the support or maintenance of the services

Utilities, data centre or other facilities charge

Taxes, capital or interest charges

Compliance costs

Service Value Potential: Is the value-added component based on a customer's perception of value from the service or expected marginal utility and warranty from using the services in comparison with what is possible using the customer's own assets.

Portfolio Management

It provides guidelines that can be considered by banks for governing investments in service management across an enterprise and managing them for value. Portfolio management contains information for all existing services, as well as every proposed service—those that are in conceptual phase.

Every service, which is a part of service portfolio, should include a business case, which is a model of what a service is expected to achieve. It is the justification for pursuing a course of action to meet stated organisational goals. Business case links back to service strategy and funding. It is the assessment of a service management in terms of potential benefits and the resources and capabilities required to provision and maintain the service. Portfolio Management framework defined by the banks should highlight controls, which are defined to develop an IT Service from conceptual phase to go- live phase and then to transition to production environment. During the development of IT services financial impact of the new service on IT Operation should also be ascertained which will assist IT Operations in Service Validation.

Demand Management

Demand Management process provides guidelines which can be used by banks to understand the business processes IT operations supports to identify, analyse, and codify Patterns of business activities (PBA) to provide sufficient basic for capacity requirement. Analysing and tracking the activity patterns of the business process makes it possible to predict demand for services. It is also possible to predict demand for underlying service assets that support these services.

Demand Management guidelines should also take into consideration IT Operations involvement in development of service from conceptual phase to go to the live phase, so that there is a transparency of demand of new service in IT Operations.

li) Design

The design phase of the IT operations provides the guidelines and processes, which can be used by the banks to manage the change in the business landscape. Components which should be considered when designing a new IT service or making a change to the existing IT service are:

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Business Processes

IT Services

Service-level Agreements
IT Infrastructure

IT Environment

Information Data

Applications

Support Services

Support Teams

Suppliers

Service design: This should not consider components in isolation, but must also consider the relationship between each of the components and their dependencies on any other component or service.

Design phase: Provides a set of processes and guidelines that can be used by banks to design IT services, supported by IT operations, that satisfies business objectives, compliance requirements and risk and security requirements. The processes also provide guidelines to identify and manage risks and to design secure and resilient IT services.

Service Catalogue Management

Over the years, banks' IT infrastructure has grown and developed. In order to establish an accurate IT landscape, it is recommended that an *IT Service Catalogue* is defined, produced and maintained. It can be considered as a repository that provides information on all IT services supported by IT Operations framework.

The Service Catalogue Management process provides guidelines, used by banks to define and manage service catalogue, which provides a consistent and accurate information on all IT services available to customers (internal or external). It also ensures that the service catalogue is available to users, who are approved to access it. It should contain details of all services that are in production, as well as the services that are being prepared for transition. Banks may consider following attributes to be included into the service catalogue:

Definition of Service

Categorization of Service (business application and IT support)

Service Criticality

Disaster Recovery Class

Service-level Agreement Parameters

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Service Environment (Production, Testing, Quality Assurance, Staging, etc.)

IT Support Status (Operational and Transaction, etc.)

Configuration Management Group

Incident Management Group

Problem Management Group

Change and Release Management Group

Service Owner

Service-level Manager

Principal Business Activities Details

Interdependency on Configuration Items

Interdependency on Service Portfolio

Service catalogue provides details of services available to customers such as intended use,

business processes they enable and the level and quality of service the customer can expect from each service. Banks can also consider incorporating “charge back mechanism”, as defined in financial management into the service catalogue.

A Service catalogue has two aspects:

Business Service Catalogue: It contains details of all IT services delivered to a customer, together with relationships with business units and business processes that rely on IT services. This is the customer view of the catalogue. Business Service Catalogue facilitates development of robust Service Level Management process.

Technical Service Catalogue: It contains details of all IT services delivered to a customer, together with his or her relationship with supporting and shared services, relationship to configuration items (CIs). CIs can be a service asset or component, or any other item that is under control of configuration management. Depending on established strategy configuration, an item may vary widely in complexity, size and type. It can range from entire services or systems to a single software module or a minor software component. (Configuration Items are explained in details in “Service Assets and Configuration Management” section of the guidelines.) It facilitates the development of the relationship between services, underlying CIs, SLAs and OLAs, and the support groups, which support services throughout its life-cycle.

Service Level Management

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

This process defines the framework that can be used by banks to plan, co-ordinate and draft, agree, monitor and report service attributes used to measure the service quality. Its framework also includes guidelines for ongoing review of service achievements to ensure that the required and cost-justifiable service quality is maintained and improved. Beside current services and SLAs, this management provides guidelines to ensure that new requirements are captured. That new or changed services and SLAs are developed to match the business needs and expectations.

Service Level Management process should be able to meet the following objectives:

Define, document, agree, monitor, measure, report and review the level of IT services

Ensure specific and quantifiable targets are defined for IT services

Ensure that IT Operations and consumers have clear, unambiguous expectations of the level of services to be delivered

Ensure that pro-active measures, to improve the level of service delivered, are implemented if cost-justified

While defining SLM framework for banks, the following aspects should also be considered

Operational-level agreement to ensure that Operational Level Agreements (OLAs) with other support groups are defined and developed; these OLAs should be in line with SLAs which it supports

Underpinning supplier contract to ensure all underpinning supplier contracts with the vendors or suppliers are defined and developed: these contracts should be in line with SLAs, which it supports

While defining Service Level Agreement as a part of Service Level Management framework, the following options can be considered:

Service based SLA: Its structure covers attributes for single service across an organisation. For instance, SLA for internet banking service

Customer based SLA: The structure covers attributes for all services for a defined set of customers. For instance, SLA for SMEs customers

Multi-Level SLA: Multi-level SLA

structure can be defined as per the organizational hierarchy. For instance, SLA for corporate offices, branches and head offices

Attributes that are included in SLAs should be ones which can effectively be monitored and measured. Attributes which are included in the SLAs can be categorised into operational, response, availability and security attributes. Service Level Management framework should also define guidelines for reviews of Service Level Agreements, Operational Level Agreements, and underpinning contracts to ensure that they are aligned to business needs and strategy. These should ensure that services covered, and targets for each, are relevant. And that nothing significant is changed that invalidates the agreement in any way. Service Level Management framework defined should also have guidelines defined for logging and management, including escalation of complaints and compliments.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Capacity Management

The process provides the framework and guidelines that can be adapted by banks to ensure that cost-justifiable IT capacity exists and matches to current- and future-agreed business requirements as identified in Service Level Agreement.

The Capacity Management process provides guidelines to:

Produce and maintain capacity plan that reflects the current and future business requirements

Manage service performance so that it meets or exceeds the agreed performance targets

Diagnosis and resolution of performance and capacity-related incidents and problems

Assess impact of all changes on capacity plan and performance of IT services supported by IT Operations

Ensure that pro-active measures are undertaken to improve the performance of services, whenever it is cost-justifiable.

One of the key activities defined as a part of capacity management process is to produce and maintain, at an ongoing basis, the capacity plan, which depicts current level of resource utilization and service performance. Capacity plans can also include forecasting future requirements to support business activities. *The process can be subdivided into three:*

Business Capacity Management: Defines guidelines for translating business-need plans into requirements for IT services and supporting infrastructure, ensuring that the future business requirements for IT services are quantified, designed, planned and implemented. Inputs for future IT requirements come from the Service Portfolio and Demand Management.

Service Capacity Management: This defines guidelines for management, control and prediction of end-to-end performance and capacity of live and operational IT service usage and workloads. It provides guidelines to ensure that the performance of IT services is monitored and measured.

Component Capacity Management: It defines guidelines to identify and understand the performance, capacity and utilization of each individual component within a technology used to support IT services, including infrastructure, environment, data and applications.

A major difference between sub-processes is in the data that is being monitored and collected. For example, the level of utilization of individual components in the infrastructure: processors, disks and network links will be under Component Capacity Management. While transaction throughput rates and response times will be under Service Capacity Management. Business Capacity Management will be concerned with data, specific to

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

business volumes. Banks adapting capacity management process should ensure that its framework encompass all areas of technology (hardware, software, human resource, facilities, etc.)

Availability Management

Availability and reliability of IT services can directly influence customer satisfaction and reputation of banks. Therefore Availability Management is essential in ensuring that the IT delivers the “right level” of service required by the business to satisfy its objectives. The process provides framework and guidelines that can be adapted by banks to ensure that the level of service availability (for all services) is matched, or exceeds the current and future requirements, as defined in the Service Level Agreement.

Availability Management process provides guidelines so that banks can:

Produce and maintain an appropriate up-to-date Availability Plan that reflects the current and future needs of the business

Ensure that service availability achievements meet or exceed agreed targets, by managing services and resources-related availability targets

Assist with diagnosis and resolution of availability-related incidents and problems

Ensure that pro-active measures to improve the availability of services are implemented wherever it is cost justifiable to do so

When implementing Availability Management processes, banks should consider including the following:

All operational services and technology, supported by IT Operations function and for which there is a formal SLA

New services where Service Level Requirement and Agreement have been established

Aspects of IT's services and components that may impact availability, which may include training, skills, process effectiveness, procedures and tools

Availability Management process has two key elements:

Reactive activities: The reactive aspect of availability management involves monitoring, measuring, analysis and management of events, incidents, problems and changes, involving unavailability

Proactive activities: This aspect involves planning, design and improvement of availability

Attributes that can be used by the banks for reporting availability of IT services, can be:

Availability: The ability of a service, component or CI, to perform the agreed function when required.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Agreed Service Time - Downtime

$$\text{Availability (\%)} = \frac{\text{Service Time}}{\text{Agreed Service Time}} \times 100$$

Downtime should only be included in the above calculation, when it occurs within the “Agreed Service Time”.

Mean Time Between Service Incidents (MTBSI): MTBSI refers to how long a service; component or CI can perform its agreed function without interruption.

Available time in hours

$$\text{MTBSI} = \frac{\text{Available time in hours}}{\text{Number of Breaks}}$$

Number of Breaks

Mean Time Between Failures (MTBF): MTBF refers to how long a service; component or CI can perform its agreed function without reporting a failure.

Available time in hours – Total downtime in Hours

$$\text{MTBF} = \frac{\text{Available time in hours – Total downtime in Hours}}{\text{Number of breaks}}$$

Number of breaks

Mean Time Between Failures (MTBF): is the mean time between the recovery from one incident and occurrence of the next incident, it is also known as uptime. This metric relates to the reliability of the IT Service supported by IT Operations.

Mean Time to Repair (MTTR): MTTR refers to how quickly and effectively a service, component or CI can be restored to normal working after failure.

Total downtime in Hours

$$\text{MTTR} = \frac{\text{Total downtime in Hours}}{\text{Number of breaks}}$$

Number of breaks

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Mean Time to Repair (MTTR): This is the average time between occurrence of a fault and service recovery. It is also known as downtime. This metric relates to the recoverability and serviceability of the IT Services supported by IT Operations.

Vital Business Functions

When defining availability targets for a business service, banks should consider identifying Vital Business Function (VBF). VBF represents critical business elements of a process supported by IT services. For example, an ATM will have following business functions:

Cash dispensing

Reconciliation with the relevant account

Statement printing.

Out of these three, cash dispensing and reconciliation should be considered as vital business functions, influencing the availability design and associated costs.

Supplier Management

Complex business demands require extensive skills and capabilities from IT to support business processes, therefore collaboration with service providers and value networks are an integral part of end-to-end business solution. Supplier Management process provides framework and guidelines that can be used by banks to manage relationships with vendors, suppliers and contractors. This framework ensures that suppliers and services they provide are managed to support IT service targets and business expectations. The purpose of this management process is to obtain value for money from suppliers, and to ensure that suppliers perform to the targets contained within contracts and agreements, while conforming to all terms and conditions.

Supplier Management process provides guidelines which can be used by the banks to:

Implement and enforce supplier policies

Maintenance of supplier and contact database

Supplier and contact categorization and risk assessment

Supplier and contract evaluation and selection

Development, negotiation and agreement of contracts

Contract review, renewal and termination

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Management of suppliers and supplier performance

Agreement and implementation of service and supplier improvement plans

Maintenance of standard contracts, terms and conditions

Management of contractual dispute resolution

Management of sub-contracted suppliers

iii) Transition

The transition phase provides frameworks and processes that may be utilised by banks to:

Evaluate service capabilities and risk profile of new or changes service before it is released into production environment

Evaluate and maintain integrity of all identified service assets and configuration items required to support the service

Service Asset and Configuration Management

Service Asset and Configuration Management process provides framework and guidelines that can be used by the banks to manage service assets and configuration items that supports business services.

The framework provides guidelines to:

Identify, control, record, audit and verify service assets and configuration items, including service baseline version controls their attributes and relationships.

Manage and protect integrity of service assets and configuration items through the service lifecycle by ensuring only authorised assets are used and only authorised changes are made.

Ensure integrity of configuration items required to support business services and IT infrastructure by establishing and maintaining an accurate and complete Configuration Management System.

Provide accurate information of configuration items to assist in change and release management process.

Service asset management manages assets across its lifecycle from acquisition through disposal. Implementation of Service Asset and Configuration Management framework has cost and resources implications and therefore strategic discussions needs to be made about the priorities to be addressed. For instance banks can decide on initially focusing on the basic IT assets (hardware and

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

software) and the services and assets that are business critical or covered by legal regulatory compliance.

Components that can be considered as part of Service Asset and Configuration Management are:

Configuration Items: These can be a service asset or component, or any item that is under the control of configuration management. Depending on established strategy

configuration, the item may vary widely in complexity, size and type. It can range from an entire service or system to a single software module or a minor software component.

If desired, banks can define a hierarchical structure for configuration items. For instance banks can define Core Banking as a configuration item which can have different application as a subset Configuration Item of the Core Banking configuration item. Each configuration item can have modules as sub set which can have two configuration item, these being hosting and application support. Hosting can then be further sub-divided into configuration item that can be servers, operating systems, databases, network components.

Configuration Management System: To manage large and complex IT environment banks may consider implementation of supporting system known as Configuration Management System. Beside holding information about configuration items, their components and relationship between configuration items Configuration Management System can also be used to correlate services and configuration items; this kind of snapshot will assist in proactively identifying incidents, events etc.

Secure libraries: Secure library is a collection of software, electronic or document CIs. Access to items in a secure library is restricted. The secure library is used for controlling and releasing components throughout the service lifecycle.

Definitive Media Library: Definitive media library (DML) is a secure library that may be used to store definitive authorised versions of all media CIs. It stores master copies of versions that have passed quality assurance checks.

Configuration Baseline: This baseline is the configuration of a service, product or infrastructure that has been formally reviewed and agreed on, that thereafter serves as the basis for further activities and that can be changed only through formal change procedure. Configuration baseline captures and represents a set of configuration items that are related to each other.

Snapshot: It defines the current state of configuration items or an environment.

Change Management: This process provides guidelines which can be used by the banks for handling changes to ensure that the changes are recorded, assessed, authorised, prioritised, planned, tested, implemented, documented and reviewed in a controlled manner and environment. The primary objective of the change management procedures is to ensure assessment of:

Risks

Change authorization

Business Continuity

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Change impact

iv) Operations

This phase, as a part of Service Management lifecycle, is responsible for executing and performing processes that optimise the cost of the quality of services. As a part of the organisation, it's responsible for enabling businesses to meet objectives. As a part of technology, it's responsible for effective functioning of components that support business services.

Event Management

Event Management process provides the guidelines which can be used by the banks to define the framework for monitoring all the relevant events that occurs through the IT

infrastructure. It provides the entry point for the execution of many Service Operations processes and activities.

Event can be defined as any detectable or discernible occurrence that has significance for the management of the IT infrastructure, or delivery of IT services. *Event Management framework when defined will have two mechanisms for monitoring, these are:*

Active Monitoring: Active monitoring is related to polling of business significant Configuration Items to determine their status and availability. Any diversion from normal status should be reported to appropriate team for action.

Passive Monitoring: Passive monitoring detects and correlate operational alerts or communications generated by Configuration Items.

Event Management can be applied to any aspect of Service Management that needs to be controlled. These components can be:

Configuration Items

Environment conditions

Software licence monitoring

Security breaches

Event Management portfolio can have different kind of event, some of these are:

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Informational: Events signifying regular operations for instance notification that a scheduled job has completed

Warning: Events signifying diversion from normal course of action, for instance a user attempting to login with incorrect password. Exceptional events will require further investigation to determine an environment which may have led to an exception

Exceptions: Events, which are unusual. Events may require closer monitoring. In some case the condition will resolve itself. For instance, unusual combinations of workloads as they are completed, normal operations will restore. In other cases, operations intervention will be required if the situation is repeated

Incident Management

An incident is an unplanned interruption to an IT service, or the reduction in the quality of an IT service. Failure of a configuration item that has not yet impacted service shall also be an incident.

Incident Management process provides guidelines that can be implemented by the banks for the management of incidents so that restoration of service operations as quickly as possible and to minimise adverse impact on business operations. The primary objective of the Incident Management procedures is to ensure best possible level of service quality and availability.

Problem Management

Problem Management process provides a framework, which can be implemented by banks to minimise the adverse impact of incidents on the IT Infrastructure and the business by identifying root cause, logging known errors, providing and communicating workarounds, finding permanent solutions, and preventing recurrence of incidents related to these errors. Problem Management increases stability and integrity of the infrastructure.

Problem Management process includes activities required to carry out the root causes of incidents and to determine the resolution to these underlying problems. Problem management procedures also include implementation of the resolution through Change

Management procedures and Release Management procedures. This also includes appropriate turnaround and resolutions to incidents that cannot be resolved due to business cases, or technical short falls. Periodic trend analysis of the problems in respect of systems or customer facing channels may be carried out and appropriate action taken.

Access Management

Access Management process provides the guidelines, which can be implemented by banks to limit access to IT services only to those individuals and applications that are duly authorised based on organisational policies and standards. Access Management enables the organisation to manage confidentiality, integrity of the organisation's data, IT infrastructure, and applications.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Various payment and settlement systems

1 The Payment and Settlement Systems Act 2007, set up by the RBI, provides for the regulation and supervision of payment systems in India and designates the apex institution (RBI) as the authority for that purpose and all related matters. To exercise its powers and perform its functions and discharge its duties, the RBI is authorized under the Act to constitute a committee of its central board, which is known as the Board for Regulation and Supervision of Payment and Settlement Systems (BPSS). The Act also provides the legal basis for 'netting' and 'settlement finality'.

The PSS Act, 2007 received the assent of the President on 20th December 2007 and came into force with effect from 12th August 2008

The PSS Act, 2007 provides for the regulation and supervision of payment systems in India and designates the Reserve Bank of India (Reserve Bank) as the authority for that purpose and all related matters. The Reserve Bank is authorized under the Act to constitute a Committee of its Central Board known as the Board for Regulation and Supervision of Payment and Settlement Systems (BPSS), to exercise its powers and perform its functions and discharge its duties under this statute. The Act also provides the legal basis for "netting" and "settlement finality". This is of great importance, as in India, other than the Real Time Gross Settlement (RTGS) system all other payment systems function on a net settlement basis.

Under the PSS Act, 2007, two Regulations have been made by the Reserve Bank of India, namely, the Board for Regulation and Supervision of Payment and Settlement Systems Regulations, 2008 and the Payment and Settlement Systems Regulations, 2008. Both these Regulations came into force along with the PSS Act, 2007 on 12th August 2008

2. The Board for Regulation and Supervision of Payment and Settlement Systems Regulation, 2008 deals with the constitution of the Board for Regulation and Supervision of Payment and Settlement Systems (BPSS), a Committee of the Central Board of Directors of the Reserve Bank of India. It also deals with the composition of the BPSS, its powers and functions, exercising of powers on behalf of BPSS, meetings of the BPSS and quorum, the constitution of Sub-Committees/Advisory Committees by BPSS, etc. The BPSS exercises the powers on behalf of the Reserve Bank, for regulation and supervision of the payment and settlement systems under the PSS Act, 2007.

The Payment and Settlement Systems Regulations, 2008 covers matters like form of application for authorization for commencing/ carrying on a payment system and grant of authorization, payment instructions and determination of standards of payment systems, furnishing of returns/documents/other information, furnishing of accounts and balance sheets by system provider etc

3. India has multiple payments and settlement systems, both gross and net settlement systems. For gross settlement India has a [Real Time Gross Settlement](#) (RTGS) system called by the same name and net settlement systems include Electronic Clearing Services (ECS Credit), Electronic Clearing Services (ECS Debit), [credit cards](#), [debit cards](#), the [National Electronic Fund Transfer](#) (NEFT) system and [Immediate Payment Service](#).

4. Electronic Payment and Settlement Systems in India

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

The Reserve Bank of India is doing its best to encourage alternative methods of payments which will bring security and efficiency to the payments system and make the whole process easier for banks.

The Indian banking sector has been growing successfully, innovating and trying to adopt and implement electronic payments to enhance the banking system. Though the Indian payment systems have always been dominated by paper-based transactions, e-payments are not far behind. Ever since the introduction of e-payments in India, the banking sector has witnessed growth like never before.

According to a survey by celent, the ratio of e-payments to paper based transactions has considerably increased between 2004 and 2008. This has happened as a result of advances in technology and increasing consumer awareness of the ease and efficiency of internet and mobile transactions.^[2]

In the case of India, the RBI has played a pivotal role in facilitating e-payments by making it compulsory for banks to route high value transactions through Real Time Gross Settlement (RTGS) and also by introducing NEFT (National Electronic Funds Transfer) and NECS (National Electronic Clearing Services) which has encouraged individuals and businesses to switch as it is clearly one of the fastest growing countries for payment cards in the Asia-Pacific region. Behavioral patterns of Indian customers are also likely to be influenced by their internet accessibility and usage, which currently is about 32 million PC users, 68% of whom have access to the net. However these statistical indications are far from the reality where customers still prefer to pay "in line" rather than online, with 63% payments still being made in cash. E-payments have to be continuously promoted showing consumers the various routes through which they can make these payments like ATM's, the internet, mobile phones and drop boxes.

Due to the efforts of the RBI and the (BPSS) now over 75% of all transaction volume are in the electronic mode, including both large-value and retail payments. Out of this 75%, 98% come from the RTGS (large-value payments) whereas a meager 2% come from retail payments. This means consumers have not yet accepted this as a regular means of paying their bills and still prefer conventional methods. Retail payments if made via electronic modes are done by ECS (debit and credit), EFT and card payments.^[2]

5. Electronic Clearing Service (ECS Credit)

Known as "Credit-push" facility or one-to-many facility this method is used mainly for large-value or bulk payments where the receiver's account is credited with the payment from the institution making the payment. Such payments are made on a timely-basis like a year, half a year, etc. and used to pay salaries, dividends or commissions. Over time it has become one of the most convenient methods of making large payments.

6. Electronic Clearing Services (ECS Debit)

Known as many-to-one or "debit-pull" facility this method is used mainly for small value payments from consumers/ individuals to big organizations or companies. It eliminates the need for paper and instead makes the payment through banks/corporates or government departments. It facilitates individual payments like telephone bills, electricity bills, online and card payments and insurance payments. Though easy this method lacks popularity because of lack of consumer awareness.

7. Credit cards and Debit cards

As mentioned above India is one of the fastest growing countries in the plastic money segment. Already there are 130 million cards in circulation, which is likely to increase at a very fast pace due to rampant consumerism. India's card market has been recording a growth rate of 30% in the last 5 years. Card payments form an integral part of e-payments in India because customers make many payments on their card-paying their bills, transferring funds and shopping.

Ever since Debit cards entered India, in 1998 they have been growing in number and today they consist of nearly 3/4th of the total number of cards in circulation.

Credit cards have shown a relatively slower growth even though they entered the market one decade before debit cards. Only in the last 5 years has there been an impressive growth in the number of credit cards- by 74.3% between 2004 and 2008. It is expected to grow at a rate of about 60% considering levels of employment and disposable income. Majority of credit card purchases come from expenses on jewellery, dining and shopping.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Another recent innovation in the field of plastic money is co branded credit cards, which combine many services into one card-where banks and other retail stores, airlines, telecom companies enter into business partnerships. This increases the utility of these cards and hence they are used not only in ATM's but also at Point of sale (POS) terminals and while making payments on the net.

8.Real-time gross settlement

The acronym 'RTGS' stands for real time gross settlement. The Reserve Bank of India (India's Central Bank) maintains this payment network. Real Time Gross Settlement is a funds transfer mechanism where transfer of money takes place from one bank to another on a 'real time' and on 'gross' basis. This is the fastest possible money transfer system through the banking channel. Settlement in 'real time' means payment transaction is not subjected to any waiting period. The transactions are settled as soon as they are processed. 'Gross settlement' means the transaction is settled on one to one basis without bunching with any other transaction. Considering that money transfer takes place in the books of the Reserve Bank of India, the payment is taken as final and irrevocable.

Fees for RTGS vary from bank to bank. RBI has prescribed upper limit for the fees which can be charged by all banks both for NEFT and RTGS. Both the remitting and receiving must have core banking in place to enter into RTGS transactions. Core Banking enabled banks and branches are assigned an Indian Financial System Code (IFSC) for RTGS and NEFT purposes. This is an eleven digit alphanumeric code and unique to each branch of bank. The first four letters indicate the identity of the bank and remaining seven numerals indicate a single branch. This code is provided on the cheque books, which are required for transactions along with recipient's account number.

RTGS is a large value (minimum value of transaction should be ₹2,00,000) funds transfer system whereby financial intermediaries can settle interbank transfers for their own account as well as for their customers. The system effects final settlement of interbank funds transfers on a continuous, transaction-by-transaction basis throughout the processing day. Customers can access the RTGS facility between 9 am to 4:30 pm (Interbank up to 6:30 pm) on weekdays and 9 am to 2:00 pm (Interbank up to 3:00 pm) on Saturdays. However, the timings that the banks follow may vary depending on the bank branch. Time Varying Charges has been introduced w.e.f. 1 October 2011 by RBI. The basic purpose of RTGS is to facilitate the transactions which need immediate access for the completion of the transaction.

Banks could use balances maintained under the cash reserve ratio (CRR) and the intra-day liquidity (IDL) to be supplied by the central bank, for meeting any eventuality arising out of the real time gross settlement (RTGS). The RBI fixed the IDL limit for banks to three times their net owned fund (NOF).

The IDL will be charged at ₹25 per transaction entered into by the bank on the RTGS platform. The marketable securities and treasury bills will have to be placed as collateral with a margin of five per cent. However, the apex bank will also impose severe penalties if the IDL is not paid back at the end of the day.

The RTGS service window for customer's transactions is available from 8:00 hours to 19:00 hours on week days and from 8:00 hours to 13:00 hours on Saturdays.

No Transaction on weekly holidays and public holidays.

Service Charge for RTGS

a) Inward transaction– no charge to be levied.

b) Outward transactions –

- For transactions of ₹2 lakhs to ₹5 lakhs -up to ₹25 per transaction plus applicable Time Varying Charges (₹1/- to ₹5/-); total not exceeding ₹30 per transaction, (+ GST).

- Above ₹5 lakhs - ₹50 per transaction plus applicable Time Varying Charges (₹1/- to ₹5/-); total charges not exceeding ₹55 per transaction, (+ GST).

No time varying charges are applicable for RTGS transactions settled up to 1300 hrs.

9.National Electronic Funds Transfer (NEFT)

Started in Nov.-2005,^[1] the National Electronic Fund Transfer (NEFT) system is a nationwide system that facilitates individuals, firms and corporates to electronically transfer funds from any bank branch to any individual, firm or corporate having an account with any other bank branch in the country.It is

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

done via electronic messages. Even though it is not on real time basis like RTGS (Real Time Gross Settlement), hourly batches are run in order to speed up the transactions.

For being part of the NEFT funds transfer network, a bank branch has to be NEFT-enabled. NEFT has gained popularity due to it saving on time and the ease with which the transactions can be concluded. As at end-January 2011, 74,680 branches / offices of 101 banks in the country (out of around 82,400 bank branches) are NEFT-enabled. Steps are being taken to further widen the coverage both in terms of banks and branches offices. As on 30.12.2017 total no of NEFT enabled branches are increased to 139682 of 188 Banks.

(https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=112)

10. Indo-Nepal Remittance Facility Scheme

Indo-Nepal Remittance Facility is a cross-border remittance scheme to transfer funds from India to Nepal, enabled under the NEFT Scheme. The scheme was launched to provide a safe and cost-efficient avenue to migrant Nepalese workers in India to remit money back to their families in Nepal. A remitter can transfer funds up to ₹50,000 (maximum permissible amount) from any of the NEFT-enabled branches in India. The beneficiary would receive funds in Nepalese Rupees.

11. Immediate Payment Service (IMPS)

Immediate Payment Service (IMPS) is an initiative of National Payments Corporation of India (NPCI). It is a service through which money can be transferred immediately from one account to the other account, within the same bank or accounts across other banks. Upon registration, both the individuals are issued an MMID (Mobile Money Identifier) Code from their respective banks. This is a 7 digit numeric code. To initiate the transaction, the sender in his mobile banking application need to enter the registered mobile number of the receiver, MMID of the receiver and amount to be transferred. Upon successful transaction, the money gets credited in the account of the receiver instantly. This facility is available 24X7 and can be used through mobile banking application. Some banks have also started providing this service through internet banking profile of their customers. Though most banks offer this facility free of cost to encourage paperless payment system, ICICI bank and Axis bank charge for it as per their respective NEFT charges.

Nowadays, money through this service can be transferred directly also by using the receiver's bank account number and IFS code. In such case, neither the receiver of the money need to be registered for mobile banking service of his bank, nor does he need MMID code. IMPS facility differs from NEFT and RTGS as there is no time limit to carry out the transaction. This facility can be availed 24X7 and on all public and bank holidays including RBI holidays.

12. Bharat Bill Payment System

Bharat Bill Payment System (BBPS) is an integrated bill payment system in India offering interoperable and accessible bill payment service to customers through a network of agents, enabling multiple payment modes, and providing instant confirmation of payment. This is still in implementation stage. Guidelines for implementation of this system were issued on November 28, 2014.

13. Channels of e-payment

In their effort to enable customers to make payments the electronic way banks have developed many channels of payments viz. the internet, mobiles, ATM's (Automated Teller Machines) and drop boxes.

The internet as a channel of payment is one of the most popular especially among the youth. Debit and credit payments are made by customers on various bank's websites for small purchases, (retail payments) and retail transfers (ATM transfers).

ATM's serve many other purposes, apart from functioning as terminals for withdrawals and balance inquiries, such as payment of bills through ATM's, applications for cheques books and loans can also be made via ATM's.

Banks also provide telephone and mobile banking facilities. Through call agents payments can be made and as the number of telephone and mobile subscribers are expected to rise, so is this channel of payment expected to gain popularity.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Drop boxes provide a solution to those who have no access to the internet or to a telephone or mobile. These drop-boxes are kept in the premises of banks and the customers can drop their bills along with the bill payment slips in these boxes to be collected by third party agents¹

14.Role of the RBI in encouraging e-payments

As the apex financial and regulatory institution in the country it is compulsory for the RBI to ensure that the payments system in the country is as technologically advanced as possible and in view of this aim, the RBI has taken several initiatives to strengthen the e-payments system in India and encourage people to adopt it.

Raghuram Rajan, Ex-Governor, RBI, and Nandan Nilekani, Ex-Chairman, UIDAI and Advisor, NPCI, and at the launch of Unified Payments Interface (UPI) in Mumbai.

Imagine paying for everyday purchases directly from your bank, without the need for carrying cash. The RBI's new interface helps you do just that. Reserve Bank of India Governor Raghuram Rajan launched the Unified Payments Interface (UPI) system, as its latest offering in boosting digital money transfers.

The interface has been developed by National Payments Corporation of India (NPCI), the umbrella organisation for all retail payments in the country. The UPI seeks to make money transfers easy, quick and hassle free.

- The Payment and Settlement Systems Act, 2007 was a major step in this direction. It enables the RBI to "regulate, supervise and lay down policies involving payment and settlement space in India." Apart from some basic instructions to banks as to the personal and confidential nature of customer payments, supervising the timely payment and settlement of all transactions, the RBI has actively encouraged all banks and consumers to embrace e-payments.
- In pursuit of the above-mentioned goal the RBI has granted NBFC's (Non-Banking Financial Companies) the permission to issue co branded credit cards forming partnerships with commercial banks.
- The Kisan Credit Card Scheme was launched by NABARD in order to meet the credit needs of farmers, so that they can be free of paper money hassles and use only plastic money.
- A domestic card scheme known as RuPay has recently been started by the National Payments Corporation of India (NPCI), promoted by RBI and Indian Banks Association (IBA), inspired by Unionpay in China, which will be promoting the use of cards ie. "plastic money". Initially functioning as an NPO, Rupay will focus on potential customers from rural and semi-urban areas of India. Rupay will have a much wider coverage than Visa, MasterCard or American Express cards which have always been used for card-based settlements.
- The NREGA (National Rural Employment Guarantee Scheme) introduced by the Government will ensure rural employment in turn ensuring that the employees get wages. Each employee will have a smart card functioning as his personal identification card, driver's license, credit card which will also function as an electronic pass book, thus familiarising the rural populations with e-payments^[2]

However, the Indian banking system suffers from some defects due to certain socio-cultural factors which hampers the spread of the e-payments culture even though there are many effective electronic payment channels and systems in place. Despite the infrastructure being there nearly 63% of all payments are still made in cash. A relatively small percentage of the population pays their bills electronically and most of that population is from urban India-the metropolitans. Also in some cases the transaction is done partially online and partially "offline". The main reason for this apathy to switch to e-payments comes from lack of awareness of the customer despite various efforts by the Government.

15. Block Chain Technology : ICICI Bank is the first bank in the country and among the first few globally to exchange and authenticate remittance transaction messages as well as original international trade documents related to purchase order, invoice, shipping & insurance, among others, electronically on block chain in real time. The usage of block chain technology simplifies the process and makes it almost instant—to only a few minutes. Typically, this

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

process takes a few days. The block chain application co-created by ICICI Bank replicates the paper-intensive international trade finance process as an electronic de centralised ledger, that gives all the participating entities including banks the ability to access a single source of information.

CODE NAME DIGITS

IFSC - Indian Financial System Code 11

MICR -Magnetic Ink Character Recognition 09

SWIFT-Society for worldwide interbank Financial Telecommunication) 11

PAN- Permanent Account no. 10

UID /UAN – unique Identification Number 12

PIN – Postal Index Number 6

CIN-Cheque Identification Number 7

BIC (BANK IDENTIFICATION NUMBER) 8

16. PREPAID PAYMENT INSTRUMENTS : Eligibility : Banks who comply with the eligibility criteria would be permitted to issue all categories of pre-paid payment instruments. Non-Banking Financial Companies (NBFCs) and other persons would be permitted to issue only semi-closed system payment instruments. Capital requirements : Banks and Non-Banking Financial Companies which comply with the Capital Adequacy requirements prescribed by Reserve Bank of India from time-to-time, shall be permitted to issue pre-paid payment instruments. All other persons shall have a minimum paid-up capital of Rs 100 lakh and positive net owned funds. Safeguards against money laundering (KYC/AML/CFT) provisions - The maximum value of any pre-paid payment instruments (where specific limits have not been prescribed including the amount transferred) shall not exceed Rs 100,000/-. Deployment of Money collected: Non-bank persons issuing payment instruments are required to maintain their outstanding balance in an escrow account with any scheduled commercial bank subject to the following conditions:- The amount so maintained shall be used only for making payments to the participating merchant establishments. No interest is payable by the bank on such balances. Validity: All pre-paid payment instruments issued in the country shall have a minimum validity period of six months from the date of activation/issuance to the holder. The outstanding balance against any payment instrument shall not be forfeited unless the holder is cautioned at least 15 days in advance as regards the expiry of the validity of the payment instrument.

17. Money Transfer Service Scheme (MTSS) : The Reserve Bank has issued Master Directions relating to Money Transfer Service

Scheme (MTSS), which is a quick and easy way of transferring personal remittances from abroad to beneficiaries in India.

MTSS can be used for inward personal remittances into India, such as, remittances towards family maintenance and remittances

favouring foreign tourists visiting India and not for outward remittance from India.

The system envisages a tie-up between reputed money transfer companies abroad known as Overseas Principals and agents in

India known as Indian Agents who would disburse funds to beneficiaries in India at ongoing exchange rates. The Indian Agents can

in turn also appoint sub-agents to expand their network. The Indian Agent is not allowed to remit any amount to the Overseas Principal. Under MTSS, the remitters and the beneficiaries are individuals only.

The Reserve Bank of India may accord necessary permission (authorisation) to any person to act as an Indian Agent under the

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Money Transfer Service Scheme. No person can handle the business of cross-border money transfer to India in any capacity unless specifically permitted to do so by the RBI.

To become MTSS agent, min net owned funds Rs.50 lac. MTSS cap USD 2500 for individual remittance. Max remittances 30

received by an individual in India in a calendar year. Min NW of overseas principal USD 01 million, as per latest balance sheet.

18. IMPS

IMPS offer an instant, 24*7 interbank electronic fund transfer service capable of processing person to person, person to account and person to merchant remittances via mobile, internet and ATMs. It is a multichannel and multidimensional platform that makes the payments possible within fraction of seconds with all the standards and integrity maintained for security required for even high worth transactions.

MMID - Mobile Money Identifier

Each MMID is a 7 digit code linked to a unique Mobile Number. Different MMIDs can be linked to same Mobile Number.

Both Sender & Receiver have to register for Mobile Banking & get a unique ID called "MMID"

- Generation of MMID is a One-time process.
- Remitter (Sender) transfer funds to beneficiary (Receiver) using Mobile no. & 7digit MMID of beneficiary.

IFS Code

11 digit alphanumeric number, available in the users Cheque book.

IMPS Fund transfer/Remittance options:

- Using Mobile number & MMID (P2P)
- Using Account number & IFS Code (P2A)
- Using Aadhaar number (ABRS)
- Using Mobile number & MMID (P2P)
- Customer Initiated - P2M(Push)
- Merchant Initiated - P2M(Pull)

Using Mobile number & MMID (P2P)

Presently, IMPS Person-to-Person (P2P) funds transfer requires the Remitter customer to make funds transfer using Beneficiary Mobile Number and MMID. Both Remitter as well as Beneficiary needs to register their mobile number with their respective bank account and get MMID, in order to send or receive funds using IMPS.

Using Account number & IFS Code (P2A)

There may be cases where Remitter is enabled on Mobile Banking, but Beneficiary mobile number is not registered with any bank account. In such cases, Remitter shall not be able to send money to the Beneficiary using Mobile Number & MMID.

Hence on the merit of the feedback received from the banking community as well as to cater the above mentioned need, the IMPS funds transfer has been made possible using Beneficiary account number and IFS code as well, in addition to Beneficiary mobile number and MMID.

Customer Initiated - P2M(Push)

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

IMPS Merchant Payments (P2M - Person-to-merchant) service allows customers to make instant, 24*7, interbank payments to merchants or enterprises via mobile phone. IMPS enables mobile banking users a facility to make payment to merchants and enterprises, through various access channels such as Internet, mobile Internet, IVR, SMS, USSD.

Sender enter details of merchant's (Customer initiated - Push)

- Merchant Mobile Number & MMID
- Amount to be transferred
- Payment reference (optional)
- Sender's M-PIN

Merchant Initiated - P2M(Pull)

IMPS Merchant Payments (P2M - Person-to-Merchant) service allows customers to make instant, 24*7, interbank payments to merchants or enterprises via Mobile & Internet. IMPS enables mobile banking users a facility to make payment to merchants and enterprises, through various access channels such as Internet, mobile Internet, IVR, SMS, USSD.

Customer enter own details (Merchant Initiated - Pull)

- Customer own Mobile Number
- Customer own MMID
- OTP (generated from the Issuer Bank)

19.Unified Payments Interface ("UPI")

Unified Payments Interface (UPI) is a payment system launched by National Payments Corporation of India and regulated by Reserve Bank of India.

UPI is a payment system that allows money transfer between any two bank accounts by using a smartphone.

UPI allows a customer to pay directly from a bank account to different merchants, both online and offline, without the hassle of typing credit card details, IFSC code, or net banking/wallet passwords

One needs to download the app from Play Store and install in phone; Set app login; Create virtual address; Add bank account; Set M-Pin; and Start transacting using UPI

It is safe as the customers only share a virtual address and provide no other sensitive information.

All merchant payments, remittances, bill payments among others can be done through UPI.

The per transaction limit is Rs.1 lakh.

A user can make an in-app payment for goods or services purchased online.

For instance a site allows purchase of a movie-on-demand.

User clicks buy, the site/app triggers the UPI payment link and is taken to the pay screen of the UPI app, where the transaction information is verified and a click followed by entry of a secure PIN completes the purchase.

26 major banks in India offer this facility to their customers.

The launch of the Unified Payments Interface ("UPI") by National Payments Corporation of India ("NPCI"), has provided an impetus to India's move to incentivize digital payments with the vision to transform India into a digitally empowered economy and reduce dependence on cash transactions. NPCI is the umbrella body for all payment systems in India, which makes digital transactions as effortless as sending a text message.

UPI makes cutting-edge changes by supporting real time transfer of money between accounts across banks using smartphones by use of just one single interface besides creating interoperability and superior customer experience. Embracing the smartphone boom in India and the inclination of

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

customers to move to digital mobile-based solutions, UPI addresses the challenges and limitations of the existing payment systems, wherein customers are required to disclose sensitive financial details like bank account details, IFSC code, credit/debit card details and sensitive PIN numbers while initiating transactions and juggle between different mobile banking applications with their different user IDs and passwords.

Unified Payments Interface (UPI) is an instant payment system developed by the National Payments Corporation of India (NPCI), an RBI regulated entity. UPI is built over the IMPS infrastructure and allows you to instantly transfer money between any two parties' bank accounts.

UPI-PIN

UPI-PIN (UPI Personal Identification Number) is a 4-6 digit pass code you create/set during first time registration with this App. You have to enter this UPI-PIN to authorize all bank transactions. If you have already set up an UPI-PIN with other UPI Apps you can use the same on BHIM. (Note: Banks issued MPIN is different from the UPI UPI-PIN, please generate a new UPI-PIN in the BHIM app) Note: Please do not share your UPI-PIN with anyone. BHIM does not store or read your UPI-PIN details and your bank's customer support will never ask for it.

Payment Address

Payment Address is an Address which uniquely identifies a person's bank a/c. For instance, the Payment Address for BHIM customers is in the format xyz@upi. You can just share your Payment Address with anyone to receive payments (no need for bank account number/ IFSC code, etc.). You can also send money to anyone by using their Payment Address. Note: Do not share your confidential UPI PIN with anyone.

Virtual Payment address eliminates the need to provide sensitive information like a bank account details, debit/credit card details and CVV numbers. Also, unlike a mobile wallet, a customer is not required to set aside funds upfront in the mobile wallet setup with the service provider and all transfers under the UPI are made from the bank account linked with your virtual payment address. A virtual payment address is an identifier that will be mapped to a customers bank account, enabling the bank providing the UPI services to process transactions through the bank account linked with the respective virtual payment address.

Data Security

In terms of data security, UPI provides for a single click two-factor authorization, which implies that with one click, the transaction is authenticated at 2 levels, compliant with the existing regulatory guidelines issued by the Reserve Bank of India ("RBI"), without disclosing banking or personal information. As UPI primarily works based on an individual's 'virtual payment address', one can send and receive payments solely based on their 'virtual payment address' without providing any additional details. For example if you need to make a payment to a merchant for purchases made at a store, you will need to provide him only your 'virtual payment address', the merchant will then enter your 'virtual payment address' into his UPI app, the UPI app will send an authentication messages to the 'virtual payment address' linked to your mobile device, once you receive and acknowledge the message by entering your password will the transaction be completed and the amount payable to the merchant will be debited from your bank account.

Aggregator of all accounts

UPI acts as an aggregator of all accounts held by a customer enabling such customers to make transactions from multiple accounts owned by them, from one single mobile application or web interface and a customer is free to choose to use any bank's UPI application. Consequently, a customer can own multiple virtual payment addresses wherein each virtual payment address can be linked to a specific account and organise payments or collections, the way it suits them.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Moreover, special instructions like setting an upper limit for payments on certain handles, and restriction of merchants or outlets at which a certain handle can be used, and standing payment instructions make the whole process very useful to customers.

The banks offering UPI services are required to be authorised by the RBI to provide mobile banking services. It is significant to note that even though the RBI has not issued any specific guidelines on the provision of UPI services, the transactions undertaken through use of UPI are required to be compliant with the guidelines issued by RBI including but not limited to, customer registration process and KYC guidelines.

How UPI / BHIM at POS works?

