# Chapter 2 – Information Security

## Introduction:

This is the information age and the systems that support and handle it are critical to the operation of virtually all organizations. Peter Drucker's quote below underscores the criticality of information in this day and age:
*"The diffusion of technology and the commodification of information transforms the role of information into a resource equal in importance to the traditionally important resources of land, labor and capital."*

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 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.

## A. GUIDANCE FOR BANKS

### *Emerging Information Security Attacks*

**1) Phishing**: Phishing is just one of the many frauds on the Internet, trying to fool people into parting with their money. Phishing refers to the receipt of unsolicited emails by customers of financial institutions, requesting them to enter their username, password or other personal information to access their account for some reason. Customers are directed to a fraudulent replica of the original institution's website when they click on the links to enter their information, and so they remain unaware that fraud has occurred. The fraudster then has access to the customer's online bank account and to the funds contained in that account. In some cases, pop-up windows appear in front of a copy of a genuine bank website. The real web site address is displayed; however, any information that is typed into the pop-up directly goes to unauthorized users. In recent times, phishing incidents have been attempted using the names of Reserve Bank of India/IBA to target gullible people.

**2) Cross-site scripting:** Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications which allow code injections by malicious web users into the web pages viewed by other users. Examples of such code include HTML code and client-side scripts. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls.

**3) Vishing:** Vishing is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private, personal and financial information from the public for the purpose of financial reward. The term is a combination of "voice" and phishing. In Vishing, a scammer calls and pretends to be a bank representative seeking to verify account information, thus exploiting the public's trust in landline telephone services. It is typically used to steal credit card numbers or other information used in identity theft schemes from individuals.

**4) Cyber Squatting :**Cyber squatting is the act of registering a famous domain name and then selling it for a fortune. Cyber Squatters register domain names identical to popular service providers' domains so as to attract their users and benefit from it. This is an issue that has not been tackled in the IT Act, 2000.

**5) Bot Networks :**A cyber crime called 'Bot Networks', wherein spamsters and other perpetrators of cyber crimes remotely take control of computers without users realizing it, is increasing at an alarming rate. Computers get linked to Bot Networks when users unknowingly download malicious codes such as '*Trojan horse*' sent as e-mail attachments. Such affected computers, known as zombies, can work together whenever the malicious code within them gets activated, and those who are behind the Bot Networks attacks get the computing powers of thousands of systems at their disposal. Attackers often coordinate large groups of Bot-controlled systems, or Bot networks, to scan for vulnerable systems and use them to increase the speed and breadth of their attacks.

*'Trojan horse'* provides a backdoor to the computers acquired. A 'backdoor" is a method of bypassing normal authentication, or of securing remote access to a computer, while attempting to remain hidden from casual inspection. The backdoor may take the form of an installed program, or could be a modification to a legitimate program. Bot Networks create unique problems for organizations because they can be upgraded remotely with new exploits very quickly, and this could help attackers pre-empt security efforts.

**6) Email-related crimes :**

- Email spoofing: Email spoofing refers to email that appears to have originated from one source when it was actually sent from another source.
- Email Spamming: Email "spamming" refers to sending email to thousands and thousands of users - similar to a chain letter.
- Email bombing: E-mail "bombing" is characterized by abusers repeatedly sending an identical email message to a particular address.
- Sending malicious codes through email: E-mails are also used to send viruses, Trojans etc. as attachments or by sending the link to a website which downloads malicious code when visited.

**7) SMS spoofing:** It is a relatively new technology which uses the short message service (SMS), available on most mobile phones and personal digital assistants, to set who the message appears to come from by replacing the originating mobile number (Sender ID) with alphanumeric text. Spoofing has both legitimate uses (setting the company name from which the message is being sent, setting your own mobile number, or a product name) and illegitimate uses (such as impersonating another person, company, or product).

**8)Malware :**Malware is the term for maliciously crafted software code. Special computer programmes now exist that enable intruders to fool an individual into believing that traditional security is protecting him during online banking transactions. Attacks involving malware are a factor in online financial crime. It is possible for this type of malicious software to perform the following operations:

- Account information theft: Malware can capture the keystrokes for your login information. Malware can also potentially monitor and capture other data you use to authenticate identity (like special images or words).
- Fake website substitution: Malware can generate web pages that appear to be legitimate but are not. They replace a bank's legitimate website with a page that can look identical, except that the web address will vary in some way. Such a "man-in-the-middle attack" site enables an attacker to intercept user information. The attacker adds additional fields to the copy of the web page opened in the browser. When an individual submits the information, it is sent to both the bank and the malicious attacker without his/ her knowledge.
- Account hijacking: Malware can also hijack the browser and transfer funds without one's knowledge. When an individual attempts to login at a bank website, the software launches a hidden browser window on the computer, logs in to his/ her bank account, reads account balance, and creates a secret fund transfer to the intruder-owned account.