- This innovative dynamic QR-code based solution uses the store's existing credit/debit card POS terminal to enable UPI-based cashless payments.
- When a customer requests UPI Payment mode, the cashier simply needs to select the 'UPI Payment' option on his existing card POS terminal and inputs the relevant bill payment amount.
- This triggers the generation of a dynamic QR-code on the POS terminal screen itself which can be scanned into any mobile-based UPI-apps like BHIM used by the customer.
- When scanned, the QR code automatically transfers relevant transaction details and displays it on the customer's payment app for authorizing payment transfer.
- Once the payment transfer from customer's UPI-linked bank account to store's UPI-linked account is completed, the payment solution triggers a settlement confirmation to the initiating in-store POS terminal for printing out a transaction completion charge slip.

Benefits:

By enabling such a UPI payment confirmation on the merchant POS terminal itself, the new in-store UPI interface addresses a long standing implementation hurdle holding back faster spread of UPI-acceptance in large multi-lane retail stores.

With multiple checkout points, the cashiers in these stores have no direct means of payment receipt prior to releasing the purchased goods to the customer. This is unlike a small single cashier store where such a confirmation could be received via a simple text message to the single cashier's own mobile phone.

The new solution enables the crucial payment confirmation to be received on cashier-independent infrastructure like the store POS terminal - a necessity for multi-cashier stores with high cashier churn. Usage of a Dynamic QR with the merchant VPA (Virtual Private Address) or UPI ID and amount embedded in it eliminates the need for typing in of the customer or merchant credentials in the POS.

This process offers convenience besides eliminating the cumbersome and error-prone process of typing out credentials.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Key points about UPI

1. How is UPI different from IMPS?
 - UPI is providing additional benefits to IMPS in the following ways:
 - Provides for a P2P Pull functionality
 - Simplifies Merchant Payments
 - Single APP for money transfer
 - Single click two factor authentication
2. Does a customer need to register before remitting funds using UPI?
Yes, a customer needs to register with his/her PSP before remitting funds using UPI and link his accounts
3. Does the customer need to register a beneficiary before transferring funds through UPI? What details of beneficiary will be required?
No, registration of Beneficiary is not required for transferring funds through UPI as the fund would be transferred on the basis of Virtual ID/ Account+IFSC / Mobile No+MMID / Aadhaar Number. (Please check with your PSP and Issuing bank with regard to the services enabled on the App).
4. Can I link more than one bank account to the same virtual address?
Yes, several bank accounts can be linked to the same virtual address depending on the functionalities being made available by the respective PSPs. If the selected Bank name to link with UPI does not find your bank a/c, please ensure that the mobile number linked to your bank account is same as the one verified in BHIM App. If it is not the same, your bank accounts will not be fetched by the UPI platform. Only Savings and Current bank accounts are supported by BHIM.
5. What are the different channels for transferring funds using UPI?
 - The different channels for transferring funds using UPI are:
 - Transfer through Virtual ID
 - Account Number + IFSC
 - Mobile Number + MMID
 - Aadhaar Number
 - Collect / Pull money basis Virtual ID
6. What is the limit of fund transfer using UPI?
At present, the upper limit per UPI transaction is Rs. 1 Lakh.

20. Bharat Interface for Money (BHIM)

The Bharat Interface for Money (BHIM) was rolled out by Prime Minister Narendra Modi

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

on 30th December 2016, in an initiative to enable fast, secure and reliable cashless payments through mobile phones.

BHIM is inter-operable with other Unified Payment Interface (UPI) applications and bank accounts, and has been developed by the National Payments Corporation of India (NPCI).

The Android app is already available on the Google Play Store. As it is Aadhaar-enabled, the app puts an end to the fuss around other e-wallets. Moreover, an iOS version will be launched soon. One must get their bank accounts registered along with a UPI Pin for their account.

On the BHIM app, it would be <mobile number@upi> or <preferred user id@upi>. This user id would be your primary address, which can be used to send or request money through other ids linked to it.

The BHIM App supports about 35 banks.

Bharat Interface for Money (BHIM) is an app that lets you make simple, easy and quick payment transactions. BHIM is a digital payments solution app based on the Unified Payments Interface (UPI) from the National Payments Corporation of India (NPCI), the umbrella organisation for all retail payments systems in India. You can easily make direct bank to bank payments instantly and collect money using just Mobile number or Payment address.

BHIM being UPI-based, is linked directly to a bank account. All the payee needs is a bank account. If this account is UPI activated, you can just ask for the payee's Virtual Payment Address (VPA), and make the payment to that account. Otherwise, there's the option of IFSC or MMID for sending or receiving money. The advantage is there's no need to remember an account number, or to share it with anyone. The VPA is all that is needed.

If you have signed up for UPI-based payments on your bank account, which is also linked to your mobile phone number, you'll be able to use the BHIM app to carry out digital transactions. Services available are as follows:

The following are the features of BHIM:

1. Send Money: User can send money using a Virtual Payment Address (VPA), Account Number & IFSC, Aadhaar Number or QR code.
2. Request Money: User can collect money by entering Virtual Payment Address (VPA). Additionally through BHIM App, one can also transfer money using Mobile No. (Mobile No should be registered with BHIM or *99# and account should be linked)
3. Scan & Pay: User can pay by scanning the QR code through Scan & Pay & generate your QR option is also present.
4. Transactions: User can check transaction history and also pending UPI collect requests (if any) and approve or reject. User can also raise complaint for the declined transactions by clicking on Report issue in transactions.
5. Profile: User can view the static QR code and Payment addresses created or also share the QR code through various messenger applications like WhatsApp, Email etc. available on phone and download the QR code.
6. Bank Account: User can see the bank account linked with his/her BHIM App and set/change the UPI PIN. User can also change the bank account linked with BHIM App by clicking Change account provided in Menu and can also check Balance of his/her linked Bank Account by clicking "REQUEST BALANCE"

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

7. Language: Up to 8 regional languages (Tamil, Telugu, Bengali, Malayalam, Oriya, Gujarati, Kannada ,Hindi) available on BHIM to improve user experience.
8. Block User: Block/Spam users who are sending you collect requests from illicit sources.
9. Privacy: Allow a user to disable and enable mobilenumber@upi in the profile if a secondary VPA is created (QR for the disabled VPA is also disabled).

Unique features of BHIM:

- QR code based scan & pay option available, Generate your own QR code option is also available
- Option to save your beneficiaries for future references
- Access transaction history and Request Balance anytime
- Create, reset or change UPI PIN
- Report Issue and call Bank facilities are given to lodge complaints
- FAQ section is created in the app to answer all the queries reg. BHIM
- Available in 2 languages English and Hindi

Benefits of BHIM:

- Single App for sending and receiving money and making merchant payments
- Go cashless anywhere anytime
- Added security of Single click 2 factor authentication
- Seamless money collection through single identifiers, reduced risks, real time
- Mobile no. or Name used to create VIRTUAL PAYMENT ADDRESS (VPA)
- Best answer to Cash on Delivery hassle
- Send and collect using VIRTUAL PAYMENT ADDRESS (VPA) or A/c no & IFSC.
- Payments through single app in your favourite language.
- 24X7, 365 days instantaneous money transfer

Transfer Limits:

- Maximum limit per transaction is Rs. 10,000 per transaction
- Maximum limit per day is Rs. 20,000
- There is limit of 20 transactions per account per bank.

21. National Automated Clearing House (NACH)

National Payments Corporation of India (NPCI) has implemented “National Automated Clearing House (NACH)” for Banks, Financial Institutions, Corporates and Government a web based solution to facilitate interbank, high volume, electronic transactions which are repetitive and periodic in nature.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

ECS will be replaced with NACH from 1.4.2016.

NACH system will provide a national footprint and is expected to cover the entire core banking enabled bank branches spread across the geography of the country irrespective of the location of the bank branch.

NACH System can be used for making bulk transactions towards distribution of subsidies, dividends, interest, salary, pension etc. and also for bulk transactions towards collection of payments pertaining to telephone, electricity, water, loans, investments in mutual funds, insurance premium etc.

NACH's Aadhaar Payment Bridge (APB) System has been channelizing the Government subsidies and benefits to the intended beneficiaries using their Aadhaar numbers. The APB System links the Government Departments and their sponsor banks on one side and beneficiary banks and beneficiary on the other hand.

22. Cheque Truncation System (CTS) or Image-based Clearing System (ICS), in India, is a project of the Reserve Bank of India (RBI), commencing in 2010, for faster clearing of cheques. CTS is based on a cheque truncation or online image-based cheque clearing system where cheque images and magnetic ink character recognition (MICR) data are captured at the collecting bank branch and transmitted electronically.

Cheque truncation means stopping the flow of the physical cheques issued by a drawer to the drawee branch. The physical instrument is truncated at some point en-route to the drawee branch and an electronic image of the cheque is sent to the drawee branch along with the relevant information like the MICR fields, date of presentation, presenting banks etc. This would eliminate the need to move the physical instruments across branches, except in exceptional circumstances, resulting in an effective reduction in the time required for payment of cheques, the associated cost of transit and delays in processing, etc., thus speeding up the process of collection or realization of cheques.

CTS has been implemented in New Delhi, Chennai and Mumbai with effect from February 1, 2008, September 24, 2011 and April 27, 2013 respectively. After migration of the entire cheque volume from MICR system to CTS, the traditional MICR-based cheque processing has been discontinued across the country. The CTS-2010 compliant cheques are both image friendly and have enhanced security features. All banks providing cheque facility to their customers have been advised to issue only 'CTS-2010' standard cheques. Cheques not complying with CTS-2010 standards would be cleared at less frequent intervals i.e. weekly once from November 1, 2014 onwards.

Banks derive multiple benefits through the implementation of CTS, like a faster clearing cycle meaning technically possible realization of proceeds of a cheque within the same day. It offers better reconciliation/ verification, better customer service and enhanced customer window. Operational efficiency provides a direct boost to bottom lines of banks as clearing of local cheques is a high cost low revenue activity. Besides, it reduces operational risk by securing the transmission route. Centralized image archival systems ensure that data storage and retrieval is easy. Reduction of manual tasks leads to reduction of errors. Real-time tracking and visibility of the cheques, less frauds with secured transfer of images to the RBI are other benefits that banks derive from this solution

Initiatives by Government of India for Propagating e-Banking

For growth and development and to promote e-banking in India the Indian government and RBI have been taken several initiatives.

The Government of India enacted the IT Act, 2000 with effect from October 17, 2000 which provided legal recognition to electronic transactions and other means of electronic commerce.

The Reserve Bank monitors and reviews the legal requirements of e-banking on a continuous basis to ensure that challenges related to e-banking may not pose any threat to financial stability of the nation

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Dr. K.C. Chakrabarty Committee including members from IIM, IDRBT, IIT and Reserve Bank prepared the IT Vision Document- 2011-17, which provides an indicative road map i.e. guidelines to enhance the usage of IT in the banking sector.

The Reserve Bank is striving to make the payment systems more secure and efficient. It has advised banks and other stakeholders to strengthen the security aspects in internet banking by adopting certain security measures in a timely manner. RBI believes that the growing popularity of these alternate channels of payments (such as: Internet Banking, Mobile Banking, ATM etc.) brings an additional responsibility on banks to ensure safe and secure transactions through these channels.

National Payments Corporation of India (NPCI) was permitted by the RBI to enhance the number of mobile banking services and widen the IMPS (Immediate Payment Service) channels like ATMs, internet, mobile etc. Along with this, NPCI is also working to bring more mobile network operators which can provide mobile banking services through a common platform.

There has been a dramatic surge in the volume and value of mobile transactions in the recent past. MoM increase in no. of transactions from Dec 14 to Dec 15 was 135% and Dec 15 to Dec 16 was 182%. MoM increase in value of transactions from Dec 14 to Dec 15 was 330% and Dec 15 to Dec 16 was 178%.

The future:

In the backdrop of demonetization- a colloquial term for the withdrawal of 86 percent of the value of India's currency in circulation by the Government of India since 8th November 2016 followed by digital push for 'less cash' economy, a dramatic multi-fold rise in e-banking transactions and especially mobile banking transactions, is expected in the near future.

Interactive Technology for Banks

With the launch of sbiINTOUCH on 1st July, 2014, State Bank of India was the first Bank in India to introduce the concept of "Digital Banking". State of the art technology like Debit Card Printing Kiosks, Interactive Smart Tables, Interactive Digital Screens, Remote Experts through video call etc were introduced to providing a completely different experience through online self-service mode.

The key feature of these branches is that one can open one's savings bank account - Account Opening Kiosk (AOK) within 15 minutes. Besides that you can have access to a vast array of Banking related activities and products.

India's first banking robot Lakshmi made her debut in November 2016 by City Union Bank, the artificial intelligence powered robot will be the first on-site bank helper. Lakshmi, which took more than six months to develop, can answer intelligently on more than 125 subjects. Top private lender HDFC Bank, which is also experimenting with robots to answer customer queries, is testing its humanoid at its innovation lab.

BUSINESS CONTINUITY PLANNING

Introduction

The pivotal role that banking sector plays in the economic growth and stability, both at national and individual level, requires continuous and reliable services. Increased contribution of 24x7 electronic banking channels has increased the demand to formulate consolidated Business Continuity Planning (BCP) guidelines covering critical aspects of people, process and technology.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

BCP forms a part of an organisation's overall Business Continuity Management (BCM) plan, which is the "preparedness of an organisation", which includes policies, standards and procedures to ensure continuity, resumption and recovery of critical business processes, at an agreed level and limit the impact of the disaster on people, processes and infrastructure (includes IT); or to minimise the operational, financial, legal, reputational and other material consequences arising from such a disaster.

Effective business continuity management typically incorporates business impact analyses, recovery strategies and business continuity plans, as well as a governance programme covering a testing programme, training and awareness programme, communication and crisis management programme.

Roles, Responsibilities and Organisational structure Board of Directors and Senior Management

A bank's Board has the ultimate responsibility and oversight over BCP activity of a bank. The Board approves the Business Continuity Policy of a bank. Senior Management is responsible for overseeing the BCP process which includes:

- Determining how the institution will manage and control identified risks

- Allocating knowledgeable personnel and sufficient financial resources to implement the BCP

- Prioritizing critical business functions

- Designating a BCP committee who will be responsible for the Business Continuity Management

- The top management should annually review the adequacy of the institution's business recovery, contingency plans and the test results and put up the same to the Board.

- The top management should consider evaluating the adequacy of contingency planning and their periodic testing by service providers whenever critical operations are outsourced.

- Ensuring that the BCP is independently reviewed and approved at least annually;

- Ensuring employees are trained and aware of their roles in the implementation of the BCP

- Ensuring the BCP is regularly tested on an enterprise-wide basis

- Reviewing the BCP testing programme and test results on a regular basis and

- Ensuring the BCP is continually updated to reflect the current operating environment

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

1.1 BCP Head or Business Continuity Coordinator

A senior official needs to be designated as the Head of BCP activity or function.

His or her responsibilities include:

- Developing of an enterprise-wide BCP and prioritisation of business objectives and critical operations that are essential for recovery
- Business continuity planning to include the recovery, resumption, and maintenance of all aspects of the business, not just recovery of the technology components;
- Considering the integration of the institution's role in financial markets;
- Regularly updating business continuity plans based on changes in business processes, audit recommendations, and lessons learned from testing
- Following a cyclical, process-oriented approach that includes a business impact analysis (BIA), a risk assessment, management and monitoring and testing
- Considering all factors and deciding upon declaring a "crisis"

1.2 BCP Committee or Crisis Management Team

Since electronic banking has functions spread across more than one department, it is necessary that each department understands its role in the plan. It is also important that each gives its support to maintain it. In case of a disaster, each has to be prepared for a recovery process, aimed at protection of critical functions. To this end, it would be helpful if a set up like the BCP Committee, charged with the implementation of BCP, in an eventuality and all departments expected to fulfill their respective roles in a coordinated manner.

Hence, a committee consisting of senior officials from departments like HR, IT, Legal, Business and Information Security needs to be instituted with the following broad mandate:

- To exercise, maintain and to invoke business continuity plan, as needed
- Communicate, train and promote awareness
- Ensure that the Business Continuity Plan (BCP) fits with other plans and requirement of concerned authorities
- Budgetary issues
- Ensure training and awareness on BCP to concerned teams and employees
- Co-ordinating the activities of other recovery, continuity, response teams and handling key decision-making
- They determine the activation of the BCP

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Other functions entail handling legal matters evolving from the disaster, and handling public relations and media inquiries

1.3 BCP Teams

There needs to be adequate teams for various aspects of BCP at central office, as well as individual controlling offices or at a branch level, as required. Among the teams that can be considered based on need, are the incident response team, emergency action and operations team, team from particular business functions, damage assessment team, IT teams for hardware, software, network support, supplies team, team for organizing logistics, relocation team, administrative support team, coordination team. Illustrative guidelines for committees or teams for BCP are provided in Annex C.

2. Critical Components of Business Continuity Management Framework

The BCP requirements enunciated in this document should be considered. The onus lies on the Board and Senior Management for generating detailed components of BCP in the light of an individual bank's activities, systems and processes.

2.1 BCP Methodology

Banks should consider looking at BCP methodologies and standards—BS 25999 by BSI— which follows the “Plan-Do-Check-Act Principle”.

BCP methodology should include:

Phase 1: Business Impact Analysis

Identification of critical businesses, owned and shared resources with supporting functions to come up with the Business Impact Analysis (BIA)

Formulating Recovery Time Objectives (RTO), based on BIA. It may also be periodically fine-tuned by benchmarking against industry best practices

Critical and tough assumptions in terms of disaster, so that the framework would be exhaustive enough to address most stressful situations

Identification of the Recovery Point Objective (RPO), for data loss for each of the critical systems and strategy to deal with such data loss

Alternate procedures during the time systems are not available and estimating resource requirements

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Phase 2: Risk Assessment

Structured risk assessment based on comprehensive business impact analysis. This assessment considers all business processes and is not limited to the information processing facilities.

Risk management by implementing appropriate strategy/ architecture to attain the bank's agreed RTOs and RPOs.

Impact on restoring critical business functions, including customer-facing systems and payment and settlement systems such as cash disbursements, ATMs, internet banking, or call centres

Dependency and risk involved in use of external resources and support

Phase 3: Determining Choices and Business Continuity Strategy

BCP should evolve beyond the information technology realm and must also cover people, processes and infrastructure

The methodology should prove for the safety and well-being of people in the branch / outside location at the time of the disaster.

Define response actions based on identified classes of disaster.

To arrive at the selected process resumption plan, one must consider the risk acceptance for the bank, industry and applicable regulations

Phase 4: Developing and Implementing BCP

Action plans, i.e.: defined response actions specific to the bank's processes , practical manuals(do and don'ts, specific paragraph's customised to individual business units) and testing procedures

Establishing management succession and emergency powers

Compatibility and co-ordination of contingency plans at both the bank and its service providers

The recovery procedure should not compromise on the control environment at the recovery location

Having specific contingency plans for each outsourcing arrangement based on the degree of materiality of the outsourced activity to the bank's business

Periodic updating to absorb changes in the institution or its service providers. Examples of situations that might necessitate updating the plans include acquisition of new equipment, upgradation of the operational systems and changes in:

- Personnel
- Addresses or telephone numbers
- Business strategy
- Location, facilities and resources
- Legislation

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Contractors, suppliers and key customers
Processes—new or withdrawn ones
Risk (operational and financial)

2.3 Key Factors to be considered for BCP Design

Following factors should be considered while designing the BCP:

Probability of unplanned events, including natural or man-made disasters, earthquakes, fire, hurricanes or bio-chemical disaster
Security threats
Increasing infrastructure and application interdependencies
Regulatory and compliance requirements, which are growing increasingly complex
Failure of key third party arrangements
Globalisation and the challenges of operating in multiple countries.

1.4 BCP Considerations

Banks must consider implementing a BCP process to reduce the impact of disruption, caused by disasters and security failures to an acceptable level through a combination of preventive and recovery measures.

BCP should include measures to identify and reduce probability of risk to limit the consequences of damaging incidents and enable the timely resumption of essential operations. BCP should amongst others, consider reputation, operational, financial, regulatory risks.

The failure of critical systems or the interruption of vital business processes could prevent timely recovery of operations. Therefore, financial institution management must fully understand the vulnerabilities associated with interrelationships between various systems, departments, and business processes. These vulnerabilities should be incorporated into the BIA, which analyses the correlation between system components and the services they provide.

Various tools can be used to analyse these critical interdependencies, such as a work flow analysis, an organisational chart, a network topology, and inventory records. A work flow analysis can be performed by observing daily operations and interviewing employees to determine what resources and services are shared among various departments. This analysis, in conjunction with the other tools, will allow management to understand various processing priorities, documentation requirements, and the interrelationships between various systems. The following issues when determining critical interdependencies within the organisation:

Key personnel;
Vital records;
Shared equipment, hardware, software, data files, and workspace;
Production processes;

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Customer services;
Network connectivity; and
Management information systems.

Key Considerations while Formulating A BCP:

Ensuring prompt and accurate processing of securities transactions, including, but not limited to, order taking, order entry, execution, comparison, allocation, clearance and settlement of securities transactions, the maintenance of customer accounts, access to customer accounts and the delivery of funds and securities.

Honouring of all customer payouts (i.e. obligation)
Providing priority to intra-day deal payment
Providing customers prompt access to their funds and securities – measures should be undertaken to make customer funds and securities available to customers in the event of a significant business disruption.
Continuing compliance with regulatory reporting requirements etc.

A single framework of BCP should be maintained to ensure that all plans are consistent, and to identify priorities and dependencies for testing and maintenance.

A BCP framework should consider the following:

Conditions for activating plans, which describe a process to be followed (how to assess the situation, who is to be involved, etc.) before each plan is activated

Emergency procedures, which describe the actions to be taken following an incident which jeopardises business operations and/ or human life. This should include arrangements for public relations management and for effective liaison with appropriate public authorities e.g. police, fire service, health-care services and local government

Identification of the processing resources and locations, available to replace those supporting critical activities; fall back procedures which describe the actions to be taken to move essential business activities or support services to alternative temporary locations and to bring business processes back into operation in the required time-scales

Identification of information to be backed up and the location for storage, as well as the requirement for the information to be saved for back-up purpose on a stated schedule and compliance therewith

Resumption procedures, which describe the actions to be taken to return to normal business operations

A maintenance schedule which specifies how and when the plan will be tested and the process for maintaining the plan

Awareness and education activities, which are designed to create understanding of critical banking operations and functions, business continuity processes and ensure

that the processes continue to be effective

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

The responsibilities of the individuals, describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.

(g) Pandemic Planning

Pandemics are defined as epidemics, or outbreaks in humans, of infectious diseases that have the ability to spread rapidly over large areas, possibly worldwide. Adverse economic effects of a pandemic could be significant, both nationally and internationally. Due to their crucial financial and economic role, financial institutions should have plans in place that describe how they will manage through a pandemic event.

Pandemic planning presents unique challenges to financial institution management. Unlike natural disasters, technical disasters, malicious acts, or terrorist events, the impact of a pandemic is much more difficult to determine because of the anticipated difference in scale and duration. Further, while traditional disasters and disruptions normally have limited time durations, pandemics generally occur in multiple waves, each lasting two to three months. Consequently, no individual or organisation is safe from the adverse effects that might result from a pandemic event.

One of the most significant challenges likely from a severe pandemic event will be staffing shortages due to absenteeism. These differences and challenges highlight the need for all financial institutions, no matter their size, to plan for a pandemic event when developing their BCP.

It is important for institutions to actively keep abreast of international and national developments and health advisories issued in this regard.

Accordingly, a bank's BCP needs to provide for the following:

A preventive programme to reduce the likelihood that a bank's operations will be significantly affected by a pandemic event, including: monitoring of potential outbreaks, educating employees, communicating and coordinating with critical service providers and suppliers, in addition to providing appropriate hygiene training and tools to employees.

A documented strategy that provides for scaling the institution's pandemic efforts so they are consistent with the effects of a particular stage of a pandemic outbreak, such as first cases of humans contracting the disease overseas or in India and first cases within the organisation itself. The strategy will also need to outline plans that state how to recover from a pandemic wave and proper preparations for any following wave(s).

A comprehensive framework of facilities, systems, or procedures that provide the organisation the capability to continue its critical operations in the event that large numbers of the institution's staff are unavailable for prolonged periods. Such procedures could include social distancing to minimise staff contact, telecommuting, redirecting customers from branch to electronic banking services, or conducting operations from alternative sites.

The framework should consider the impact of customer reactions and the potential demand for, and increased reliance on, online banking, telephone banking, ATMs, and call support

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

services. In addition, consideration should be given to possible actions by public health and other government authorities that may affect critical business functions of a financial institution.

A testing programme to ensure that the institution's pandemic planning practices and capabilities are effective and will allow critical operations to continue.

An oversight programme to ensure ongoing review and updates to the pandemic plan so that policies, standards, and procedures include up-to-date, relevant information provided by governmental sources or by the institution's monitoring programme.

Banks may also consider insurance to transfer risk to a third party, however taking due care regarding certainty of payments in the event of disruptions.

Testing A BCP

– *Banks must regularly test BCP to ensure that they are up to date and effective:* Testing of BCP should include all aspects and constituents of a bank i.e. people, processes and resources (including technology). BCP, after full or partial testing may fail. Reasons are incorrect assumptions, oversights or changes in equipment or personnel. BCP tests should ensure that all members of the recovery team and other relevant staff are aware of the plans. The test schedule for BCPs should indicate how and when each component of a plan is to be tested. It is recommended to test the individual components of the plans(s) frequently, typically at a minimum of once a year. A variety of techniques should be used in order to provide assurance that the plan(s) will operate in real life.

– *Banks should involve their Internal Auditors (including IS Auditors) to audit the effectiveness of BCP:* And its periodic testing as part of their Internal Audit work and their findings/ recommendations in this regard should be incorporated in their report to the Board of Directors.

– *Banks should consider having a BCP drill planned along with the critical third parties:* In order to provide services and support to continue with pre-identified minimal required processes.

– *Banks should also periodically moving their operations:* Including people, processes and resources (IT and non-IT) to the planned fall-over or DR site in order to test the BCP effectiveness and also gauge the recovery time needed to bring operations to normal functioning.

– *Banks should consider performing the above test without movement of bank personnel to the DR site.* This will help in testing the readiness of alternative staff at the DR site.

– *Banks should consider having unplanned BCP drill:* Wherein only a restricted set of people and certain identified personnel may be aware of the drill and not the floor or business personnel. In such cases banks should have a "Lookout Team" deployed at the location to study and assimilate the responses and needs of different teams. Based on the outcome of this study, banks should revise their BCP Plan to suit the ground requirements.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

3.1 Testing Techniques

The below are few of the illustrative techniques that can be used for BCP testing purposes:

Table-top testing for scenarios (discussing business recovery arrangements using example interruptions)

Simulations (particularly for training people in their post-incident or crisis management roles)

Technical recovery testing (ensuring information systems can be restored effectively)

Testing recovery at an alternate site (running business processes in parallel with recovery operations away from the main site)

Tests of supplier facilities and services (ensuring externally provided services and products will meet the contracted commitment)

Complete rehearsals (testing that the organisation, personnel, equipment, facilities and processes can cope with interruptions)

Simulation testing: It is when participants choose a specific scenario and simulate an on-location BCP situation. It involves testing of all resources: people, IT and others, who are required to enable the business continuity for a chosen scenario. The focus is on demonstration of capability, including knowledge, team interaction and decision-making capabilities. It can also specify role playing with simulated response at alternate locations/facilities to act out critical steps, recognise difficulties, and resolve problems.

Component testing: This is to validate the functioning of an individual part or a sub-process of a process, in the event of BCP invocation. It focuses on concentrating on in-depth testing of the part or sub-process to identify and prepare for any risk that may hamper its smooth running. For example, testing of ATM switch.

Each organisation must define frequency, schedule and clusters of Business Areas, selected for test after a thorough Risk and Business Impact Analysis has been done.

The bank can consider broad guidelines provided below for determining the testing frequency based on critical of a process:

Impact on	Table-top	Call tree	Simulation	Component	Complete
-----------	-----------	-----------	------------	-----------	----------

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

processes	testing		testing	testing	Rehearsals
High	Quarterly	Quarterly	Quarterly	Quarterly	Annually
Medium	Quarterly	Half-yearly	Half-yearly	Annually	Annually
Low	Half-yearly	Annually	NA	NA	NA

Maintenance and Re-assessment of Plans

BCPs should be maintained by annual reviews and updates to ensure their continued effectiveness. Procedures should be included within the organisation's change management programme to ensure that business continuity matters are appropriately addressed. Responsibility should be assigned for regular reviews of each business continuity plan. The identification of changes in business arrangements/processes, not yet reflected in the business continuity plans, should be followed by an appropriate update of the plan on a periodic basis, say quarterly. This would require a process of conveying any changes to the institution's business, structure, systems, software, hardware, personnel, or facilities to the BCP coordinator/team. If significant

changes have occurred in the business environment, or if audit findings warrant changes to the BCP or test programme, the business continuity policy guidelines and programme requirements should be updated accordingly.

Changes should follow the bank's formal change management process in place for its policy or procedure documents. This formal change control process should ensure that the updated plans are distributed and reinforced by regular reviews of the complete plan.

A copy of the BCP, approved by the Board, should be forwarded for perusal to the RBI on an annual basis. In addition, the bank should also submit:

- An annual statement at the end of each financial year describing the critical systems, their Rots and the bank's strategy to achieve them, and
- A quarterly statement, reporting major failures during the period for critical systems, customer segment or services impacted due to the failures and steps taken to avoid such failures in future.

Procedural aspects of BCP

An effective BCP should take into account the potential of wide area disasters, which impact an entire region, and for resulting loss or inaccessibility of staff. It should also consider and address inter dependencies, both market-based and geographic, among financial system participants as well as infrastructure service providers.

Further, banks should also consider the need to put in place necessary backup sites for their critical payment systems which interact with the systems at the Data centres of the Reserve Bank.

Banks may also consider running some critical processes and business operations from primary and the secondary sites, wherein each would provide back-up to the other.

Namely prioritising process and alternative location for personnel in the following categories:

- Dealers and traders
- Operations (e.g. teller, loan desk, cash desk etc.)
- Treasury department staff
- Sales staff
- IT staff
- Corporate functions (HR, Admin) staff
- Comprehensive testing would help banks to further fine-tune BCP/DR processes to ensure their robustness and also enable smooth switch-over to the DR site, as per the priority and scale of processes identified for each process.

All critical processes should be documented to reduce dependency on personnel for scenarios where the staff is not able to reach the designated office premises.

Backup/standby personnel should be identified for all critical roles. A call matrix should be developed to better co-ordinate future emergency calls involving individual financial authorities, financial sector trade associations, and other banks and stakeholders. In addition the organisation should have calling tree with branches

across specific region/business processes. Based on the nature of the emergency a particular branch/the entire calling tree should be activated.

The relevant portion of the BCP adopted should also be disseminated to all concerned, including the customers, so that the awareness would enable them to react positively and in consonance with the BCP. This would help maintain the customer's faith on the banking institution, and the possibility of a bank-run would be exponentially minimised. The part of the plan kept in the public domain should normally be confined to information relating to the general readiness of the banks in this regard without any detailed specifics, to protect the banks from becoming vulnerable to security threats

Banks should consider formulating a clear 'Communication Strategy' with the help of media management personnel to control the content and form of news being percolated to their customers in times of panic.

Banks should consider having a detailed BCP plan for encountering natural calamity/ disaster situation. A formal exception policy should be documented which will guide the affected areas Personnel to act independently till connection to the outside world is resumed.

The above mentioned guideline should have exceptions documented for critical process which will ensure continuation of critical process without the regular operational formalities.

After appropriate approvals or permissions are obtained internally and from RBI, banks should consider having a guideline ready on relaxing certain rules/ requirements for customers affected by the calamity.

Like:

Extending loan/interest payment timeliness

Issuance of fresh loan with minimal required documents

Waving off late payment fees and penalties in certain cases

Allowing more than normal cash withdrawal from ATM's

Banks can consider expediting cheque clearing for customers by directing all cheques to a different region than the one affected by the calamity. In case of severe calamity banks should consider restricting existing loans to facilitate rebuilding efforts by the Govt. for the calamity areas. The banks may also be consider ensuring quick processing of loan applications, preferably within 48 hours of receipt of such applications. It should consider dispatching credit bill, agreement notes, etc. due to customer by having an arrangement to print the same at an alternative location and should consider accepting late payments for credit card dues for customers in the calamity affected area.

Banks may also endeavor for resumption of banking services by setting up satellite offices, extension counters or mobile banking facilities.

Infrastructure Aspects of BCP

– Banks should consider paying special attention to availability of basic amenities such as electricity, water and first-aid box in all offices. (e.g. evaluate the need of electricity backup not just for its systems but also for its people and running the infrastructure like central air-conditioning.)

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

- Banks should consider assigning ownership for each area. Emergency procedures, manual fallback plans and resumption plans should be within the responsibility of the owners of the appropriate business resources or processes involved.
- In-house telecommunications systems and wireless transmitters on buildings should have backup power. Redundant systems, such as analogue line phones and satellite phones (where appropriate), and other simple measures, such as ensuring the availability of extra batteries for mobile phones, may prove essential to maintaining communications in a wide-scale infrastructure failure.
- Possible fallback arrangements should be considered and alternative services should be carried out in co-ordination with the service providers, contractors, suppliers under written agreement or contract, setting out roles and responsibilities of each party, for meeting emergencies. Also, imposition of penalties, including legal action, may be initiated by an organisation against service providers or contractors or suppliers, in the event of noncompliance or non-co-operation.
- When new requirements are identified, established emergency procedures: e.g. evacuation plans or any existing fallback arrangements, should be amended as appropriate.
- Banks may consider having backup resources (erg. stationery required for cheque printing, special printers, stamps) at a secondary operational location.
- The plans may also suitably be aligned with those of the local government authorities
- Banks should consider not storing critical papers, files, servers in the ground floors where there is possibility of floods or water logging. However, banks should also consider avoiding top floors in taller building to reduce impact due to probable fire.
- Fire-proof and water-proof storage areas must be considered for critical documents.
- Banks should consider having alternative means of power source (like procurement of more diesel/ emergency battery backup etc.) for extended period of power cuts.
- Banks should consider having an emergency helpline number or nationalised IVR message to resolve queries of customers and ensure that panic situation is avoided. For this an alternative backup area call centre should be identified to take over part load of the calamity affected area. Designated person/ team must be responsible for enabling line diversion. A similar service can also be considered for the benefit of employee related communication.

Human Aspects of BCP

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

People are a vital component of any organisation. They should therefore be an integral part of a BCP. Generally, plans are often too focused on the technical issues, therefore, it is suggested that a separate section relating to people should be incorporated, including details on staff welfare, counseling, relocation considerations, etc. BCP awareness programme should also be implemented which serve to strengthen staff involvement in BCP. This can be done through induction programme newsletters, staff training exercises, etc.

Banks must consider training more than one individual staff for specific critical jobs (i.e. in the absence of one employee the work must not be stalled or delayed). They must consider cross-training employees for critical functions and document-operating procedures. Banks

should consider possibility of enabling work-from-home capabilities and resources for employees performing critical functions.

Role of HR in the BCP context

Crisis Management Team: As a core member of the CMT, HR provides guidance to team on people-related issues, including evacuation, welfare, whether to invoke the HR incident line, alternative travel arrangements and what to communicate to staff.

HR Incident Line: Operated from within the centralised HR function, the incident helpline is invoked in those instances, where there are possible casualties or missing staff, as a result of an incident. Invoked by the CMT, the line is manned by qualified HR officers trained in how to deal with distressed callers. The staff may be provided with an emergency card, which includes the incident line number. Information on the hotline is updated on a regular basis. The facility enables line managers to keep the central crisis team up to speed on the whereabouts and well-being of staff. Ongoing welfare and support for staff is also provided via an employee assistance provider.

Exceptional Travel arrangements: Transportation plans should be considered in the event of the need to relocate. Key staff needs to be identified including details of where they are located, and vehicles are on standby to transport them if required.

Technology Aspects of BCP

There are many applications and services in banking system that are highly mission critical in nature and therefore requires high availability, and fault tolerance to be considered while designing and implementing the solution. This aspect is to be taken into account especially while designing the data centre solution and the corporate network solution.

Data Recovery Strategies

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Prior to selecting a data recovery (DR) strategy, a DR planner should refer to their organisation's BCP, which should indicate key metrics of recovery point objective and recovery time objective for business processes:

Recovery Point Objective (RPO)—The acceptable latency of data that will be recovered

Recovery Time Objective (RTO)—The acceptable amount of time to restore the function

Recovery Point Objective must ensure that the Maximum Tolerable Data Loss for each activity is not exceeded. The Recovery Time Objective must ensure that the Maximum Tolerable Period of Disruption (MTPD), for each activity, is not exceeded. The metrics specified for the business processes must then be mapped to the underlying IT systems and infrastructure that support those processes. Once, RTO and RPO metrics have been mapped to the IT infrastructure, the DR planner can determine the most suitable recovery strategy for each system. An important note here, however, is that the business ultimately sets the IT budget. Therefore, RTO and RPO metrics need to fit with the available budget and the critical of the business process/function.

A List of Common Strategies for Data Protection:

Backups made to tape and sent off-site at regular intervals (preferably daily)

Backups made to disk on-site and automatically copied to off-site disk, or made directly to off-site disk

Replication of data to an off-site location, which overcomes the need to restore the data (only the systems then need to be restored or synced). This generally makes

use of storage area network (SAN) technology

High availability systems that keep both data and system replicated, off-site, enabling continuous access to systems and data

In many cases, an organisation may elect to use an outsourced disaster recovery provider to provide a stand-by site and systems rather than using their own remote facilities. In addition to preparing for the need to recover systems, organisations must also implement precautionary measures with an objective of preventing a disaster in the first place. *These may include some of the following:*

Local mirrors of systems or data. Use of disk protection technology such as RAID

Surge protectors—to minimise the effect of power surges on delicate electronic equipment

Uninterrupted power supply (UPS) or backup generator to keep systems going in the event of a power failure

Fire preventions—alarms, fire extinguishers

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Anti-virus software and security measures

A disaster recovery plan is a part of the BCP. It dictates every facet of the recovery process, including:

What events denote possible disasters;

What people in the organisation have the authority to declare a disaster and thereby put the plan into effect;

The sequence of events necessary to prepare the backup site once a disaster has been declared;

The roles and responsibilities of all key personnel with respect to carrying out the plan;

An inventory of the necessary hardware and software required to restore production;

A schedule listing the personnel that will be staffing the backup site, including a rotation schedule to support ongoing operations without burning out the disaster team members.

A disaster recovery plan must be a living document; as the data centre changes, the plan must be updated to reflect those changes.

It is to be noted that the technology issues are a derivative of the Business Continuity plan and Management.

For example, BCP and Management will lead to the Business Impact Analysis, which will lead to the Performance Impact Analysis (PIA). That will depend on the Technology Performance of the total IT Solution Architecture.

To amplify business impact analysis is to identify the critical operations and services, key internal and external dependencies and appropriate resilience levels. It also analysis the risks and quantify the impact of those risks from the point of view of the business disruptions. For example, in order to provide state of the art customer services both at the branch level and the delivery channels we need to take into account the services levels that are committed.

If an ATM transaction has to take place in 10 seconds and cash withdrawal or deposit has to take place in 60 seconds at the counter, then based on the load one can compute the number of customers who can be serviced in a day. The above example is to understand the fact that the business latency introduced by the system is a combination of technology, process and people. Therefore, the technical latency is a derivative of the committed business latency and the technology solution architecture has to deliver the same under varying loads.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Technology Solution Architecture to address specific BCM requirements are:

Performance

Availability

Security and Access Control

Conformance to standards to ensure Interoperability

Performance of the technology solution architecture for operations needs to be quantified. It should be possible to measure, as and when required, the quantified parameters. (For example, if the latency for a complex transaction initiated at the branch has to be completed in four seconds under peak load, it should be possible to have adequate measuring environments to ensure that performance degradations have not taken place due to increasing loads.)

Solution architecture has to be designed with high -availability, and no single point of failure. It is inevitable that a complex solution architecture with point products from different sources procured and implemented at different points in time will have some outage once in a while and the important issue is that with clearly defined SLAs, mean time to restore, it should be possible to identify the fault and correct the same without any degradation in performance.

Accordingly, with respect to the performance and availability aspects the following architectures have to be designed and configured to provide high levels of up time round the clock to ensure uninterrupted functioning.

Summation of the required processes:

- Data centre solution architecture
- DR solution architecture
- Near site solution architecture
- Enterprise network and security architecture
- Branch or delivery channel architecture

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

– *Based on the above observation, banks are required to do the following:* Take up the performance and availability audit of the solutions deployed to ensure that the architecture is designed and implemented with no single point of failure.

– Audit the deployed architecture for all the mission critical applications and services and resolve the concerns that arise in a time bound manner.

– Periodically investigate the outages that are experienced from time to time, which are mini disasters that result in non availability of services for a short span of time, systems not responding when transactions are initiated at the branch level, delivery channels not functioning for a brief period of time to ensure that the customer service is not affected.

Srinivas Kante

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

– Ensure availability of appropriate technology solutions to measure and monitor the functioning of products. And, have competent and capable technical people within the system to resolve issues expeditiously.

The issues detailed above have to be borne in mind while finalising the data centre architecture and the corporate network architecture which are expected to have redundancy built in the solution with no single point of failure.

With reference to the network architecture it is recommended that the Banks built in redundancies as under:

Link level redundancy

Path level redundancy

Route level redundancy

Equipment level redundancy

Service provider level redundancy

Issues in choosing a backup site and implementing a DC or DR solution:

Backup site: Is a location where an organisation can easily relocate following a disaster, such as fire, flood, terrorist threat or other disruptive event. This is an integral part of the disaster recovery plan and wider business continuity planning of an organisation. A backup site can be another location operated by the organisation, or contracted via a company that specialises in disaster recovery services. In some cases, an organisation will have an agreement with a second organisation to operate a joint backup site.

There are three main types of backup sites:

cold sites

warm sites

hot sites

Differences between them are determined by costs and effort required to implement each.

Another term used to describe a backup site is a work area recovery site.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Cold Sites: A cold site is the most inexpensive type of backup site for an organisation to operate. It does not include backed up copies of data and information from the original location of the organisation, nor does it include hardware already set up. The lack of hardware contributes to the minimal start up costs of the cold site, but requires additional time following the disaster to have the operation running at a capacity close to that prior to the disaster.

Hot Sites: A hot site is a duplicate of the original site of the organisation, with full computer systems as well as near-complete backups of user data. Real-time synchronisation between the two sites may be used to mirror the data environment of the original site, using wide area network links and specialised software. Following a disruption to the original site, the hot site exists so that the organisation can relocate with minimal losses to normal operations. Ideally, a hot site will be up and running within a matter of hours or even less. Personnel may still have to be moved to the hot site so it is possible that the hot site may be operational from a data processing perspective before staff has relocated. The capacity of the hot site may or may not match the capacity of the original site depending on the organisation's requirements. This type of backup site is the most expensive to

operate. Hot sites are popular with organisations that operate real time processes such as financial institutions, government agencies and ecommerce providers

Warm Sites: A warm site is, quite logically, a compromise between hot and cold. These sites will have hardware and connectivity already established, though on a smaller scale than the original production site or even a hot site. Warm sites will have backups on hand, but they may not be complete and may be between several days and a week old. An example would be backup tapes sent to the warm site by courier

8.1 The following issues arise in choosing a back up site and implementing a DC/DR solution:

Solution architectures of DC and DR are not identical for all the applications and services. Critical applications and services, namely the retail, corporate, trade finance and government business solutions as well as the delivery channels are having the same DR configurations whereas surround or interfacing applications do not have the DR support. Banks will have to conduct periodical review with reference to the above aspect and upgrade the DR solutions from time to time and ensure that all the critical applications and services have a perfect replica in terms of performance and availability.

The configurations of servers, network devices and other products at the DC and DR have to be identical at all times. This includes the patches that are applied at the DC periodically and the changes made to the software from time to time by customization and parameterization to account for the regulatory requirements, system changes etc .

Periodic checks with reference to ensuring data and transaction integrity between DC and DR are mandatory. It could be done over the week end or as a part of the EoD / BoD process.

Solutions have to have a defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) parameter. These two parameters have a very clear bearing on the technology aspects as well as the process defined for cut over to the DR and the competency levels required moving over in the specified time frame.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Values chosen for the RTO and RPO is more to follow the industry practice and not derived from first principles. Therefore, the DR drills that are conducted periodically have to ensure that the above parameters are strictly complied with.

Technology operations processes which support business operations (such as EOD/ BOD) need to formally included into the IT Continuity Plan.

Banks may also consider Recovery Time Objective and Recovery Point Objectives (RTO/ RPO) for services being offered and not just a specific application. For example--for internet portal and not retail banking. This is done to avoid any inconsistency in business users understanding.