**9) Denial-of-service attacks:** A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently. A denial-of-service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. In a distributed denial-of-service (DDoS) attack, large numbers of compromised systems (sometimes called a Bot net) attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying the service of the system to legitimate users.

Although a DoS attack does not usually result in theft of information or other security loss, it can cost the target person or company a great deal of time and money. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services. A denial-of-service attack can also destroy programming and files in affected computer systems. In some cases, DoS attacks have forced websites accessed by millions of people to temporarily cease operation. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks and credit card payment gateways. The telephony denial-of-service (TDoS) attack is a new kind using telecommunications, particularly attempted in the western countries.

The TDOS attack is a way to divert a victim's attention from what is really going on, and a way to make the victim unavailable to banks and other financial institutions. In this scheme, fraudsters try to change the victim's profile information by contacting financial institutions (i.e. email addresses, telephone numbers and bank account numbers). Fraudsters then use automated dialing programs and multiple accounts to overwhelm victims' cell phones and land lines with thousands of calls. When victims answer the calls they hear nothing on the other end, an innocuous recorded message, advertisement, or a telephone menu. Calls are typically short in duration but so numerous that victims in some cases change their phone numbers to terminate the attack. These TDoS attacks are used as a diversion to prevent financial and brokerage institutions from verifying victim account changes and transactions. Fraudsters thus get adequate time to transfer funds from financial online accounts.

**10)Pharming :**Farming or Pharming is typically a DNS (Domain Name System) attack commonly called DNS Poisoning. If the system is infected with a "Virus" that poisons the DNS system, whenever the victim next visits online banking site, he/she may not be directed to the actual web page, instead sent to a false "Pharming Page".

**11) Insider threats:** Given the extensive use of Information Technology by banks, the risk of unauthorized access, disclosure and modification of information by insiders or employees of banks is high. Even unintentional errors could have undesirable implications. There is a need to institute robust security processes to mitigate such threats.

## Increasing concerns on security:

As online banking through various electronic delivery channels becomes increasingly popular, it has become an attractive fraud target. Some reasons that force banks to step up security measures are :

- ***Browser weaknesses:*** Trojans and other malware like man-in-the-browser attacks, that are difficult to detect, hijack the transaction inside of a browser session, and subsequently attack the application and database on the server. Most of the top 100 banks of the world are reported to have experienced similar incidents.
- ***Consumers as endpoints:*** Banks deliver services to business customers through the browser. However, they are not in control of the customers' computing environment. Many banks across the world provision online services to small businesses on consumer systems with inadequate security for business activity.
- ***Multi-channel banking:***. The cyber threat environment is growing more complex, especially as web banking expands from web and file transfer to mobile/smart phone and social channels and as the workforce grows younger. An integrated multi-channel approach to information, transactions and fraud is necessary to lower costs and increase effectiveness.
- ***Single Sign On(SSO).*** Banks are seeking new corporate/business portal solutions or independent SSO applications to solve the security usability problem. If the bank looks for an SSO solution in an existing packaged online banking offering, it may not get the integrated authentication and entitlements it needs. Most solutions secure the session and as malware attacks are now happening at the application level, transaction authentication needs to be cryptographically distinct from the session.
- ***Organized crime*****:** Internet fraudsters have created an end-to-end supply chain to advance malware attacks and the online vector used to efficiently deploy them. While the security technology market is creating security-as-a-service solutions, criminals are creating fraud-as-aservice activities and fraud has moved from the consumer to businesses that initiate payments and bank online. There is huge potential for damage to national security through cyber attacks. The internet is a means for money laundering and funding terrorist attacks in an organized manner.

The requirement is to put in place robust information security governance processes and effective implementation of information security measures.

## 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.
  Data diddling forms one of the means which involves changing data prior to or during input into a computer. It also includes automatically changing the financial information for some time before processing and then restoring original information. There are many ways in which integrity could be violated without malicious intent. In the simplest case, a user on a system could mistype someone's data. 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.