DR drills currently conducted periodically come under the category of planned shutdown. Banks have to evolve a suitable methodology to conduct the drills which are closer to the real disaster scenario so that the confidence levels of the technical team taking up this exercise is built to address the requirement in the event of a real disaster.

It is also recommended that the support infrastructure at the DC and DR, namely the electrical systems, air-conditioning environment and other support systems have no single point of failure and do have a building management and monitoring system to constantly and continuously monitor the resources. If it is specified that the solution has a high availability of

95 measured on a monthly basis and a mean time to restore of 2 hrs in the event of any failure, it has to include the support system also.

Data replication mechanism followed between DC and DR is the asynchronous replication mechanism and implemented across the industry either using database replication techniques or the storage based replication techniques. They do have relative merits and demerits. The RTO and RPO discussed earlier, along with the replication mechanism used and the data transfer required to be accomplished during the peak load will decide the bandwidth required between the DC and the DR. The RPO is directly related to the latency permissible for the transaction data from the DC to update the database at the DR. Therefore, the process implemented for the data replication requirement has to conform to the above and with no compromise to data and transaction integrity.

Given the need for drastically minimizing the data loss during exigencies and enable quick recovery and continuity of critical business operations, banks may need to consider near site DR architecture. Major banks with significant customer delivery channel usage and significant participation in financial markets/payment and settlement systems may need to have a plan of action for creating a near site DR architecture over the medium term (say, within three years).

8.2 Issues/Challenges in DC/DR implementation by the Banks

Despite considerable advances in equipment and telecommunications design and recovery services, IT disaster recovery is becoming challenging. Continuity and recovery aspects are impacting IT strategy and cost implications are challenging IT budgets.

The time window for recovery is shrinking in face of the demand for 24 / 365 operations. Some studies claim that around 30 percent of high-availability applications have to be recovered in less than three hours. A further 45 percent within 24 hours, before losses become unsustainable; others claim that 60 percent of Enterprise Resource Planning (ERP) Systems have to be restored in under 24 hours. This means that traditional off-site backup and restore methods are often no longer adequate. It simply takes too long to recover incremental and full image backups of various inter-related applications (backed up at different times), synchronise them and re-create the position as at disaster. Continuous operation--data

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

mirroring to off-site locations and standby computing and telecommunications—may be the only solution.

A risk assessment and business impact analysis should establish the justification for continuity for specific IT and telecommunication services and applications.

Achieving robust security (security assurance) is not a onetime activity. It cannot be obtained just by purchasing and installing suitable software and hardware. It is a continuous process that requires regular assessment of the security health of the organisation and proactive steps to detect and fix any vulnerability. Every bank should have in place quick and reliable access to expertise for tracking suspicious behavior, monitoring users and performing forensics. Adequate reporting to the authorities concerned – such as the RBI/ IDBRT/CERT-In and other institutions should be an automatic sub process whenever such events occur.

Important steps that need to be institutionalised are the following:

Rigorous self-assessment of security measures by banks and comprehensive security audit by external agencies, as detailed under the “Chapter on Information Security” earlier.

Random Security Preparedness. It is proposed that a sufficiently large “question bank” related to security health of the organization be prepared and given to RBI's inspection teams who go for inspection of banks. A random subset of these queries could then be given to a bank's IT team for which answers need to be provided in near real time. Sample checks related to user accounts could be the number of new accounts, terminated accounts, most active accounts. There could also be demonstrations of data recovery from archives.

Telecommunications issues may also arise: It is important to ensure that relevant links are in place and that communications capability is compatible. The adequacy of voice and data capacity needs to be checked. Telephony needs to be switched from the disaster site to the standby site. A financial institution's BCP should consider addressing diversity guidelines for its telecommunications capabilities. This is particularly important for the financial services sector that provides critical payment, clearing, and settlement processes; however, diversity guidelines should be considered by all financial institutions and should be commensurate with the institution's size, complexity, and overall risk profile. Diversity guidelines may include arrangements with multiple telecommunications providers. However, diverse routing may be difficult to achieve since primary telecommunications carriers may have an agreement with the same sub-carriers to provide local access service, and these sub-carriers may also have a contract with the same local access service providers. Financial institutions do not have any control over the number of circuit segments that will be needed, and they typically do not have a business relationship with any of the sub-carriers. Consequently, it is important for financial institutions to understand the relationship between their primary telecommunications carrier and these various sub-carriers and how this complex network connects to their primary and back-up facilities. To determine whether telecommunications providers use the same sub-carrier or local access service provider, banks may consider performing an end-to-end trace of all critical or sensitive circuits to search for single points of failure such as a common switch, router, PBX, or central telephone office.

Banks may consider the following telecommunications diversity components to enhance BCP:

Alternative media, such as secure wireless systems

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Internet protocol networking equipment that provides easily configurable re-routing and traffic load balancing capabilities

Local services to more than one telecommunications carrier's central office, or diverse physical paths to independent central offices

Multiple, geographically diverse cables and separate points of entry

Frame relay circuits that do not require network interconnections, which often causes delays due to concentration points between frame relay providers

Separate power sources for equipment with generator or uninterrupted power supply back-up

(vii) Separate connections to back-up locations

Regular use of multiple facilities in which traffic is continually split between the connections; and

Separate suppliers for hardware and software infrastructure needs.

Banks need to monitor their service relationship with telecommunications providers: In order to manage the inherent risks more effectively. In coordination with vendors, management should ensure that risk management strategies include

the following, at a minimum:

- Establish service level agreements that address contingency measures and change management for services provided;
- Ensure that primary and back-up telecommunications paths do not share a single point of failure
- Establish processes to periodically inventory and validate telecommunications circuits and routing paths through comprehensive testing.

Some vendors offer a drop-ship service as an alternative to occupying the standby site. That is, in the event of equipment failure, for instance, they will drop off a replacement rather than insist the client occupy the standby site, with all the inconvenience that may involve. But it is essential that a site survey is undertaken to ensure they can be parked on the required site. Most commercial standby sites offering IT and work area recovery facilities do not guarantee a service: the contract merely provides access to the equipment. Although most reputable

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

vendors will negotiate a Service Level Agreement that specifies the quality of the service, it is rarely offered.

It is important to ensure that a bank's service will not suffer from unacceptable downtime or response. The vendor may have skilled staff available – but this is rarely guaranteed and they come at a cost. In terms of cost, there may be additional fees to pay for testing, on invocation of a disaster, and for occupation in a disaster. The vendor charging structure also needs to be carefully considered.

Outsourcing Risks: In theory a commercial hot or warm standby site is available 24 / 365. It has staff skilled in assisting recovery. Its equipment is constantly kept up to date, while older equipment remains supported. It is always available for use and offers testing periods once or twice a year. The practice may be different. These days, organizations have a wide range of equipment from different vendors and different models from the same vendor. Not every commercial standby site is able to support the entire range of equipment that a bank may have. Instead, vendors form alliances with others – but this may mean that a bank's recovery effort is split between more than one standby site. The standby site may not have identical IT equipment: instead of the use of an identical piece of equipment, it will offer a partition on a compatible large computer or server. Operating systems and security packages may not be the same version as the client usually uses. These aspects may cause setbacks when attempting recovery of IT systems and applications – and weak change control at the recovery site could cause a disaster on return to the normal site.

It is the responsibility of the IT manager/bank to ensure effective recovery by those vendors, who apply the highest standards, supporting this by a stringent contract, clearly defining service specifications and technical requirements, and service-level agreements.

Information and network security

Introduction:

Information and the knowledge based on it have increasingly become recognized as 'information assets', which are vital enablers of business operations. Hence, they require organizations to provide adequate levels of protection. For banks, as purveyors of money in physical form or in bits and bytes, reliable information is even more critical and hence information security is a vital area of concern.

Robust information is at the heart of risk management processes in a bank. Inadequate data quality is likely to induce errors in decision making. Data quality requires building processes, procedures and disciplines for managing information and ensuring its integrity, accuracy, completeness and timeliness. The fundamental attributes supporting data quality should include accuracy, integrity, consistency, completeness, validity, timeliness, accessibility, usability and auditability. The data quality provided by various applications depends on the quality and integrity of the data upon which that information is built. Entities that treat information as a critical organizational asset are in a better position to manage it proactively.

Information security not only deals with information in various channels like spoken, written, printed, electronic or any other medium but also information handling in terms of creation, viewing, transportation, storage or destruction. This is in contrast to IT security which is mainly concerned with

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

security of information within the boundaries of the network infrastructure technology domain. From an information security perspective, the nature and type of compromise is not as material as the fact that security has been breached.

To achieve effective information security governance, bank management must establish and maintain a framework to guide the development and maintenance of a comprehensive information security programme.

Basic Principles of Information Security:

For over twenty years, information security has held confidentiality, integrity and availability (known as the CIA triad) to be the core principles. There is continuous debate about extending this classic trio. Other principles such as Authenticity, Non-repudiation and accountability are also now becoming key considerations for practical security installations.

Confidentiality: Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred. Breaches of confidentiality take many forms like Hacking, Phishing, Vishing, Email-spoofing, SMS spoofing, and sending malicious code through email or Bot Networks, as discussed earlier.

Integrity: In information security, integrity means that data cannot be modified without authorization. This is not the same thing as referential integrity in databases.

Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when he/she is able to modify his own salary in a payroll database, when an employee uses programmes and deducts small amounts of money from all customer accounts and adds it to his/her own account (also called salami technique), when an unauthorized user vandalizes a web site, and so on.

On a larger scale, if an automated process is not written and tested correctly, bulk updates to a database could alter data in an incorrect way, leaving the integrity of the data compromised. Information security professionals are tasked with finding ways to implement controls that prevent errors of integrity.

Availability: For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service (DoS) and distributed denial-of service (DDoS) attacks.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Authenticity: In computing, e-business and information security it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are.

Non-repudiation: In law, non-repudiation implies one's intention to fulfill one's obligations under a contract / transaction. It also implies that a party to a transaction cannot deny having received or having sent an electronic record. Electronic commerce uses technology such as digital signatures and encryption to establish authenticity and non-repudiation.

In addition to the above, there are other security-related concepts and principles when designing a security policy and deploying a security solution. They include identification, authorization, accountability, and auditing.

Identification: Identification is the process by which a subject professes an identity and accountability is initiated. A subject must provide an identity to a system to start the process of authentication, authorization and accountability. Providing an identity can be typing in a username, swiping a smart card, waving a proximity device, speaking a phrase, or positioning face, hand, or finger for a camera or scanning device. Proving a process ID number also represents the identification process. Without an identity, a system has no way to correlate an authentication factor with the subject.

Authorization: Once a subject is authenticated, access must be authorized. The process of authorization ensures that the requested activity or access to an object is possible given the rights and privileges assigned to the authenticated identity. In most cases, the system evaluates an access control matrix that compares the subject, the object, and the intended activity. If the specific action is allowed, the subject is authorized. Else, the subject is not authorized.

Accountability and auditability: An organization's security policy can be properly enforced only if accountability is maintained, i.e., security can be maintained only if subjects are held accountable for their actions. Effective accountability relies upon the capability to prove a subject's identity and track their activities. Accountability is established by linking a human to the activities of an online identity through the

security services and mechanisms of auditing, authorization, authentication, and identification. Thus, human accountability is ultimately dependent on the strength of the authentication process. Without a reasonably strong authentication process, there is doubt that the correct human associated with a specific user account was the actual entity controlling that user account when an undesired action took place.

Information Security Governance

Information security governance consists of the leadership, organizational structures and processes that protect information and mitigation of growing information security threats like the ones detailed above.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Critical outcomes of information security governance include:

Alignment of information security with business strategy to support organizational objectives

Management and mitigation of risks and reduction of potential impacts on information resources to an acceptable level

Management of performance of information security by measuring, monitoring and reporting information security governance metrics to ensure that organizational objectives are achieved
Optimisation of information security investments in support of organizational objectives

It is important to consider the organisational necessity and benefits of information security governance. They include increased predictability and the reduction of uncertainty in business operations, a level of assurance that critical decisions are not based on faulty information, enabling efficient and effective risk management, protection from the increasing potential for legal liability, process improvement, reduced losses from security-related events and prevention of catastrophic consequences and improved reputation in the market and among customers.

A comprehensive security programme needs to include the following main activities:

Development and ongoing maintenance of security policies
Assignment of roles, responsibilities and accountability for information security
Development/maintenance of a security and control framework that consists of standards, measures, practices and procedures
Classification and assignment of ownership of information assets
Periodic risk assessments and ensuring adequate, effective and tested controls for people, processes and technology to enhance information security
Ensuring security is integral to all organizational processes
Processes to monitor security incidents
Effective identity and access management processes
Generation of meaningful metrics of security performance
Information security related awareness sessions to users/officials including senior officials and board members

Organizational Structure, Roles and Responsibilities:

Boards of Directors/Senior Management

The Board of Directors is ultimately responsible for information security. Senior Management is responsible for understanding risks to the bank to ensure that they are adequately addressed from a governance perspective. To do so effectively requires managing risks, including information security risks, by integrating information security governance in the

overall enterprise governance framework of the organization. It is reported that the effectiveness of information security governance is dependent on the involvement of the Board/senior management in approving policy and appropriate monitoring of the information security function.

The major role of top management involves implementing the Board approved information security policy, establishing necessary organizational processes for information security and providing

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

necessary resources for successful information security. It is essential that senior management establish an expectation for strong cyber security and communicate this to their officials down the line. It is also essential that the senior organizational leadership establish a structure for implementation of an information security programme to enable a consistent and effective information security programme implementation apart from ensuring the accountability of individuals for their performance as it relates to cyber security.

Given that today's banking is largely dependent on IT systems and since most of the internal processing requirements of banks are electronic, it is essential that adequate security systems are fully integrated into the IT systems of banks. It would be optimal to classify these based on the risk analysis of the various systems in each bank and specific risk mitigation strategies need to be in place.

Information security team/function

Banks should form a separate information security function/group to focus exclusively on information security management. There should be segregation of the duties of the Security Officer/Group dealing exclusively with information systems security and the Information Technology Division which actually implements the computer systems. The organization of the information security function should be commensurate with the nature and size of activities of a bank including a variety of e-banking systems and delivery channels of a bank. The information security function should be adequately resourced in terms of the number of staff, level of skills and tools or techniques like risk assessment, security architecture, vulnerability assessment, forensic assessment, etc. While the information security group/function itself and information security governance related structures should not be outsourced, specific operational components relating to information security can be outsourced, if required resources are not available within a bank. However, the ultimate control and responsibility rests with the bank.

Information Security Committee

Since information security affects all aspects of an organization, in order to consider information security from a bank -wide perspective a steering committee of executives should be formed with formal terms of reference. The Chief Information Security Officer would be the member secretary of the Committee. The committee may include, among others, the Chief Executive Officer (CEO) or designee, chief financial officer (CFO), business unit executives, Chief Information Officer (CIO)/ IT Head, Heads of human resources, legal, risk management, audit, operations and public relations.

A steering committee serves as an effective communication channel for management's aims and directions and provides an ongoing basis for ensuring alignment of the security programme with organizational objectives. It is also instrumental in achieving behavior change toward a culture that promotes good security practices and compliance with policies.

Major responsibilities of the Information Security Committee, inter-alia, include:

Developing and facilitating the implementation of information security policies, standards and procedures to ensure that all identified risks are managed within a bank's risk appetite

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Approving and monitoring major information security projects and the status of information security plans and budgets, establishing priorities, approving standards and procedures

Supporting the development and implementation of a bank-wide information security management programme

Reviewing the position of security incidents and various information security assessments and monitoring activities across the bank

Reviewing the status of security awareness programmes

Assessing new developments or issues relating to information security

Reporting to the Board of Directors on information security activities

Minutes of the Steering Committee meetings should be maintained to document the committee's activities and decisions and a review on information security needs to be escalated to the Board on a quarterly basis.

Chief information security officer (CISO)

A sufficiently senior level official, of the rank of GM/DGM/AGM, should be designated as Chief Information Security Officer, responsible for articulating and enforcing the policies that banks use to protect their information assets apart from coordinating the security related issues / implementation within the organization as well as relevant external agencies. The CISO needs to report directly to the Head of Risk Management and should not have a direct reporting relationship with the CIO. However, the CISO may have a working relationship with the CIO to develop the required rapport to understand the IT infrastructure and operations, to build effective security in IT across the bank, in tune with business requirements and objectives.

Critical components of information security:

Policies and procedures:

Banks need to frame Board approved Information Security Policy and identify and implement appropriate information security management measures/practices keeping in view their business needs.

The policies need to be supported with relevant standards, guidelines and procedures. A policy framework would, inter-alia, incorporate/take into consideration the following:

- An information security strategy that is aligned with business objectives and the legal requirements

- Objectives, scope, ownership and responsibility for the policy

- Information security organisational structure

- Information security roles and responsibilities that may include information security-specific roles like IT security manager/officer, administrators, information security specialists and information asset-specific roles like owners, custodians, end-users

- Periodic reviews of the policy – at least annually and in the event of significant changes necessitating revision

- A periodic compliance review of the policy – about the adherence of users to information security policies and put up to the information security committee.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Exceptions: An exception policy for handling instances of non-compliance with the information security policy including critical aspects like exception criteria including whether there is genuine need for exceptions, management of the exception log or register, authority to grant exemptions, expiry of exceptions and the periodicity of review of exceptions granted. Where exemptions are granted, banks need to review and assess the adequacy of compensating controls initially and on an ongoing basis. A sign-off needs to be obtained from the CISO on the exceptions

Penal measures for violation of policies and the process to be followed in the event of violation

Identification, authorisation and granting of access to IT assets (by individuals and other IT assets)

Addressing the various stages of an IT asset's life to ensure that information security requirements are considered at each stage of the lifecycle

An incident monitoring and management process to address the identification and classification of incidents, reporting, escalation, preservation of evidence, the investigation process

Management of technology solutions for information security like a firewall, anti-virus/anti-malware software, intrusion detection/prevention systems, cryptographic systems and monitoring/log analysis tools/techniques

Management and monitoring of service providers that provides for overseeing the management of information security risks by third parties

Clearly indicating acceptable usage of IT assets including application systems that define the information security responsibilities of users (staff, service providers and customers) in regard to the use of IT assets

Requirements relating to recruitment and selection of qualified staff and external contractors that define the framework for vetting and monitoring of personnel, taking into account the information security risk

Strategy for periodic training and enhancing skills of information security personnel, requirement of continuous professional education

Specific policies that would be required include, but not limited to, the following:

- Logical Access Control
- Asset Management
- Network Access Control
- Password management
- E-mail security
- Remote access
- Mobile computing
- Network security
- Application security
- Backup and archival
- Operating system security
- Database administration and security
- Physical security
- Capacity Management
- Incident response and management
- Malicious software
- IT asset/media management
- Change Management
- Patch Management
- Internet security
- Desktop
- Encryption
- Security of electronic delivery channels

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Wireless security Application/data migration

Accountability for security is increased through clear job descriptions, employment agreements and policy awareness acknowledgements. It is important to communicate the general and specific security roles and responsibilities for all employees within their job descriptions. The job descriptions for security personnel should also clearly describe the systems and processes they will protect and their responsibility towards control processes. Management should expect all employees, officers and contractors/consultants to comply with security and acceptable-use policies and protect the institution's assets, including information.

Given the critical role of security technologies as part of the information security framework, banks need to subject them to suitable controls across their lifecycle like guidelines on their usage, standards and procedures indicating the detailed objectives and requirements of individual information security-specific technology solutions, authorisation for individuals who would be handling the technology, addressing segregation of duties issues, appropriate configurations of the devices that provide the best possible security, regularly assessing their effectiveness and fine-tuning them accordingly, and identification of any unauthorised changes.

Digital evidence is similar to any other form of legal proof - it needs to withstand challenges to its integrity, its handling must be carefully tracked and documented, and it must be suitably authenticated by concerned personnel as per legal requirements. Since the evidence resides on or is generated by a digital device, a trained information security official or skilled digital forensics examiner may need to be involved in the handling process to ensure that any material facts is properly preserved and introduced. A suitable policy needs to be in place in this regard.

Risk Assessment

The likelihood that a threat will use a vulnerability to cause harm creates a risk. When a threat does use a vulnerability to inflict harm, it has an impact. In the context of information security, the impact is a loss of availability, integrity and confidentiality, and possibly other losses (lost income, loss of life, loss of property).

Risk assessment is the core competence of information security management. The risk assessment must, for each asset within its scope, identify the threat/vulnerability combinations that have a likelihood of impacting the confidentiality, availability or integrity of that asset - from a business, compliance or contractual perspective. Standards like ISO27001 and ISO 27002 are explicit in requiring a risk assessment to be carried out before any controls are selected and implemented and are equally explicit that the selection of every control must be justified by a risk assessment.

In broad terms, the risk management process consists of:

- Identification of assets and estimation of their value. Some aspects to be included are people, buildings, hardware, software, data (electronic, print) and supplies

- Conducting a threat assessment which may include aspects like acts of nature, acts of war, accidents, malicious acts originating from inside or outside the organization

- Conducting a vulnerability assessment for each vulnerability and calculating the probability that it will be exploited. Evaluating policies, procedures, standards, training, physical security, quality control and technical security in this regard

- Calculating the impact that each threat would have on each asset through qualitative or quantitative analysis

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Identifying, selecting and implementing appropriate controls. Providing proportional response including considerations like productivity, cost effectiveness, and the value of the asset

Evaluating the effectiveness of the control measures. Ensuring the controls provide the required cost-effective protection.

The process of risk management is an ongoing iterative process. The business environment is constantly changing and new threats and vulnerabilities emerge every day. The choice of countermeasures or controls used to manage risks must strike a balance between productivity, cost-effectiveness of the countermeasure and the value of the informational asset being protected. The risk assessment should be carried out by a team of people who have knowledge of specific areas of the business. The assessment may use a subjective qualitative analysis based on informed opinion, or where reliable figures and historical information is available, quantitative analysis.

Quantitative methods involve assigning numerical measurements that can be entered into the analysis to determine total and residual risks. The various aspects that are considered a part of measurements include costs to safeguard the information and information systems, value of that information and those systems, threat frequency and probability, and the effectiveness of controls. A shortcoming of quantitative methods is a lack of reliable and predictive data on threat frequency and probability. This shortcoming is generally addressed by assigning numeric values based on qualitative judgments.

Qualitative analysis involves the use of scenarios and attempts to determine the seriousness of threats and the effectiveness of controls. Qualitative analysis is by definition subjective, relying upon judgment, knowledge, prior experience and industry information. Qualitative techniques may include walk-throughs, surveys/questionnaires, interviews and specific workgroups to obtain information about the various scenarios.

Inventory and information/data classification

Effective control requires a detailed inventory of information assets. Such a list is the first step in classifying the assets and determining the level of protection to be provided to each asset.

The inventory record of each information asset should, at the least, include:

- A clear and distinct identification of the asset
- Its relative value to the organization
- Its location
- Its security/risk classification
- Its asset group (where the asset forms part of a larger information system)
- Its owner
- Its designated custodian

Information assets have varying degrees of sensitivity and criticality in meeting business objectives. By assigning classes or levels of sensitivity and criticality to information resources and establishing specific security rules/requirements for each class, it is possible to define the level of access controls that should be applied to each information asset. Classification of information reduces the risk and cost of over- or under - protecting information resources in aligning security with business objectives since it helps to build and maintain a consistent and uniform perspective of the security requirements

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

for information assets throughout the organization. ISO 27001 standards require the inventorying of information assets and the classification, handling and labelling of information in accordance with preset guidelines.

Defining roles and responsibilities

All defined and documented responsibilities and accountabilities must be established and communicated to all relevant personnel and management. Some of the major ones include:

Information owner

This is a business executive or business manager who is responsible for a bank's business information asset. Responsibilities would include, but not be limited to:

- Assigning initial information classification and periodically reviewing the classification to ensure it still meets business needs
- Ensuring security controls are in place commensurate with the classification

- Reviewing and ensuring currency of the access rights associated with information assets they own

- Determining security requirements, access criteria and backup requirements for the information assets they own

Information custodian

The information custodian, usually an information systems official, is the delegate of the information owner with primary responsibilities for dealing with backup and recovery of the business information. Responsibilities include, but are not limited to, the following:

- Performing backups according to the backup requirements established by the information owner

- When necessary, restoring lost or corrupted information from backup media to return the application to production status

- Ensuring record retention requirements are met based on the information owner's requirements

Application owner

The application owner is the manager of the business line who is fully accountable for the performance of the business function served by the application. Responsibilities, inter-alia, include:

- Establishing user access criteria, availability requirements and audit trails for their applications

- Ensuring security controls associated with the application are commensurate with support for the highest level of information classification used by the application

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Performing or delegating the following - day-to-day security administration, approval of exception access requests, appropriate actions on security violations when notified by the security administration, the review and approval of all changes to the application prior to being placed in the production environment, and verification of the currency of user access rights to the application

User manager

The user manager is the immediate manager or supervisor of an employee or HR official of the business function in which an employee works. He has the ultimate responsibility for all user IDs and information assets owned by bank employees. In the case of non employee individuals such as contractors, consultants, etc., this manager is responsible for the activity and for the bank assets used by these individuals. He/she is usually the manager responsible for hiring the outside contractor. Responsibilities include the following:

- Informing security administration of the termination of any employee so that the user ID owned by that individual can be revoked, suspended or made inaccessible in a timely manner
- Informing security administration of the transfer of any employee if the transfer involves the change of access rights or privileges
- Reporting any security incident or suspected incident to the Information Security function
- Ensuring that employees are aware of relevant security policies, procedures and standards to which they are accountable

Security Administrator

Security administrators have the powers to set system-wide security controls or administer user IDs and information resource access rights. These security administrators usually report to the Information Security function. Responsibilities include the following:

- Understanding different data environments and the impact of granting access to them
- Ensuring access requests are consistent with the information directions and security guidelines
- Administering access rights according to criteria established by the Information Owners
- Creating and removing user IDs as directed by the user manager
- Administering the system within the scope of their job description and functional responsibilities
- Distributing and following up on security violation reports

End user

The end users would be any employees, contractors or vendors of the bank who use information systems resources as part of their job. Responsibilities include :

- Maintaining confidentiality of log-in password(s)
- Ensuring security of information entrusted to their care
- Using bank business assets and information resources for management approved purposes only

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Adhering to all information security policies, procedures, standards and guidelines

Promptly reporting security incidents to management.

Access Control

An effective process for access to information assets is one of the critical requirements of information security. Internal sabotage, clandestine espionage or furtive attacks by trusted employees, contractors and vendors are among the most serious potential risks that a bank faces. Current and past employees, contractors, vendors and those who have an intimate knowledge of the inner workings of the bank's systems, operations and internal controls have a significant advantage over external attackers. A successful attack could jeopardise customer confidence in a bank's internal control systems and processes.

Hence, access to information assets needs to be authorised by a bank only where a valid business need exists and only for the specific time period that the access is required. The various factors that need to be considered when authorising access to users and information assets, inter-alia, include business role, physical location, method of connectivity, remote access, time, anti-malware and patch update status, nature of device used and software /operating system.

The provision of access involves various stages like identification and authentication which involves determination of the person or IT asset requesting access and confirmation of the purported identity and authorisation. This involves an assessment of whether access is allowed to an information asset by the request or based on the needs of the business and the level of information security required. These processes are applicable to both users as well as IT assets.

A bank should take appropriate measures to identify and authenticate users or IT assets. The required strength of authentication needs to be commensurate with risk. Common techniques for increasing the strength of identification and authentication include the use of strong password techniques (i.e. increased length, complexity, re-use limitations and frequency of change) and increasing the number and/or type of authentication factors used.

The examples where increased authentication strength may be required, given the risks involved include : administration or other privileged access to sensitive or critical IT assets, remote access through public networks to sensitive assets and activities carrying higher risk like third-party fund transfers, etc. The period for which authentication is valid would need to be commensurate with the risk.

Among the important controls that banks need to consider are:

- A systematic process of applying and authorizing the creation of user ids and the access control matrix

- Conducting a risk assessment and granting access rights based on the same. For example, contractors and temporary staff would have higher inherent risks

- Implementation of role-based access control policies designed to ensure effective segregation of duties

- Changing default user names and/or passwords of systems and prohibiting sharing of user ids and passwords including generic accounts

- Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment

- Processes to notify in a timely manner the information security function regarding user additions, deletions and role changes

- Periodic reconciliation of user ids in a system and actual users required to have access and deletion of unnecessary ids, if any

- Audit of logging and monitoring of access to IT assets by all users

- Regular reviews of user access by information asset owners to ensure appropriate access is maintained

- Applying the four-eyes principle to very critical/sensitive IT assets

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Considering de-activating user ids of users of critical applications who are on prolonged leave

- (vii) Banks may consider using automated solutions to enable effective access control and management of user ids. Such solutions should also be managed effectively to ensure robust access management.

For accountability purposes, a bank should ensure that users and IT assets are uniquely identified and their actions are auditable.

Transaction processes and systems should be designed to ensure that no single employee/outsourced service provider could enter, authorize and complete a transaction. Segregation should be maintained between those initiating static data (including web page content) and those responsible for verifying its integrity. Further, segregation should be maintained between those developing and those administering e-banking systems.

E-banking systems should be tested to ensure that segregation of duties cannot be bypassed. Mutual authentication system may be considered. Mutual Authentication, also called two-way authentication, is a security feature in which a client process must prove his identity to a server, and the server must prove its identity to the client, before any application traffic is sent over the client-to-server connection. Identity can be proved through a trusted third party and use of shared secrets or through cryptographic means as with a public key infrastructure. For e.g., with the mutual authentication implemented, a connection can occur only when the client trusts the server's digital certificate and the server trusts the client's certificate. The exchange of certificates will happen through special protocols like the [Transport Layer Security \(TLS\)](#) protocol. This process reduces the risk that an unsuspecting network user will inadvertently reveal security information to a malicious or insecure web site.

System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the banking systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below needs to be considered:

- Implementing two-factor authentication for privileged users
- Instituting strong controls over remote access by privileged users
- Restricting the number of privileged users

- Granting privileged access on a "need-to-have" or "need-to-do" basis
- Maintaining audit logging of system activities performed by privileged users
- Ensuring that privileged users do not have access to systems logs in which their activities are being captured
- Conducting regular audit or management review of the logs
- Prohibiting sharing of privileged IDs and their access codes
- Disallowing vendors and contractors from gaining privileged access to systems without close supervision and monitoring

- Protecting backup data from unauthorized access.

Information security and information asset life-cycle

Information security needs to be considered at all stages of an information asset's life-cycle like planning, design, acquisition and implementation, maintenance and disposal. Banks need to apply systematic project management oriented techniques to manage material changes during these stages and to ensure that information security requirements have been adequately addressed.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Planning and design level controls need to be in place to ensure that information security is embodied in the overall information systems architecture and the implemented solutions are in compliance with the information security policies and requirements of a bank.

Ongoing support and maintenance controls would be needed to ensure that IT assets continue to meet business objectives. Major controls in this regard include change management controls to ensure that the business objectives continue to be met following change; configuration management controls to ensure that the configuration minimises vulnerabilities and is defined, assessed, maintained and managed; deployment and environment controls to ensure that development, test and production environments are appropriately segregated; and patch management controls to manage the assessment and application of patches to software that addresses known vulnerabilities in a timely manner

The other relevant controls include service level management, vendor management, capacity management and configuration management which are described in later chapters. Decommissioning and destruction controls need to be used to ensure that information security is not compromised as IT assets reach the end of their useful life. (for example, through archiving strategies and deletion of sensitive information prior to the disposal of IT assets.)

Personnel security

Application owners grant legitimate users access to systems that are necessary to perform their duties and security personnel enforce the access rights in accordance with institution standards. Because of their internal access levels and intimate knowledge of financial institution processes, authorized users pose a potential threat to systems and data. Employees, contractors, or third-party employees can also exploit their legitimate computer access for malicious or fraudulent reasons. Further, the degree of internal access granted to some users can increase the risk of accidental damage or loss of information and systems.

Risk exposures from internal users include altering data, deleting production and back-up data, disrupting/destroying systems, misusing systems for personal gain or to damage the institution, holding data hostage and stealing strategic or customer data for espionage or fraud schemes.

Banks should have a process to verify job application information on all new employees. Additional background and credit checks may be warranted based on the sensitivity of a particular job or access level. Personnel with privileged access like administrators, cyber security personnel, etc. should be subjected to rigorous background checks and screening. Institutions should verify that contractors are subject to similar screening procedures. The verification considerations would include:

- Character references – business and personal

- Confirmation of prior experience, academic record, and professional qualifications

- Confirmation of identity through a government issued identification

There also needs to be a periodic rotation of duties among users or personnel as a prudent risk measure.

Physical security

The confidentiality, integrity, and availability of information can be impaired through physical access and damage or destruction to physical components. Conceptually, those physical security risks are mitigated through zone-oriented implementations. Zones are physical areas with differing physical security requirements. The security requirements of each zone are a function of the sensitivity of the data contained or accessible through the zone and the information technology components in the zone.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

The requirements for each zone should be determined through the risk assessment. The risk assessment should include, but is not limited to, threats like aircraft crashes, chemical effects, dust, electrical supply interference, electromagnetic radiation, explosives, fire, smoke, theft/destruction, vibration/earthquake, water, criminals, terrorism, political issues (e.g. strikes, disruptions) and other threats based on the entity's unique geographical location, building configuration, neighboring environment/entities, etc.

A bank needs to deploy the following environmental controls:

- Secure location of critical assets providing protection from natural and man-made threats

- Restrict access to sensitive areas like data centres, which also includes detailed procedures for handling access by staff, third party providers and visitors

- Suitable preventive mechanisms for various threats indicated above

- Monitoring mechanisms for the detection of compromises of environmental controls relating to temperature, water, smoke, access alarms, service availability alerts (power supply, telecommunication, servers), access log reviews etc

User Training and Awareness

It is acknowledged that the human link is the weakest link in the information security chain. Hence, there is a vital need for an initial and ongoing training and information security awareness programme. The programme may be periodically updated keeping in view changes in information security, threats/vulnerabilities and/or the bank's information security framework. There needs to be a mechanism to track the effectiveness of training programmes through an assessment/testing process designed on testing the understanding of the relevant information security policies, not only initially but also on a periodic basis. At any point of time, a bank needs to maintain an updated status on user training and awareness relating to information security and the matter needs to be an important agenda item during Information Security Committee meetings.

Some of the areas that could be incorporated as part of the user awareness programme include:

- Relevant information security policies/procedures

- Acceptable and appropriate usage of IT assets

- Access controls including standards relating to passwords and other authentication requirements

- Measures relating to proper email usage and internet usage

- Physical protection

- Remote computing and use of mobile devices

- Safe handling of sensitive data/information

- Being wary of social engineering attempts to part with confidential details

- Prompt reporting of any security incidents and concerns

Incident management

Incident management is defined as the process of developing and maintaining the capability to manage incidents within a bank so that exposure is contained and recovery achieved within a specified time objective. Incidents can include the misuse of computing assets, information disclosure or events that threaten the continuance of business processes.

Major activities that need to be considered as part of the incident management framework include:

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Developing and implementing processes for preventing, detecting, analyzing and responding to information security incidents
Establishing escalation and communication processes and lines of authority
Developing plans to respond to and document information security incidents
Establishing the capability to investigate information security incidents through various modes like forensics, evidence collection and preservation, log analysis, interviewing, etc.

Developing a process to communicate with internal parties and external organizations (e.g., regulator, media, law enforcement, customers)
Integrating information security incident response plans with the organization's disaster recovery and business continuity plan
Organizing, training and equipping teams to respond to information security incidents

Periodically testing and refining information security incident response plans
Conducting post-mortem analysis and reviews to identify causes of information security incidents, developing corrective actions and reassessing risk, and adjusting controls suitably to reduce the related risks in the future

Common incident types include, but not limited to, outages/degradation of services due to hardware, software or capacity issues, unauthorised access to systems, identity theft, data leakage/loss, malicious software and hardware, failed backup processes, denial of service attacks and data integrity issues.

A bank needs to have clear accountability and communication strategies to limit the impact of information security incidents through defined mechanisms for escalation and reporting to the Board and senior management and customer communication, where appropriate. Incident management strategies would also typically assist in compliance with regulatory requirements. Institutions would also need to pro-actively notify CERT-In/IDRBT/RBI regarding cyber security incidents.

All security incidents or violations of security policies should be brought to the notice of the CISO.

Application Control and Security:

Financial institutions have different types of applications like the core banking system, delivery channels like ATMs, internet banking, mobile banking, phone banking, network operating systems, databases, enterprise resource management (ERP) systems, customer relationship management (CRM) systems, etc., all used for different business purposes. Then these institutions have partners, contractors, consultants, employees and temporary employees. Users usually access several different types of systems throughout their daily tasks, which makes controlling access and providing the necessary level of protection on different data types difficult and full of obstacles. This complexity may result in unforeseen and unidentified holes in the protection of the entire infrastructure including overlapping and contradictory controls, and policy and regulatory noncompliance.

There are well-known information systems security issues associated with applications software, whether the software is developed internally or acquired from an external source. Attackers can potentially use many different paths through the application to do harm to the business. Each of these paths represents a risk that may or may not be serious enough to warrant attention. Sometimes, these paths are easy to find and exploit and sometimes they are extremely difficult. Similarly, the harm that is caused may range from minor to major. To determine the risk to itself, a bank can evaluate the likelihood associated with the threat agent, attack vector, and security weakness and combine it with an estimate of the technical and business impact to the organization. Together, these factors determine the overall risk.

The following are the important Application control and risk mitigation measures that need to be implemented by banks:

- Each application should have an owner which will typically be the concerned business function that uses the application

- Some of the roles of application owners include:

 - Prioritizing any changes to be made to the application and authorizing the changes

 - Deciding on data classification/de-classification and archival/purging procedures for the data pertaining to an application as per relevant policies/regulatory/statutory requirements

 - Ensuring that adequate controls are built into the application through active involvement in the application design, development, testing and change process

 - Ensuring that the application meets the business/functional needs of the users

 - Ensuring that the information security function has reviewed the security of the application

 - Taking decisions on any new applications to be acquired / developed or any old applications to be discarded

 - Informing the information security team regarding purchase of an application and assessing the application based on the security policy requirements

 - Ensuring that the Change Management process is followed for any changes in application

 - Ensuring that the new applications being purchased/developed follow the Information Security policy

 - Ensuring that logs or audit trails, as required, are enabled and monitored for the applications

All application systems need to be tested before implementation in a robust manner regarding controls to ensure that they satisfy business policies/rules of the bank and regulatory and legal prescriptions/requirements. Robust controls need to be built into the system and reliance on any manual controls needs to be minimized. Before the system is live, there should be clarity on the audit trails and the specific fields that are required to be captured as part of audit trails and an audit trail or log monitoring process including personnel responsible for the same.

A bank needs to incorporate information security at all stages of software development. This would assist in improving software quality and minimizing exposure to vulnerabilities. Besides business functionalities, security requirements relating to system access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, security event tracking and exception handling are required to be clearly specified at the initial stages of system development/acquisition. A compliance check against the bank's security standards and regulatory/statutory requirements would also be required.

All application systems need to have audit trails along with policy/procedure of log monitoring for such systems including the clear allocation of responsibility in this regard. Every application affecting critical/sensitive information, for example, impacting financial, customer, control, regulatory and legal aspects, must provide for detailed audit trails/ logging capability with details like transaction id, date, time, originator id, authorizer id, actions undertaken by a given user id, etc. Other details like logging the IP address of the client machine, terminal identity or location may also be considered.

Applications must also provide for, inter-alia, logging unsuccessful logon attempts, access to sensitive options in the application, e.g., master record changes, granting of access rights, use of system utilities, changes in system configuration, etc. The audit trails need to be stored as per a defined period as per any internal/regulatory/statutory requirements and it should be ensured that they are not tampered with.

There should be documented standards/procedures for administering the application, which are approved by the application owner and kept up-to-date. The development, test and production environments need to be properly segregated.

Access should be based on the principle of least privilege and "need to know" commensurate with the job responsibilities. Adequate segregation of duties needs to be enforced.

There should be controls on updating key 'static' business information like customer master files, parameter changes, etc.

Any changes to an application system/data need to be justified by genuine business need and approvals supported by documentation and subjected to a robust change management process. The change management would involve generating a request, risk assessment, authorization from an appropriate authority, implementation, testing and verification of the change done.

Potential security weaknesses / breaches (for example, as a result of analyzing user behaviour or patterns of network traffic) should be identified.

There should be measures to reduce the risk of theft, fraud, error and unauthorized changes to information through measures like supervision of activities and segregation of duties.

Applications must not allow unauthorized entries to be updated in the database. Similarly, applications must not allow any modifications to be made after an entry is authorized. Any subsequent changes must be made only by reversing the original authorized entry and passing a fresh entry.

Direct back-end updates to database should not be allowed except during exigencies, with a clear business need and after due authorization as per the relevant policy.

Access to the database prompt must be restricted only to the database administrator. Robust input validation controls, processing and output controls needs to be built in to the application.

There should be a procedure in place to reduce the reliance on a few key individuals.

Alerts regarding use of the same machine for both maker and checker transactions need to be considered.

There should be a proper linkage between a change request and the corresponding action taken. For example, the specific accounting head or code which was created as a result of a specific request should be established clearly.

Error / exception reports and logs need to be reviewed and any issues need to be remedied /addressed at the earliest.

Critical functions or applications dealing with financial, regulatory and legal, MIS and risk assessment/management, (for example, calculation of capital adequacy, ALM, calculating VaR, risk weighted assets, NPA classification and provisioning, balance sheet compilation, AML system, revaluation of foreign currency balances, computation of MTM gains / losses, etc..) needs to be done through proper application systems and not manually or in a semi-automated manner through spreadsheets. These pose risks relating to data integrity and reliability. Use of spreadsheets in this regard should be restricted and should be replaced by appropriate IT applications within a definite time-frame in a phased manner.

Banks may obtain application integrity statements in writing from the application system vendors providing for reasonable level of assurance about the application being free of malware at the time of sale, free of any obvious bugs, and free of any covert channels in the code (of the version of the application being delivered as well as any subsequent versions/modifications done).

For all critical applications, either the source code must be received from the vendor or a software escrow agreement should be in place with a third party to ensure source code availability in the event the vendor goes out of business. It needs to be ensured that product updates and programme fixes are also included in the escrow agreement.

Applications should be configured to logout the users after a specific period of inactivity. The application must ensure rollover of incomplete transactions and otherwise ensure integrity of data in case of a log out.

There should be suitable interface controls in place. Data transfer from one process to another or from one application to another, particularly for critical systems, should not have any manual intervention in order to prevent any unauthorized modification. The process needs to be automated and properly integrated with due authentication mechanism and audit trails by enabling "Straight Through Processing" between applications or from data sources to replace any manual intervention/semi-automated processes like extracting data in text files and uploading to the target system, importing to a spreadsheet, etc. Further, proper validations and reconciliation of data needs to be carried out between relevant interfaces/applications across the bank. The bank needs to suitably integrate the systems and applications, as required, to enhance data integrity and reliability.

Multi-tier application architecture needs to be considered for relevant critical systems like internet banking systems which differentiate session control,

presentation logic, server side input validation, business logic and database access.

In the event of data pertaining to Indian operations being stored and/or processed abroad, for example, by foreign banks, there needs to be suitable controls like segregation of data and strict access controls based on 'need to know' and robust change controls. The bank should be in a position to adequately prove the same to

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

the regulator. Regulator's access to such data/records and other relevant information should not be impeded in any manner and RBI would have the right to cause an inspection to be made of the processing centre/data centre and its books and accounts by one or more of its officers or employees or other persons.

An application security review/testing, initially and during major changes, needs to be conducted using a combination of source code review, stress loading, exception testing and compliance review to identify insecure coding techniques and systems vulnerabilities to a reasonable extent.

Critical application system logs/audit trails also need to be backed up as part of the application backup policy.

Robust System Security Testing, in respect of critical e-banking systems, needs to incorporate, inter-alia, specifications relating to information leakage, business logic, authentication, authorization, input data validation, exception/error handling, session management, cryptography and detailed logging, as relevant. These need to be carried out atleast on annual basis.

Migration controls:

There needs to be a documented Migration Policy indicating the requirement of road-map / migration plan / methodology for data migration (which includes verification of completeness, consistency and integrity of the migration activity and pre and post migration activities along with responsibilities and timelines for completion of same). Explicit sign offs from users/application owners need to be obtained after each stage of migration and after complete migration process. Audit trails need to be available to document the conversion, including data mappings and transformations.

The key aspects that are required to be considered include:

- a. Integrity of data— indicating that the data is not altered manually or electronically by a person, programme, substitution or overwriting in the new system. Integrity thus, includes error creep due to factors like transposition, transcription, etc.

Completeness— ensuring that the total number of records from the source database is transferred to the new database (assuming the number of fields is the same)

Confidentiality of data under conversion—ensuring that data is backed up before migration for future reference or any emergency that might arise out of the data migration process

Consistency of data— the field/record called for from the new application should be consistent with that of the original application. This should enable consistency in repeatability of the testing exercise

Continuity—the new application should be able to continue with newer records as addition (or appendage) and help in ensuring seamless business continuity

It is a good practice that the last copy of the data before conversion from the old platform and the first copy of the data after conversion to the new platform are maintained separately in the archive for any future reference.

The error logs pertaining to the pre-migration/ migration/ post migration period along with root cause analysis and action taken need to be available for review.

Banks may need to migrate the complete transaction data and audit trails from the old system to the new system. Else, banks should have the capability to access the older transactional

data and piece together the transaction trail between older and newer systems, to satisfy any supervisory/legal requirements that may arise.

Implementation of new technologies:

Banks need to carry out due diligence with regard to new technologies since they can potentially introduce additional risk exposures. A bank needs to authorise the large scale use and deployment in production environment of technologies that have matured to a state where there is a generally agreed set of industry-accepted controls and robust diligence and testing has been carried out to ascertain the security issues of the technology or where compensating controls are sufficient to prevent significant impact and to comply with the institution's risk appetite and regulatory expectations.

Any new business products introduced along with the underlying information systems need to be assessed as part of a formal product approval process which incorporates, inter-alia, security related aspects and fulfilment of relevant legal and regulatory prescriptions. A bank needs to develop an authorisation process involving a risk assessment balancing the benefits of the new technology with the risk.

Encryption

Encryption Types:

Symmetric encryption is the use of the same key and algorithm by the creator and reader of a file or message. The creator uses the key and algorithm to encrypt, and the reader uses both to decrypt. Symmetric encryption relies on the secrecy of the key. If the key is captured by an attacker, either when it is exchanged between the communicating parties, or while one of the parties uses or stores the key, the attacker can use the key and the algorithm to decrypt messages or to masquerade as a message creator.

Asymmetric encryption lessens the risk of key exposure by using two mathematically related keys, the private key and the public key. When one key is used to encrypt, only the other key can decrypt. Therefore, only one key (the private key) must be kept secret. The key that is exchanged (the public key) poses no risk if it becomes known. For instance, if individual A has a private key and publishes the public key, individual B can obtain the public key, encrypt a message to individual A, and send it. As long as an individual keeps his private key secure from disclosure, only individual A will be able to decrypt the message.

Typical areas or situations requiring deployment of cryptographic techniques, given the risks involved, include transmission and storage of critical and/or sensitive data/information in an 'un-trusted' environment or where a higher degree of security is required, generation of customer PINs which are typically used for card transactions and online services, detection of any unauthorised alteration of data/information and verification of the authenticity of transactions or data/information.

Since security is primarily based on the encryption keys, effective key management is crucial. Effective key management systems are based on an agreed set of standards, procedures, and secure methods that address

Generating keys for different cryptographic systems and different applications
Generating and obtaining public keys and distributing keys to intended users, including how keys should be activated when received

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Storing keys, including how authorized users obtain access to keys and changing or updating keys, including rules on when keys should be changed and how this will be done

Dealing with compromised keys, revoking keys and specifying how keys should be withdrawn or deactivated

Recovering keys that are lost or corrupted as part of business continuity management

Archiving, destroying keys

Logging the auditing of key management-related activities

Instituting defined activation and deactivation dates, limiting the usage period of keys

Secure key management systems are characterized by the following precautions:

Additional physical protection of equipment used to generate, store and archive cryptographic keys

Use of cryptographic techniques to maintain cryptographic key confidentiality

Segregation of duties, with no single individual having knowledge of the entire cryptographic key (i.e. two-person controls) or having access to all the components making up these keys

Ensuring key management is fully automated (e.g., personnel do not have the opportunity to expose a key or influence the key creation)

Ensuring no key ever appears unencrypted

Ensuring keys are randomly chosen from the entire key space, preferably by hardware

Ensuring key-encrypting keys are separate from data keys. No data ever appears in clear text that was encrypted using a key-encrypting key. (A key encrypting key is used to encrypt other keys, securing them from disclosure.)

Make sure that keys with a long life are sparsely used. The more a key is used, the greater the opportunity for an attacker to discover the key

Ensuring keys are changed frequently.

Ensuring keys that are transmitted are sent securely to well-authenticated parties.

Ensuring key-generating equipment is physically and logically secure from construction through receipt, installation, operation, and removal from service.

Normally, a minimum of 128-bit SSL encryption is expected. Constant advances in computer hardware, cryptanalysis and distributed brute force techniques may induce use of larger key lengths periodically. It is expected that banks will properly evaluate security requirements associated with their internet banking systems and other relevant systems and adopt an encryption solution that is commensurate with the degree of confidentiality and integrity required. Banks should only select encryption algorithms which are well established international standards and which have been subjected to rigorous scrutiny by an international cryptographer community or approved by authoritative professional bodies, reputable security vendors or government agencies.

Data security

Banks need to define and implement procedures to ensure the integrity and consistency of all data stored in electronic form, such as databases, data warehouses and data archives.

A data security theory seeks to establish uniform risk-based requirements for the protection of data elements. To ensure that the protection is uniform within and outside of the institution, tools such as data classifications and protection profiles can be used, as indicated earlier in the chapter.

Data classification and protection profiles are complex to implement when the network or storage is viewed as a utility. Because of that complexity, some institutions treat all information

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

at that level as if it were of the highest sensitivity and implement encryption as a protective measure. The complexity in implementing data classification in other layers or in other aspects of an institution's operation may result in other risk mitigation procedures being used. Adequacy is a function of the extent of risk mitigation, and not the procedure or tool used to mitigate risk.

Policies regarding media handling, disposal, and transit should be implemented to enable the use of protection profiles and otherwise mitigate risks to data. If protection profiles are not used, the policies should accomplish the same goal as protection profiles, which is to deliver the same degree of residual risk without regard to whether the information is in transit or storage, who is directly controlling the data, or where the storage may be.

There should be secure storage of media. Controls could include physical and environmental controls such as fire and flood protection, limiting access by means like physical locks, keypad, passwords, biometrics, etc., labelling, and logged access. Management should establish access controls to limit access to media, while ensuring that all employees have authorization to access the minimum data required to perform their responsibilities. More sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (e.g., integrity checkers, cryptographic hashes). Furthermore, policies should minimize the distribution of sensitive information, including printouts that contain the information. Periodically, the security staff, audit staff, and data owners should review authorization levels and distribution lists to ensure they remain appropriate and current.

The storage of data in portable devices, such as laptops and PDAs, poses unique problems. Mitigation of those risks typically involves encryption of sensitive data, host-provided access controls, etc.

Banks need appropriate disposal procedures for both electronic and paper based media. Contracts with third-party disposal firms should address acceptable disposal procedures. For computer media, data frequently remains on media after erasure. Since that data can be recovered, additional disposal techniques should be applied to sensitive data like physical destruction, overwriting data, degaussing etc.

Banks should maintain the security of media while in transit or when shared with third parties. Policies should include contractual requirements that incorporate necessary risk-based controls, restrictions on the carriers used and procedures to verify the identity of couriers.

Banks should encrypt customer account and transaction data which is transmitted, transported, delivered or couriered to external parties or other locations, taking into account all intermediate junctures and transit points from source to destination.

A few other aspects that also needs to be considered include appropriate blocking, filtering and monitoring of electronic mechanisms like e-mail and printing and monitoring for unauthorised software and hardware like password cracking software, key loggers, wireless access points, etc.

Concerns over the need to better control and protect sensitive information have given rise to a new set of solutions aimed at increasing an enterprise's ability to protect its information assets. These solutions vary in their capabilities and methodologies, but collectively they have been placed in a category known as data leak prevention (DLP). It provides a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep content inspection and with a centralized management framework.

Most DLP solutions include a suite of technologies that facilitate three key objectives:

- Locate and catalogue sensitive information stored throughout the enterprise

- Monitor and control the movement of sensitive information across enterprise networks

- Monitor and control the movement of sensitive information on end-user systems Banks may consider such solutions, if required, after assessing their potential to improve data security.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Vulnerability Assessment

Soon after new vulnerabilities are discovered and reported by security researchers or vendors, attackers engineer the malicious exploit code and then launch that code against targets of interest. Any significant delays in finding or fixing software with critical vulnerabilities provides ample opportunity for persistent attackers to break through, gaining control over the vulnerable machines and getting access to the sensitive data they contain. Banks that do not scan for vulnerabilities and address discovered flaws proactively face a significant likelihood of having their computer systems compromised.

The following are some of the measures suggested:

Automated vulnerability scanning tools need to be used against all systems on their networks on a periodic basis, say monthly or weekly or more frequently.

Banks should ensure that vulnerability scanning is performed in an authenticated mode (i.e., configuring the scanner with administrator credentials) at least quarterly, either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested, to overcome limitations of unauthenticated vulnerability scanning.

Banks should compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed either by patching, implementing a compensating control, or by documenting and accepting a reasonable business risk. Such acceptance of business risks for existing vulnerabilities should be periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed increasing the risk.

Vulnerability scanning tools should be tuned to compare services that are listening on each machine against a list of authorized services. The tools should be further tuned to identify changes over time on systems for both authorized and unauthorized services.

The security function should have updated status regarding numbers of unmitigated, critical vulnerabilities, for each department/division, plan for mitigation and should share vulnerability reports indicating critical issues with senior management to provide effective incentives for mitigation.

Establishing on-going security monitoring processes

A bank needs to have robust monitoring processes in place to identify events and unusual activity patterns that could impact on the security of IT assets. The strength of the monitoring controls needs to be proportionate to the criticality of an IT asset. Alerts would need to be investigated in a timely manner, with an appropriate response determined.

Common monitoring processes include activity logging (including exceptions to approved activity), for example, device, server, network activity, security sensor alerts; monitoring staff or third-party access to sensitive data/information to ensure it is for a valid business reason, scanning host systems for known vulnerabilities, checks to determine if information security controls are operating as expected and are being

complied with, checking whether powerful utilities / commands have been disabled on attached hosts by using tools like 'network sniffer'), environment and customer profiling, checking for the existence and configuration of unauthorised wireless networks by using automated tools, discovering the existence of unauthorised systems by using network discovery and mapping tools and detecting unauthorised changes to electronic documents and configuration files by using file integrity monitoring software.

Banks' networks should be designed to support effective monitoring. Design considerations include network traffic policies that address the allowed communications between computers or groups of computers, security domains that implement the policies, sensor placement to identify policy violations and anomalous traffic, nature and extent of logging, log storage and protection and ability to implement additional sensors on an ad hoc basis when required.

Banks would need to establish a clear allocation of responsibility for regular monitoring, and the processes and tools in this regard should be in a position to manage the volume of monitoring required, thereby reducing the risk of an incident going undetected.

Highly sensitive and/or critical IT assets would need to have logging enabled to record events and monitored at a level proportional to the level of risk.

Users, like system administrators, with elevated access privileges should be subjected to a greater level of monitoring in light of the heightened risks involved.

The integrity of the monitoring logs and processes should be safeguarded through appropriate access controls and segregation of duties.

Banks should frequently review all system accounts and disable any account that cannot be associated with a business process and business owner. Reports that may be generated from systems and reviewed frequently may include, among others, a list of locked out accounts, disabled accounts, accounts with passwords that exceed the maximum password age, and accounts with passwords that never expire.

Banks should establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor.

Banks should regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

Banks should monitor account usage to determine dormant accounts that have not been used for a given period, say 15 days, notifying the user or user's manager of the dormancy. After a longer period, say 30 days, the account may be disabled.

On a periodic basis, say monthly or quarterly basis, banks should require that managers match active employees and contractors with each account belonging to their managed staff. Security/system administrators should then disable accounts that are not assigned to active employees or contractors.

Banks should monitor attempts to access deactivated accounts through audit logging.

Banks should validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries. If systems cannot generate logs in a standardized format, banks need to deploy log normalization tools to convert logs into a standardized format.

System administrators and information security personnel should consider devising profiles of common events from given systems, so that they can tune detection to focus on unusual activity, reducing false positives, more rapidly identify anomalies, and prevent overwhelming the analysts with insignificant alerts.

The following technologies/factors provide capabilities for effective attack detection and analysis:

Security Information and Event Management (SIEM) - SIEM products provide situational awareness through the collection, aggregation, correlation and analysis of disparate data from various sources. The information provided by these tools help in understanding the scope of an incident.

Intrusion Detection and Prevention System (IDS and IPS) - IPS products that have detection capabilities should be fully used during an incident to limit any further impact on the organization. IDS and IPS products are often the primary source of information leading to the identification of an attack. Once the attack has been identified, it is essential to enable the appropriate IPS rule sets to block further incident propagation and to support containment and eradication.

Network Behaviour Analysis (NBA) - Network wide anomaly-detection tools will provide data on traffic patterns that are indicative of an incident. Once an incident has been identified through the use of these tools, it is important to capture that

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

information for the purposes of supporting further mitigation activities, including operational workflow to ensure that the information from these tools is routed to the appropriate response team.

Managed Security Service Provider (MSSP) - If an organization has outsourced security event management to an MSSP, the latter should provide notification when an incident requires attention. Organisation must obtain as much information on the incident as possible from MSSP and implement remediation steps as recommended by MSSP.

Banks also need to pro-actively monitor various authentic sources like CERT-In, security vendors, etc. for any security related advisories and take suitable measures accordingly.

Security measures against Malware:

Malicious software is an integral and a dangerous aspect of internet based threats which target end-users and organizations through modes like web browsing, email attachments, mobile devices, and other vectors. Malicious code may tamper with a system's contents, and capture sensitive data. It can also spread to other systems. Modern malware aims to avoid signature-based and behavioral detection, and may disable anti-virus tools running on the targeted system. Anti-virus and anti-spyware software, collectively referred to as anti-malware tools, help defend against these threats by attempting to detect malware and block their execution.

Typical controls to protect against malicious code use layered combinations of technology, policies and procedures and training. The controls are of the preventive and detective/corrective in nature. Controls are applied at the host, network, and user levels:

At host level: The various measures at the host level include host hardening(including patch application and proper security configurations of the

operating system (OS), browsers, and other network-aware software), considering implementing host-based firewalls on each internal computer and especially laptops assigned to mobile users. Many host-based firewalls also have application hashing capabilities, which are helpful in identifying applications that may have been trojanized after initial installation, considering host IPS and integrity checking software combined with strict change controls and configuration management, periodic auditing of host configurations, both manual and automated.

At network level: The various measures include limiting the transfer of executable files through the perimeter, IDS and IPS monitoring of incoming and outgoing network traffic, including anti-virus, anti-spyware and signature and anomaly-based traffic monitors, routing Access Control Lists(ACLs) that limit incoming and outgoing connections as well as internal connections to those necessary for business purposes, proxy servers that inspect incoming and outgoing packets for indicators of malicious code and block access to known or suspected malware distribution servers, filtering to protect against attacks such as cross-site scripting and SQL injection.

At user level: User education in awareness, safe computing practices, indicators of malicious code, and response actions.

Enterprise security administrative features may be used daily to check the number of systems that do not have the latest anti-malware signatures. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers.

Banks should employ anti-malware software and signature auto update features to automatically update signature files and scan engines whenever the vendor publishes updates. After applying an update, automated systems should verify that each system has received its signature update. The bank should monitor anti-virus console logs to correct any systems that failed to be updated. The systems deployed for client security should be delivering simplified administration through central management and providing critical visibility into threats and vulnerabilities. It should also integrate with existing infrastructure software, such as Active Directory for enhanced protection and greater control.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Administrators should not rely solely on AV software and email filtering to detect worm infections. Logs from firewalls, intrusion detection and prevention sensors, DNS servers and proxy server logs should be monitored on a daily basis for signs of worm infections including but not limited to:

Outbound SMTP connection attempts from anything other than a bank's SMTP mail gateways

Excessive or unusual scanning on TCP and UDP ports 135-139 and 445
Connection attempts on IRC or any other ports that are unusual for the environment
Excessive attempts from internal systems to access non-business web sites
Excessive traffic from individual or a group of internal systems
Excessive DNS queries from internal systems to the same host name and for known "nonexistent" host names. Using a centralized means such as a syslog host to collect logs from various devices and systems can help in the analysis of the information

Banks should configure laptops, workstations, and servers so that they do not auto-run content from USB tokens, USB hard drives, CDs/DVDs, external SATA devices, mounted network shares, or other removable media.

Banks should configure systems so that they conduct an automated antimalware scan of removable media when it is inserted.

Banks can also consider deploying the Network Access Control (NAC) tools to verify security configuration and patch level compliance of devices before granting access to a network. Network Admission Control (NAC) restricts access to the network based on the identity or security posture of an organization. When NAC is implemented, it will force a user or a machine seeking network access for authentication prior to granting actual access to the network. A typical (non-free) WiFi connection is a form of NAC. The user must present some sort of credentials (or a credit card) before being granted access to the network. The network admission control systems allow noncompliant devices to be denied access, placed in a quarantined area, or given restricted access to computing resources, thus keeping insecure nodes from infecting the network. The key component of the Network Admission Control program is the Trust Agent, which resides on an endpoint system and communicates with routers on the network. The information is then relayed to a Secure Access Control Server (ACS) where access control decisions are made. The ACS directs the router to perform enforcement against the endpoint.

Email Attachment Filtering - Banks should filter various attachment types at the email gateway, unless required for specific business use. Some examples include .ade .cmd .eml .ins .mdb .mst .reg .url .wsf .adp .com .exe .isp .mde .pcd .scr .vb .wsh .bas .cpl

.hlp .js .msc .pif .sct .vbe .bat .crt .hta .jse .msi .pl .scx .vbs .chm .dll .inf .lnk .msp .pot

.shs .wsc... etc. Banks should consider only allowing file extensions with a documented business case and filtering all others.

Patch Management:

A Patch Management process needs to be in place to address technical system and software vulnerabilities quickly and effectively in order to reduce the likelihood of a serious business impact arising.

There should be documented standards / procedures for patch management. The standards / procedures for patch management should include a method of defining roles and responsibilities for patch management, determining the importance of systems (for e.g., based on the information handled, the business processes supported and the environments in which they are used) , recording patches that have been applied (for e.g., using an inventory of computer assets including their patch level).

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

The patch management process should include aspects like:

- Determining methods of obtaining and validating patches for ensuring that the patch is from an authorised source
- Identifying vulnerabilities that are applicable to applications and systems used by the organisation

- Assessing the business impact of implementing patches (or not implementing a particular patch)

- Ensuring patches are tested

- Describing methods of deploying patches, for example, through automated manner

- Reporting on the status of patch deployment across the organisation

- Including methods of dealing with the failed deployment of a patch (e.g., redeployment of the patch).

Methods should be established to protect information and systems if no patch is available for an identified vulnerability, for example, disabling services and adding additional access controls. Organizations should deploy automated patch management tools and software update tools for all systems for which such tools are available and safe.

Organizations should measure the delay in patching new vulnerabilities and ensure the delay is not beyond the benchmarks set forth by the organization, which should be less for critical patches, say not more than a week, unless a mitigating control that blocks exploitation is available.

Critical patches must be evaluated in a test environment before being updated into production on enterprise systems. If such patches break critical business applications on test machines, the organization must devise other mitigating controls that block exploitation on systems where the patch is difficult to be deployed because of its impact on business functionality.

Change Management:

A change management process should be established, which covers all types of change. For example, upgrades and modifications to application and software, modifications to business information, emergency 'fixes', and changes to the computers / networks that support the application.

The change management process should be documented, and include approving and testing changes to ensure that they do not compromise security controls, performing changes and signing them off to ensure they are made correctly and securely, reviewing completed changes to ensure that no unauthorised changes have been made.

The following steps should be taken prior to changes being applied to the live environment:

Change requests should be documented (e.g., on a change request form) and accepted only from authorised individuals and changes should be approved by an appropriate authority

The potential business impacts of changes should be assessed (for e.g., in terms of the overall risk and impact on other components of the application)

Changes should be tested to help determine the expected results (for e.g., deploying the patch into the live environment)

Changes should be reviewed to ensure that they do not compromise security controls (e.g., by checking software to ensure it does not contain malicious code, such as a trojan horse or a virus)

Back-out positions should be established so that the application can recover from failed changes or unexpected results

Changes to the application should be performed by skilled and competent individuals who are capable of making changes correctly and securely and signed off by an appropriate business official.

Audit trails

Banks need to ensure that audit trails exist for IT assets satisfying the bank's business requirements including regulatory and legal requirements, facilitating audit, serving as forensic evidence when required and assisting in dispute resolution. This could include, as applicable, various areas like transaction with financial consequences, the opening, modifications or closing of customer accounts, modifications in sensitive master data, accessing or copying of sensitive data/information; and granting, modification or revocation of systems access rights or privileges for accessing sensitive IT assets.

Audit trails should be secured to ensure the integrity of the information captured, including the preservation of evidence. Retention of audit trails should be in line with business, regulatory and legal requirements.

Some considerations for securing the integrity of log files include :

- Encrypting log files that contain sensitive data or that are transmitting over the network

- Ensuring adequate storage capacity to avoid gaps in data gathering

- Securing back-up and disposal of log files

- Logging the data to write-only media like a write-once/read-many (WORM) disk or drive

- Setting logging parameters to disallow any modification to previously written data

As indicated earlier, network and host activities typically are recorded on the host and sent across the network to a central logging facility which may process the logging data into a common format. The process, called normalization, enables timely and effective log analysis.

Other aspects related to logging to be considered include:

- All remote access to an internal network, whether through VPN, dial-up, or other mechanism, should be logged verbosely

- Operating systems should be configured to log access control events associated with a user attempting to access a resource like a file or directory without the appropriate permissions

- Security personnel and/or administrators designated in this regard should identify anomalies in logs and actively review the anomalies, documenting their findings on an ongoing basis

Each bank can consider at least two synchronized time sources are available in their network from which all servers and network equipment retrieve time information on a regular basis, so that timestamps in logs are consistent

Network boundary devices, including firewalls, network-based IPSs, and inbound and outbound proxies may be configured to log verbosely all traffic (both allowed and blocked) arriving at the device

Given the multiplicity of devices and systems, banks should consider deploying a Security Information and Event Management (SIEM) system tool for log aggregation and consolidation from multiple machines/systems and for log correlation and analysis, as indicated earlier in the chapter. Furthermore, event logs may be correlated with information from vulnerability scans to fulfill two goals. First, personnel should verify that the activity of the regular vulnerability scanning tools themselves is logged. And, secondly, personnel should be able to correlate attack detection events with earlier vulnerability scanning results to determine whether the given exploit was used against a known-vulnerable target.

E-banking systems should be designed and installed to capture and maintain forensic evidence in a manner that maintains control over the evidence, and prevents tampering and the collection of false evidence.

In instances where processing systems and related audit trails are the responsibility of a third-party service provider, the bank should ensure that it has access to relevant audit trails maintained by the service provider apart from ensuring that the audit trails maintained by the service provider meet the bank's standards.

Information security reporting and metrics

Security monitoring arrangements should provide key decision-makers and Senior Management/Board of Directors with an informed view of aspects like the effectiveness and efficiency of information security arrangements, areas where improvement is required, information and systems that are subject to an unacceptable level of risk, performance against quantitative, objective targets, actions required to help minimize risk (e.g., reviewing the organization's risk appetite, understanding the information security threat environment and encouraging business and system owners to remedy unacceptable risks).

There should be arrangements for monitoring the information security condition of the organisation, which are documented, agreed with top management and performed regularly. Information generated by monitoring the information security condition of the organization should be used to measure the effectiveness of the information security strategy, information security policy and security architecture.

Analysis performed as part of security monitoring and reporting arrangement may include, inter-alia, the following:

- Details relating to information security incidents and their impact
- Steps taken for non-recurrence of such events in the future
- Major Internal and external audit/vulnerability assessment/penetration test findings and remediation status
- Operational security statistics, such as firewall log data, patch management details and number of spam e-mails
- Costs associated with financial losses, legal or regulatory penalties and risk profile(s)

- Progress against security plans/strategy
- Capacity and performance analysis of security systems
- Infrastructure and software analysis

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Srinivas Kante

Information collected as part of security reporting arrangements should include details about all aspects of information risk like criticality of information, identified vulnerabilities and level of threats, potential business impacts and the status of security controls in place. Information about the security condition of the organisation should be provided to key decision-makers/stake holders like the Board, top management, members of Information Security Committee, and relevant external bodies like regulator as required.

Metrics can be an effective tool for security managers to discern the effectiveness of various components of their security policy and programs, the security of a specific system, product or process, effectiveness and efficiency of security services delivery, the impact of security events on business processes and the ability of staff or departments within an organization to address security issues for which they are responsible. Additionally, they may be used to raise the level of security awareness within the organization. The measurement of security characteristics can allow management to increase control and drive further improvements to the security procedures and processes.

Each dimension of the IT security risk management framework can be measured by at least one metric to enable the monitoring of progress towards set targets and the identification of trends. The use of metrics needs to be targeted towards the areas of greatest criticality. Generally, it is suggested that effective metrics need to follow the SMART acronym i.e. specific, measurable, attainable, repeatable and time-dependent.

In addition, a comprehensive set of metrics that provide for prospective and retrospective measures, like key performance indicators and key risk indicators, can be devised.

The efficacy of a security metrics system in mitigating risk depends on completeness and accuracy of the measurements and their effective analysis. The measurements should be reliable and sufficient to justify security decisions that affect the institution's security posture, allocate resources to security-related tasks, and provide a basis for security-related reports.

Some illustrative metrics include coverage of anti-malware software and their updation percentage, patch latency, extent of user awareness training, vulnerability related metrics, etc.

Information security and Critical service providers/vendors

Banks use third-party service providers in a variety of different capacities. It can be an Internet service provider (ISP), application or managed service provider (ASP/MSP) or business service provider (BSP). These providers may often perform important functions for the bank and usually may require access to confidential information, applications and systems.

When enterprises use third parties, they can become a key component in an enterprise's controls and its achievement of related control objectives. Management should evaluate the role that the third party performs in relation to the IT environment, related controls and control objectives.

The effectiveness of third-party controls can enhance the ability of an enterprise to achieve its control objectives. Conversely, ineffective third-party controls can weaken the ability of a bank to achieve its control objectives. These weaknesses can arise from many sources including gaps in the control environment arising from the outsourcing of services to the third party, poor control design, causing controls to operate ineffectively, lack of knowledge and/or inexperience of personnel responsible for control functions and over-reliance on the third party's controls (when there are no compensating controls within the enterprise).

Third-party providers can affect an enterprise (including its partners), its processes, controls and control objectives on many different levels. This includes effects arising from such things as economic viability of the third-party provider, third-party provider

access to information that is transmitted through their communication systems and applications, systems and application availability, processing integrity, application development and change management processes and the protection of systems and information assets through backup recovery, contingency planning and redundancy.

The lack of controls and/or weakness in their design, operation or effectiveness can lead to consequences like loss of information confidentiality and privacy, systems not being available for use when needed, unauthorized access and changes to systems, applications or data, changes to systems, applications or data occurring that result in system or security failures, loss of data, loss of data integrity, loss of data protection, or system unavailability, loss of system resources and/or information assets and Increased costs incurred by the enterprise as a result of any of the above.

The relationship between the enterprise and a third-party provider should be documented in the form of an executed contract. The various details and requirements on the matter are covered under chapter on "IT outsourcing".

Network Security

Protection against growing cyber threats requires multiple layers of defenses, known as defense in depth. As every organization is different, this strategy should therefore be based on a balance between protection, capability, cost, performance, and operational considerations. Defense in depth for most organizations should at least consider the following two areas:

- Protecting the enclave boundaries or perimeter

- Protecting the computing environment.

The enclave boundary is the point at which the organization's network interacts with the Internet. To control the flow of traffic through network borders and to police its content looking for attacks and evidence of compromised machines, boundary defenses should be multi-layered, relying on firewalls, proxies, DMZ perimeter networks, and network-based Intrusion Prevention Systems and Intrusion Detection Systems.

It should be noted that boundary lines between internal and external networks are diminishing through increased interconnectivity within and between organizations and use of wireless systems. These blurring lines sometimes allow attackers to gain access inside networks while bypassing boundary systems. However, even with this blurring, effective security deployment still rely on carefully configured boundary defenses that separate networks with different threat levels, different sets of users, and different levels of control. Effective multi-layered defenses of perimeter networks help to lower the number of successful attacks, allowing security personnel to focus on attackers who have devised methods to bypass boundary restrictions.

An effective approach to securing a large network involves dividing the network into logical security domains. A logical security domain is a distinct part of a network with security policies that differ from other domains and perimeter controls enforcing access at a network level. The differences may be far broader than perimeter controls, encompassing personnel, host, and other issues. Before establishing security domains, banks need to map and configure the network to identify and control all access points. Network configuration considerations could include the following actions:

- Identifying the various applications and systems accessed via the network

- Identifying all access points to the network including various telecommunications channels like ethernet, wireless, frame relay, dedicated lines, remote dial-up access, extranets, internet

- Mapping the internal and external connectivity between various network segments

- Defining minimum access requirements for network services

- Determining the most appropriate network configuration to ensure adequate security and performance for the bank

Srinivas Kante

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

With a clear understanding of network connectivity, banks can avoid introducing security vulnerabilities by minimizing access to less-trusted domains and employing encryption and other controls for less secure connections. Banks can then determine the most effective deployment of protocols, filtering routers, firewalls, gateways, proxy servers, and/or physical isolation to restrict access. Some applications and business processes may require complete segregation from the corporate network, for example, preventing connectivity between corporate network and wire transfer system. Others may restrict access by placing the services that must be accessed by each zone in their own security domain, commonly called a De-Militarized Zone.

Security domains are bounded by perimeters. Typical perimeter controls include firewalls that operate at different network layers, malicious code prevention, outbound filtering, intrusion detection and prevention devices, and controls over infrastructure services such as DNS. The perimeter controls may exist on separate devices or be combined or consolidated on one or more devices. Consolidation on a single device could improve security by reducing administrative overhead. However, consolidation may increase risk through a reduced ability to perform certain functions and the existence of a single point of failure. A few network protection devices are briefly explained as under:

Firewalls: The main purpose of a firewall is access control. By limiting inbound (from the Internet to the internal network) and outbound communications (from the internal network to the Internet), various attack vectors can be reduced. Firewalls may provide additional services like Network Address Translation and Virtual Private Network Gateway.

Financial institutions have four primary firewall types from which to choose: packet filtering, stateful inspection, proxy servers, and application-level firewalls. Any product may have characteristics of one or more firewall types. The selection of a firewall type is dependent on many characteristics of the security zone, such as the amount of traffic, the sensitivity of the systems and data, and applications.

Packet Filter Firewalls

Packet filter firewalls evaluate the headers of each incoming and outgoing packet to ensure it has a valid internal address, originates from a permitted external address, connects to an authorized protocol or service, and contains valid basic header instructions. If the packet does not match the pre-defined policy for allowed traffic, then the firewall drops the packet. Packet filters generally do not analyze the packet contents beyond the header information. Among the major weaknesses associated with packet filtering firewalls include inability to prevent attacks that exploit application-specific vulnerabilities and functions because the packet filter does not examine packet contents and logging functionality is limited to the same information used to make access control decisions.

Stateful Inspection Firewalls

Stateful inspection firewalls are packet filters that monitor the state of the TCP connection. Each TCP session starts with an initial "handshake" communicated through TCP flags in the header information. When a connection is established the firewall adds the connection information to a table. The firewall can then compare future packets to the connection or state table. This essentially verifies that inbound traffic is in response to requests initiated from inside the firewall.

Proxy Server Firewalls

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Proxy servers act as an intermediary between internal and external IP addresses and block direct access to the internal network. Essentially, they rewrite packet headers to substitute the IP of the proxy server for the IP of the internal machine and forward packets to and from the internal and external machines. Due to that limited capability, proxy servers are commonly employed behind other firewall devices. The primary firewall receives all traffic, determines which application is being targeted, and hands off the traffic to the appropriate

proxy server. Common proxy servers are the domain name server (DNS), Web server (HTTP), and mail (SMTP) server. Proxy servers frequently cache requests and responses, providing potential performance benefits. Additionally, proxy servers provide another layer of access control by segregating the flow of Internet traffic to support additional authentication and logging capability, as well as content filtering. Web and e-mail proxy servers, for example, are capable of filtering for potential malicious code and application-specific commands. Proxy servers are increasing in importance as protocols are tunnelled through other protocols.

Application-Level Firewalls

Application-level firewalls perform application-level screening, typically including the filtering capabilities of packet filter firewalls with additional validation of the packet content based on the application. Application-level firewalls capture and compare packets to state information in the connection tables. Unlike a packet filter firewall, an application level firewall continues to examine each packet after the initial connection is established for specific application or services such as telnet, FTP, SMTP, etc. The application-level firewall can provide additional screening of the packet payload for commands, protocols, packet length, authorization, content, or invalid headers. Application level firewalls provide the strongest level of security.

Firewall Policy

A firewall policy states management's expectation for how the firewall should function and is a component of the overall security management framework. Acceptable inbound communication types for the organization need to be explicitly defined in the firewall policies. As the firewall is usually one of the first lines of defense, access to the firewall device itself needs to be strictly controlled.

At a minimum, the policy should address various aspects like Firewall topology and architecture and type of firewalls being utilized, physical placement of the firewall components, permissible traffic and monitoring firewall traffic, firewall updating, coordination with security monitoring and intrusion response mechanisms, responsibility for monitoring and enforcing the firewall policy, protocols and applications permitted, regular auditing of a firewall's configuration and testing of the firewall's effectiveness, and contingency planning.

Firewalls should not be relied upon, however, to provide full protection from attacks. Banks should complement firewalls with strong security policies and a range of other controls. In fact, firewalls are potentially vulnerable to attacks including spoofing trusted IP addresses, denial of service by overloading the firewall with excessive requests or malformed packets, sniffing of data that is being transmitted outside the network, hostile code embedded in legitimate HTTP, SMTP, or other traffic that meet all firewall rules, etc. Banks can reduce their vulnerability to these attacks through network configuration and design, sound implementation of its firewall architecture that includes multiple filter points, active firewall monitoring and management, and integrated security monitoring. In many cases,

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

additional access controls within the operating system or application will provide additional means of defense.

Given the importance of firewalls as a means of access control, good firewall related practices include:

- Using a rule set that disallows all inbound and outbound traffic that is not specifically allowed
- Using NAT and split DNS to hide internal system names and addresses from external networks

- Using proxy connections for outbound HTTP connections and filtering malicious code
- Hardening the firewall by removing all unnecessary services and appropriately patching, enhancing, and maintaining all software on the firewall unit

- Restricting network mapping capabilities through the firewall, primarily by blocking inbound ICMP (Internet Control Messaging Protocol) traffic

- Backing up firewalls to internal media and not backing up the firewall to servers on protected networks

- Logging activity, with daily administrator review and limiting administrative access to few individuals

- Using security monitoring devices and practices to monitor actions on the firewall and to monitor communications allowed through the firewall

- Administering the firewall using encrypted communications and strong authentication, accessing the firewall only from secure devices, and monitoring all administrative access
- Making changes only through well-administered change control procedures.

The firewall also needs to be configured for authorized outbound network traffic. In the case of a compromised host inside the network, outbound or egress filtering can contain that system and prevent it from communicating outbound to their controller – as in the case with botnets. Often times, firewalls default to allowing any outbound traffic, therefore, organizations may need to explicitly define the acceptable outbound communication policies for their networks. In most cases the acceptable outbound connections would include SMTP to any address from only your SMTP mail gateway(s), DNS to any address from an internal DNS server to resolve external host names, HTTP and HTTPS from an internal proxy server for users to browse web sites, NTP to specific time server addresses from an internal time server(s), any ports required by Anti-Virus, spam filtering, web filtering or patch management software to only the appropriate vendor address(es) to pull down updates and any other rule where the business case is documented and signed off by appropriate management.

Perimeters may contain proxy firewalls or other servers that act as a control point for Web browsing, e-mail, P2P, and other communications. Those firewalls and servers frequently are used to enforce the institution's security policy over incoming communications. Enforcement is through anti-virus, anti-spyware, and anti-spam filtering, the blocking of downloading of executable files, and other actions. To the extent that filtering is done on a signature basis, frequent updating of the signatures may be required, as had been explained earlier.

Perimeter servers also serve to inspect outbound communications for compliance with the institution's security policy. Perimeter routers and firewalls can be configured to enforce policies that forbid the origination of outbound communications from certain computers. Additionally, proxy servers could be configured to identify and block customer data and other data that should not be transmitted outside the security domain.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

b) Intrusion Detection Systems (IDS)

The goal of an IDS is to identify network traffic in near real time. Most IDSs use signatures to detect port scans, malware, and other abnormal network communications. The ideal placement of an IDS is external to the organization as well as internally, just behind the firewall. This would enable a bank to view the traffic approaching the organization as well as the traffic that successfully passed through the firewall. Conversely, there will be visibility on internal traffic trying to communicate externally to the network – particularly useful for situations where malicious activity originates from inside the firewall.

To use a network IDS (NIDS) effectively, an institution should have a sound understanding of the detection capability and the effect of placement, tuning, and other network defences on the detection capability.

Srinivas Kante

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

The signature-based detection methodology reads network packets and compares the content of the packets against signatures, or unique characteristics, of known attacks. When a match is recognized between current readings and a signature, the IDS generates an alert. A weakness in the signature-based detection method is that a signature must exist for an alert to be generated. Signatures are written to either capture known exploits, or to alert to suspected vulnerabilities. Vulnerability-based detection is generally broad based, alerting on many exploits for the same vulnerability and potentially alerting on exploits that are not yet known which is not the case with exploit-based signatures which may be based on specific exploits only and may not alert when a new or previously unknown exploit is attempted.

This problem can be particularly acute if the institution does not continually update its signatures to reflect lessons learned from attacks on itself and others, as well as developments in attack tool technologies. It can also pose problems when the signatures only address known attacks. Another weakness is in the capacity of the NIDS to read traffic. If the NIDS falls behind in reading network packets, traffic may be allowed to bypass the NIDS. Such traffic may contain attacks that would otherwise cause the NIDS to issue an alert.

The anomaly -based detection method generally detects deviations from a baseline. The baseline can be either protocol- based, or behaviour-based. The protocol-based baseline detects differences between the detected packets for a given protocol and the Internet's RFCs (Requests for Comment) pertaining to that protocol. For example, a header field could exceed the RFC-established expected size.

The behaviour -based anomaly detection method creates a statistical profile of normal activity on the host or network. Normal activity generally is measured based on the volume of traffic, protocols in use, and connection patterns between various devices. Benchmarks for activity are established based on that profile. When current activity exceeds the identified boundaries, an alert is generated. Weaknesses in this system involve the ability of the system to accurately model activity, the relationship between valid activity in the period being modelled and valid activity in future periods, and the potential for malicious activity to take place while the modelling is performed. This method is best employed in environments with predictable, stable activity.

Anomaly detection can be an effective supplement to signature- based methods by signalling attacks for which no signature yet exists. Proper placement of NIDS sensors is a strategic decision determined by the information the bank is trying to obtain. Placement outside the firewall will deliver IDS alarms related to all attacks, even those that are blocked by the firewall. With this information, an institution can develop a picture of potential adversaries and their expertise based on the probes they issue against the network.

Because the placement is meant to gain intelligence on attackers rather than to alert on attacks, tuning generally makes the NIDS less sensitive than if it is placed inside the firewall. A NIDS outside the firewall will generally alert on the greatest number of unsuccessful attacks while NIDS monitoring behind the firewall is meant to detect and alert on hostile intrusions. Multiple NIDS units can be used, with placement determined by the expected attack paths to sensitive data. In general, the closer the NIDS is to sensitive data, the more important the tuning, monitoring, and response to NIDS alerts. It is generally recommended that NIDS can be placed at any location where network traffic from external entities is allowed to enter controlled or private networks.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

“Tuning” refers to the creation of signatures and alert filters that can distinguish between normal network traffic and potentially malicious traffic apart from involving creation and implementation of different alerting and logging actions based on the severity of the perceived attack. Proper tuning is essential to both reliable detection of attacks and the

Srinivas Kante

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

enabling of a priority-based response. If IDS is not properly tuned, the volume of alerts it generates may degrade the intrusion identification and response capability.

Switched networks pose a problem for a network IDS since the switches ordinarily do not broadcast traffic to all ports while NIDS may need to see all traffic to be effective. When switches do not have a port that receives all traffic, a bank may have to alter its network to include a hub or other device to allow the IDS to monitor traffic. Encryption poses a potential limitation for a NIDS. If traffic is encrypted, the NIDS's effectiveness may be limited to anomaly detection based on unencrypted header information. This limitation can be overcome by decrypting packets within the IDS at rates commensurate with the flow of traffic. Decryption is a device-specific feature that may not be incorporated into all NIDS units.

All NIDS detection methods result in false positives (alerts where no attack exists) and false negatives (no alert when an attack does take place). While false negatives are obviously a concern, false positives can also hinder detection. When security personnel are overwhelmed with the number of false positives, their review of NIDS reports may be less effective thereby allowing real attacks to be reported by the NIDS but not suitably acted upon. Additionally, they may tune the NIDS to reduce the number of false positives, which may increase the number of false negatives. Risk-based testing is necessary in this regard to ensure the detection capability is adequate.

c) Network Intrusion Prevention Systems

Network Intrusion Prevention Systems (NIPS) are an access control mechanism that allow or disallow access based on an analysis of packet headers and packet payloads. They are similar to firewalls because they are located in the communications line, compare activity to pre-configured decisions of the type of packets to filter or block, and respond with pre-configured actions. The IPS units generally detect security events in a manner similar to IDS units and are subject to the same limitations. After detection, however, the IPS unit has the capability to take actions beyond simple alerting to potential malicious activity and logging of packets such as blocking traffic flows from an offending host. The ability to sever communications can be useful when the activity can clearly be identified as malicious. When the activity cannot be clearly identified, for example where a false positive may exist, IDS-like alerting commonly is preferable to blocking. Although IPS units are access control devices, many of these units implement a security model that is different from firewalls. Firewalls typically allow only the traffic necessary for business purposes, or only "known good" traffic. IPS units typically are configured to disallow traffic that triggers signatures, or "known bad" traffic, while allowing all else. However, IPS units can be configured to more closely mimic a device that allows only "known good" traffic. IPS units also contain a "white list" of IP addresses that should never be blocked. The list helps ensure that an attacker cannot achieve a denial of service by spoofing the IP of a critical host.

d) Quarantine

Quarantining a device protects the network from potentially malicious code or actions. Typically, a device connecting to a security domain is queried for conformance to the domain's security policy. If the device does not conform, it is placed in a restricted part of the network until it does conform. For example, if the patch level is not current, the device is not allowed into the security domain until the appropriate patches are downloaded and installed.

e) DNS Placement

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Effective protection of the institution's DNS servers is critical to maintaining the security of the institution's communications. Much of the protection is provided by host security. However, the placement of the DNS also is an important factor. The optimal placement is split DNS, where one firewalled DNS server serves public domain information to the outside

and does not perform recursive queries, and a second DNS server, in an internal security domain and not the DMZ, performs recursive queries for internal users.

Improving the security of networks

In addition to the above, the following are among the factors that need to be followed for improving the security of networks:

- Inventory of authorized and unauthorized devices and software.

- Secure Configurations/hardening for all hardware and software on Laptops, Workstations, and Servers and Network Devices such as Firewalls, Routers and Switches. Configuration management begins with well-tested and documented security baselines for various systems. There need to be documented security baselines for all types of information systems.

- Identifying all connections to critical networks and conducting risk analysis including necessity for each connection. All unnecessary connections to critical networks to be disconnected.

- Implementation of the security features recommended by device and system vendors.

- Establishing strong controls over any medium that is used as a backdoor into the critical network. If backdoors or vendor connections do exist in critical systems, strong authentication must be implemented to ensure secure communications.

- Implementation of internal and external intrusion detection system, incident response system and establishing 24x7 incident monitoring

- Performing technical audits including vulnerability assessment of critical devices and networks, and any other connected networks, to identify security concerns

- Conducting physical security surveys and assessing all remote sites connected to the critical network to evaluate their security. Any location that has a connection to the critical network is a target, especially unmanned or unguarded remote sites. There is also a need to identify and assess any source of information including remote telephone / computer network / fiber optic cables that could be tapped; radio and microwave links that are exploitable; computer terminals that could be accessed; and wireless local area network access points. Identify and eliminate single points of failure.

- Establishing critical "Red Teams" to identify and evaluate possible attack scenarios. There is a need to feed information resulting from the "Red Team" evaluation into risk management processes to assess the information and establish appropriate protection strategies.

- Documenting network architecture and identifying systems that serve critical functions or contain sensitive information that require additional levels of protection.