- ***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 to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction. 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, ie, 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.
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 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
- 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.

***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:**

**1) *Policies and procedures:***

1) 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.
2) The policies need to be supported with relevant standards, guidelines and procedures. A policy framework would,inter-alia, incorporate/take into consideration the following:
   a. An information security strategy that is aligned with business objectives
   b. Objectives, scope, ownership and responsibility for the policy
   c. Information security organisational structure
   d. 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

e. Periodic reviews of the policy – at least annually and in the event of significant changes necessitating revision
f. A periodic compliance review of the policy – about the adherence of users to information security policies and put up to the information security committee.
g. 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
h. Penal measures for violation of policies and the process to be followed in the event of violation
i. Identification, authorisation and granting of access to IT assets (by individuals and other IT assets)
j. Addressing the various stages of an IT asset's life to ensure that information security requirements are considered at each stage of the lifecycle
k. An incident monitoring and management process to address the identification and classification of incidents, reporting, escalation, preservation of evidence, the investigation process
l. 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
m. Management and monitoring of service providers that provides for overseeing the management of information security risks by third parties
n. 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
o. 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
p. Strategy for periodic training and enhancing skills of information security personnel, requirement of continuous professional education
q. Specific policies that would be required include, but not limited to, the following:
    i. Logical Access Control
    ii. Asset Management
    iii. Network Access Control
    iv. Password management
    v. E-mail security
    vi. Remote access
    vii. Mobile computing
    viii. Network security
    ix. Application security
    x. Backup and archival
    xi. Operating system security
    xii. Database administration and security
    xiii. Physical security
    xiv. Capacity Management
    xv. Incident response and management
    xvi. Malicious software
    xvii. IT asset/media management

xviii. Change Management
xix. Patch Management
xx. Internet security
xxi. Desktop
xxii. Encryption
xxiii. Security of electronic delivery channels
xxiv. Wireless security
xxv. Application/data migration

3) 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.

4) 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.

5) 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.

### 2) *Risk Assessment*

1) 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).
2) 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.

3) The ISO/IEC 27002:2005 Code of practice for information security management recommends the following be examined during a risk assessment:
- Security policy,
- Organization of information security
- Asset management

- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Regulatory compliance

4) 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
   - 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.

5) 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.

6) 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.

7) 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.

### 3) *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 for information assets throughout the organization. ISO 27001 standards require the inventorying of information assets and the classification, handling and labeling of information in accordance with preset guidelines.

### 4) *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
- 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
- Adhering to all information security policies, procedures, standards and guidelines
- Promptly reporting security incidents to management.

### 5) *Access Control*

(i) 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.

(ii) 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 updation status, nature of device used and software /operating system.

(iii) 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.

(iv) 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.

(v) 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.

(vi) Among the important controls that banks need to consider are:

- (a) A systematic process of applying and authorizing the creation of user ids and the access control matrix
- (b) Conducting a risk assessment and granting access rights based on the same. For example, contractors and temporary staff would have higher inherent risks
- (c) Implementation of role-based access control policies designed to ensure effective segregation of duties
- (d) Changing default user names and/or passwords of systems and prohibiting sharing of user ids and passwords including generic accounts
- (e) Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment
- (f) Processes to notify in a timely manner the information security function regarding user additions, deletions and role changes
- (g) Periodic reconciliation of user ids in a system and actual users required to have access and deletion of unnecessary ids, if any
- (h) Audit of logging and monitoring of access to IT assets by all users
- (i) Regular reviews of user access by information asset owners to ensure appropriate access is maintained
- (j) Applying the four-eyes principle to very critical/sensitive IT assets
- (k) 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.

(viii) For accountability purposes, a bank should ensure that users and IT assets are uniquely identified and their actions are auditable.

(ix) Transaction processes and systems should be designed to ensure that no single employee/outsourced service provider could enter, authorize and complete a transaction.

(x) 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.

(xi) E-banking systems should be tested to ensure that segregation of duties cannot be bypassed.

(xii) 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.

(xiii) 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:

a) Implementing two-factor authentication for privileged users
b) Instituting strong controls over remote access by privileged users
c) Restricting the number of privileged users
d) Granting privileged access on a “need-to-have”  or “need-to-do” basis
e) Maintaining audit logging of system activities performed by privileged users
f) Ensuring that privileged users do not have access to systems logs in which their activities are being captured
g) Conducting regular audit or management review of the logs
h) Prohibiting sharing of privileged IDs and their access codes
i) Disallowing vendors and contractors from gaining privileged access to systems without close supervision and monitoring
j) Protecting backup data from unauthorized access.