- Establishing a rigorous, ongoing risk management process.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Establishing a network protection strategy and layered security based on the principle of defense-in-depth is an absolute necessity for banks. This would require suitable measures to address vulnerabilities across the hardware, operating system, middleware, database, network and application layers. Security is not an event but a process which requires all its various components to be functioning well together for their effectiveness. Additionally, each layer must be protected against other systems at the same layer. For example, to protect against insider threat, restrict users to access only those resources necessary to perform their job functions.

Srinivas Kante

- m. Establishing system backups and disaster recovery plans. Establish a disaster recovery plan that allows for rapid recovery from any emergency (including a cyber attack).

Establishing policies and conducting training to minimize the likelihood that organizational personnel would inadvertently disclose sensitive information regarding critical system design, operations, or security controls through social engineering attempts. Any requests for information by unknown persons need to be sent to a central network security location for verification and fulfillment. People can be a weak link in an otherwise secure network, as had been indicated earlier in the chapter.

Network control functions should be performed by individuals possessing adequate training and experience. Network control functions should be separated, and the duties should be rotated on a regular basis, where possible. Network control software must restrict operator access from performing certain functions (e.g., the ability to amend/delete operator activity logs).

Network control software should maintain an audit trail of all operator activities. Audit trails should be periodically reviewed by operations management to detect any unauthorized network operations activities.

Network operation standards and protocols should be documented and made available to the operators, and should be reviewed periodically to ensure compliance.

Network access by system engineers should be monitored and reviewed closely to detect unauthorized access to the network.

Another important security improvement is the ability to identify users at every step of their activity. Some application packages use predefined user id. New monitoring tools have been developed to resolve this problem.

Remote Access:

Banks may sometimes provide employees, vendors, and others with access to the institution's network and computing resources through external connections. Those connections are typically established through modems, the internet, or private communications lines. The access may be necessary to remotely support the institution's systems or to support institution operations at remote locations. In some cases, remote access may be required periodically by vendors to make emergency programme fixes or to support a system.

Remote access to a bank's provides an attacker with the opportunity to manipulate and subvert the bank's systems from outside the physical security perimeter. The management should establish policies restricting remote access and be aware of all remote-access devices attached to their systems. These devices should be strictly controlled.

Good controls for remote access include the following actions:

- Disallowing remote access by policy and practice unless a compelling business need exists and requiring management approval for remote access

- Regularly reviewing remote access approvals and rescind those that no longer have a compelling business justification

- Appropriately configuring and securing remote access devices

- Appropriately and in a timely manner patching, updating and maintaining all software on remote access devices

- Using encryption to protect communications between the access device and the institution and to protect sensitive data residing on the access device

- Periodically auditing the access device configurations and patch levels

Using VLANs, network segments, directories, and other techniques to restrict remote access to authorized network areas and applications within the institution

Logging remote access communications, analyzing them in a timely manner, and following up on anomalies

Centralize modem and Internet access to provide a consistent authentication process, and to subject the inbound and outbound network traffic to appropriate perimeter protections and network monitoring

Logging and monitoring the date, time, user, user location, duration, and purpose for all remote access including all activities carried out through remote access

Requiring a two-factor authentication process for remote access (e.g., PIN based token card with a one-time random password generator, or token based PKI)

Implementing controls consistent with the sensitivity of remote use. For example, remote use to administer sensitive systems or databases may include the controls like restricting the use of the access device by policy and configuration, requiring authentication of the access device itself and ascertaining the trustworthiness of the access device before granting access

If remote access is through modems the following steps should be taken:

Require an operator to leave the modems unplugged or disabled by default, to enable modems only for specific and authorized external requests, and disable the modem immediately when the requested purpose is completed

Configure modems not to answer inbound calls, if modems are for outbound use only
Use automated callback features so the modems only call one number although this is subject to call forwarding schemes

Install a modem bank where the outside number to the modems uses a different prefix than internal numbers and does not respond to incoming calls

While using TCP/IP Internet-based remote access, organizations need to establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure. Available VPN technologies apply the Internet Engineering Task Force (IETF) IPsec security standard advantages are their ubiquity, ease of use, inexpensive connectivity, and read, inquiry or copy only access. Disadvantages include the fact that they are significantly less reliable than dedicated circuits, lack a central authority, and can have troubleshooting problems.

Banks need to be aware that using VPNs to allow remote access to their systems can create holes in their security infrastructure. The encrypted traffic can hide unauthorized actions or malicious software that can be transmitted through such channels. Intrusion detection systems and virus scanners able to decrypt the traffic for analysis and then encrypt and forward it to the VPN endpoint should be considered as preventive controls. A good practice will terminate all VPNs to the same end-point in a so called VPN concentrator, and will not accept VPNs directed at other parts of the network.

Distributed Denial of service attacks(DDoS/DoS):

Banks providing internet banking should be responsive to unusual network traffic conditions/system performance and sudden surge in system resource utilization which could be an indication of a DDoS attack. Consequently, the success of any pre-emptive and reactive actions depends on the deployment of appropriate tools to effectively detect, monitor and analyze anomalies in networks and systems.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

As part of the defence strategy, banks should install and configure network security devices discussed earlier in the chapter for reasonable preventive/detective capability. Potential bottlenecks and single points of failure vulnerable to DDoS attacks could be identified through source code

Srinivas Kante

review, network design analysis and configuration testing. Addressing these vulnerabilities would improve resilience of the systems.

Banks can also consider incorporating DoS attack considerations in their ISP selection process. An incident response framework should be devised and validated periodically to facilitate fast response to a DDoS onslaught or an imminent attack. Banks may also need to be familiar with the ISPs' incident response plans and suitably consider them as part of their incident response framework. To foster better coordination, banks should establish a communication protocol with their ISPs and conduct periodic joint incident response exercises.

Implementation of ISO 27001 Information Security Management System

Commercial banks should implement Information Security Management System (ISMS) best practices for their critical functions/processes.

The best known ISMS is described in ISO/IEC 27001 and ISO/IEC 27002 and related standards published jointly by ISO and IEC. ISO 27001 is concerned with how to implement, monitor, maintain and continually improve an Information Security Management System while ISO 27002 provides detailed steps or a list of security measures which can be used when building an ISMS. Other frameworks such as COBIT and ITIL though incorporate security aspects, but are mainly geared toward creating a governance framework for information and IT more generally. As with all management processes, an ISMS must remain effective and efficient in the long term, adapting to changes in the internal organization and external environment. ISO/IEC 27001, thus, incorporates the typical "Plan-Do-Check-Act" (PDCA), or Deming cycle, approach:

The Plan phase is about designing the ISMS, assessing information security risks and selecting appropriate controls.

The Do phase involves implementing and operating the controls.

The Check phase objective is to review and evaluate the performance (efficiency and effectiveness) of the ISMS.

In the Act phase, changes are made where necessary to bring the ISMS back to peak performance.

An ISMS developed and based on risk acceptance/rejection criteria, and using third party accredited certification to provide an independent verification of the level of assurance, is an extremely useful management tool. It offers the opportunity to define and monitor service levels internally as well as with contractor/partner organizations, thus demonstrating the extent to which there is effective control of security risks.

Further, a bank should also regularly assess the comprehensiveness of its information security risk management framework by comparison to peers and other established control frameworks and standards including any security related frameworks issued by reputed institutions like IDRBT or DSCI.

While implementing ISO 27001 and aspects from other relevant standards, banks should be wary of a routine checklist kind of mindset but ensure that the security management is dynamic in nature through proactively scanning the environment for new threats and suitably attuned to the changing milieu.

Wireless Security

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Wireless networks security is a challenge since they do not have a well-defined perimeter or well-defined access points. It includes all wireless data communication devices like personal computers, cellular phones, PDAs, etc. connected to a bank's internal networks.

Unlike wired networks, unauthorized monitoring and denial of service attacks can be performed without a physical wire connection. Additionally, unauthorized devices can potentially connect to the network, perform man-in-the-middle attacks, or connect to other wireless devices. To mitigate those risks, wireless networks rely on extensive use of encryption to authenticate users and devices and to shield communications. If a bank uses a wireless network, it should carefully evaluate the risk and implement appropriate additional controls. Examples of additional controls may include one or more of the following:

- Treating wireless networks as untrusted networks, allowing access through protective devices similar to those used to shield the internal network from the Internet environment

- Using end-to-end encryption in addition to the encryption provided by the wireless connection

- Using strong authentication and configuration controls at the access points and on all clients

- Using an application server and dumb terminals

- Shielding the area in which the wireless LAN operates to protect against stray emissions and signal interference

- Monitoring and responding to unauthorized wireless access points and clients

All wireless Access Points / Base Stations connected to the corporate network must be registered and approved by Information Security function of a bank. These Access Points / Base Stations need to be subjected to periodic penetration tests and audits. Updated inventory on all wireless Network Interface Cards used in corporate laptop or desktop computers must be available. Access points/Wireless NIC should not be installed /enabled on a bank's network without the approval of information security function.

Banks should ensure that each wireless device connected to the network matches an authorized configuration and security profile, with a documented owner of the connection and a defined business need. Organizations should deny access to those wireless devices that do not have such a configuration and profile.

Banks should ensure that all wireless access points are manageable using enterprise management tools.

Network vulnerability scanning tools should be configured to detect wireless access points connected to the wired network. Identified devices should be reconciled against a list of authorized wireless access points. Unauthorized (i.e., rogue) access points should be deactivated.

Banks should use wireless intrusion detection systems (WIDS) to identify rogue wireless devices and detect attack attempts and successful compromise. In addition to WIDS, all wireless traffic should be monitored by a wired IDS as traffic passes into the wired network.

Where a specific business need for wireless access has been identified, banks should configure wireless access on client machines to allow access only to authorized wireless networks.

For devices that do not have an essential wireless business purpose, organizations should consider disable wireless access in the hardware configuration (BIOS or EFI), with password protections to lower the possibility that the user will override such configurations.

Banks should regularly scan for unauthorized or misconfigured wireless infrastructure devices, using techniques such as "war driving" to identify access points and clients accepting peer-to-peer connections. Such unauthorized or misconfigured devices should be removed from the network, or have their configurations altered so that they comply with the security requirements of the organization.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Banks should ensure all wireless traffic leverages at least AES encryption used with at least WPA2 protection. Banks should ensure wireless networks use authentication protocols such as EAP/TLS or PEAP, which provide credential protection and mutual authentication.

Banks should ensure wireless clients use strong, multi-factor authentication credentials to mitigate the risk of unauthorized access from compromised credentials.

Banks should disable peer-to-peer wireless network capabilities on wireless clients, unless such functionality meets a documented business need.

Banks should disable wireless peripheral access of devices (such as Bluetooth), unless such access is required for a documented business need.

Banks may consider configuring all wireless clients used to access other critical networks or handle organization data in a manner so that they cannot be used to connect to public wireless networks or any other networks beyond those specifically allowed by the bank.

Some requirements relating to VPN that may be considered :

Access should be provided only if there's a genuine business case

All computers with wireless LAN devices must utilize a Virtual Private Network (VPN) that configured to drop all unauthenticated and unencrypted traffic

Wireless implementations must maintain point-to-point hardware encryption of at least 128 bits

Supporting a hardware address, like MAC address, that can be registered and tracked and supporting strong user authentication which checks against an external database such as TACACS+, RADIUS etc

Implementation of mutual authentication of user and authentication server and survey needs to be done before location of access points to ensure that signals are confined within the premise as much as possible

Communication between the workstations and access points should be encrypted using dynamic session keys

Business Continuity Considerations:

Events that trigger the implementation of a business continuity plan may have significant security implications. Depending on the event, some or all of the elements of the security environment may change. Different tradeoffs may exist between availability, integrity, confidentiality, and accountability, with a different appetite for risk on the part of management. Business continuity plans should be reviewed as an integral part of the security process.

Risk assessments should consider the changing risks that appear in business continuity scenarios and the different security posture that may be established. Strategies should consider the different risk environment and the degree of risk mitigation necessary to protect the institution in the event the continuity plans must be implemented. The implementation should consider the training of appropriate personnel in their security roles, and the implementation and updating of technologies and plans for back-up sites and communications networks. These security considerations should be integrated with the testing of business continuity plan implementations. More information on "Business Continuity Planning" is provided in a separate chapter.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Srinivas Kante

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Information security assurance

Penetration Testing:

Penetration testing is defined as a formalized set of procedures designed to bypass the security controls of a system or organization for the purpose of testing that system's or organization's resistance to such an attack.

Penetration testing is performed to uncover the security weaknesses of a system and to determine the ways in which the system can be compromised by a potential attacker. Penetration testing can take several forms but, in general, a test consists of a series of "attacks" against a target. The success or failure of the attacks, and how the target reacts to each attack, will determine the outcome of the test.

The overall purpose of a penetration test is to determine the subject's ability to withstand an attack by a hostile intruder. As such, the tester will be using the tricks and techniques a real-life attacker might use. This simulated attack strategy allows the subject to discover and mitigate its security weak spots before a real attacker discovers them. Because a penetration test seldom is a comprehensive test of the system's security, it should be combined with other monitoring to validate the effectiveness of the security process.

Penetration testing needs to be conducted at least on an annual basis.

Audits

Auditing compares current practices against a set of policies/standards/guidelines formulated by the institution, regulator including any legal requirements. Bank management is responsible for demonstrating that the standards it adopts are appropriate for the institution. Audits should not only look into technical aspects but also the information security governance process.

Assessment

An assessment is a study to locate security vulnerabilities and identify corrective actions. An assessment differs from an audit by not having a set of standards to test against. It differs from a penetration test by providing the tester with full access to the systems being tested. Assessments may be focused on the security process or the information system. They may also focus on different aspects of the information system, such as one or more hosts or networks. Vulnerability assessment was explained earlier in the chapter.

The assurance work needs to be performed by appropriately trained and independent information security experts/auditors. The strengths and weaknesses of critical internet-based applications, other critical systems and networks needs to be carried out before each initial implementation, and at least annually thereafter. Any findings needs to be reported and monitored using a systematic audit remediation or compliance tracking methodology.

A bank needs to regularly assess information security vulnerabilities and evaluate the effectiveness of the existing IT security risk management framework, making any necessary adjustments to ensure

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

emerging vulnerabilities are addressed in a timely manner. This assessment should also be conducted as part of any material change.

Robust performance evaluation processes are needed to provide organizations with feedback on the effectiveness of cyber security policy and technical implementation. A sign of a mature organization is one that is able to self-identify issues, conduct root cause analyses, and implement effective corrective actions that address individual and systemic problems. Self-assessment processes that are normally part of an effective cyber security program include routine scanning for vulnerabilities, automated auditing of the network, and - assessments of organizational and individual business line security related performance.

A bank should manage the information security risk management framework on an ongoing basis as a security programme following project management approach, addressing the control gaps in a systematic way.

General information regarding delivery channels

Provision of various electronic banking channels like ATM/debit cards/internet banking/phone banking should be issued only at the option of the customers based on specific written or authenticated electronic requisition along with a positive acknowledgement of the terms and conditions from the customer. A customer should not be forced to opt for services in this regard. Banks should provide clear information to their customers about the risks and benefits of using e-banking delivery services to enable customers to decide on choosing such services.

When new operating features or functions, particularly those relating to security, integrity and authentication, are being introduced, the bank should ensure that customers have sufficient instruction and information to be able to properly utilize them.

To raise security awareness, banks should sensitize customers on the need to protect their PINs, security tokens, personal details and other confidential data.

Banks are responsible for the safety and soundness of the services and systems they provide to their customers. Reciprocally, it is also important that customers take appropriate security measures to protect their devices and computer systems and ensure that their integrity is not compromised when engaging in online banking. Customers should implement the measures advised by their banks regarding protecting their devices or computers which they use for accessing banking services.

In view of the constant changes occurring in the internet environment and online delivery channels, management should institute a risk monitoring and compliance regime on an ongoing basis to ascertain the performance and effectiveness of the risk management process. When risk parameters change, the risk process needs to be updated and enhanced accordingly. Re-evaluation of past risk-control measures and equations, renewed testing and auditing of the adequacy and effectiveness of the risk management process and the attendant controls and security measures taken should be conducted.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Internet banking:

Banks need to ensure suitable security measures for their web applications and take reasonable mitigating measures against various web security risks indicated earlier in the chapter.

ii. Web applications should not store sensitive information in HTML hidden fields, cookies, or any other client-side storage leading to compromise in the integrity of the data. Critical web applications should enforce at least SSL v3 or Extended Validation –SSL / TLS 1.0 128 bit encryption level for all online activity.

iii. Re-establishment of any session after interruption should require normal user

identification, authentication, and authorization. Moreover, strong server side validation should be enabled.

Banks need to follow a defense in depth strategy by applying robust security measures across various technology layers

Authentication practices for internet banking:

Authentication methodologies involve three basic “factors”:

- Something the user knows (e.g., password, PIN);
- Something the user has (e.g., ATM card, smart card); and
- Something the user is (e.g., biometric characteristic, such as a fingerprint).

Properly designed and implemented multifactor authentication methods are more reliable and stronger fraud deterrents and are more difficult to compromise. The principal objectives of two-factor authentication are to protect the confidentiality of customer account data and transaction details as well as enhance confidence in internet banking by combating various cyber attack mechanisms like phishing, keylogging, spyware/malware and other internet-based frauds targeted at banks and their customers.

Implementation of two-factor authentication and other security measures for internet banking:

In view of the proliferation of cyber attacks and their potential consequences, banks should implement two-factor authentication for fund transfers through internet banking.

The implementation of appropriate authentication methodologies should be based on an assessment of the risk posed by the institution's Internet banking systems. The risk should be evaluated in light of the type of customer (e.g., retail or corporate/commercial); the customer transactional capabilities (e.g., bill payment, fund transfer), the sensitivity of customer information being communicated to both the bank and the volume of transactions involved. Beyond the technology factor, the success of a particular authentication method depends on appropriate policies, procedures, and controls. An effective authentication method should take into consideration customer acceptance, ease of use, reliable performance, scalability to accommodate growth, and interoperability with other systems.

There is a legal risk in not using the asymmetric cryptosystem and hash function for authenticating electronic transactions. However, it is observed that some banks still use weak

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

user id/password based authentication for fund transfers using internet banking. For carrying out critical transactions like fund transfers, the banks, at the least, need to implement robust and dynamic two-factor authentication through user id/password combination and second factor like (a) a digital signature (through a token containing digital certificate and associated private key) (preferably for the corporate customers) or (b) OTP/dynamic access code through various modes (like SMS over mobile phones or hardware token).

To enhance online processing security, confirmatory second channel procedures (like telephony, SMS, email etc) should be applied in respect of transactions above pre-set values, creation of new account linkages, registration of third party payee details, changing account details or revision to funds transfer limits. In devising these security features, the bank should take into account their efficacy and differing customer preferences for additional online protection.

Based on mutual authentication protocols, customers could also authenticate the bank's web site through security mechanisms such as personal assurance messages/images, exchange of challenge response security codes and/or the secure sockets layer (SSL) server certificate verification. In recent times, Extended Validation Secure Sockets Layer (EV-SSL) Certificates are increasingly being used. These are special SSL Certificates that work with high security Web browsers to clearly identify a Web site's organizational identity. It should, however, be noted that SSL is only designed to encrypt data in transit at the network transport layer. It does not provide end-to-end encryption security at the application layer.

An authenticated session, together with its encryption protocol, should remain intact throughout the interaction with the customer. Else, in the event of interference, the session should be terminated and the affected transactions resolved or reversed out. The customer should be promptly notified of such an incident as the session is being concluded or subsequently by email, telephone or through other means.

Changes in mobile phone number may be done through request from a branch only
Implementation of virtual keyboard

A cooling period for beneficiary addition and SMS and E-mail alerts when new beneficiaries are added

Customers should be advised to adopt various good security precautions and practices in protecting their personal computer and to avoid conducting financial transactions from public or internet café computers.

Risk based transaction monitoring or surveillance process needs to be considered as an adjunct.

An online session would need to be automatically terminated after a fixed period of time unless the customer is re-authenticated for the existing session to be maintained. This prevents an attacker from keeping an internet banking session alive indefinitely.

By definition true multifactor authentication requires the use of solutions from two or more of the three categories of factors. Using multiple solutions from the same category at different points in the process may be part of a layered security or other compensating control approach, but it would not constitute a true multifactor authentication.

As an integral part of the two factor authentication architecture, banks should also implement appropriate measures to minimise exposure to a middleman attack which is more commonly known as a man-in-the-middle attack (MITM), man-in-the browser (MITB) attack or man-in-the application attack. The banks should also consider, and if deemed appropriate, implement the following control and security measures to minimise exposure to man-in-the middle attacks:

Specific OTPs for adding new payees: Each new payee should be authorized by the customer based on an OTP from a second channel which also shows payee details or the customer's handwritten signature from a manual procedure which is verified by the bank.

Individual OTPs for value transactions (payments and fund transfers): Each value transaction or an approved list of value transactions above a certain rupee threshold determined by the customer should require a new OTP.

OTP time window: Challenge-based and time-based OTPs provide strong security because their period of validity is controlled entirely by the bank and does not depend on user behaviour. It is recommended that the banks should not allow the OTP time window to exceed 100 seconds on either side of the server time since the smaller the time window, the lower the risk of OTP misuse.

Payment and fund transfer security: Digital signatures and key-based message authentication codes (KMAC) for payment or fund transfer transactions could be considered for the detection of unauthorized modification or injection of transaction data in a middleman attack. For this security solution to work effectively, a customer using a hardware token would need to be able to distinguish the process of generating a one-time password from the process of digitally signing a transaction. What he signs digitally must also be meaningful to him, which means the token should at least explicitly show the payee account number and the payment amount from which a hash value may be derived for the purpose of creating a digital signature. Different crypto keys should be used for generating OTPs and for signing transactions.

Second channel notification / confirmation: The bank should notify the customer, through a second channel, of all payment or fund transfer transactions above a specified value determined by the customer.

Session time-out: An online session would be automatically terminated after a fixed period of time unless the customer is re-authenticated for the existing session to be maintained. This prevents an attacker from keeping an internet banking session alive indefinitely.

SSL server certificate warning: Internet banking customers should be made aware of and shown how to react to SSL or EV-SSL certificate warning

EMERGING TECHNOLOGIES AND INFORMATION SECURITY:

Discussed below are some emerging technologies which are increasingly being adopted/likely to be considered in the near future. However, the security concerns in respect of such technologies need to be considered.

Virtualization

Background:

Over the last 10 years, the trend in the data center has been towards decentralization, also known as horizontal scaling. Centralized servers were seen as too expensive to purchase and maintain. Due to this expense, applications were moved from a large shared server to their own physical machine. Decentralization helped with the ongoing maintenance of each application, since patches and upgrades could be applied without interfering with other running systems. For the same reason, decentralization improves security since a compromised system is isolated from other systems on the network.

However, decentralization's application sandboxes come at the expense of more power consumption, more physical space requirement, and a greater management effort which increased annual maintenance costs per machine. In addition to this maintenance overhead, decentralization decreases the efficiency of each machine, leaving the average server idle 85% of the time. Together, these inefficiencies often eliminate any savings promised by decentralization.

Virtualization is a modified solution between centralized and decentralized deployments. Instead of purchasing and maintaining an entire computer for one application, each application can be given its own operating system, and all those operating systems can reside on a single piece of hardware. This provides the benefits of decentralization, like security and stability, while making the most of a machine's resources.

Challenges of Virtualization

Compatibility and support – Often software developers are not ready to guarantee fail-safe operation of all their programs in virtual machines.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Licensing – There is a need for thorough examination of licenses of OS, as well as other software as far as virtualization is concerned. OS manufacturers introduce some limitations on using their products in virtual machines (especially OEM versions). Such scenarios are often described in separate license chapters. There may also be some problems with licensing software based on number of processors, as a virtual machine may emulate different number of processors than in a host system.

Staff training - This problem is currently one of the most burning ones, as are difficulty in finding exclusive virtualization experts, who can deploy and maintain a virtual infrastructure. "Heavy" virtualization platforms may require serious training of staff who will maintain them.

Reliability - As several virtual servers work on a single physical server, failures of hardware components may affect all the virtual servers running on it. Planning and implementing disaster recovery strategies to ensure reliability of a virtual infrastructure will be a better solution.

Addressing security issues in virtualization:

There is a misconception that if we virtualize, let's say, a Windows 2003 Server, that virtualized system should be secure because it is completely separate from the VM Server operating system and it could be potentially "protected" by VM Server. This is not true and there are a lot of aspects one needs to know about virtualization security.

The ultimate attack on a virtual host system would be for a guest system to run malicious code allowing it to gain elevated privilege and gain access to the underneath VM Server. If the malicious code could create a new "phantom" virtual machine that could be controlled by the attacker, they would have full access to the virtual host and all virtual guests. With this form of "hyperjacking", the attacker would be invisible to traditional virtualization management software and security tools. From there, the attacker would perform a DoS (denial of service) attack by overloading the virtual guest systems.

The below covers full virtualization environments that are most commonly used in servers. A few major indicative measures are provided below. Additionally, detailed vendor recommended security measures may be followed.

a. *Securing the virtualization platform* - Privileged partition operating system hardening – (i) Limit VM resource use: set limits on the use of resources (e.g., processors, memory, disk space, virtual network interfaces) by each VM so that no one VM can monopolize resources on a system. (ii) Ensure time synchronization: ensure that host and guests use synchronized time for investigative and forensic purposes.

b. *Unnecessary programmes and services*: all unnecessary programs should be uninstalled, and all unnecessary services should be disabled.

c. *Host OS* must be patched regularly and in a timely fashion to ensure that the host OS is protecting the system itself and guest OSs properly. In addition, the same patching requirements apply to the virtualization software.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

d. *Partitioning and resource allocation space restrictions*: volumes or disk partitioning should be used to prevent inadvertent denials of service from virtual machines (guest operating systems, OSs) filling up available space allocations, and allow role-based access controls to be placed individually on each virtual machine (guest OS).

e. *Disconnect unused physical devices*: individual VMs can be configured to directly or indirectly control peripheral devices attached to the host system. VMs should be configured by default to disable such connections. Connections to peripheral devices should be enabled only when necessary.

f. *Virtual devices*: ensure that virtual devices for guest OSs are associated with the appropriate physical devices on the host system, such as the mapping between virtual network interface cards (NICs) to the proper physical NICs.

g. *File sharing should not be allowed between host and guest OSs*: while it might be convenient to enable the sharing of system files between the host and guest OSs, allowing such introduces an unacceptable risk of a guest OS possibly maliciously changing a host OS file.

h. Just as with physical servers, virtual systems need to be regularly backed-up for error recovery.

i. Carrying out logging and auditing is critical along with correlating server and network logs across virtual and physical infrastructures to reveal security vulnerabilities and risk

J. Network access for the host OS should be restricted to management services only, and, if necessary, network access to storage (iSCSI).

K. A firewall should ideally be placed on the host OS to protect the system, or a firewall should at least be local to a small number of systems for protection purposes, with access allowed only for management purposes. Additionally, the firewall should restrict access to only those systems authorized to manage the virtual infrastructure

l. *Guest operating system hardening* - Minimize number of accounts- guests should have accounts necessary for running each VM only with passwords that are strong, hard to guess, changed frequently, and only provided to staff that must have access. Separate credentials should be used for access to each guest OS; credentials should not be shared across guest OSs, and should *not* be the same as used for access to the host OS

m. The guest OS should be protected by a firewall running on the host OS, or at least running locally (i.e., local to a small number of systems for protection purposes). Firewall needs to discriminate against inappropriate and/or malicious traffic using networking communications effective for the environment (e.g., if bridging is used instead of routing).

n. Consider using introspection capabilities to monitor the security of activity occurring between guest OSs. This is particularly important for communications that in a non-virtualized environment were carried over networks and monitored by network security controls (such as network firewalls, security appliances, and network IDS/IPS sensors).

Cloud Computing

Background: Computing environment owned by a company is shared with client companies through web-based service over Internet which hosts all the programs to run everything from e-mail to word processing to complex data analysis programs. This is called cloud computing.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

The term cloud computing probably comes from the use of a cloud image to represent the Internet or some large networked environment. We don't care much what's in the cloud or what goes on there except that we get the services we require. Service may include software, platform or infrastructure.

At the backend, cloud computing can make use of virtualization and grid computing. In grid computing, networked computers are able to access and use the resources of every other computer on the network.

Cloud Computing Concerns

Perhaps the biggest concerns about cloud computing are security and privacy. The idea of handing over important data to another company worries some people. Corporate executives might hesitate to take advantage of a cloud computing system because they can't keep their company's information under lock and key.

Privacy is another matter. If a client can log in from any location to access data and applications, it's possible the client's privacy could be compromised. Cloud computing companies will need to find ways to protect client privacy by implementing reliable authentication techniques.

A cloud computing system must ensure backup of all its clients' information.

Some questions regarding cloud computing are more legal. Does the user or company subscribing to the cloud computing service own the data? Does the cloud computing system, which provides the actual storage space, own it? Is it possible for a cloud computing company to deny a client access to that client's data? Several companies, law firms and universities are debating these and other questions about the nature of cloud computing. Thus, there are issues relating to data security and privacy, compliance and legal/contractual issues.

A few examples of cloud computing risks that need to be managed include:

Enterprises need to be particular in choosing a provider. Reputation, history and sustainability should all be factors to consider. Sustainability is of particular importance to ensure that services will be available and data can be tracked.

The cloud provider often takes responsibility for information handling, which is a critical part of the business. Failure to perform to agreed-upon service levels can impact not only confidentiality but also availability, severely affecting business operations.

The dynamic nature of cloud computing may result in confusion as to where information actually resides. When information retrieval is required, this may create delays.

The geographical location of data storage and processing is not definite unlike traditional data centre. Trans-border data flows, business continuity requirements, log retention, data

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

retention, audit trails are among the issues that contribute to compliance challenges in Cloud Computing environment.

Third-party access to sensitive information creates a risk of compromise to confidential information. In cloud computing, this can pose a significant threat to ensuring the protection of intellectual property (IP), trade secrets and confidential customer information.

The contractual issues in the cloud services can relate to ownership of intellectual property, unilateral contract termination, vendor lock-in, fixing liability and obligations of Cloud service providers, exit clause, etc.

Public clouds allow high-availability systems to be developed at service levels often impossible to create in private networks, except at extraordinary costs. The downside to this availability is the potential for commingling of information assets with other cloud customers, including competitors. Compliance to regulations and laws in different geographic regions can be a challenge for enterprises. At this time there is little legal precedent regarding liability in the cloud. It is critical to obtain proper legal advice to ensure that the contract specifies the areas where the cloud provider is responsible and liable for ramifications arising from potential issues.

Due to the dynamic nature of the cloud, information may not immediately be located in the event of a disaster. Business continuity and disaster recovery plans must be well documented and tested. The cloud provider must understand the role it plays in terms of backups, incident response and recovery. Recovery time objectives should be stated in the contract.

Service providers must demonstrate the existence of effective and robust security controls, assuring customers that their information is properly secured against unauthorized access, change and destruction. Key questions to decide are: What employees (of the provider) have access to customer information? Is segregation of duties between provider employees maintained? How are different customers' information segregated? What controls are in place to prevent, detect and react to breaches

IS AUDIT

Introduction:

In the past decade, with the increased technology adoption by Banks, the complexities within the IT environment have given rise to considerable technology related risks requiring effective management.

This led the Banks to implement an Internal Control framework, based on various standards and its own control requirements and the current RBI guidelines. As a result, Bank's management and RBI, need an assurance on the effectiveness of internal controls implemented and expect the IS Audit to provide an independent and objective view of the extent to which the risks are managed.

As a consequence, the nature of the Internal Audit department has undergone a major transformation and IS audits are gaining importance as key processes are automated, or enabled by technology. Hence, there is a need for banks to re-assess the IS Audit processes and ensure that IS Audit objectives are effectively met.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

The scope of IS Audit includes:

Determining effectiveness of planning and oversight of IT activities

Evaluating adequacy of operating processes and internal controls

Determining adequacy of enterprise-wide compliance efforts, related to IT policies and internal control procedures

Identifying areas with deficient internal controls, recommend corrective action to address deficiencies and follow-up, to ensure that the management effectively implements the required actions

Following areas have been covered under this chapter:

IS Audit: The organisation's structure, roles and responsibilities. The chapter identifies the IS Audit stakeholders, defines their roles, responsibilities and competencies required to adequately support the IS Audit function

Audit Charter or Policy (to be included in the IS Audit): This point addresses the need to include IS Audit as a part of the Audit Charter or Policy

Planning an IS Audit: This point addresses planning for an IS Audit, using Risk Based Audit Approach. It begins with an understanding of IT risk assessment concepts, methodology and defines the IS Audit Universe, scoping and planning an audit execution

Executing an IS Audit: This describes steps for executing the audit, covering activities such as understanding the business process and IT environment, refining the scope and identifying internal controls, testing for control design and control objectives, appropriate audit evidence, documentation of work papers and conclusions of tests performed

Reporting and Follow-up: Describes the audit summary and memorandum, the requirements for discussing findings with the management, finalising and submitting reports, carrying out follow-up procedures, archiving documents and ensuring continuous auditing

Quality Review: This addresses the quality aspects which ensures supervision and exercising due care.

Role and Responsibilities / Organisational structure

Board of Directors and Senior Management

Board of Directors and senior management are responsible for ensuring that an institution's system of internal controls operates effectively. One important element of an effective

internal control system is an internal audit function that includes adequate IT coverage. To meet its responsibility of providing an independent audit function with sufficient resources to ensure adequate IT coverage, the Board, or its Audit Committee, should enable an internal audit function, capable of evaluating IT controls adequately.

Audit Committee of the Board

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

An institution's board of directors establishes an "Audit Committee" to oversee audit functions and to report on audit matters periodically to the Board of Directors. Banks should enable adequately skilled Audit Committee composition to manage the complexity of the IS Audit oversight.

A designated member of an Audit Committee needs to possess the knowledge of Information Systems, related controls and audit issues. Designated member should also have competencies to understand the ultimate impact of deficiencies identified in IT internal control framework by the IS Audit. The committee should devote appropriate time to IS audit findings identified during IS Audits and members of the Audit Committee need to review critical issues highlighted and provide appropriate guidance to a bank's management.

As a part of its overall responsibilities, the committee should also be ultimately responsible for the following IS Audit areas:

Bank's compliance with legal and regulatory requirements such as (among others) Information Technology Act-2000, Information Technology (Amendment) Act-2008, Banker's Books (Evidence) Act-1891, The Banking Regulation Act-1949, Reserve Bank of India Act-1934 and RBI circulars and guidelines

Appointment of the IS Audit Head

Performance of IS Audit

Evaluation of significant IS Audit issues

(A Board or its Audit Committee members should seek training to fill any gaps in the knowledge, related to IT risks and controls.)

Internal Audit/Information System Audit function

Internal Audit is a part of the Board's assurance process with regard to the integrity and effectiveness of systems and controls. It is an independent group that reports directly to the Audit Committee or the Board of Directors. IS Audit, being an integral part of Internal Audit, requires an organisation structure with well-defined roles which needs to function in alignment with the Internal Audit, and provide technical audit support on key focus areas of audit or its universe, identified by an Internal Audit department. A well-defined IS Audit organisation structure ensures that the tasks performed fulfill a bank's overall audit objective, while preserving its independence, objectivity and competence.

In this regard, banks require a separate IS Audit function within an Internal Audit department led by an IS Audit Head reporting to the Head of Internal Audit or Chief Audit Executive (CAE). The personnel needs to assume overall responsibility and accountability of IS Audit functions. Where the bank leverages external resources for conducting IS Audit on areas where skills are lacking, the responsibility and accountability for such external IS Audits still remain with the IS Audit Head and CAE.

Critical Components and Processes

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Because the IS Audit is an integral part of the Internal Auditors, auditors will also be required to be independent, competent and exercise due professional care.

Independence: IS Auditors should act independently of the bank's management. In matters

related to the audit, the IS Audit should be independent of the auditee, both in attitude and appearance. The Audit Charter or Policy, or engagement letter (in case of external professional service provider), should address independence and accountability of the audit function. In case independence is impaired (in fact or appearance), details of the impairment should be disclosed to the Audit Committee or Board. Independence should be regularly assessed by the Audit Committee. In case of rotation of audit staff members from IT department to the IS Audit, care should be taken to ensure that the past role of such individuals do not impact their independence and objectivity as an IS Auditor.

Additionally, to ensure independence for the IS Auditors, Banks should make sure that:

Auditors have access to information and applications

Auditors have the right to conduct independent data inspection and analysis

Competence: IS Auditors should be professionally competent, having skills, knowledge, training and relevant experience. They should be appropriately qualified, have professional certifications and maintain professional competence through professional education and training. As IT encompasses a wide range of technologies, IS Auditors should possess skills that are commensurate with the technology used by a bank. They should be competent audit professionals with sufficient and relevant experience. Qualifications such as CISA (offered by ISACA), DISA (offered by ICAI), or CISSP (offered by ISC2), along with two or more years of IS Audit experience, are desirable. Similar qualification criteria should also be insisted upon, in case of outsourced professional service providers.

Due Professional Care: IS Auditors should exercise due professional care, which includes following the professional auditing standards in conducting the audit. The IS Audit Head should deal with any concerns in applying them during the audit. IS Auditors should maintain the highest degree of integrity and conduct. They should not adopt methods that could be seen as unlawful, unethical or unprofessional to obtain or execute an audit.

Outsourcing relating to IS Audit

Banks may decide to outsource execution of segments of audit plan to external professional service providers, as per the overall audit strategy decided in co-ordination with the CAE and the Audit Committee. This may be due to inadequate staff available internally within the bank to conduct audits, or insufficient levels of skilled staff. The work outsourced shall be restricted to execution of audits identified in the plan. Banks need to ensure that the overall ownership and responsibility of the IS Audit, including the audit planning process, risk assessment and follow-up of compliance remains within the bank. External assistance may be obtained initially to put in place necessary processes in this regard.

Both the CAE and Audit Committee should ensure that the external professional service providers appointed should be competent in the area of work that is outsourced and should have relevant prior experience in that area.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Audit Charter, Audit Policy to include IS Audit

Audit Charter or Policy is a document, which guides and directs activities of an internal audit function. IS Audit, being integral part of an Internal Audit department, should also be governed by the same charter or policy. The charter should be documented to contain a clear description of its mandate, purpose, responsibility, authority and accountability of relevant members or officials in respect of the IS Audit (namely the IS Auditors, management and Audit Committee) apart from the operating principles. The IS Auditor will have to determine how to achieve the implementation of the applicable IS Audit standards, use professional judgment in their application, and be prepared to justify any departure therefrom.

Contents of the Audit Policy

The Policy should clearly address the aspects of responsibility, authority and accountability

of the IS auditor. *Aspects to be considered:*

Responsibility:

Some of the aspects include:

- Mission Statement
- Scope or Coverage
- Audit Methodology
- Objectives
- Independence
- Relationship with External Audit
- Auditee's Requirements
- Critical Success Factors
- Key Performance Indicators
- Other Measures of Performance
- Providing Assurance on Control Environment
- Reviewing Controls on Confidentiality, Integrity and Availability of Data or Systems

Authority:

Includes the following:

- Risk Assessment
- Mandate to perform an IS Audit
- Allocation of resources
- Right to access the relevant information, personnel, locations and systems
- Scope or limitations of scope
- Functions to be audited
- Auditee's expectations
- Organizational structure
- Gradation of IS Audit Officials or Staff

Accountability: Some of the aspects in this regard include the following:

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Reporting Lines to Senior Management, Board of Directors or Designated Authority
Assignment Performance Appraisals
Personnel Performance Appraisals
Staffing or Career Development
Training and Development of Skills including maintenance of professional certification/s, continuing professional education

Auditees' Rights
Independent Quality Reviews
Assessment of Compliance with Standards
Benchmarking Performance and Functions
Assessment of Completion of the Audit Plan
Agreed Actions (e.g. penalties when either party fails to carry out responsibilities)
Co-ordinate with and provide Oversight over other control functions like risk management, security and compliance
The policy should also cover Audit Rating Methodology and Quality Assurance Reviews. There should also be annual review of IS Audit Policy or Charter to ensure continued relevance.

Communication with the Auditees

Effective communication with the auditees involves considering the following:

- Describing a service, its scope, availability and timeliness of delivery
- Providing cost estimates or budgets, if needed
- Describing problems and possible resolutions
- Providing adequate and accessible facilities for effective communication
- Determining relationship between the service offered, and the needs of the auditee

The Audit Charter forms a basis for communication with an auditee. It should include relevant references to service-level agreements for aspects like the following, as applicable:

- Availability for Unplanned Work
- Delivery of reports
- Costs
- Response to Auditee's Complaints
- Quality of Service
- Review of Performance
- Communication with the Auditee
- Needs Assessment
- Control Risk Self-assessment
- Agreement of Terms of Reference for Audit

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Reporting Process

Agreement of Findings

Quality Assurance Process

The IS Auditor should consider establishing a quality assurance process (e.g., interviews, customer satisfaction surveys, or assignment performance surveys) to understand his expectations relevant to the function. These needs should be evaluated against the Charter, to improve the service or change the service delivery or Audit Charter, if necessary.

Engagement Letter

Engagement letters are often used for individual assignments. They set out the scope and objectives of a relationship between an external IS audit agency and an organisation. The letter should address the three aspects of responsibility, authority and accountability.

Following aspects needs to be considered:

Responsibility: The aspects addressed includes scope, objectives, independence, risk assessment, specific auditee requirements and deliverables

Authority: The aspects to be addressed include right of access to information, personnel, locations and systems relevant to the performance of the assignment, scope or any limitations of scope and documentary evidence or information of agreement to the terms and conditions of the engagement

Accountability: Areas addressed include designated or intended recipients of reports, auditees' rights, quality reviews, agreed completion dates and agreed budgets or fees if available

Planning an IS Audit

(a) Introduction

An effective IS Audit programme addresses IT risk exposures throughout a bank, including areas of IT management and strategic planning, data centre operations, client or server architecture, local and wide-area networks, telecommunications, physical and information security, electronic banking, applications used in banking operations, systems development, and business continuity planning.

A well-planned, properly structured audit programme is essential to evaluate risk management practices, internal control systems and compliance with policies concerning IT-related risks of every size and complexity. Effective programmes are risk -focused, promote sound IT controls, ensure timely resolution of audit deficiencies, and inform the Audit Committee of the effectiveness of Risk Management practices and internal control systems.

In the past, the Internal Audit concentrated on transaction testing, testing of accuracy and reliability of accounting records and financial reports, integrity, reliability and timeliness of control reports, and adherence to legal and regulatory requirements.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

However, in the changing scenario, there is an increased need for widening, as well as redirecting, the scope of Internal Audit to evaluate the adequacy of IT Risk Management procedures and internal control systems. To achieve these, banks are moving towards risk-based internal audit, which include, in addition to selective transaction testing, an evaluation of the Risk Management systems and control procedures prevailing in a bank's operations.

Risk-based Internal Audit (RBIA) approach helps in planning the IS Audit.

It includes the following components:

Understanding IT Risk Assessment Concepts

Adopting a suitable IT Risk Assessment Methodology—used to examine auditable units in the IS audit universe and select areas for review to include in the IS Annual Plan that have the greatest risk exposure

Steps involved are:

Step 1: System Characterisation

Step 2: Threat Identification

Step 3: Vulnerability Identification

Step 4: Control Analysis

Step 5: Likelihood Determination

Step 6: Impact Analysis

Step 7: Risk Determination

As a part of RBIA, planning the IS Audit involves the following:

Defining the IS Audit Universe: This covers the IS Audit Universe, which defines the areas to be covered

Scoping for IS Audit: This addresses the scoping requirements and includes:
Defining control objectives and activities

Considering materiality

Building a fraud risk perspective

Planning Execution of an Audit: This describes the steps of a planning process before IS Audit starts execution of the plan

Documenting an audit plan

Nature and extent of test of control

Sampling techniques

Standards and frameworks

Resource management

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

The above components are clarified in the sub-sections below:

(b) Risk Based IS Audit

This internal audit approach is aimed at developing a risk-based audit plan keeping in mind the inherent risks of a business or location and effectiveness of control systems managing inherent risks. In this approach, every bank business or location, including risk management function, undergoes a risk assessment by the internal audit function.

RBI issued the "Guidance Note on Risk-based Internal Audit" in 2002 to all scheduled commercial banks, introducing the system of "risk-based internal audit".

The guidance note at a broad-level provided the following aspects:

- Development of a well-defined policy for risk-based internal audit
- Adoption of a risk assessment methodology for formulating risk based audit plan
- Development of risk profile and drawing up of risk matrix taking inherent business risk and effectiveness of the control system for monitoring the risk
- Preparation of annual audit plan, covering risks and prioritization, based on level and direction of each risk
- Setting up of communication channels between audit staff and management, for reporting issues that pose a threat to a bank's business
- Periodic evaluation of the risk assessment methodology
- Identification of appropriate personnel to undertake risk-based audit, and imparting them with relevant training
- Addressing transitional and change management issues

The overall plan, arrived at, using the risk assessment approach enables the Internal Audit to identify and examine key business areas that have highest exposure and enables effective allocation of Audit resources. As stated earlier, IS Audit, being an integral part of the Internal Audit, there is a need for IS Auditors to focus on the IT risks, related to the high-risk business areas identified by the Internal Audit for review during a year. This enables the IS Audit to provide an assurance to the management on the effectiveness of risk management and internal controls underlying the high-risk business processes, which when read in conjunction with the Internal Audit reports, provides a holistic view of the effectiveness.

Risk-based IS Audit needs to consider the following:

- Identification of an institution's data, application, technology, facilities, and personnel
- Identification of business activities and processes within each of those categories
- Profiles of significant business units, departments and product lines and systems, and their associated business risks and control features, resulting in a document describing the structure of risk and controls throughout the institution

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Use a measurement or scoring system that ranks and evaluates business and control risks for business units, departments and products

Includes Board or Audit Committee approval of risk assessments and annual Risk-based Audit Plans that establish audit schedules, cycles, work programme scope and resource allocation for each area audited

Implementation of the Audit Plan

Further, while identifying IT risks, an IS Auditor must consider the impact of non-alignment with any information security-related guidelines issued by RBI based on recommendations in Chapter 2 of this report. It should also be ensured that all systems, domains and processes, irrespective of their risk-levels, are covered within a period of three years.

(c) Adopting a Suitable Risk Assessment Methodology

The IS Auditor must define, adopt and follow a suitable risk assessment methodology. This should be in consonance with the focus on risks, to be addressed as a part of the overall Internal Audit Strategy.

A successful risk-based IS Audit Programme can be based on an effective scoring system arrived at by considering all relevant risk factors.

Major risk factors used in scoring systems include: Adequacy of internal controls, business criticality, regulatory requirements, amount or value of transactions processed, if a key customer information is held, customer facing systems, financial loss potential, number

of transactions processed, availability requirements, experience of management and staff, turnover, technical competence, degree of delegation, technical and process complexity, stability of application, age of system, training of users, number of interfaces, availability of documentation, extent of dependence on the IT system, confidentiality requirements, major changes carried out, previous audit observations and senior management oversight.

On the basis of risk matrix of business criticality and system or residual risk, applications or systems can be graded, based on where they fall on the “risk map” and accordingly their audit frequency can be decided. Banks should develop written guidelines on the use of risk assessment tools and risk factors and review these with the Audit Committee or the Board. Risk assessment guidelines will vary for banks depending on size, complexity, scope of activities, geographic diversity and technology systems used. Auditors should use the guidelines to grade major risk areas and define range of scores or assessments

(e.g., groupings such as low, medium, or high risk or a numerical sequence such as 1 to 5).

The written risk assessment guidelines should specify the following elements:

Maximum length for audit cycles based on the risk assessment process: For example, very high to high risk applications audit cycle can be at a frequency ranging from six months upto 12, medium risk applications can be 18 months (or below) and up to 36 months for low-risk areas. Audit cycles should not be open-ended.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Timing of risk assessments for each business area or department: While risk assessment is expected to be on an annual basis, frequent assessments may be needed if an institution experiences rapid growth or change in operation or activities.

Documentation requirements to support risk assessment and scoring decisions

Guidelines for overriding risk assessments in special cases and the circumstances under which they can be overridden: Example: due to major changes in system, additional regulatory or legal requirements, a medium risk application may have to be audited more frequently.

Notwithstanding the above, IT governance, information security governance -related aspects, critical IT general controls such as data centre controls and processes and critical business applications/systems having financial/compliance implications, including regulatory reporting, risk management, customer access (delivery channels) and MIS systems, needs to be subjected to IS Audit at least once a year (or more frequently, if warranted by the risk assessment).

IS Auditors should periodically review results of internal control processes and analyse financial or operational data for any impact on a risk assessment or scoring. Accordingly, auditee units should be required to keep auditors up-to-date on major changes, such as introduction of a new product, implementation of a new system, application conversions, significant changes in organisation or staff, regulatory and legal requirements, security incidents.

Defining the IS Audit Universe

An Audit Universe is an outcome of the risk assessment process. It defines the audit areas to be covered by the IS Auditor. It is usually a high-level structure that identifies processes, resources, risks and controls related to IT, allowing for a risk-based selection of the audit areas. The IT risks faced by banks due to emerging technologies, prioritisation of IS Audit Universe, selection of types of audits that need to be performed, optimisation of available resources, and ensuring quality of findings, are challenges faced by IS Audit.

The IS Audit Universe can be built around the four types of IT resources and processes:

Such as application systems, information or data, infrastructure (technology and facilities

such as hardware, operating systems, database management systems, networking, multimedia, and the environment that houses and supports them and enable processing of applications) and people (internal or outsourced personnel required to plan, organise, acquire, implement, deliver, support, monitor and evaluate the information systems and services).

The challenge is to provide the “right level of granularity” in the definition of the universe, so as to make it effective and efficient.

Though this is different for every bank, below are some of the considerations for defining IS Audits:

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Using overly-broad definitions for IS Audits (e.g. IT general controls) will ensure a scope creep in audit procedures. The IS Audit Head should make sure that the definition of each IS Audit is an accurate description of what is being reviewed.

Audit Universe for a year should touch upon all layers in the IT environment. Though each IT environment is different, layers tend to be the same. If an IS Audit plan does not include some review for each of the layers, odds are that the plan, as a whole, is deficient.

IS Audits should be structured in such a way as to provide for effective and logical reporting. For example: IS Audits of pervasive technologies (e.g. networks or processes) are more effective when audited at an enterprise level.

IS Audits should address appropriate risks. In many cases, IS Audit budgets are determined before the IT risk assessment is performed. This inevitably leads to one of two situations:

An inadequate number of audit hours are spread over too many audits, which results in consistently poor quality audits, because there is not enough time.

Audits that should be performed are not performed because the budget does not allow it.

Scoping for IS Audit

Information gathered by the IS Auditors during IT risk assessment about the IT system processing and operational environment, threats, vulnerabilities, impact and controls, enables identification of the control objectives and activities to be tested for design and implementation effectiveness and its operating effectiveness.

Scoping plays a crucial role in overall effectiveness. This is exacerbated by the need for the IS Auditors to integrate with the process, operational or financial auditors, and the procedures they are performing, particularly in environments with large integrated CBS applications, where a high number of key process controls are contained within the systems. *(An illustrative list of areas which can form a part of IS Audit scope are given in Annex-B.)*

IS Audits should also cover branches, with focus on large and medium branches, in areas such as control of passwords, user ids, operating system security, anti-malware, maker-checker, segregation of duties, physical security, review of exception reports or audit trails, BCP policy and or testing.

Reports and circulars issued by RBI for specific areas which also need to be covered in the

IS Audit Scope:

Report of the Committee on Computer Audit (dated: April 2, 2002) Circular on Information System Audit—A Review of Policies and Practices

(dated: April 30, 2004 (RBI/2004/191 DBS.CO.OSMOS.BC/ 11 /33.01.029/2003-04)

Defining Control Objectives and Activities

IT control objectives, based on well known frameworks can be included in the scope.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Materiality

When conducting financial statement audits, Internal Auditors measure materiality in monetary terms, since areas that are audited are also measured and reported in monetary terms. However, since IS Auditors conduct audit on non-financial items, alternative measures are required to assess materiality. Such assessments are a matter of professional judgment. They include consideration of its effect on a bank as a whole, of errors, omissions, irregularities and illegal acts, which may have happened as a result of "internal control weaknesses" in an area being audited. ISACA IS Auditing Guideline G6: specifies that if the IS Audit focus relates to systems or operations that process financial transactions, the value of assets controlled by the system(s), or the value of transactions processed per day/week/month/year, should be considered in assessing materiality. In case, the focus is on systems that do not process financial transactions, then following measures should be considered:

Criticality of the business processes supported by the system or operation

Cost of system or operation (hardware, software, staff, third-party services, overheads or a combination of these)

Potential cost of errors (possibly in terms of irrecoverable development costs, cost of publicity required for warnings, rectification costs, health and safety costs, high wastage, etc.)

Number of accesses/transactions/inquiries processed per period

Nature, timing and extent of reports prepared, and files maintained

Service-level agreement requirements and cost of potential penalties

Penalties for failure to comply with legal and contractual requirements

IS Auditors should review the following additional areas that are critical and high risk such as:

IT Governance and information security governance structures and practices implemented by the Bank

Testing the controls on new development systems before implementing them in live environment.

A pre-implementation review of application controls, including security features and controls over change management process, should be performed to confirm that:

Controls in existing application are not diluted, while migrating data to the new application

Controls are designed and implemented to meet requirements of a bank's policies and procedures, apart from regulatory and legal requirements

Functionality offered by the application is used to meet appropriate control objectives

A post implementation review of application controls should be carried out to confirm if the controls as designed are implemented, and are operating, effectively. Periodic review of application controls should be a part of an IS audit scope, in order to detect the impact of application changes on controls. This should be coupled with review of underlying environment—operating

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

system, database, middleware, etc.—as weaknesses in the underlying environment can negate the effectiveness of controls at the application layer. Due care should be taken to ensure that IS Auditors have access only to the test environment for performing the procedures and data used for testing should be, as far as practical, be a replica of live environment.

Srinivas Kante

Detailed audit of SDLC process to confirm that security features are incorporated into a new system, or while modifying an existing system, should be carried out.

A review of processes followed by an implementation team to ensure data integrity after implementation of a new application or system, and a review of data migration from legacy systems to the new system where applicable, should be followed.

IS Auditors may validate IT risks (identified by business teams) before launching a product or service. Review by IS Auditor may enable the business teams to incorporate additional controls, if required, in the system before the launch.

Building Fraud Risk Perspective

In planning and performing an audit to reduce risks to a low level, the auditor should consider the risk of irregularities and illegal acts. He should maintain professional skepticism during an audit, recognising the possibility that “material mis-statements due to irregularities and illegal acts” could exist, irrespective of their evaluation of risk of irregularities and illegal acts.

IS Auditors are also required to consider and assess the risk of fraud, while performing an audit. They should design appropriate plans, procedures and tests, to detect irregularities, which can have a material effect on either a specific area under an audit, or the bank as a whole. IS Auditors should consider whether internal control weaknesses could result in material irregularities, not being prevented or detected. The auditor should design and perform procedures to test the appropriateness of internal control and risk of override of controls. They should be reasonably conversant with fraud risk factors and indicators, and assess the risk of irregularities connected with the area under audit.

In pursuance to the understanding gathered during threat identification step of the IT Risk Assessment process, the auditors should identify control objectives and activities. These are required to be tested to address fraud risk. He should consider “fraud vulnerability assessments” undertaken by the “Fraud Risk Management Group”, while identifying fraud risk factors in the IT risk assessment process. He should be aware that certain situations may increase a bank’s vulnerability to fraud risk (e.g. introduction of a new line of business, new products, new delivery channels and new applications or systems.)

In preparing an audit scope, auditors should consider fraud risk factors including these:

- Irregularities and illegal acts that are common to banking industry
- Corporate ethics, organisational structure, adequacy of supervision, compensation and reward structures, the extent of performance pressures

- Management's behavior with regard to ethics
- Employee dissatisfaction resulting from potential layoffs, outsourcing, divestiture or restructuring
- Poor financial or operational performance
- Risk arising out of introduction of new products and processes
- Bank's history of fraud
- Recent changes in management teams, operations or IT systems
- Existence of assets held, or services offered, and their susceptibility to irregularities
- Strength of relevant controls implemented
- Applicable regulatory or legal requirements
- History of findings from previous audits
- Findings of reviews, carried out outside the audit, such as the findings from external auditors, consultants, quality assurance teams, or specific investigations

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Findings reported by management, which have arisen during the day-to-day course of

Srinivas Kante

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

business

Technical sophistication and complexity of the information system(s) supporting the area under audit

Existence of in-house (developed or maintained) application systems, as compared with the packaged software for core business systems

Instances of fraud should be reported to appropriate bank stakeholders:

Frauds involving amounts of Rs 1 crore (and above) should be reported to Special Committee formed to monitor and follow up large fraud cases

Other fraud cases should be reported to Fraud Review Councils or independent groups formed to manage frauds

The status of fraud cases should be reported to Audit Committee as a part of their review of IS audit

IS Auditors should also extend necessary support to Fraud Review Councils or independent groups or Special Committees in their investigations

Planning the Execution

The IS Audit Head is responsible for the annual IS Audit Plan, prepared after considering the risk assessment and scoping document. The plan covers overall audit strategy, scoped areas, details of control objectives identified in the scoping stage, sample sizes, frequency or timing of an audit based on risk assessment, nature and extent of audit and IT resource skills availability, deployment and need for any external expertise. A report on the status of planned versus actual audits, and any changes to the annual audit plan, needs to be periodically presented to Audit Committee and Senior Management on a periodic basis.

There are well-known guidance on IS Audit. The Institute of Chartered Accountants of India (ICAI), in March 2009, published the "Standard on Internal Audit (SIA) 14: Internal Audit in an Information Technology Environment" covering requirements of the planning stage, which an auditor should follow. IIA has provided guidance on defining the IS Audit Universe, through the guide issued on "Management of IS Auditing" under the "Global Technology Audit Guide" series. ITGI has provided guidance on audit planning in its "IT Assurance Guide using COBIT".

Suggested guidelines for implementation by banks are as follows:

Documenting the Audit Plan

The plan (either separately or as part of overall internal audit plan) should be a formal document, approved by the Audit Committee initially and during any subsequent major changes. The plan should be prepared so that it is in compliance with any appropriate external requirements in addition to well-known IS Auditing Standards.

Audit Plan Components include:

Internal Audit Subject: Name of the Audit Subject

Nature of Audit: Compliance with legal, regulatory or standards, performance metrics assessment or security configuration testing

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Schedule: Period of audit and its expected duration

Scoped Systems: Identified IT resources that are in the scope based on the risk assessment process

System Overview: Details of System Environment based on the risk assessment process

Audit Details: Details of risks and controls identified, based on the risk assessment process

Nature and Extent of Tests: Controls testing for effectiveness of design and implementation of controls, substantive testing for operating effectiveness of controls implemented

Method of Internal Audit: Brief audit approach and methodology

Team and Roles and Responsibilities: Identified skills and names of IS Auditors including their roles and responsibilities

Points of Contact: Contact names of auditee department

Co-ordination: Names of the project lead and higher official for escalation of issues

Information: Report details of past audits on the subject

Nature and Extent of Tests of Control Types

of testing that can be performed are as below:

Test of Control Design: Controls that have been identified are evaluated for appropriateness in mitigating the risks

Test of Control Implementation: Tests are performed to confirm that the control that has been appropriately designed is implemented and is operating at the time of testing. Mitigating or compensating controls are also reviewed wherever necessary

Assessing Operational Effectiveness of Controls: Wherever the controls designed are found to be in operation, additional testing is performed for the period of reliance (audit period) to confirm if they are operating effectively and consistently

On case-to-case basis, the auditor should exercise professional judgment and decide the nature and extent of procedures that need to be adopted for conclusions. ISA 330 gives guidance on the nature, timing and extent of procedures.

iii. Sampling techniques

During an audit, auditors should obtain sufficient, reliable and relevant evidence to achieve their objectives. Findings and conclusions should be supported by appropriate analysis and interpretation. Auditors should consider sample selection techniques, which result in a statistically-based representative sample for performing compliance or substantive testing. Statistical sampling involves the use of techniques from which mathematically-constructed conclusions regarding the population can be drawn. Non-statistical sampling is not statistically -based. Its results should not be extrapolated over the population as a sample is unlikely to be representative of the population. Examples of compliance testing of controls where sampling could be considered, include user-access rights, programme change control procedures, procedures documentation, programme documentation, follow-up of exceptions, review of logs and software licences audits. Examples of substantive tests where sampling could be considered, include re-performance of a complex calculation (e.g., interest applied), on a sample of accounts, sample of transactions to vouch to supporting documentation, etc.

Design of A Sample

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

While designing the size and structure of an audit sample, auditors may consider the following guidelines:

- Sampling Unit: The unit will depend on the sample purpose. For compliance testing of controls, attribute sampling is typically used, where the unit is an event or transaction (e.g., a control such as an authorisation of transaction).
- Audit objectives: IS Auditors should consider the audit objectives to be achieved and the audit procedures, which are most likely to achieve those objectives. In addition, when sampling is appropriate, consideration should be given to the nature of the audit evidence sought, and possible error conditions.
- Population: Population is an entire set of data from which auditors wish to sample, in order to reach a conclusion. Hence, the population from which a sample is drawn, has to be appropriate and verified as a “complete” for audit objective.
- Stratification: To assist in efficient and effective design of a sample, stratification may be appropriate. Stratification is a process of dividing a population into “sub-populations” with similar characteristics, explicitly defined, so that each sample unit can belong to only one stratum.

Selection of A Sample

IS Auditors should use statistical sampling methods. They may consider using the following:

- Random Sampling: It ensures that all combinations of units in the population have an equal chance of selection
- Systematic Sampling: It involves selecting units using a fixed interval between selections, the first interval having a random start. Examples include “Monetary Unit Sampling” or “Value Weighted Selection”, where each individual monetary value (e.g., Rs 100) in the population, is given an equal chance of selection. As an individual monetary unit cannot ordinarily be examined separately, the item which includes that monetary unit is selected for examination. This method systematically weighs the selection in favour of the larger amounts, but gives every monetary value an equal opportunity for selection. Another example includes selecting every ‘nth sampling unit’.

Standards and Frameworks

One challenge that the IS Auditors face is knowing what to audit against as a fully-developed IT control baselines for applications and technologies that may not have been developed. Rapid evolution of technology is likely to render baselines useless, after a period of time. However, this does not detract from the concept of control objectives.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Control objectives, by definition, should remain more or less constant (from environment to environment). Consider the objective that critical business data and programmes should be backed up and recoverable. Now, each environment may do that differently; backups could be manual, or automated, or a tool may be used. They could be incremental only, or there may be complete backups of everything. Backups could be done daily, weekly, or monthly. Storage of backups could be onsite in a fireproof safe, off-site at another company facility, or outsourced to a third party. Method used by the organisation to manage backups would certainly impact the audit procedures and budget, but the control objective will not change. IS Auditor should be able to start with a set of IT control objectives, and though not specific to particular environments, select an appropriate framework.

Resource Management

A bank's auditors play a critical role in efficiency and effectiveness of audits. IT encompasses a wide range of technology and sophistication—the skill set needed to audit a Firewall configuration is vastly different from the skill set needed to audit application controls. It is critical to match the skills needed to perform a particular IS Audit, with the appropriate auditor. IS Auditors should also have the appropriate analytical skills to determine and report the root cause of deficiencies. Bank's hiring and training practices should ensure that it has qualified IS Auditors where education and experience should be consistent with job responsibilities. Audit management should also provide an effective programme of continuing education and development.

The main issue is having staff with the requisite range of IS Audit skills, needed to audit an IS Audit universe, effectively. If internal expertise is inadequate, the Board should consider using qualified external sources, such as management consultants, independent auditors, or professionals, to supplement internal resources and support bank's objectives.

Executing IS Audit

As mentioned earlier, auditors must understand the business and IT environment, risks and internal control framework. During audit, auditors should obtain evidences, perform test

procedures, appropriately document findings, and conclude a report. This section provides guidance on matters that IS Auditor should consider while executing the Plan.

ICAI, in March 2009, had published a "Standard on Internal Audit (SIA) 14: Internal Audit in an Information Technology Environment" covering the requirements of executing a plan that an IS Auditor should follow. Additionally, IIA has also provided guidance in their "Management of IS Auditing" under their "Global Technology Audit Guide" series. The ITGI has also provided guidance on execution of assurance initiative in its "IT Assurance Guide Using COBIT".

Guidance on executing the IS Audit entails the following steps:

Refining the understanding of business process and IT environment

Refining the scope and identifying internal controls

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Testing Control Design

Testing the outcome of the control objectives

Collecting audit evidence

Documenting test results

Concluding tests performed

Considering use of audit accelerators

Considering the use of Computer-Aided Automated Tools (CAATs)

Considering the work of others

Considering third-party review by service providers

The above are covered in the following sections:

(a) Refine understanding of the business process and IT environment:

The first step of the execution stage is refining the understanding of an IT environment, in which a review is being planned. This implies understanding of a bank's business processes to confirm the correct scope and control objectives. The scope of the IS Audit need to be communicated to and agreed upon by stakeholders.

Output from this step consists of documented evidence regarding:

- Who performs the task(s), where it is performed and when
- Inputs required to perform the task and outputs generated by it
- Automated tasks performed by systems and system configurations
- System-generated information used by business
- Stated procedures for performing tasks

The IS Auditor can structure this step along the following lines:

Interview and use activity lists and RACI charts

Collect and read process description, policies, input or output, issues, meeting minutes, past audit reports, past audit recommendations, business reports

Prepare a scoping task (process objective, goals and metrics)

Build an understanding of enterprise IT architecture

(b) Refining Scope and Identifying Internal Controls:

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

While understanding and evaluating internal controls of a bank, areas mentioned under “Scope of IS Audit” needs to be covered. However, the nature and extent of control risks may vary, depending on nature and characteristics of a bank’s information system:

Reliance on systems or programmes that are inaccurately processing data, or processing inaccurate data, or both

Unauthorised access to data which may result in destruction of data, or improper changes to data, including recording of unauthorised or non-existent transactions, or inaccurate recording of transactions

Possibility of IT personnel gaining access to privileges, beyond those necessary, to perform their assigned duties, thereby breaking down segregation of duties

Unauthorised changes to data in master files

Unauthorised changes to systems or programmes

Failure to make necessary changes to systems or programmes

Inappropriate manual intervention

Potential loss of data or inability to access data

(c) Testing Control Design:

This section lists the different techniques that will be used in detailed audit steps. Testing of controls is performed covering the main test objectives:

Evaluation of control design

Confirmation that controls are in place within the operation

Assess the operational effectiveness of controls

Additionally, control efficiency could be tested

In the testing phase, different types of testing can be applied. Five generic testing methods include enquire and confirm, inspect, compare actual with expected findings, re-perform or re-calculate and review automated evidence collection through analyzing data using computer assisted audit techniques and extracting exceptions or key transactions.

To assess the adequacy of the design of controls the following steps should be performed:

- Observe, inspect and review control approach. Test the design for completeness, relevance, timeliness and measurability
- Enquire whether, or confirm that, the responsibilities for control practices and overall accountability have been assigned
- Test whether accountability and responsibilities are understood and accepted. Verify that the right skills and the necessary resources are available

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

– Enquire through interviews with key staff involved whether they understand the control mechanism, its purpose and the accountability and responsibilities.

IS Auditor must determine whether:

Documented control processes exist

Appropriate evidence of control processes exists

Responsibility and accountability are clear and effective

Compensating controls exist, where necessary

Additionally, specifically in internal audit assignments, cost-effectiveness of a control design may also be verified, with the following audit steps:

– If the control design is effective: Investigate whether it can be made more efficient by optimising steps, looking for synergies with other mechanisms, and reconsidering the balance of prevention versus detection and correction. Consider the effort spent in maintaining the control practices

– If the control is operating effectively: Investigate whether it can be made more cost-effective. Consider analysing performance metrics of activities associated, automation opportunities or skill level

(d) Test the Outcome of Control Objectives

Audit steps performed ensure that control measures established are working as prescribed and conclude on the appropriateness of the control environment. To test the effectiveness of a control, the auditor needs to look for direct and indirect evidence of the control's impact on the process outputs. This implies the direct and indirect substantiation of measurable contribution of the control to the IT, process and activity goals, thereby recording direct and indirect evidence of actually achieving the outcomes or various control objectives (based on those documented in standards like COBIT, as relevant).

The auditor should obtain direct or indirect evidence for selected items or periods to ensure that the control under review is working effectively by applying a selection of testing techniques as presented in step on test of control design. The IS Auditor should also perform a limited review of the adequacy of the process deliverables, determine the level of substantive testing and additional work needed to provide assurance that the IT process is adequate. Substantive testing would involve performing analytical procedures and tests of details, to gain assurance on areas where control weaknesses are observed. Substantive testing is performed to ascertain the actual impact of control weaknesses.

(e) Audit Evidence

IS Auditors should obtain sufficient and reliable audit evidence to draw reasonable conclusions on which to base the audit results.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Sufficient Evidence: Evidence can be considered sufficient if it supports all material questions in the audit objective and scope. Evidence should be objective and sufficient to enable a qualified independent party to re-perform tests and obtain the same results. The evidence should be commensurate with the materiality of an item and risks involved. In instances where IS Auditor believes sufficient audit evidence cannot be obtained, they should disclose this in a manner consistent with the communication of the audit results.

Appropriate Evidence: Appropriate evidence shall include the following indicative criteria:

Procedures as performed by the IS Auditor
Results of procedures performed by the IS Auditor
Source documents (electronic or paper), records and corroborating information used to support the audit

Findings and results of an audit

When obtaining evidence from a test of control design, auditors should consider the completeness of an audit evidence to support the assessed level of control risk.

Reliable Evidence: IS Auditors should take note of following examples of evidence that is more reliable when it is:

- Written form and not oral expressions
- Obtained from independent sources
- Obtained by IS Auditors, rather than from the bank being audited
- Certified by an independent party

Procedures used to gather evidence can be applied through the use of manual audit procedures, computer-assisted techniques, or a combination of both. For example: a system, which uses manual control totals to balance data entry operations might provide audit evidence that the control procedure is in place by way of an appropriately reconciled and annotated report. IS Auditors should obtain audit evidence by reviewing and testing this report. Detailed transaction records may only be available in machine-readable format, requiring IS Auditors to obtain evidence using computer-assisted techniques.

When information produced by a bank is used by auditors, they should obtain evidence about the completeness and accuracy by the following means:

Performing tests of the operating effectiveness of controls over the production and maintenance of information, to be used as audit evidence

Performing audit procedures directly on information to be used as audit evidence

Auditors should consider the following controls over production and maintenance of information produced by a bank:

- Controls over the integrity, accuracy, and completeness of the source data

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

- Controls over the creation and modification of the applicable report logic and parameters

(f) Documentation

Audit evidence gathered should be documented and organised to support findings and conclusions. IS Audit documentation is a record of the work performed and evidence supporting findings and conclusions.

The potential uses of documentation:

Demonstration of the extent to which the auditor has complied with professional standards related to IS auditing

Assistance with audit planning, performance and review

Facilitation of third-party reviews

Evaluation of the auditors' quality assurance programme

Support in circumstances such as insurance claims, fraud cases and lawsuits

Assistance with professional development of the staff

Documentation should include, at a minimum, a record of:

- Planning and preparation of the audit scope and objectives
- Audit steps performed and audit evidence gathered
- Audit findings, conclusions and recommendations
- Reports issued as a result of the audit work
- Supervisory review

Extent of an IS Auditor's documentation may depend on needs for a particular audit and should include such things as:

IS Auditor's understanding of an area to be audited, and its environment

His understanding of the information processing systems and internal control environment

Audit evidence, source of audit documentation and date of completion

Bank's response to recommendations

Documentation should include audit information, required by law, government regulations, or by applicable professional standards. Documentation should be clear, complete and understandable, by a reviewer. IS Audit owns evidences documented by them, in order to substantiate conclusions on tests performed and specific observations reported to management and Audit Committee.

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

(g) Conclusion on Tests Performed

IS Auditors should evaluate conclusions drawn as a basis for forming an opinion on the audit. Conclusions should be substantiated by evidences, collected and documented. The IS Audit Team may be required to provide and maintain evidences in respect of observations reported by them.

IS Auditors may perform following activities required to conclude on tests performed based on nature and amount of identified control failures and likelihood of undetected errors:

- Decide whether the scope of IS Audit was sufficient to enable the auditors to draw reasonable conclusions on which to base audit opinion
- Perform audit procedures designed to obtain sufficient appropriate audit evidence: events upto the date of audit report may be included and identified in the report
- Prepare an audit summary memorandum documenting findings and conclusions on important issues of IS Auditing and reporting, including judgments made by an IS Audit team
- Obtain appropriate representations from bank management
- Prepare a report appropriate to circumstances, and in conformity with, applicable professional standards and regulatory and legal requirements

Communicate, as necessary, with Audit Committee or Senior Management

Maintain effective controls over processing and distribution of reports relating to the IS Audit

If audit evidence or information indicate that irregularities could have occurred, IS auditors should recommend the bank management on matters that require detailed investigation to enable the management to initiate appropriate investigative actions. The auditors should also consider consulting the Audit Committee and legal counsel about the advisability and risks of reporting the findings outside the Bank.

RBI (vide its circular DBS.CO.FrMC.BC.No.7/23.04.001/ 2009-10, dated: September 16, 2009) requires that fraud cases should be reported to law enforcement agencies and to the RBI. Banks should appropriately include requirements for reporting to RBI, of such instances, in engagement letters issued to external IS Auditors.

(h) Audit Accelerators

Since IS Audit budgets can be difficult to estimate and manage, CAEs can consider using testing accelerators—tools or techniques that help support procedures that the IS Auditors will be performing—to increase efficiency and effectiveness. CAEs can use an accelerator to do the same audit in less time, or do more detailed audit procedures in the same amount of time. Audit accelerators can be divided into two categories:

- Audit Facilitators: Tools that help support the overall management of an audit (e.g., an electronic workpaper management tool)

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

– Testing Accelerators: Tools that automate the performance of audit tests (e.g., data analysis tools).

Audit Facilitators

These include Electronic Workpapers, project management software, flow charting software and open issue tracking software.

Testing Accelerators

Testing accelerators can automate time-consuming audit tasks, such as reviewing large populations of data. Also, using a tool to perform audit procedures helps establish consistency. For example, if a tool is used to assess server security configuration, servers tested with that tool will be assessed along the same baselines. Performing these procedures manually allows for a degree of interpretation on the part of the IS Auditor. Lastly, the use of tools enables IS Auditors to test an entire population of data, rather than just a sample of transactions. This provides for a much higher degree of audit assurance.

Data Analysis Software: These allow an auditor to perform robust statistical analysis of large data sets. They can also be used to support process or operational audits like KYC reviews. They can support types of testing. One consideration when using a data analysis tool is that it may be difficult to extract the data from the original source. It is critical that audit procedures be performed to ensure the completeness and accuracy of the source data.

Security Analysis Tools: These are a broad set of tools that can review a large population of devices or users and identify security exposures. There are different types of security analysis tools. Generally they can be categorised as follows:

Network Analysis Tools: These consist of software programmes that can be run on a network and gather information about it. IS Auditors can use these tools for a variety of audit procedures, including:

Verifying the accuracy of network diagrams by mapping corporate network
Identifying key network devices that may warrant additional audit attention

Gathering information about what traffic is permitted across a network (which would directly support the IT risk assessment process).

<https://iibfadda.blogspot.com/>

Facebook Group : IIBF & NISM Adda

Email: srinivaskante4u@gmail.com

Hacking Tools: Most technologies have a number of standard vulnerabilities, such as the existence of default IDs and passwords or default settings when the technology is installed out-of-the-box. Hacking tools provide for an automated method of checking for these. Such tools can be targeted against Firewalls, servers, networks and operating systems.

Application Security Analysis Tools: If an organisation is using large integrated business application, key internal controls are highly security dependent. Application-level security must be well-designed and built in conjunction with the application's processes and controls.

The CAE should be aware that most of these come with a set of pre-configured rules, or vendor-touted "best practices". Implementation of one will need to be accompanied by a substantive project to create a rule set that is relevant for that particular organisation. Failure to do so will result in audit reports that contain a number of either false-positives or false-negatives.

CAEs should be aware of the following considerations, with respect to IS Audit Accelerators:

Tools cost money. The CAE should be sure that the benefits outweigh the costs

That IS Auditors will need to be trained on the new tool. It is not uncommon that a tool sits unused in an Internal Audit Department

That the tool will need support, patch management and upgrades. Depending on the quality, it may require a standalone server, as well. For this, any tool selection should be managed with the IT department's assistance

Sometimes, IT management or third -party service providers are not allowed tools to access the production environment directly. They are instead asked to do so from a copy of data from an alternative site, or standby server. Any use of tools or scripts should be thoroughly discussed with and approved by IT management and be tested fully before deploying.

(i) Computer-Assisted Audit Techniques (CAATS)

IS Auditors can use an appropriate combination of manual techniques and CAATs. IS Audit function needs to enhance the use of CAATs, particularly for critical functions or processes carrying financial or regulatory or legal implications. The extent to which CAATs can be used will depend on factors such as efficiency and effectiveness of CAATs over manual techniques, time constraints, integrity of the Information System and IT environment and level of audit risk.

CAATs may be used in critical areas (like detection of revenue leakage, treasury functions, assessing impact of control weaknesses, monitoring customer transactions under AML requirements and generally in areas where a large volume of transactions are reported).

Process involved in using CAATs involve the following steps:

Set audit objectives of CAATs

Determine accessibility and availability of a bank's IS facilities, programs, systems and data
Define procedures to be undertaken (e.g., statistical sampling, recalculation, or confirmation)

Define output requirements

Determine resource requirements: i.e. personnel, CAATs, processing environment, bank's IS facilities or audit IS facilities

Obtain access to the bank's IS facilities, programmes, systems and data, including file definitions
Document CAATs to be used, including objectives, high-level flowcharts, and run instructions

CAATs may be used to perform the following audit procedures among others:

- Test of transactions and balances, such as recalculating interest
- Analytical review procedures, such as identifying inconsistencies or significant fluctuations
- Compliance tests of general controls: testing set-up or configuration of the operating system, or access procedures to the programme libraries
- Sampling programmes to extract data for audit testing
- Compliance tests of application controls such as testing functioning of a programmed control
- Re-calculating entries performed by the entity's accounting systems
- Penetration testing

In instances, where CAATs may be used to extract sensitive programmes, system information or production data, IS Auditors should safeguard the programme, system information or production data, with an appropriate level of confidentiality and security. In doing so, IS Auditors should consider the level of confidentiality and security required by the bank, owning the data and any relevant legislation. IS Auditors should be provided with "view access" to systems and data. In case audit procedures cannot be performed in the live environment, appropriate test environment should be made available to IS Auditors. Systems and data under test environment should be synchronised to the live environment.

IS Auditors should use and document results of appropriate procedures to provide for ongoing integrity, reliability, usefulness and security of the CAATs. Example: this should include a review of programme maintenance and change controls over embedded audit software to determine that only authorised changes were made to the CAATs.

In instances where CAATs reside in an environment not under the control of the IS Auditor, an appropriate level of control should, in effect, be placed to identify changes. When the CAATs are changed, IS Auditors should obtain assurance of their integrity, reliability, usefulness and security, through appropriate planning, design, testing, processing and review of documentation, before placing their reliance.

(j) Continuous Auditing

Traditionally, testing of controls performed by an internal audit team was on a retrospective and cyclical basis, often many months after business activities have occurred. The testing procedures have often been based on a sampling approach. They included activities such as reviews of policies, procedures, approvals and reconciliations. Today, however, it is recognised that this approach only affords internal auditors a narrow scope, and is often too late to be of “real value” to business performance or regulatory compliance.

Continuous auditing is a method used to perform control and risk assessments automatically on a more frequent basis using technology which is key to enabling such an approach. Continuous auditing changes the audit paradigm from periodic reviews of a sample of transactions to ongoing audit testing of 100 percent of transactions. It becomes an integral part of modern auditing at many levels. It also should be closely tied to management activities such as performance monitoring, scorecard or dashboard and enterprise risk management.

A continuous audit approach allows internal auditors to fully understand critical control points, rules, and exceptions. With automated, frequent analyses of data, they are able to perform control and risk assessments in real time or near real time. They can analyse key business systems for both anomalies at the transaction level and for data-driven indicators of control deficiencies and emerging risk.

Finally, with continuous auditing, the analysis results are integrated into all aspects of the audit process, from the development and maintenance of the enterprise audit plan to the conduct and follow-up of specific audits. Depending on the level of implementation and

sustenance of risk-based IS Audit approach; banks may explore implementation of continuous auditing in critical areas in a phased manner.

(k) Application Control Audit:

Detailed pre-implementation application control audits and data migration audits in respect of critical systems needs to be subjected to independent external audit. Banks also need to conduct a post-implementation detailed application control audit. Furthermore, banks should also include application control audits in a risk based manner as part of the regular Internal Audit/IS Audit plans with focus on data integrity (among other factors). General internal auditors with requisite functional knowledge need to be involved along with the IS Auditors in the exercise to provide the requisite domain expertise.

Some of the considerations in application control audit (based on ISACA guidelines) include:

An IS Auditor should understand the IS environment to determine the size and complexity of the systems, and the extent of dependence on information systems by the bank

Application-level risks at system and data-level include, system integrity risks relating to the incomplete, inaccurate, untimely or unauthorized processing of data; system-security risks

relating to unauthorized access to systems or data; data risks relating to its completeness, integrity, confidentiality and accuracy; system-availability risks relating to the lack of system operational capability; and system maintainability risks in terms of adequate change control procedures.

Application controls to address the application-level risks may be in the form of computerized controls built into the system, manually performed controls, or a combination of both. Risks of manual controls in critical areas need to be considered. Where the option to place reliance on programmed controls is taken, relevant general IT controls should be considered, as well as controls specifically relevant to the audit objective. Objectives should be developed to address criteria such as integrity, availability, compliance, reliability and confidentiality. Effectiveness and efficiency can also be additional criteria.

As part of documenting the flow of transactions, information gathered should include both computerized and manual aspects of the system. Focus should be on data input (electronic or manual), processing, storage and output which are of significance to the audit objective.

Consideration should also be given to documenting application interfaces with other systems. The auditor may confirm the documentation by performing procedures such as a walk-through test.

Specific controls to mitigate application risks may be identified. Sufficient audit evidence obtained to assure the auditor that controls are operating as intended through procedures such as inquiry and observation, review of documentation and testing of the application system controls, where programmed controls are being tested. Use of computer-assisted audit techniques (CAATs) also needs to be considered.

Nature, timing and extent of testing should be based on the level of risk to the area under review and audit objectives. In absence of strong general IT controls, an IS auditor may make an assessment of the effect of this weakness on the reliability of the computerized application controls.

If an IS auditor finds significant weaknesses in the computerized application controls, assurance should be obtained (depending on the audit objective), if possible, from the manually performed processing controls.

Effectiveness of computerized controls is dependent on general IT controls. Therefore, if general IT controls are not reviewed, ability to place reliance on controls may be limited. Then the IS Auditor should consider alternative procedures.

Where weaknesses identified during the application systems review are considered

to be significant or material, appropriate level of management should be advised to undertake immediate corrective action.

Using the Work of Others

Purpose of an IS Audit standard is to establish and provide a guidance to auditors who can use the work of experts on an audit. The following are standards, to test the reliability of the work of an expert:

IS Auditors should, where appropriate, consider using the work of other experts for audit. They should assess, and then be satisfied with professional qualifications, competencies, relevant experience, resources, independence and quality control processes, prior to engagement.

They should assess, review and evaluate work of experts, as a part of an audit, and then conclude the extent of use and reliance of the work.

They should determine and conclude whether the work of experts is adequate and competent to enable them to conclude on current audit objectives. Such conclusion should be documented

They should apply additional test procedures to gain and include scope limitation, where required evidence is not obtained through additional test procedures

An expert could be an IS Auditor from external auditing firm, a management consultant, an IT domain expert, or an expert in the area of audit, who has been appointed by management or by the IS Audit Team

An expert could be internal or external to the bank. If an expert is engaged by another part of the organisation, reliance may be placed on the bank's report. In some cases, this may reduce the need of an IS Audit coverage, though IS Auditors do not have supporting documentation and work papers. IS Auditors should be cautious in providing an opinion on such cases

An IS Auditor should have access to all papers, supporting documents and reports of other experts, where such access does not create legal issues. Where access creates legal issues, or such papers are not accessible, auditors should determine and conclude on the extent of use and reliance on expert's work

The IS Auditor's views, relevance and comments on adopting the expert's report should form a part of the IS Auditor's Report

Third Party Review of Service Providers

A bank may use a third-party service provider (service organisation) to obtain services of packaged software applications and technology environment, which enables customers to process financial and operational transactions (ATM management, networking and infrastructure development and maintenance, document imaging and indexing, software development and maintenance). RBI has issued "Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks" (circular no: DBOD.NO.BP.40/21.04.158/ 2006-07 dated November 3, 2006), asking banks to adhere to guidelines before outsourcing activities related to financial services.

Services provided by a third party are relevant to the scope of IS Audit. Especially, when those services and controls within them, are a part of the bank's information systems. Though controls at the service organisation are likely to relate to financial reporting, there may be other controls that may also be relevant to the IS Audit (controls over safeguarding of assets or document images).

A service organisation's services are a part of a bank's information system, including related business processes, relevant to IS Audit if these services affect any of the following:

Segments of Information System that are significant to the bank's IS operations

Procedures within information system, by which an user entity's transactions are

initiated, recorded, processed, corrected (when necessary), transferred to a general ledger and reported, in financial statements

The way events and conditions, other than transactions, significant to bank's Information System are captured

IS Auditors will have to obtain an understanding of how a bank uses services of a service organisation in the bank's IS operations, including:

Nature of services provided by the organisation and significance of those to the bank's information system, including the effect thereof on the bank's internal control

Nature and materiality of transactions, accounts or financial reporting processes, affected by the service organisation

Degree of interaction between activities of the organisation and bank

Nature of relationship between the bank and organisation, including relevant contractual terms for activities undertaken by the organisation

In situations, services provided by the organisation may not appear to be "material" to the bank's IS operations. But, the service nature may be. IS Auditors should determine that an understanding of those controls is necessary in the circumstances. *Information on the nature of services, provided by an organisation, may be available from a variety of sources:*

User manual

System overview

Technical manuals

Contract or service-level agreement between the bank and organisation

Reports by service organisation, internal auditors, or regulatory authorities, on service organisation controls

Reports by an auditor of the organisation (service auditor), including management letters

IS Auditors may use a service auditor to perform procedures such as tests of controls at service organisation, or substantive procedures on the bank's IS operations, served by a service organisation.

5) Reporting and Follow-up

This phase involves reporting audit findings to the CAE and Audit Committee. Before reporting the findings, it is imperative that IS Auditors prepare an audit summary memorandum providing overview of the entire audit processing from planning to audit findings, discuss the findings with auditee and obtain responses. Additionally, reviewing the actions taken by management to mitigate the risks observed in audit findings and appropriately updating the audit summary memorandum is also important. Reporting entails deciding the nature, timing and extent of follow-up activities and planning future audits.

Professional bodies like ISACA, IIA, ICAI have issued guidance in this regard.

Reporting and follow-up entails following activities or steps:

- Drafting audit summary and memorandum
- Discussing findings with management
- Finalising and submitting reports
- Reviewing the Actions taken report
- Undertaking follow-up procedures
- Archiving documents

These are covered in the following sections:

Audit Summary and Memorandum: An IS Auditor should perform audits or reviews of control procedures and form a conclusion about, and reporting on, the design and operating effectiveness of the control procedures based on the identified criteria. The conclusion for an audit is expressed as a positive expression of opinion and provides a high level of assurance. The conclusion for a review is expressed as a statement of negative assurance and provides only a moderate level of assurance.

Discuss Findings with Management: Bank's management is responsible for deciding the appropriate action to be taken in response to reported observations and recommendations. IS Auditors are responsible for assessing such management action for appropriateness and the timely resolution of the matters reported as observations and recommendations.

Senior Management may decide to accept the risk of not correcting the reported condition because of cost or other considerations. The Board (or the Audit Committee, if one exists) should be informed of Senior Management's decision on significant observations and recommendations. When Auditors IS believes that an organisation has accepted a level of residual risk that is inappropriate for the organisation, they should discuss the matter with Internal Audit and Senior Management. If the IS Auditors are not in agreement with the decision, regarding residual risk, IS Auditors and Senior Management should report the matter to the Board, or Audit Committee, for resolution.

Events sometimes occur, subsequent to the point in time or period of time of the subject matter being tested, but prior to the date of the IS Auditor's report, that have a material effect on the subject matter and therefore require adjustment or disclosure in the presentation of the subject matter or assertion.

(c) Finalise and Submit Reports

IS Auditors should review and assess the conclusions drawn from the evidence obtained as the basis for forming an opinion on the effectiveness of the control procedures based on the identified criteria.

Major findings identified during an audit should have a definite time line indicated for remedial actions, these should be followed up intensively and compliance should be confirmed.

An IS Auditor's report about the effectiveness of control procedures should cover aspects like:

- Description of the scope of the audit, including:
 - Identification or description of the area of activity
 - Criteria used as a basis for the IS Auditor's conclusion
 - A statement that the maintenance of an effective internal control structure, including control procedures for the area of activity, is the responsibility of management
- A statement that IS Auditors have conducted the engagement to express an opinion on the effectiveness of control

(d) Review Action Taken Report

After reporting of findings and recommendations, IS Auditors should request and evaluate relevant information to conclude whether appropriate action has been taken by management in a timely manner. If management's proposed actions to implement reported recommendations have been discussed with, or provided to, the IS Auditor, these actions should be recorded as a management response in the final report. The nature, timing and extent of the follow-up activities should take into account the significance of the reported finding and the impact if corrective action is not taken. The timing of IS Audit follow-up activities in relation to the original reporting should be a matter of professional judgment dependent on a number of considerations, such as the nature or magnitude of associated risks and costs to the entity.

(e) Follow-up Procedures

Procedures for follow-up activities should be established which includes:

- The recording of a time frame within which management should respond to agreed-upon recommendations
- An evaluation of management's response
- A verification of the response, if thought appropriate
- Follow-up work, if thought appropriate
- A communications procedure that escalates outstanding and unsatisfactory responses/ actions to the appropriate levels of management
- A process for providing reasonable assurance of management's assumption of associated risks, in the event that remedial action is delayed or not proposed to be implemented

- An automated tracking system or database can assist in the carrying out of follow-up activities.

(f) Update Audit Summary Memorandum

An audit summary memorandum should be prepared and addresses the following:

- Conclusion about specific risk
- Changes in the bank, its environment and banking industry that come to the attention after the completion of the audit planning memorandum and that caused to change audit plan – Conclusion regarding the appropriateness of the going concern assumption and the effect, if any, on financial statements
- The result of subsequent reviews and conclusion regarding the effect of subsequent events on financial statements
- Conclusion reached in evaluation of misstatements, including disclosure deficiencies
- If contradiction or inconsistency with final conclusion regarding a significant matter is observed, there should be proper documentation of addressing the inconsistency – Conclusion of whether the audit procedures performed and the audit evidence obtained were appropriate and consistent to support the audit conclusion

(g) Archival of Documents

Banks are recommended to have an archiving/ retention policy to archive the audit results.

Banks to have an archiving policy that:

- Ensures integrity of the data
- Defines appropriate access rights
- Decides on the appropriate archiving media
- Ensures ease of recovery

Quality Review

This section is aimed at emphasising quality of work of IS Auditors, while performing duties as an auditor. Appropriate levels in IS Audit function are recommended to assess audit quality by reviewing documentation, ensuring appropriate supervision of IS Audit members and assessing whether IS Audit members have taken due care while performing their duties. This will bring efficiency, control and improve quality of the IS Audit.

Evidences and Documentation

IS Auditors may perform the following progressive reviews of the evidences and documentation:

- A detailed review of each working paper prepared by a less-experienced member of the IS Audit team, by a more experienced member, who did not participate in the preparation of such working paper
- A primary review of the evidences and documentation by the Manager or IS Audit Head. Where the manager performs a primary review, this does not require that each working paper be reviewed in detail by the manager, as each working paper has already been reviewed in detail by the person who performed the detailed review.
- An overriding review of the working papers by the CAE, as needed

Supervision

IS Audit staff should be supervised to provide reasonable assurance that audit objectives are accomplished and applicable professional auditing standards are met.

Due Care

The standard of “due care” is that level of diligence which a prudent and competent person would exercise under a given set of circumstances. “Due professional care” applies to an individual who professes to exercise a special skill such as IS auditing. Due professional care requires the individual to exercise that skill to a level commonly possessed by auditors with the specialty.

Due professional care applies to the exercise of professional judgment in the conduct of work performed. It implies that the professional approaches matters requiring professional judgment with proper diligence. Despite the exercise of due professional care and professional judgment, situations may arise where an incorrect conclusion may be drawn from a diligent review of the available facts and circumstances. Therefore, the subsequent discovery of incorrect conclusions does not, in and of itself, indicate inadequate professional judgment or lack of diligence on the part of the IS Auditor.

Due professional care should extend to every aspect of the audit, including the evaluation of audit risk, the formulation of audit objectives, the establishment of the audit scope, the selection of audit tests, and the evaluation of test results.

In doing this, IS Auditors should determine or evaluate:

Type and level of audit resources required to meet audit objectives

Significance of identified risks and the potential effect of such risks on the audit

Audit evidence gathered

Competence, integrity and conclusions of others upon whose work IS Auditors places reliance

Intended recipients of audit reports have an appropriate expectation that IS Auditors have exercised due professional care throughout the course of the audit. IS Auditors should not accept an assignment unless adequate skills, knowledge, and other resources are available to complete the work in a manner expected of a professional. IS Auditors should conduct the audit with diligence while adhering to professional standards. IS Auditors should disclose the circumstances of any non-compliance with professional standards in a manner consistent with the communication of the audit results.

Independent Assurance of the Audit function

With a view to provide assurance to bank's management and regulators, banks are required to conduct a quality assurance, at least once in three years, on the bank's Internal Audit, including IS Audit function, to validate approach and practices adopted by them in the discharge of its responsibilities as laid out in the Audit Policy.

Objectives of performing a quality assessment are:

- Assess efficiency and effectiveness of an Internal Audit for current and future business goals
- Determine value addition from Internal Audit to the business units
- Benchmark, identify and recommend, successful practices of Internal Audit
- Assess compliance to standards for professional practice of Internal Audit

Others:

As a matter of prudence, banks should rotate IS Auditors in a specific area on periodic basis,

An information system (IS) audit or information technology(IT) audit is an examination of the controls within an entity's Information technology infrastructure. These reviews may be performed in conjunction with a financial statement audit, internal audit, or other form of attestation engagement. It is the process of collecting and evaluating evidence of an organization's information systems, practices, and operations. Obtained evidence evaluation can ensure whether the organization's information systems safeguard assets, maintains data integrity, and are operating effectively and efficiently to achieve the organization's goals or objectives.

An IS audit is not entirely similar to a financial statement audit. An evaluation of internal controls may or may not take place in an IS audit. Reliance on internal controls is a unique characteristic of a financial audit. An evaluation of internal controls is necessary in a financial audit, in order to allow the auditor to place reliance on the internal controls, and therefore, substantially reduce the amount of testing necessary to form an opinion regarding the financial statements of the company. An IS audit, on the other hand, tends to focus on determining risks that are relevant to information assets, and in assessing controls in order to reduce or mitigate these risks. An IT audit may take the form of a "general control review" or an "specific control review". Regarding the protection of information assets, one purpose of an IS audit is to review and evaluate an organization's information system's availability, confidentiality, and integrity by answering the following questions:

1. Will the organization's computerized systems be available for the business at all times when required? (Availability)
2. Will the information in the systems be disclosed only to authorized users? (Confidentiality)
3. Will the information provided by the system always be accurate, reliable, and timely? (Integrity).

The performance of an IS Audit covers several facets of the financial and organizational functions of our Clients. The diagram to the right gives you an overview of the Information Systems Audit flow: From Financial Statements to the Control Environment and Information Systems Platforms.

Information Systems Audit Methodology

Our methodology has been developed in accordance with International Information Systems Audit Standards e.g ISACA Information Systems Audit Standards and Guidelines and the Sabarne Oxley COSO Standard. The beginning point of this methodology is to carry out planning activities that are geared towards integrating a Risk Based Audit Approach to the IS Audit.

PHASE 1: Audit Planning

In this phase we plan the information system coverage to comply with the audit objectives specified by the Client and ensure compliance to all Laws and Professional Standards. The first thing is to obtain an Audit Charter from the Client detailing the purpose of the audit, the management responsibility, authority and accountability of the Information Systems Audit function as follows:

1. **Responsibility:** The Audit Charter should define the mission, aims, goals and objectives of the Information System Audit. At this stage we also define the Key Performance Indicators and an Audit Evaluation process;
2. **Authority:** The Audit Charter should clearly specify the Authority assigned to the Information Systems Auditors with relation to the Risk Assessment work that will be carried out, right to access the Client's information, the scope and/or limitations to the scope, the Client's functions to be audited and the auditee expectations; and
3. **Accountability:** The Audit Charter should clearly define reporting lines, appraisals, assessment of compliance and agreed actions.

The Audit Charter should be approved and agreed upon by an appropriate level within the Client's Organization.

See Template for an Audit Charter/ Engagement Letter [here](#).

In addition to the Audit Charter, we should be able to obtain a written representation ("Letter of Representation") from the Client's Management acknowledging:

1. Their responsibility for the design and implementation of the Internal Control Systems affecting the IT Systems and processes
2. Their willingness to disclose to the Information Systems Auditor their knowledge of irregularities and/or illegal acts affecting their organisation pertaining to management and employees with significant roles within the internal audit department.
3. Their willingness to disclose to the IS Auditor the results of any risk assessment that a material misstatement may have occurred

See a Template for a Letter of Representation [here](#).

PHASE 2 – Risk Assessment and Business Process Analysis

Risk is the possibility of an act or event occurring that would have an adverse effect on the organisation and its information systems. Risk can also be the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss of, or damage to, the assets. It is ordinarily measured by a combination of effect and likelihood of occurrence.

More and more organisations are moving to a risk-based audit approach that can be adapted to develop and improve the continuous audit process. This approach is used to assess risk and to assist an IS auditor's decision to do either compliance testing or substantive testing. In a risk based audit approach, IS auditors are not just relying on risk. They are also relying on internal and operational controls as well as knowledge of the organisation. This type of risk assessment decision can help relate the cost/benefit analysis of the control to the known risk, allowing practical choices.

The process of quantifying risk is called Risk Assessment. Risk Assessment is useful in making decisions such as:

1. The area/business function to be audited
2. The nature, extent and timing of audit procedures
3. The amount of resources to be allocated to an audit

The following types of risks should be considered:

Inherent Risk: Inherent risk is the susceptibility of an audit area to error which could be material, individually or in combination with other errors, assuming that there were no related internal controls. In assessing the inherent risk, the IS auditor should consider both pervasive and detailed IS controls. This does not apply to circumstances where the IS auditor's assignment is related to pervasive IS controls only. A pervasive IS Control are general controls which are designed to manage and monitor the IS environment and which therefore affect all IS-related activities. Some of the pervasive IS Controls that an auditor may consider include:

- The integrity of IS management and IS management experience and knowledge
- Changes in IS management

- Pressures on IS management which may predispose them to conceal or misstate information (e.g. large business-critical project over-runs, and hacker activity)
- The nature of the organisation's business and systems (e.g., the plans for electronic commerce, the complexity of the systems, and the lack of integrated systems)
- Factors affecting the organisation's industry as a whole (e.g., changes in technology, and IS staff availability)
- The level of third party influence on the control of the systems being audited (e.g., because of supply chain integration, outsourced IS processes, joint business ventures, and direct access by customers)
- Findings from and date of previous audits

A detailed IS control is a control over acquisition, implementation, delivery and support of IS systems and services. The IS auditor should consider, to the level appropriate for the audit area in question:

- The findings from and date of previous audits in this area
- The complexity of the systems involved
- The level of manual intervention required
- The susceptibility to loss or misappropriation of the assets controlled by the system (e.g., inventory, and payroll)
- The likelihood of activity peaks at certain times in the audit period
- Activities outside the day-to-day routine of IS processing (e.g., the use of operating system utilities to amend data)
- The integrity, experience and skills of the management and staff involved in applying the IS controls

Control Risk: Control risk is the risk that an error which could occur in an audit area, and which could be material, individually or in combination with other errors, will not be prevented or detected and corrected on a timely basis by the internal control system. For example, the control risk associated with manual reviews of computer logs can be high because activities requiring investigation are often easily missed owing to the volume of logged information. The control risk associated with computerised data validation procedures is ordinarily low because the processes are consistently applied. The IS auditor should assess the control risk as high unless relevant internal controls are:

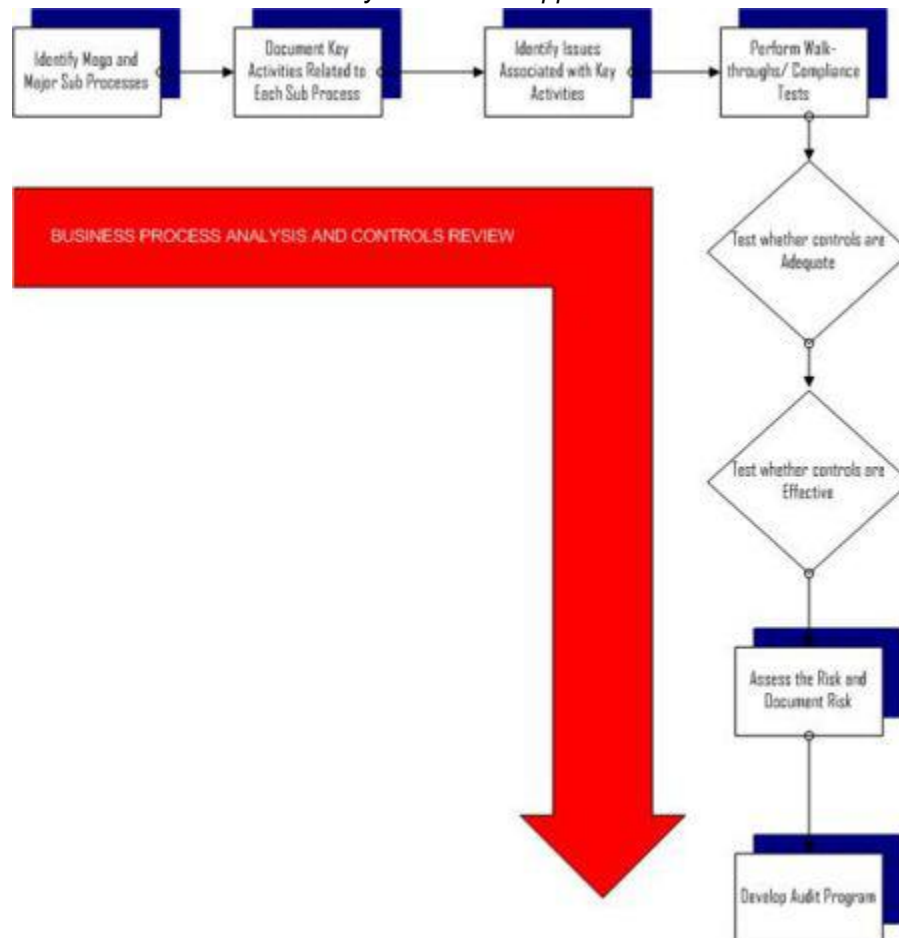
- Identified
- Evaluated as effective
- Tested and proved to be operating appropriately

Detection Risk: Detection risk is the risk that the IS auditor's substantive procedures will not detect an error which could be material, individually or in combination with other errors. In determining the level of substantive testing required, the IS auditor should consider both:

- The assessment of inherent risk
- The conclusion reached on control risk following compliance testing

The higher the assessment of inherent and control risk the more audit evidence the IS auditor should normally obtain from the performance of substantive audit procedures.

Our Risk Based Information Systems Audit Approach



A risk based approach to an Information Systems Audit will enable us to develop an overall and effective IS Audit plan which will consider all the potential weaknesses and /or absence of Controls and determine whether this could lead to a significant deficiency or material weakness.

In order to perform an effective Risk Assessment, we will need to understand the Client's Business Environment and Operations. Usually the first phase in carrying out a Risk Based IS Audit is to obtain an understanding of the Audit Universe. In understanding the Audit Universe we perform the following:

- Identify areas where the risk is unacceptably high

- Identify critical control systems that address high inherent risks
- Assess the uncertainty that exists in relation to the critical control systems

In carrying out the Business Process Analysis we:

- Obtain an understanding of the Client Business Processes
- Map the Internal Control Environment
- Identify areas of Control Weaknesses

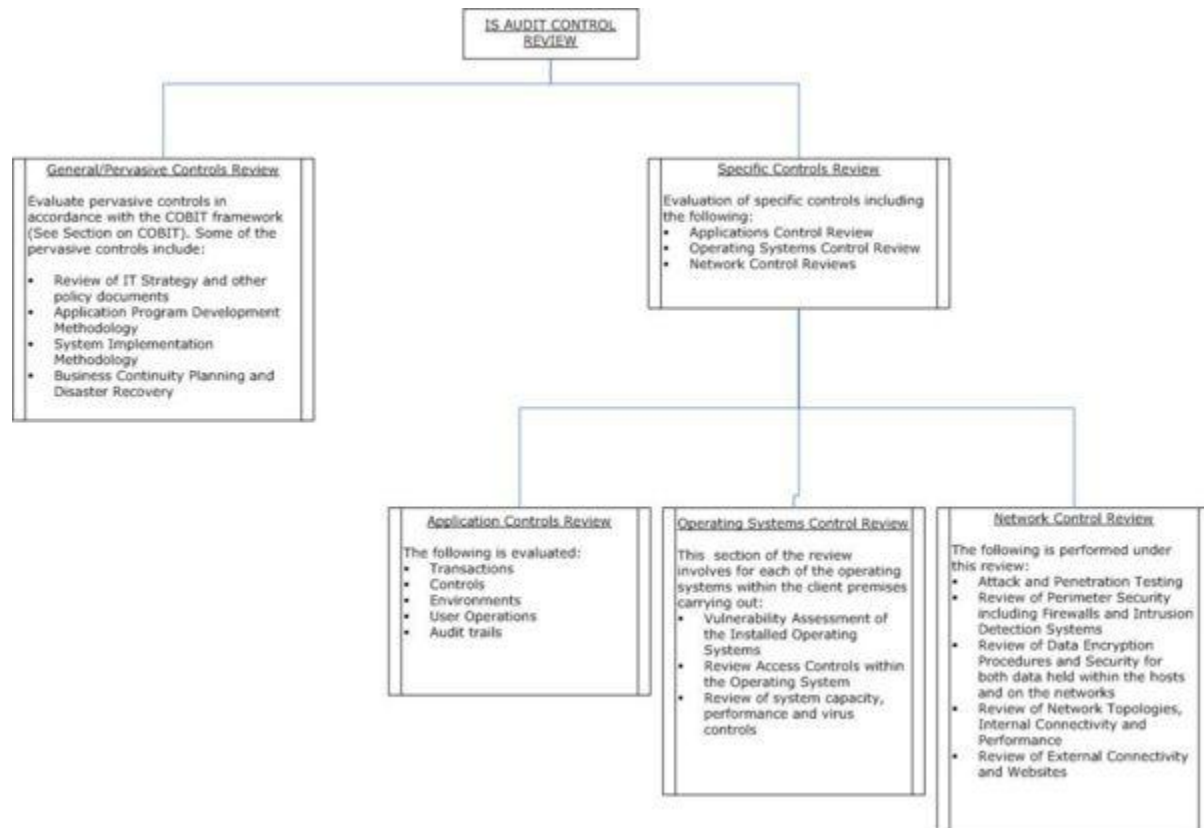
The Chat to the right summarises the business process analysis phase.

The template xxx will provide you with a guideline to document an Organisations Business Sub Processes identified during the risk analysis phase. For each of the sub-processes, we identify a list of What Could Go Wrong (WCGW). This WCGW represent the threat existing on a particular process. A single process would have multiple WCGW's. For each of the WCGW's identified in the prior phase we will determine the Key Activities within that process. For each Key Activity:

1. We will identify the Information Systems Controls
2. For each of the Controls Identified, we would rate the impact/effect of the lack of that control (on a rating of 1 - 5, with 5 indicating the highest impact), we will then determine the likelihood of the threat occurring(also on a rating of 1 - 5 with 5 representing the highest likelihood).

<< Outline specific risk assessment methodology here>>

PHASE 3 – Performance of Audit Work



In the performance of Audit Work the Information Systems Audit Standards require us to provide supervision, gather audit evidence and document our audit work. We achieve this objective through:

- Establishing an Internal Review Process where the work of one person is reviewed by another, preferably a more senior person.
- We obtain sufficient, reliable and relevant evidence to be obtained through Inspection, Observation, Inquiry, Confirmation and recomputation of calculations
- We document our work by describing audit work done and audit evidence gathered to support the auditors' findings.

Based on our risk assessment and upon the identification of the risky areas, we move ahead to develop an Audit Plan and Audit Program. The Audit Plan will detail the nature, objectives, timing and the extent of the resources required in the audit.

See Template for a Sample Audit Plan.

Based on the compliance testing carried out in the prior phase, we develop an audit program detailing the nature, timing and extent of the audit procedures. In the Audit Plan various Control Tests and Reviews can be done. They are sub-divided into:

1. General/ Pervasive Controls
2. Specific Controls

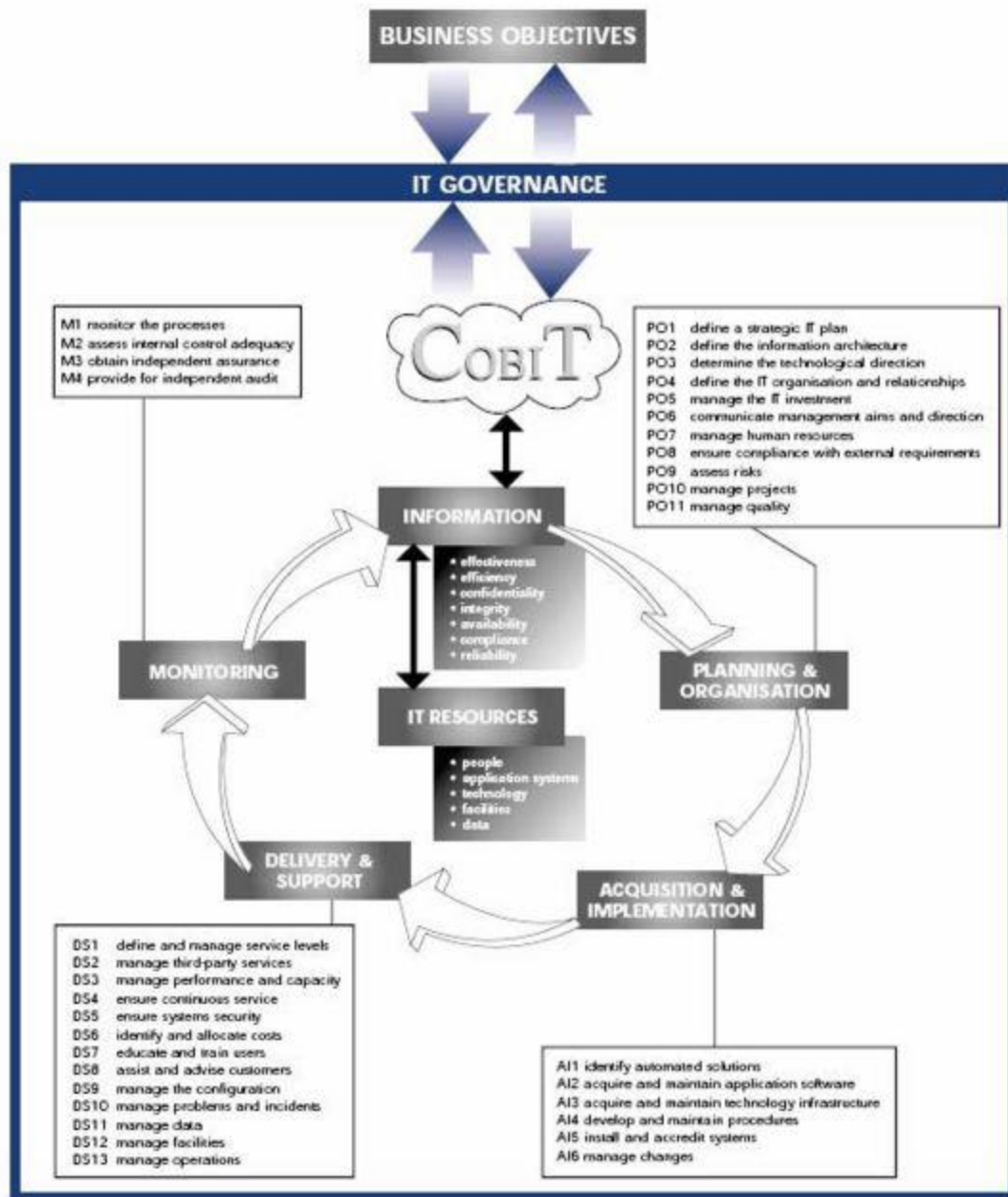
The Chart below to the left shows the Control Review Tests that can be performed in the two Control Tests above.

Control Objectives for Information and related Technology (COBIT)

The Control Objectives for Information and related Technology (COBIT) is a set of best practices (framework) for information (IT) management created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1992.

COBIT provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control in a company.

COBIT IT PROCESSES DEFINED WITHIN THE FOUR DOMAINS



COBIT helps meet the multiple needs of management by bridging the gaps between business risks, control needs and technical issues. It provides a best practices framework for managing IT resources and presents management control activities in a manageable and logical structure. This framework will help optimise technology information investments and will provide a suitable benchmark measure.

The Framework comprises a set of 34 high-level Control Objectives, one for each of the IT processes listed in the framework. These are then grouped into four domains: planning and organisation, acquisition and implementation, delivery and support, and monitoring. This structure covers all aspects of information processing and storage and the technology that supports it. By addressing these 34 high-level control objectives, we will ensure that an adequate control system is provided for the IT environment. A diagrammatic representation of the framework is shown below.

We shall apply the COBIT framework in planning, executing and reporting the results of the audit. This will enable us to review the General Controls Associated with IT Governance Issues. Our review shall cover the following domains;

- Planning and organisation of information resources;
- The planning and acquisition of systems and path in stage growth model of information systems;
- The delivery and support of the IS/IT including facilities, operations, utilisation and access;
- Monitoring of the processes surrounding the information systems;
- The level of effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability associated with the information held in; and
- The level of utilisation of IT resources available within the environment of the IS including people, the application systems of interface, technology, facilities and data.

The above control objectives will be matched with the business control objectives to apply specific audit procedures that will provide information on the controls built in the application, indicating areas of improvement that we need to focus on achieving.

Application Control Review

An Application Control Review will provide management with reasonable assurance that transactions are processed as intended and the information from the system is accurate, complete and timely. An Application Controls review will check whether:

- Controls effectiveness and efficiency
- Applications Security
- Whether the application performs as expected

A Review of the Application Controls will cover an evaluation of a transaction life cycle from Data origination, preparation, input, transmission, processing and output as follows:

1. Data Origination controls are controls established to prepare and authorize data to be entered into an application. The evaluation will involve a review of source document design and storage, User procedures and manuals, Special purpose forms, Transaction ID codes, Cross

reference indices and Alternate documents where applicable. It will also involve a review of the authorization procedures and separation of duties in the data capture process.

2. Input preparation controls are controls relating to Transaction numbering, Batch serial numbering, Processing, Logs analysis and a review of transmittal and turnaround documents
3. Transmission controls involve batch proofing and balancing, Processing schedules, Review of Error messages, corrections monitoring and transaction security
4. Processing controls ensure the integrity of the data as it undergoes the processing phase including Relational Database Controls, Data Storage and Retrieval
5. Output controls procedures involve procedures relating to report distribution, reconciliation, output error processing, records retention.

The use of Computer Aided Audit Techniques (CAATS) in the performance of an IS Audit

The Information Systems Audit Standards require us that during the course of an audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by the appropriate analysis and interpretation of this evidence. CAATs are useful in achieving this objective.

Computer Assisted Audit Techniques (CAATs) are important tools for the IS auditor in performing audits. They include many types of tools and techniques, such as generalized audit software, utility software, test data, application software tracing and mapping, and audit expert systems. For us, our CAATs include ACL Data Analysis Software and the Information Systems Audit Toolkit (ISAT).

CAATs may be used in performing various audit procedures including:

- Tests of details of transactions and balances (Substantive Tests)
- Analytical review procedures
- Compliance tests of IS general controls
- Compliance tests of IS application controls

CAATs may produce a large proportion of the audit evidence developed on IS audits and, as a result, the IS auditor should carefully plan for and exhibit due professional care in the use of CAATs. The major steps to be undertaken by the IS auditor in preparing for the application of the selected CAATs are:

- Set the audit objectives of the CAATs
- Determine the accessibility and availability of the organisation's IS facilities, programs/system and data
- Define the procedures to be undertaken (e.g., statistical sampling, recalculation, confirmation, etc.)

- Define output requirements
- Determine resource requirements, i.e., personnel, CAATs, processing environment (organisation's IS facilities or audit IS facilities)
- Obtain access to the clients's IS facilities, programs/system, and data, including file definitions
- Document CAATs to be used, including objectives, high-level flowcharts, and run instructions
- Make appropriate arrangements with the Auditee and ensure that:
 1. Data files, such as detailed transaction files are retained and made available before the onset of the audit.
 2. You have obtained sufficient rights to the client's IS facilities, programs/system, and data
 3. Tests have been properly scheduled to minimise the effect on the organisation's production environment.
 4. The effect that changes to the production programs/system have been properly considered.

See Template here for example tests that you can perform with ACL

PHASE 4: Reporting

Upon the performance of the audit test, the Information Systems Auditor is required to produce and appropriate report communicating the results of the IS Audit. An IS Audit report should:

1. Identify an organization, intended recipients and any restrictions on circulation
2. State the scope, objectives, period of coverage, nature, timing and the extend of the audit work
3. State findings, conclusions, recommendations and any reservations, qualifications and limitations
4. Provide audit evidence

The Information Systems (IS) audit group assesses the University's critical systems, technology architecture and processes to assure information assets are protected, reliable, available and compliant with University policies and procedures, as well as applicable laws and regulations. We emphasize the importance of mitigating security risks during our audit coverage of the University's application, operating

and networking systems. Through our integrated and IT governance audits, we evaluate information technology's impact on the University's processes and its abilities to achieve its goals and objectives. Our evaluations are objective and professional, utilizing COBIT (Control Objectives for Information and related Technology) framework, an international standard for good IT control practices.

ISA provides the following audit services:

- **IT Governance** - IT governance audits include reviews of the organization's fiduciary responsibility in satisfying the quality of IT delivery services while aligning with the business objectives and establishing an adequate system of internal controls.
- **Information Systems** - Information systems audits focus on security controls of physical and logical security of the server including change control, administration of server accounts, system logging and monitoring, incident handling, system backup and disaster recovery.
- **Integrated Audits** - Integrated audits include reviews of the business operations and their dependency of automated systems to support the business process. We consider information technology and financial and operational processes as mutually dependent for establishing an effective and efficient control environment. From the technology perspective, the audit focuses on application controls, administration of user access, application change control and backup and recovery to assure reliability, integrity and availability of the data.
- **Control Self-assessments** - Control Self-assessments are designed for department that manages and operates a technology environment. These self-assessment tools can be used to identify potential areas of control weakness in the management of the technology environment.

Compliance - Compliance audits include University policies and procedures, Payment Card Industry (PCI), the Health Insurance Portability and Accountability Act (HIPAA), Family Education Rights and Privacy Act (FERPA) and any other applicable laws and regulations

IT & LEGAL ISSUES

Introduction

Basel Committee on Banking Supervision, in its "Consultative Document on Operational Risk", defines "operational risk" as the risk of direct, or indirect, loss resulting from inadequate or failed internal processes, people and systems, or from external events. This definition includes legal risk¹.

The Information Technology Act, 2000 (IT Act, 2000) was enacted to handle certain issues relating to Information Technology. The IT Amendment Act, 2008 has made further modifications to address more issues such as cyber crimes. It is critical that impact of cyber laws is taken into consideration by banks to obviate any risk arising there from.

A. Guidance for Banks

Roles and Responsibilities and Organizational Structure

Board: The Risk Management Committee at the Board-level needs to put in place, the processes to ensure that legal risks arising from cyber laws are identified and addressed. It also needs to ensure that the concerned functions are adequately staffed and that the human resources are trained to carry out the relevant tasks in this regard

Operational Risk Group: This group needs to incorporate legal risks as part of operational risk framework and take steps to mitigate the risks involved in consultation with its legal functions within the bank.

Legal Department: The legal function within the bank needs to advise the business groups on the legal issues arising out of use of Information Technology with respect to the legal risk identified and referred to it by the Operational Risk Group.

Computer related offences and Penalty/Punishment

The IT Act, 2000 as amended, exposes the banks to both civil² and criminal³ liability. The civil liability could consist of exposure to pay damages by way of compensation upto ₹ 5 crore under the amended Information Technology Act before the Adjudicating Officer and beyond ₹ five crore in a court of competent jurisdiction. There could also be exposure to criminal liability to the top management of the banks given the provisions of Chapter XI of the amended IT Act⁴ and the exposure to criminal liability could consist of imprisonment for a term which could extend from three years to life imprisonment as also fine. Further, various computer related offences are enumerated in the aforesaid provisions.

Critical aspects

Legal risk and operational risk are same. Most risks are sought to be covered by documentation, particularly where the law is silent. The Basel-II accord

<http://www.bis.org/publ/bcbsca07.pdf>

Sections 43-45

Sections 65-74

covers “legal risk” under “operational risk.” Documentation forms an important part of the banking and financial sector. For many, documentation is a panacea to the legal risks that may arise in banking activities. But then, it has also been realized and widely acknowledged that loopholes do exist in documentation.

Legal risks need to be incorporated as part of operational risks and the position need to be periodically communicated to the top management and Board/Risk Management Committee of the Board.

As the law on data protection and privacy, in the Indian context are in an evolving stage, banks have to keep in view the specific provisions of IT Act, 2000 (as amended in 2008), various judicial and quasi judicial pronouncements and related developments in the Cyber laws in India as part of legal risk mitigation measures. Banks are also required to keep abreast of latest developments in the IT Act, 2000 and the rules, regulations, notifications and orders issued there under pertaining to bank transactions and emerging legal standards on digital signature, electronic signature, data protection, cheque truncation, electronic fund transfer etc. as part of overall operational risk management process.

The Information Technology (Amendment) Act, 2008

The main Indian act that addresses legal challenges specifically as they relate to the Internet is the Information Technology (Amendment) Act, 2008, or for short, the IT Act. We highlight the sections that have the greatest relevance for the Internet and democracy. This includes sections relating to government takedowns, monitoring and interception of communication and intermediary liability.

[Section 69A and the Blocking Rules: Allowing the Government to block content under certain circumstances](#)

Section 69A of the IT (Amendment) Act, 2008, allows the Central Government to block content where it believes that this content threatens the security of the State; the sovereignty, integrity or defence of India; friendly relations with foreign States; public order; or to prevent incitement for the commission of a cognisable offence relating to any of the above. A set of procedures and safeguards to which the Government has to adhere when doing so have been laid down in what have become known as the Blocking Rules.

- [Section 79 and the IT Rules: Privatising censorship in India](#)

Section 79 of the Information Technology (Amendment) Act, 2008 regulates the liability of a wide range of intermediaries in India. The section came in the limelight mostly because of the infamous Intermediary Guidelines Rules, or IT Rules, which were made under it. The IT Rules constitute an important and worrying move towards the privatisation of censorship in India.

- [Sections 67 and 67A: No nudity, please](#)

The large amounts of 'obscene' material that circulate on the Internet have long attracted comment in India. Not surprisingly, then, in the same way as obscenity is prohibited offline in the country, so it is online as well. The most important tools to curtail it are sections 67 and 67A of the IT Act, prohibiting obscene and sexually explicit material respectively.

- Section 66A: Do not send offensive messages

Section 66A of the Information Technology (Amendment) Act, 2008 prohibits the sending of offensive messages through a communication device (i.e. through an online medium). The types of information this covers are offensive messages of a menacing character, or a message that the sender knows to be false but is sent for the purpose of 'causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will.' If you're booked under Section 66A, you could face up to 3 years of imprisonment along with a fine.

- Freedom of expression

To balance freedom of expression with other human rights is, at times, a difficult and delicate task. From hate speech to intermediary liability, we tease out and shed greater light on the various challenges that make this task particularly complicated, proposing ways forward that can further strengthen and promote the right to freedom of expression, in India and beyond, as well.

- Cyber security, surveillance and human rights

With the advent of new technology, new security threats have emerged for people, businesses and states. Oftentimes, responses to such threats, including states' exercise of their unprecedented power to surveil their populations, have been criticised for their negative impact on human rights. Can security and human rights no longer be reconciled in the Internet age?

The Information Technology (Amendment) Act, 2008 an act to amend the IT Act 2000 received the assent of the President on 5th February 2009. Several legal & security experts are in the process of analyzing the contents and possible impacts of the amendments. The objective of this note is to try and study the possible implications and impacts on Indian companies. This note is not intended to be a comprehensive analysis of the amendments, but only certain key points which could impact Indian Companies

Data Protection

The IT Act 2000 did not have any specific reference to Data Protection, the closest being a provision to treat data vandalism as an offense. The Government introduced a separate bill called "Personal Data Protection Act 2006" which is pending in the Parliament and is likely to lapse. The ITA 2008 has introduced two sections which address Data Protection aspects to an extent, which gives rise to certain key considerations for the sector.

The sections under consideration are:

Section 43A: Compensation for failure to protect data

Section 72A: Punishment for disclosure of information in breach of lawful contract

Section 43A states

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any

person, such body corporate shall be liable to pay damages by way of compensation, to the person so affected.

By way of explanation: "Body corporate means Indian companies"

"Reasonable security practices mean a mutual contract between the customer and service provider OR as per the specified law. In absence of both then as specified by the Central Government

Hence it would be important for Indian companies to seriously look at SLA's and agreements which have been signed with clients to understand the data protection implications. The same goes for understanding the applicable laws.

A major modification is that this clause doesn't mention the compensation limit of Rs. 1 Crore which was there as part of section 43 of the ITA 2000. This implies that there is no upper limit for damages that can be claimed. This essentially is "unlimited liability" for Indian companies, which could cause serious business implications.

Section 72A:

Under this section disclosure without consent exposes a person including an "intermediary" to three years imprisonment or fine upto Rs. Five lacs or both.

This section uses the term "personal information" and not "sensitive personal information" as in section 43A. Hence it could apply to any information which is obtained in order to deliver services. Hence in some ways broadens the definition of information.

2. Information Preservation

Across the amendments there are several references to "service providers" or "intermediaries", which in some form would apply to all Indian companies.

e.g. Section 67C: Preservation and Retention of information by intermediaries.

Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe". Any intermediary who intentionally or knowingly contravenes the provisions shall be punished with an imprisonment for a term which may extend to 3 years and shall also be liable to fine.

The notifications on time for preservation etc. are not yet released. However since this is a "cognizable" offense any police inspector can start investigations against the CEO of a company.

Apart from the two aspects discussed in this note, there are other areas which could also be considerations for E.g.

Sec 69: Power to issue directions for interception or monitoring or decryption of any information through any computer resource.

Sec 69B: Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security.etc.

In summary, IT Risk management and response needs to be looked at by all companies for various reasons including customer assurance, compliance, customer regulations, protection of information assets etc. The ITA 2008 amendments provide us with few additional factors for considerations which could have significant impact on business. Information technology regulations and laws would only get more stringent and defined; hence it's imperative for organizations to be aware and prepared.

PILLARS OF INFORMATION SECURITY

Security is a constant worry when it comes to information technology. Data theft, hacking, malware and a host of other threats are enough to keep any IT professional up at night.

Information security follows three overarching principles:

- Confidentiality: This means that information is only being seen or used by people who are authorized to access it.
- Integrity: This means that any changes to the information by an unauthorized user are impossible (or at least detected), and changes by authorized users are tracked.
- Availability: This means that the information is accessible when authorized users need it.

Information Assurance (IA) refers to the steps involved in protecting information systems, like computer systems and networks. There are commonly five terms associated with the definition of information assurance:

- Integrity
- Availability
- Authentication
- Confidentiality
- Nonrepudiation



IA is a field in and of itself. It can be thought of as a specialty of Information Technology (IT), because an IA specialist must have a thorough understanding of IT and how information systems work and are

interconnected. With all of the threats that are now common in the IT world, such as viruses, worms, phishing attacks, social engineering, identity theft and more, a focus on protection against these threats is required. IA is that focus.

1. Confidentiality, in the context of computer systems, allows authorized users to access sensitive and protected data. Specific mechanisms ensure confidentiality and safeguard data from harmful intruders.

Confidentiality is one of the five pillars of Information Assurance (IA). The other four are authentication, availability, integrity and nonrepudiation.

Sensitive information or data should be disclosed to authorized users only. In IA, confidentiality is enforced in a classification system. For example, a U.S. government or military worker must obtain a certain clearance level, depending on a position's data requirements, such as, classified, secret or top secret. Those with secret clearances cannot access top secret information.

Best practices used to ensure confidentiality are as follows:

An authentication process, which ensures that authorized users are assigned confidential user identification and passwords. Another type of authentication is biometrics.

Role-based security methods may be employed to ensure user or viewer authorization. For example, data access levels may be assigned to specified department staff.

Access controls ensure that user actions remain within their roles. For example, if a user is authorized to read but not write data, defined system controls may be integrated.

1. Integrity, in the context of computer systems, refers to methods of ensuring that data is real, accurate and safeguarded from unauthorized user modification. Integrity is one of the five pillars of Information Assurance (IA). The other four are authentication, availability, confidentiality and nonrepudiation.

Data integrity maintenance is an information security requirement. Integrity is a major IA component because users must be able to trust information. Untrusted data is devoid of integrity. Stored data must remain unchanged within an information system (IS), as well as during data transport.

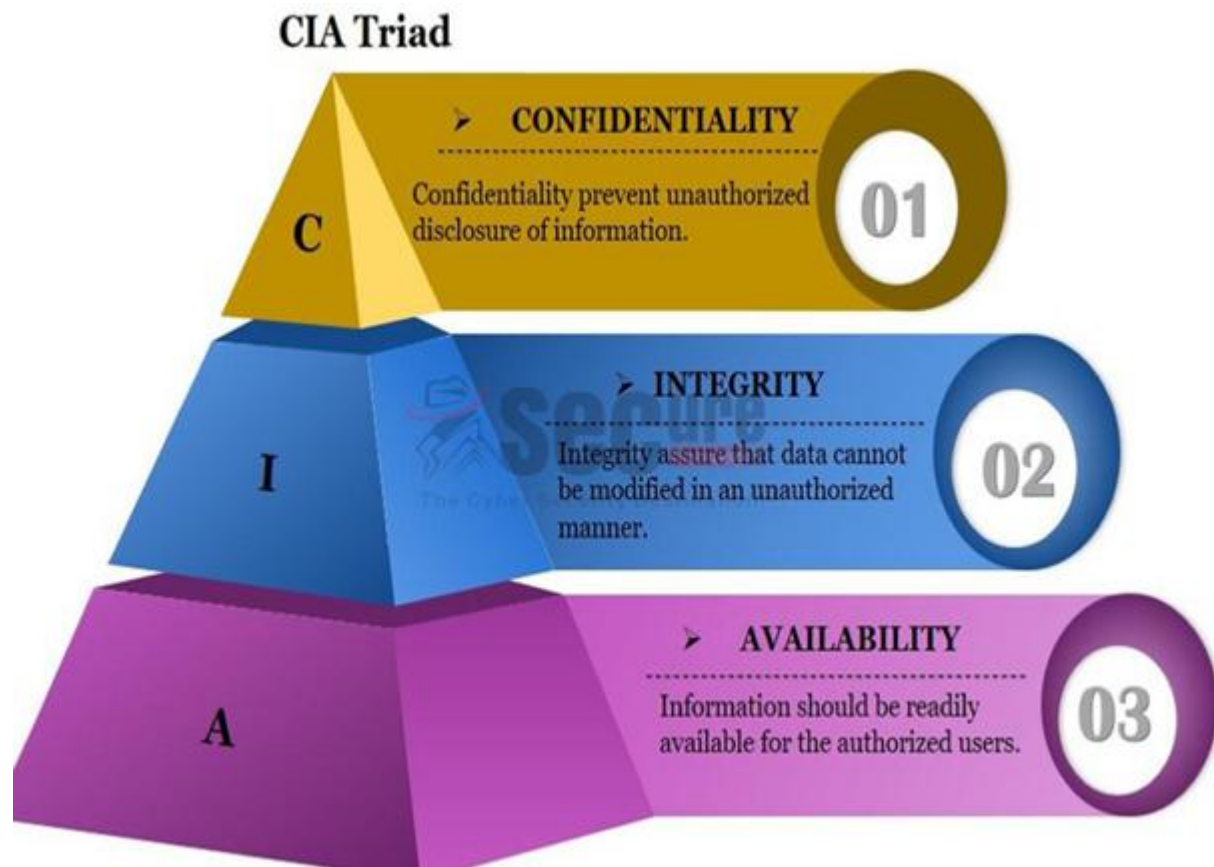
Events like storage erosion, error and intentional data or system damage can create data changes. For example, hackers may cause damage by infiltrating systems with malware, including Trojan horses, which overtake computer systems, as well as worms and viruses. An employee may create company damage through intentionally false data entry.

Data integrity verification measures include checksums and the use of data comparison

3. Availability, in the context of a computer system, refers to the ability of a user to access information or resources in a specified location and in the correct format. Availability is one of the five pillars of Information Assurance (IA). The other four are integrity, authentication, confidentiality and nonrepudiation.

When a system is regularly non-functioning, information availability is affected and significantly impacts users. In addition, when data is not secure and easily available, information security is affected, i.e., top secret security clearances. Another factor affecting availability is time. If a computer system cannot deliver information efficiently, then availability is compromised.

Data availability must be ensured by storage, which may be local or at an offsite facility. In the case of an offsite facility, an established business continuity plan should state the availability of this data when onsite data is not available. At all times, information must be available to those with clearance.



4 Nonrepudiation is a method of guaranteeing message transmission between parties via digital signature and/or encryption. It is one of the five pillars of information assurance (IA). The other four are availability, integrity, confidentiality and authentication.

Nonrepudiation is often used for digital contracts, signatures and email messages.

By using a data hash, proof of authentic identifying data and data origination can be obtained. Along with digital signatures, public keys can be a problem when it comes to nonrepudiation if the message recipient has exposed, either knowingly or unknowingly, their encrypted or secret key..

5. In the context of computer systems, authentication is a process that ensures and confirms a user's identity. Authentication is one of the five pillars of information assurance (IA). The other four are integrity, availability, confidentiality and nonrepudiation.

Authentication begins when a user tries to access information. First, the user must prove his access rights and identity. When logging into a computer, users commonly enter usernames and passwords for authentication purposes. This login combination, which must be assigned to each user, authenticates access. However, this type of authentication can be circumvented by hackers.

A better form of authentication, biometrics, depends on the user's presence and biological makeup (i.e., retina or fingerprints). This technology makes it more difficult for hackers to break into computer systems.

The Public Key Infrastructure (PKI) authentication method uses digital certificates to prove a user's identity. There are other authentication tools, too, such as key cards and USB tokens. One of the greatest authentication threats occurs with email, where authenticity is often difficult to verify. For example, unsecured emails often appear legitimate.



Physical Security

Physical security describes measures designed to ensure the physical protection of IT assets like facilities, equipment, personnel, resources and other properties from damage and unauthorized physical access. Physical security measures are taken in order to protect these assets from physical threats including theft, vandalism, fire and natural disasters

Physical security is often the first concern in facilities with high asset concentration, especially that used in critical systems for business processes. Physical security is especially important for IT resources, as their proper operation demands that the hardware assets and infrastructure they are running on be kept away from anything that could hinder their function. This includes tampering by unauthorized personnel and unforeseen events like accidents and natural disasters.



There are two phases of physical security:

- **Deterrence:** Methods and measures that are meant to deter attackers and intruders or prevent natural events and accidents from affecting protected assets. The simple method for this is through the use of physical barriers and signs. The signs serve as a warning to any intruder that their actions will bring physical harm or prosecution. The physical barriers are meant to prevent access entirely or simply to provide protection from external factors like storms or vehicular accidents.
- **Detection:** Allows security personnel to detect and locate potential intruders using surveillance equipment like cameras, motion sensors, security lights and personnel like security guards and watch dog

Physical security pertains to preventative measures used to halt intruders from physically accessing the location. Denoting physical or electronic equipment that protects tangible aspects of the site, physical security is effective in stopping unwanted trespassers or unauthorized visitors. Physical security solutions like visitor management protect unauthorized visitors. You can never be too safe in ensuring that those who enter are granted the proper permissions to do so. Unauthorized visitors could be looking to extract company data, do harm to employees, or even steal equipment such as computers and monitors. Physical security allows for established barriers wherever needed to ensure only those with clearance can enter. Additional physical security measures include:

- **Vaults** – Their sturdy construction provides boundless protection, whether it be for valuables or information such as documents and data storage drives. Vaults have the capabilities to withstand physical damages by potential intruders to keep the contents safe. Breaking into a vault is so difficult that it acts as a deterrent against possible theft.
- **CCTV** – Closed circuit television (CCTV) allows most any location throughout your facility to be monitored and recorded. Helpful in identifying those who break in while also discouraging would-be invaders, video surveillance and CCTV are effective, and some of the most common, physical security measures. CCTV also cuts down on security costs as it allows fewer people to monitor more of the facility as opposed to appointing guards to a post.
- **Alarms** – In the event of unauthorized entry, alarms signal the authorities and ensure proper responses are taken with the uninvited party. Alarms reduce staffing needs and increase response time by eliminating the need for physically having a person to contact law enforcement.

Logical Security

On the internet alone there are an estimated 1.2 million terabytes of data. With so much information available to anyone with internet access, our expansion digitally has caused the world to shrink due to our

interconnectedness. The resulting small world, however, doesn't denote that everything needs sharing. Logical Security refers to the safeguards in place to protect access to the data storage system itself. It is used once inside the work site and makes it difficult for those without certain permissions to gain access to systems in which they do not belong. If someone were to make it past the physical security, logical security ensures that they cannot get into computer systems without credentials to keep your network safe from intrusion.

Examples of effective logical security solutions include:

- **User Profiles** – Providing authorized individuals with accounts access to the system makes it easier to keep track of individuals accessing what and when. Shared networks monitor who modifies documents and records users logging in for reference later if fraud is suspected.
- **Passwords** – While employees have access to the premises, you still want to ensure security within your system. Passwords are the ideal way to prevent unwanted parties from getting in. Strong passwords prevent hackers from entering and disturbing the integrity of your data.
- **Biometrics** – Including retina scans, fingerprint analysis, and vocal recognition, biometrics uses physiology as a means of identification.

Corporate IT Security Policy

Significant technological advances have changed the way we do business. That is, the internet, email, and text messages have virtually replaced faxes, letters and telexes in the corporate world. The internet is used to obtain information and efficiently communicate with clients, business associates, and partners.

While internet usage comes with numerous advantages such as the speed of communication and an increase in the bottom line, it also contains several drawbacks that can seriously hinder business productivity and growth. For example, personnel can use the internet as a distraction to peruse their Facebook, Twitter, and Instagram accounts, shop on Amazon or eBay, check the latest sports statistics, exchange personal emails with colleagues, friends, and so on. These activities not only heighten the risk of incoming malware, but also lower employee productivity and revenue.

Therefore, devising a corporate IT security policy will help to mitigate the negative consequences associated with internet use – and email specifically.

The “nuts and bolts” of an IT security policy

I want to start by saying that a cookie-cutter approach to developing an IT security policy doesn't exist. Every organization varies in its business practices and protocols, so one IT security policy won't fit the needs of every organization. An IT security policy should be a customized document that accurately represents a specific business environment and specifically meets its needs. Don't model your IT security policy exactly on Google's or Apple's IT security policies because what works for them might not work for you.

An IT security policy is essentially a written strategy (plan) that covers the implementation of Information Security methods, technologies, and concepts. This policy offers overarching guidelines for company security procedures without precisely stating how the data will be protected. Some freedom is provided for IT managers to decide which electronic devices, software, and methods would be best to implement policy guidelines. An IT security policy shouldn't explicitly state which vendors and technologies should be utilized. The basic purpose is to establish ground rules and parameters used to then work out more specific data security practices.

The policy should encompass all of its mission-critical data and electronic systems – including the internet, email, computer networks, and so forth. Further, three vital points need to be considered when devising a corporate IT security policy:

- the confidentiality of sensitive mission-critical information
- the availability of this information
- the protection of information from destruction (think viruses, worms, Trojans), internal misuse and abuse.

The Top 3 Reasons for a Corporate IT Security Policy

An IT security policy provides a launching pad for further IT security procedures, a basis for consistent application, and a stable reference guide for IT security breaches when they do occur. Rather than throwing this policy on the shelf to collect dust, use it to ensure that your corporate data remains secure and exact appropriate penalties when it's not. Below are three additional ways that an IT security policy may prove beneficial:

1. **Corporate legal liability** – When an IT security policy explicitly states

- how and when to use email, the internet, electronic devices, and computer networks
- how sensitive corporate data should be handled
- and the correct use of passwords and encryption,

your threat of exposure to malware and confidential data leaks will decrease markedly.

Emails – personal and corporate – will inevitably make an organization vulnerable to (spear) phishing attacks, viruses, and other malicious software. Employees who exchange emails within or outside of the company may include racial and sexist jokes, sexually explicit content, and other material that may be deemed offensive by the recipients of these emails. This activity opens the company to massive legal liabilities if employees file lawsuits because they feel harassed or offended by these emails.

An IT security policy (and its enforcement) will weed out offenders and hold up as a tight defense in a court of law as the company can show that it did everything in its power to discourage offensive emails and resolve all related issues.

2. Third parties – When individuals and businesses (i.e. vendors, auditors, clients, investors, etc.) partner with you, they will probably want to know if you have an established IT security policy before they share their confidential information, such as bank statements, social security numbers, names, addresses, and other identity-specific information.

For example, a clearing corporation offers all manner of finance processing and programming services for insurance companies, banks, and even government agencies. Naturally they have a stringent IT security policy to ensure none of those financial records were ever subject to phishing attacks.

3. Compliance with Govt & local legislation – Finally, companies create IT security policies to meet the standards and regulations of government laws on the protection of electronic information.

On a slightly unrelated note, if your IT security policy contains a section on monitoring employee corporate and personal emails, clearly inform your employees that IT will monitor all inbound and outbound emails. If employees don't know that their emails are being monitored and then come under scrutiny for a suspicious email, they may file a lawsuit against the company for invasion of privacy.

To protect the company against this type of litigation, make them aware of your IT security and email policies through informational sessions and training. Doing so will place the responsibility of compliance on their shoulders and reduce the risk of unethical activity.

Most full IT security plans would include the following nine policy topics:

1. **Acceptable Use Policy**

Since inappropriate use of corporate systems exposes the company to risk, it is important to specify exactly what is permitted and what is prohibited. The purpose of this policy is to detail the acceptable use of corporate information technology resources for the protection of all parties involved.

The scope of this policy includes any and all use of corporate IT resources, including but not limited to, computer systems, email, the corporate network, and the corporate Internet connection.

For example, Annese's Acceptable Use policy outlines things like email use, confidentiality, social media and web browsing, personal use, and how to report security incidents. Your Acceptable Use Policy should be the one policy everyone in your organization acknowledges via signature that they have read and understand.

2. **Confidential Data Policy**

Confidential data is typically the data that holds the most value to a company. Often, confidential data is valuable to others as well, and thus can carry greater risk than general company data. For these reasons, it is good practice to dictate security standards that relate specifically to confidential data.

This policy would detail how confidential data should be handled, and examples of what your organization deems confidential.

3. Email Policy

Email is an essential component of business communication; however it does present challenges due to its potential to introduce security threats to the network. Email can also have an effect on the company's liability by providing a written record of communications. Your email policy would detail your organization's usage guidelines for the email system.

This policy will help the company reduce risk of an email-related security incident, foster good business communications both internally and externally, and provide for consistent and professional application of the company's email principles.

The scope of this policy includes the company's email system in its entirety, including desktop and/or web-based email applications, server-side applications, email relays, and associated hardware. It covers all electronic mail sent from the system, as well as any external email accounts accessed from the company network.

4. Mobile Device Policy

A more mobile workforce is a more flexible and productive workforce. For this reason, business use of mobile devices is growing, and as these devices become vital tools to conduct business, more and more sensitive data is stored on them, and thus the risk associated with their use is growing.

This policy covers any mobile device capable of coming into contact with your companies' data.

5. Incident Response Policy

A security incident can come take many forms: a malicious attacker gaining access to the network, a virus or other malware infecting computers, or even a stolen laptop containing confidential data. A well thought-out Incident Response Policy is critical to successful recovery from a data incident.

This policy covers all incidents that may affect the security and integrity of your company's information assets, and outlines steps to take in the event such an incident occurs.

6. Network Security Policy

Everyone needs a secure network infrastructure to protect the integrity of their corporate data and mitigate risk of a security incident. The purpose of a specific network infrastructure security policy is to establish the technical guidelines for IT security, and to communicate the controls necessary for a secure network infrastructure.

This policy might include specific procedures around device passwords, logs, firewalls, networked hardware, and/or security testing.

7. Password Policy

The easiest entry point to building your security policy, a password policy is the first step in enabling employees to safeguard your company from cyberattack. (Annese is sharing our own password policy as

part of the template to get you started here.)

Passwords are the front line of protection for user accounts. A poorly chosen password may result in the compromise of your organization's entire corporate network. This policy would apply to any person who is provided an account connected to your corporate network or systems, including: employees, guests, contractors, partners, vendors, etc.

8. Physical Security Policy

The purpose of this policy is to protect your company's physical information systems by setting standards for secure operations. In order to secure your company data, thought must be given to the security of the company's physical Information Technology (IT) resources to ensure that they are protected from standard risks.

This policy would apply to your organization's company-owned or company-provided network devices as well as any person working in or visiting a corporate office.

9. Wireless Network and Guest Access Policy

Every organization should have a wireless policy that would likely need to include your guest access requirements. Wireless access can be done securely if certain steps are taken to mitigate known risks.

Guest access to the company's network is often necessary for customers, consultants, or vendors who are visiting company offices. This may simply take the form of outbound Internet access, or the guest may require access to specific resources on the company's network. Therefore, guest access to the company's network must be tightly controlled.

This policy would outline steps the company wishes to take to secure its wireless infrastructure. These policies would cover anyone who accesses the network via a wireless connection, guest included.

Banking Sector

The **Reserve Bank of India** issued **new guidance** in April 2011 for banks to mitigate the risks of use of information technology in banking operations. RBI guidelines are result of the Working Group's recommendations on information security, electronic banking, technology risk management and cyber fraud. The Working Group was formed under the chairmanship of G. Gopalakrishna, the executive director of RBI in April 2010.

The guidance is largely driven by the need for mitigating cyber threats emerging from increasing adoption of IT by commercial banks in India.

Recommendations are made in nine broad areas, including-

1. **IT Governance:** emphasizes the IT risk management accountability on a bank's board of directors and executive management. Focus includes creating an organizational structure and process to ensure that a bank's IT security sustains and extends business strategies and objectives.

1. **Information Security:** maintaining a framework to guide the development of a comprehensive information security program, which includes forming a separate information security function to focus exclusively on information security and risk management, distinct from the activities of an information technology department. These guidelines specify that the chief information security officer needs to report directly to the head of risk management and should not have a direct reporting relationship with the chief information officer.
2. **IT Operations:** specialized organizational capabilities that provide value to customers, including IT service management, infrastructure management, application lifecycle management and IT operations risk framework.
3. **IT Services Outsourcing:** places the ultimate responsibility for outsourcing operations and management of inherent risk in such relationships on the board and senior management. Focus includes effective selection of service provider, monitoring and control of outsourced activities and risk evaluation and management.
4. **Information Security Audit:** the need for banks to re-assess IS audit processes and ensure that they provide an independent and objective view of the extent to which the risks are managed. This topic focuses on defining the roles and responsibilities of the IS audit stakeholders and planning and execution of the audit.
5. **Cyberfraud:** defines the need for an industry wide framework on fraud governance with particular emphasis on tackling electronic channel based frauds. Focus includes creating an organizational structure for fraud risk management and a special committee for monitoring large value fraud.
6. **Business Continuity Planning:** focuses on policies, standards and procedures to ensure continuity, resumption and recovery of critical business processes. Also, this topic emphasizes implementing a framework to minimize the operational, financial, legal, reputational and other material consequences arising from such a disaster.
7. **Customer Education:** the need to implement consumer awareness framework and programs on a variety of fraud related issues.
8. **Legal Issues:** defines the need to put effective processes in place to ensure that legal risks arising from cyber laws are identified and addressed at banks. It also focuses on board's consultation with legal department on steps to mitigate business risks within the bank.

Security Governance

Security governance is the means by which *you* control and direct *your* organisation's approach to security. When done well, security governance will effectively coordinate the security activities of your organisation. It enables the flow of security information and decisions around your organisation.

Just as security is the responsibility of everyone within an organisation, security decision making can happen at *all levels*. To achieve this, an organisation's senior leadership should use security governance to set out the kinds of security risks they are prepared for staff to take, and those they are not.

The IT security and governance function includes ensuring, establishing and enforcing security policies, standards and procedures. IT Security Managers continuously monitor all components of the IT infrastructure for compliance and security threats and take appropriate remedial action. They also conduct IT risk analysis and assessments and then make sure there are solutions in place to mitigate the risks. An established governance framework to manage all IT Governance, Risk, and Compliance (IT-GRC) related activities enable IT security professionals to manage IT governance, IT policy, IT risk, IT compliance, IT audit and incidents in an integrated manner.

Enterprise security governance is a company's strategy for reducing the risk of unauthorized access to information technology systems and data.

Enterprise security governance activities involve the development, institutionalization, assessment and improvement of an organization's enterprise risk management (ERM) and security policies. Governance of enterprise security includes determining how various business units, personnel, executives and staff should work together to protect an organization's digital assets, ensure data loss prevention and protect the organization's public reputation.

Enterprise security governance activities should be consistent with the organization's compliance requirements, culture and management policies. The development and sustainment of enterprise security governance often involves conducting threat, vulnerability and risk analyses tests that are specific to the company's industry.

Enterprise security governance is a company's strategy for reducing the chance that physical assets owned by the company can be stolen or damaged. In this context, governance of enterprise security includes physical barriers, locks, fencing and fire response systems as well as lighting, intrusion detection systems, alarms and cameras.

PHYSICAL AND ENVIRONMENTAL SECURITY

It is generally accepted that, when it comes to protecting information resources from a physical perspective (i.e. where we are protecting tangible assets that one can touch, kick, steal, drop, etc.), the name of the game has to be about convincing a perpetrator that the cost, time and risk of discovery involved in attempting unauthorised access to information or equipment exceeds the value of the gains thus made.

Physical security is not a modern phenomenon - it exists to deter or prevent unauthorised persons from entering a physical facility or stealing something of perceived value. The safety of personnel should not be overlooked in this respect.

Little has changed over the centuries when it comes to protecting property, with locked doors/chests, armed security guards, booby-traps, etc.

Physical security considerations (at all levels from corporate to personal) should include protection from burglary, theft, vandalism, view and, potentially, terrorism, depending upon your location and what you are into! The very best in software security isn't worth very much if somebody walks off with your computer under their arm!

Additionally, environmental threats include fire, flood, natural disasters and contamination from spilled food/drink.

The following gives a brief overview of some of the options available for physically securing and protecting your equipment and data.

Secure your computer equipment. (Preventive control)

This concept is, obviously, one of the easiest to understand in the world of IT security but achieving this can be daunting. Nevertheless, the fundamental issue is not so much protecting the intrinsic value of the computer but WHAT INFORMATION IS STORED ON THAT COMPUTER OR IS ACCESSIBLE FROM IT?

You can always buy new kit and probably with significantly enhanced performance than the one you had before – OK, the insurance no-claims discount might take a bit of a hit – but loss of a high-performance machine is but little compared to loss of the valued data upon it, or worse, compounded by loss of confidentiality of that data.

Loss of information, especially client information perhaps, can also lead to reputational damage, litigation, data recovery/re-creation costs ... you name it.

So, in your risk analysis (if you have one) for protecting information, stack the impact assessment against the data, not the machine.

Having said all that, there are sensible physical protection precautions you can take:

- Keep non-portable devices (PCs, printers) in lockable premises
- Keep portable devices (laptops, smart phones, tablets) always within your protective reach when on the move
- Lock portable equipment away in cupboards overnight – never leave it on view during silent hours.

- If you have precious information on the device, regularly back it up and store the backup media securely
- If possible, remove the hard drive and keep it separate from the device
- Definitely don't leave USB keys inserted for too long – they're so small nowadays you may forget they are there
- Use some form of endpoint encryption on your device that prevents data being exported
- If using a token authentication, keep the PC/device and token separately - don't write the token PIN down and keep it with the token
- Don't leave computing equipment in a car, locked or not – even if out of sight, this would be a major bonus to what would otherwise be a common car thief!
- Use reliable cable locks where other secure storage is unavailable.

Keep computing equipment away from environmental hazards. (Preventive control)

Computing equipment, especially mobile devices, are not just under threat from malicious intent – they suffer accidents from time to time, just like many of our items of property!

Some of the controls, like taking data backups, removing hard drives, encrypting data, etc. mentioned in the previous item, are also relevant here, but the following is worth mentioning:

- Always transport a laptop in a padded laptop bag or a smaller device (e.g. tablet or smart phone) in its protective casing - both will fare better if they get dropped.
- When travelling in a taxi, especially at night when the back of the cab is dark, or if having a snooze on a train, keep your arm or leg through the strap of your (preferably locked) laptop bag. That way, if it gets snatched, at least you'll be snatched with it ... and you're less likely to leave it on the taxi by mistake. (It does happen!)
- Keep drinks well away from your device.
- If you use a server room, ensure the most appropriate fire prevention/detection systems are deployed – water-based sprinklers may save the building but will do no favours to computing equipment or associated media.

Audible alarms. (Deterrent control)

Audible devices can be fitted to your computer casing (above), either on the inside or outside, which, when disturbed will emit a loud siren that will alert anybody within earshot that something is being stolen. It will not prevent the theft but should deter (or at least embarrass) the miscreant.

The downside to these is that, in the writer's view, they can sound off spontaneously as false alarms, which can result at best in irritation or at worst ignoring it and taking no action.

Marking systems. (Detective control)

Computer equipment that is indelibly (and possibly invisibly) marked with appropriate detail, such as a postcode, is fairly easy and cheap. The marking can be performed in various ways - in the form of metallic tabs that are fixed with a strong epoxy adhesive, by an etching compound or simply by using a UV marking pen.

Associated with this, you should keep a separate record of the equipment manufacturer's serial number.

Disk drive and USB port locks. (Preventive control)

To protect your drives from misuse there are a wide range of hardware solutions that will prevent them being used at all without a key. Some are stronger than others, and some of them have pathetic locks that can be forced easily with a paperclip, but if you choose a good one it can be extremely effective.

Clear desk and screen policy (Preventive control)

A clear desk ensures that when you're not at your desk (especially out of working hours) sensitive hard copy documents are properly locked and secured against unauthorised access or copying. The threats vary from the everyday (e.g. viewing/removal by third parties, such as cleaning contractors) to the dramatic (e.g. explosion, blowing the windows out and distributing paperwork all over the district).

Although not a physical control, closely associated with this concept is the use of screen saver passwords – always, even when at home, use a timeout based upon a short period of keyboard inactivity – and be sure to position your monitor in such a way as to prevent casual viewing or “shoulder surfing”.

When leaving your desk for a short period, allow yourself time to exit from and/or lock down any sensitive work you may be doing in case “unauthorised” people approach your work area during your absence.

Remember, also, when leaving meeting rooms, to clear white boards of any information that should not be disclosed to unauthorised viewers.

Premises security (Preventive & detective control)

Premises security can be as complex or simple, expensive or economical as you like and quite often the effectiveness can be indistinguishable from each other.

So, let's start with “simple” and “economical” controls:

- Locks on doors and windows (with keys under suitable control)
- Identity badges to be worn at all times
- Visitors to be hosted, accompanied at all times ... well, nearly all times ... and checked in and out of the premises
- Keep a visitor's book with details of name, date, who is being visited (or who is hosting), time in/out and, if appropriate, vehicle registration. (NB. A visitor's book can also be critical in the event of an emergency evacuation to ensure all people on the premises are accounted for)
- Educate staff about premises security – no “tailgating”; challenging strangers, etc – and explain the rationale behind these rules, e.g. it may be for their own safety.

More sophisticated (which usually means more expensive) premises protection can also be achieved with:

- Electronic badge recognition systems which open doors and record who has been where ... but be sure not to set the badge reader sensitivity so high that it activates simply when a badge wearer walks past!
- “Data lock” devices requiring input of a PIN code – but codes do need to be periodically changed to remain effective
- CCTV – securely retain a reasonable cycle of tapes, such as up to 2 weeks
- Motion sensors activating alarms or lights
- Laser beam barriers internally or at the perimeter



Hardware security



Hardware security is vulnerability protection that comes in the form of a physical device rather than software that is installed on the hardware of a computer system.

Hardware security can pertain to a device used to scan a system or monitor network traffic. Common examples include hardware firewalls and proxy servers. Less common examples include hardware security modules (HSM), which provision cryptographic keys for critical functions such as encryption, decryption and authentication for various systems. Hardware systems can provide more robust security than software is capable of and can also add an additional layer of security for important systems.

The term *hardware security* also refers to the protection of physical systems from harm. Equipment destruction attacks, for example, focus on computing devices and networked non-computing devices such as the ever-increasing number of connected devices in M2M or IoT (Internet of Things) environments. These environments are bringing connectivity and communications to large numbers of hardware devices that must be protected through either hardware- or software-based security.

To assess the security of a hardware device, it's necessary to consider vulnerabilities existing from its manufacture as well as other potential sources such as running code and the device's data I/O on a network. Although any device should be protected if it connects even indirectly to the internet, the stringency of that protection should be in accordance with need. A system controlling the color and intensity of lights in Wi-Fi LED for a dwelling, for example, may not require much security.

Cyber crime act in India:

1. Tampering with computer source Documents Sec.65
2. Hacking with computer systems , Data Alteration Sec.66
3. Sending offensive messages through communication service, etc Sec.66A
4. Dishonestly receiving stolen computer resource or communication device Sec.66B
5. Identity theft Sec.66C
6. Cheating by personation by using computer resource Sec.66D
7. Violation of privacy Sec.66E
8. Cyber terrorism Sec.66F
9. Publishing or transmitting obscene material in electronic form Sec .67
10. Publishing or transmitting of material containing sexually explicit act, etc. in electronic form Sec.67A
11. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form Sec.67B
11. Preservation and Retention of information by intermediaries Sec.67C
12. Powers to issue directions for interception or monitoring or decryption of any information through any computer resource Sec.69
13. Power to issue directions for blocking for public access of any information through any computer resource Sec.69A
14. Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security Sec.69B
15. Un-authorized access to protected system Sec.70
16. Penalty for misrepresentation Sec.71
17. Breach of confidentiality and privacy Sec.72
18. Publishing False digital signature certificates Sec.73
19. Publication for fraudulent purpose Sec.74
20. Act to apply for offence or contraventions committed outside India Sec.75
21. Compensation, penalties or confiscation not to interfere with other punishment Sec.77
22. Compounding of Offences Sec.77A
23. Offences with three years imprisonment to be cognizable Sec.77B
24. Exemption from liability of intermediary in certain cases Sec.79
25. Punishment for abetment of offences Sec.84B
26. Punishment for attempt to commit offences Sec.84C
- Note : Sec.78 of I.T. Act empowers Police Inspector to investigate cases falling under this Act
27. Offences by Companies Sec.85
28. Sending threatening messages by e-mail Sec .503 IPC
29. Word, gesture or act intended to insult the modesty of a woman Sec.509 IPC
30. Sending defamatory messages by e-mail Sec .499 IPC
31. Bogus websites , Cyber Frauds Sec .420 IPC
32. E-mail Spoofing Sec .463 IPC
33. Making a false document Sec.464 IPC
34. Forgery for purpose of cheating Sec.468 IPC
35. Forgery for purpose of harming reputation Sec.469 IPC
36. Web-Jacking Sec .383 IPC
37. E-mail Abuse Sec .500 IPC
38. Punishment for criminal intimidation Sec.506 IPC
39. Criminal intimidation by an anonymous communication Sec.507 IPC
40. When copyright infringed:- Copyright in a work shall be deemed to be infringed Sec.51
41. Offence of infringement of copyright or other rights conferred by this Act. Any person who knowingly

infringes or abets the infringement of Sec.63

42. Enhanced penalty on second and subsequent convictions Sec.63A

43. Knowing use of infringing copy of computer programme to be an offence Sec.63B

44. Obscenity Sec. 292 IPC

45. Printing etc. of grossly indecent or scurrilous matter or matter intended for blackmail Sec.292A IPC

46. Sale, etc., of obscene objects to young person Sec .293 IPC

47. Obscene acts and songs Sec.294 IPC

48. Theft of Computer Hardware Sec. 378

49. Punishment for theft Sec.379

50. Online Sale of Drugs NDPS Act

51. Online Sale of Arms Arms Act.

Service-level agreement (SLA)

A service-level agreement (SLA) is a commitment between a service provider and a client. Particular aspects of the service – quality, availability, responsibilities – are agreed between the service provider and the service user.[1] The most common component of SLA is that the services should be provided to the customer as agreed upon in the contract. As an example, Internet service providers and telcos will commonly include service level agreements within the terms of their contracts with customers to define the level(s) of service being sold in plain language terms. In this case the SLA will typically have a technical definition in mean time between failures (MTBF), mean time to repair or mean time to recovery (MTTR); identifying which party is responsible for reporting faults or paying fees; responsibility for various data rates; throughput; jitter; or similar measurable details.

A Service Level Agreement (SLA) is the service contract component between a service provider and customer. A SLA provides specific and measurable aspects related to service offerings. For example, SLAs are often included in signed agreements between Internet service providers (ISP) and customers.

SLA is also known as an operating level agreement (OLA) when used in an organization without an established or formal provider-customer relationship.

Adopted in the late 1980s, SLAs are currently used by most industries and markets. By nature, SLAs define service output but defer methodology to the service provider's discretion. Specific metrics vary by industry and SLA purpose.

SLAs features include:

- Specific details and scope of provided services, including priorities, responsibilities and guarantees
- Specific, expected and measurable services at minimum or target levels
- Informal or legally binding
- Descriptive tracking and reporting guidelines
- Detailed problem management procedures
- Detailed fees and expenses
- Customer duties and responsibilities
- Disaster recovery procedures
- Agreement termination clauses

In outsourcing, a customer transfers partial business responsibilities to an external service provider. The SLA serves as an efficient contracting tool for current and continuous provider-customer work phases.

A service-level agreement (SLA) is a contract between a service provider and its internal or external customers that documents what services the provider will furnish and defines the performance standards the provider is obligated to meet

SLAs establish customer expectations with regard to the service provider's performance and quality in a number of ways. Some metrics that SLAs may specify include:

- Availability and uptime -- the percentage of the time services will be available.
- Specific performance benchmarks to which actual performance will be periodically compared.
- Application response time.
- The schedule for notification in advance of network changes that may affect users.
- Help desk response time for various classes of problems.
- Usage statistics that will be provided.

An SLA may specify availability, performance and other parameters for different types of customer infrastructure -- internal networks, servers and infrastructure components such as uninterruptable power supplies, for example.

Overview of SLAs: Penalties and exclusions

In addition to establishing performance metrics, an SLA may include a plan for addressing downtime and documentation for how the service provider will compensate customers in the event of a contract breach. Service credits are a typical remedy. Here, the service provider issues credits to the customer based on an SLA-specified calculation. Service providers, for example, might provide credits commensurate with the amount of time it exceeded the SLA's performance guarantee.

The SLA will also include a section detailing exclusions, that is, situations in which an SLA's guarantees -- and penalties for failing to meet them -- don't apply. The list might include events such as natural disasters or terrorist acts. This section is sometimes referred to as a force majeure clause, which aims to excuse the service provider from events beyond its control.

Who needs a service-level agreement?

SLAs are thought to have originated with network service providers, but are now widely used in a range of IT-related fields. Companies that establish SLAs include IT service providers, managed service providers, and cloud computing service providers. Corporate IT organizations, particularly those that have embraced IT service management (ITSM), enter SLAs with their in-house customers (users in other departments within the enterprise). An IT department creates an SLA so that its services can be measured, justified and perhaps compared with those of outsourcing vendors.

Service providers need SLAs to help them manage customer expectations and define the circumstances under which they are not liable for outages or performance issues. Customers can also benefit from SLAs in that they describe the performance characteristics of the service, which can be compared with other vendors' SLAs, and also set forth the means for redressing service issues -- via service credits, for example.

For a service provider, the SLA is typically one of two foundational agreements it has with customers. Many service providers establish a master services agreement to establish the general terms and conditions in which it will work with customers. The SLA is often incorporated by reference into the service provider's master services agreement. Between the two service contracts, the SLA adds greater specificity regarding the services provided and the metrics that will be used to measure their performance.

Types of SLAs: Evolution

Over the years, SLAs have expanded to govern a growing set of IT procurement models. When IT outsourcing emerged in the late 1980s, SLAs evolved as a mechanism to govern such relationships. SLAs set the expectations for a service provider performance and established penalties for missing the targets and, in some cases, bonuses for exceeding them. Since outsourcing projects were frequently customized for a particular customer, outsourcing SLAs were often drafted to govern a specific project.

As managed services and cloud computing services became more prevalent in recent years, SLAs evolved to address those approaches. Shared services, rather than customized resources, characterize the newer contracting methods, so SLAs tend to broad agreements intended to cover all of a service provider's customers.

SLAs, regardless of type, are subject to modification over time. Service providers will periodically review and update SLAs to reflect the addition of new services, changes to existing services or changes in the overarching regulatory environment

SLAs do not define how the service itself is provided or delivered. The SLA an Internet Service Provider (ISP) will provide its customers is a basic example of an SLA from an external service provider. The metrics that define levels of service for an ISP should aim to guarantee:

- A description of the service being provided— maintenance of areas such as network connectivity, domain name servers, dynamic host configuration protocol servers
- Reliability – when the service is available (percentage uptime) and the limits outages can be expected to stay within
- Responsiveness – the punctuality of services to be performed in response to requests and scheduled service dates
- Procedure for reporting problems – who can be contacted, how problems will be reported, procedure for escalation, and what other steps are taken to resolve the problem efficiently
- Monitoring and reporting service level – who will monitor performance, what data will be collected and how often as well as how much access the customer is given to performance statistics
- Consequences for not meeting service obligations – may include credit or reimbursement to customers, or enabling the customer to terminate the relationship.
- Escape clauses or constraints – circumstances under which the level of service promised does not apply. An example could be an exemption from meeting uptime requirements in circumstance that floods, fires or other hazardous situations damage the ISP's equipment.

Though the exact metrics for each SLA vary depending on the service provider, the areas covered are uniform: volume and quality of work (including precision and accuracy), speed, responsiveness, and efficiency. In covering these areas, the document aims to establish a mutual understanding of services, areas prioritized, responsibilities, guarantees, and warranties provided by the service provider.

The level of service definitions should be specific and measureable in each area. This allows the quality of service to be benchmarked and, if stipulated by the agreement, rewarded or penalized accordingly. An SLA will commonly use technical definitions that quantify the level of service such as mean time between failures (MTBF) or mean time to recovery, response, or resolution (MTTR), which specifies a “target” (average) or “minimum” value for service level performance.

SLAs are also very popular among internal departments in larger organizations. For example, the use of a SLA by an IT helpdesk with other departments (the customer) allows their performance to be defined and benchmarked. The use of SLAs is also common in outsourcing, cloud computing, and other areas where the responsibility of an organization is transferred out to another supplier

COMPUTER TERMINOLOGY

ATM: Automated Teller Machine '

SWIFT: Society for worldwide Interbank Financial Telecommunication

SFMS: Structured Financial Messaging System

OLTAS: Online Tax Accounting System

CBS: Centralized/ core Banking Solution

PIN: Personal Identification Number

LAN: Local Area Network (used in the same building)

MAN: Metropolitan Area Network (used in the same city)

WAN: Wide Area Network (used in different locations)

1DRBT: Institute for development & Research in Banking Technology

Banknet: Payment System Network established by RBI

NICNFT: National Informatics Centre Network (currency chest operation)

WWW: World Wide Web

HTTP: Hyper Text Transfer Protocol

URL: Uniform Resource Locator

VSAT: Very Small Aperture terminal

Firewall: Software programme that restricts unauthorized access to data and acts as a security to private network

Booting: Starting of a computer

Hard Disk: A device for storage of data fitted in the processor itself

Modem: Modulator & Demodulator: A device used for converting digital signals to analog signals & vice-versa

Encryption: Changing the data into coded form

Decryption: Process of decoding the data

Virus: Vital Information Resources Under Seize: Software programme that slows down the working of a computer or damages the data. Main source of virus is internet (other sources are floppy or CD)

Vaccine: Anti Virus Software programme used for preventing entry of virus or repairing the same

Digital Sign: Authentication of. electronic records by a subscriber by means of electronic method or procedure

Key used: For digital signatures, there is a pair of keys, private key & public key

RTGS: Real time Gross Settlement

ECS: Credit: One account debited, number of accounts credited

ECS: Debit: One account credited, number of accounts debited

Hacking: Knowingly concealing, destroying, altering any computer code used for computer network

Address: The location of a file. You can use addresses to find files on the Internet and your computer. Internet

addresses are also known as URLs.

IMPORTANT ABBREVIATIONS

- AI – Artificial intelligence ,

ALGOL – Algorithmic Language ,

ARP – Address resolution Protocol,

ASCII – American Standard

Code for Information Interchange

BINAC - Binary Automatic Computer,

BCC – Blind Carbon Copy ,

Bin – Binary

,BASIC - Beginner's All-purpose Symbollic

Instruction Code, BIOS – Basic Input Output System,

Bit – Binary Digit, BSNL – Bharat Sanchar Nigam Limited.

CC – Carbon Copy,

CAD – Computer Aided Design,

COBOL – Common Business Oriented Language, CD – Compact Disc, CRT –

Cathode Ray Tube ,CDR – Compact Disc Recordable ,

CDROM – Compact Disc Read Only Memory,

CDRW – Compact Disc

Rewritable, CDR/W – Compact Disk Raed/Write

DBA – Data Base Administrator,

DBMS – Data Base Management System,

DNS – Domain Name System,

DPI – Dots Per Inch,

DRAM – Dynamic Random Access Memory,

DVD – Digital Video Disc/Digital Versatile Disc,

DVDR – DVD Recordable , DVDROM –

DVD Read Only Memory ,DVDRW –DVD Rewritable ,

DVR – Digital Video Recorder ,

DOS – Disk Operating System

- EBCDIC – Extended Binary Coded Decimal Interchange Code ,

e-Commerce – Electronic Commerce, EDP – Electronic Data
Processing

- EEPROM – Electronically Erasable Programmable Read Only Memory,

ELM/e-Mail – Electronic Mail, ENIAC - Electronic

Numerical Integrator and Computer

- EOF - End Of File

, EPROM - Erasable Programmable Read Only Memory,

EXE - Executable

FAX - Far Away Xerox/ facsimile ,FDC - Floppy Disk Controller, FDD - Floppy Disk Drive ,FORTRAN -
Formula Translation, FS -

File System

,FTP - File Transfer Protocol

Gb – Gigabit ,

GB – Gigabyte ,

GIF - Graphics Interchange Format,

GSM - Global System for Mobile Communication

GLOSSORY

Access control

Controlling who has access to a computer or online service and the information it stores.

Asset

Something of value to a person, business or organization.

Authentication

The process to verify that someone is who they claim to be when they try to access a computer or online service.

Backing up

To make a copy of data stored on a computer or server to lessen the potential impact of failure or loss.

Bring your own device (BYOD)

The authorised use of personally owned mobile devices such as smartphones or tablets in the workplace.

Broadband

High-speed data transmission system where the communications circuit is shared between multiple users.

Business continuity management

Preparing for and maintaining continued business operations following disruption or crisis.

Certification

Declaration that specified requirements have been met.

Certification body

An independent organization that provides certification services.

Chargeback

A payment card transaction where the supplier initially receives payment but the transaction is later rejected by the cardholder or the card issuing company. The supplier's account is then debited with the disputed amount.

Cloud computing

Delivery of storage or computing services from remote servers online (ie via the internet).

Common text

A structure and series of requirements defined by the International Organization for Standardization, that are being incorporated in all management system International Standards as they are revised.

Data server

A computer or program that provides other computers with access to shared files over a network.

Declaration of conformity

Confirmation issued by the supplier of a product that specified requirements have been met.

DMZ

Segment of a network where servers accessed by less trusted users are isolated. The name is derived from the term “demilitarised zone”.

Encryption

The transformation of data to hide its information content.

Ethernet

Communications architecture for wired local area networks based upon IEEE 802.3 standards.

Firewall

Hardware or software designed to prevent unauthorised access to a computer or network from another computer or network.

Gap analysis

The comparison of actual performance against expected or required performance.

Hacker

Someone who violates computer security for malicious reasons, kudos or personal gain.

Hard disk

The permanent storage medium within a computer used to store programs and data.

Identification

The process of recognising a particular user of a computer or online service.

Infrastructure-as-a-service (IaaS)

Provision of computing infrastructure (such as server or storage capacity) as a remotely provided service accessed online (ie via the internet).

Inspection certificate

A declaration issued by an interested party that specified requirements have been met.

Instant messaging

Chat conversations between two or more people via typing on computers or portable devices.

Internet service provider (ISP)

Company that provides access to the internet and related services.

Intrusion detection system (IDS)

Program or device used to detect that an attacker is or has attempted unauthorised access to computer resources.

Intrusion prevention system (IPS)

Intrusion detection system that also blocks unauthorised access when detected.

'Just in time' manufacturing

Manufacturing to meet an immediate requirement, not in surplus or in advance of need.

Keyboard logger

A virus or physical device that logs keystrokes to secretly capture private information such as passwords or credit card details.

Leased circuit

Communications link between two locations used exclusively by one organization. In modern communications, dedicated bandwidth on a shared link reserved for that user.

Local area network (LAN)

Communications network linking multiple computers within a defined location such as an office building.

Macro virus

Malware (ie malicious software) that uses the macro capabilities of common applications such as spreadsheets and word processors to infect data.

Malware

Software intended to infiltrate and damage or disable computers. Shortened form of malicious software.

Management system

A set of processes used by an organisation to meet policies and objectives for that organisation.

Network firewall

Device that controls traffic to and from a network.

Outsourcing

Obtaining services by using someone else's resources.

Passing off

Making false representation that goods or services are those of another business.

Password

A secret series of characters used to authenticate a person's identity.

Personal firewall

Software running on a PC that controls network traffic to and from that computer.

Personal information

Personal data relating to an identifiable living individual.

Phishing

Method used by criminals to try to obtain financial or other confidential information (including user names and passwords) from internet users, usually by sending an email that looks as though it has been sent by a legitimate organization (often a bank). The email usually contains a link to a fake website that looks authentic.

Platform-as-a-service (PaaS)

The provision of remote infrastructure allowing the development and deployment of new software applications over the internet.

Portable device

A small, easily transportable computing device such as a smartphone, laptop or tablet computer.

Proxy server

Server that acts as an intermediary between users and others servers, validating user requests.

Restore

The recovery of data following computer failure or loss.

Risk

Something that could cause an organization not to meet one of its objectives.

Risk assessment

The process of identifying, analysing and evaluating risk.

Router

Device that directs messages within or between networks.

Screen scraper

A virus or physical device that logs information sent to a visual display to capture private or personal information.

Security control

Something that modifies or reduces one or more security risks.

Security information and event management (SIEM)

Process in which network information is aggregated, sorted and correlated to detect suspicious activities.

Security perimeter

A well-defined boundary within which security controls are enforced.

Server

Computer that provides data or services to other computers over a network.

Smartphone

A mobile phone built on a mobile computing platform that offers more advanced computing ability and connectivity than a standard mobile phone.

Software-as-a-service (SaaS)

The delivery of software applications remotely by a provider over the internet; perhaps through a web interface.

Spyware

Malware that passes information about a computer user's activities to an external party.

Supply chain

A set of organisations with linked resources and processes involved in the production of a product.

Tablet

An ultra-portable, touch screen computer that shares much of the functionality and operating system of smartphones, but generally has greater computing power.

Threat

Something that could cause harm to a system or organization.

Threat actor

A person who performs a cyber attack or causes an accident.

Two-factor authentication

Obtaining evidence of identity by two independent means, such as knowing a password and successfully completing a smartcard transaction.

Username

The short name, usually meaningful in some way, associated with a particular computer user.

User account

The record of a user kept by a computer to control their access to files and programs.

Virtual private network (VPN)

Link(s) between computers or local area networks across different locations using a wide area network that cannot access or be accessed by other users of the wide area network.

Virus

Malware that is loaded onto a computer and then run without the user's knowledge or knowledge of its full effects.

Vulnerability

A flaw or weakness that can be used to attack a system or organization.

Wide area network (WAN)

Communications network linking computers or local area networks across different locations.

Wi-Fi

Wireless local area network based upon IEEE 802.11 standards.

Worm

Malware that replicates itself so it can spread to infiltrate other computers.

****BEST OF LUCK ****

Disclaimer

While every effort has been made by me to avoid errors or omissions in this publication, any error or discrepancy noted may be brought to my notice through e-mail to Srinivaskante4u@gmail.com which shall be taken care of in the subsequent editions. It is also suggested that to clarify any doubt colleagues should cross-check the facts, laws and contents of this publication with original Govt. / RBI / Manuals/Circulars/Notifications/Memo/Spl Comm. of our bank.