### 6) *Information security and information asset life-cycle*

(i) 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.

(ii) 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.

(iii) 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

(iv) 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.)

### 7) *Personnel security*

(i) 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.

(ii) 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.

(iii) 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

(iv) There also needs to be a periodic rotation of duties among users or personnel as a prudent risk measure.

### 8) *Physical security*

(i) 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.

(ii) 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.

(iii) 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

### 9) *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:

a) Relevant information security policies/procedures
b) Acceptable and appropriate usage of IT assets
c) Access controls including standards relating to passwords and other authentication requirements
d) Measures relating to proper email usage and internet usage
e) Physical protection
f) Remote computing and use of mobile devices
g) Safe handling of sensitive data/information
h) Being wary of social engineering attempts to part with confidential details
i) Prompt reporting of any security incidents and concerns

### 10) *Incident management*

(i) 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.

(ii) Major activities that need to be considered as part of the incident management framework include:

a. Developing and implementing processes for preventing, detecting, analyzing and responding to information security incidents
b. Establishing escalation and communication processes and lines of authority
c. Developing plans to respond to and document information security incidents
d. Establishing the capability to investigate information security incidents through various modes like forensics, evidence collection and preservation, log analysis, interviewing, etc.
e. Developing a process to communicate with internal parties and external organizations (e.g., regulator, media, law enforcement, customers)
f. Integrating information security incident response plans with the organization’s disaster recovery and business continuity plan
g. Organizing, training and equipping teams to respond to information security incidents
h. Periodically testing and refining information security incident response plans
i. 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

(iii) 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.
(iv) 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.
(v) All security incidents or violations of security policies should be brought to the notice of the CISO.

### **11)** ***Application Control and Security:***

a. 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.

b. 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.

c. The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to develop, purchase and maintain applications that can be trusted. The **OWASP Top 10** focuses on identifying the most serious application security risks for a broad array of organizations. The current set of serious web A**pplication Security Risks** include is as under:

(i) Command Injection: Injection flaws, such as SQL, OS, and LDAP injection, occur when un-trusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized information. This will happen if input validation controls are not properly built into the application.

(ii) Cross Site Scripting (XSS) :This flaw occurs whenever an application takes un-trusted data and sends it to a web browser without proper validation and escaping. Cross Site Scripting (XSS) allows attackers to execute script in the victim's browser, which can hijack user sessions, deface web sites or redirect the user to malicious sites.

(iii) Session Management & Broken Authentication: Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys and session tokens, or exploit implementation flaws to assume other users' identities. An attacker can also succeed in escalation of privileges.

(iv) Insecure Direct Object Reference: A direct object reference occurs whenever a developer exposes a reference to an internal implementation object, such as a file, directory or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data. This flaw is a result of insecure coding practices.

(v) Cross-Site Request Forgery (CSRF): A CSRF attack forces a victim's (who has already logged into the system) browser to send a forged HTTP request to a vulnerable web application. This forged request will also carry information about the victim's session cookie & any other authentication information. This allows the attacker to force the victim's browser to generate requests, which the vulnerable application thinks are legitimate requests from the victim. These sorts of attacks are fairly difficult to detect, potentially leaving a user debating with the website/company as to whether or not the actions were performed by him.

(vi) Security Misconfiguration: Security depends on having a secure configuration defined for the application, framework, web server, application server and platform. All these settings should be defined, implemented, and maintained as many are not shipped with secure defaults.

(vii) Failure to Restrict URL Access: A common problem in web applications, failing to restrict URL access typically happens when a page doesn't have the correct access control policy in place. Unauthorized users are able to view content that they shouldn't have the ability to view. Having these vulnerabilities in application exposes privileged functionality to unauthorized users. It can also create a problem with application record trails. If users can access records without being authenticated the chain of custody is completely broken, preventing good auditing from taking place.

(viii) Non-validated Redirects and Forwards: Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Web application redirects are very common and frequently include user-supplied parameters in the destination URL. If they aren't validated, attackers can send the victim to a site of their choice. Thus, without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

(ix) Insecure Cryptographic Storage: Many web applications do not properly protect sensitive data, such as Credit/Debit Cards, PAN, and authentication credentials, with appropriate encryption or hashing. Attackers may use this weakly protected data to conduct identity theft, credit card fraud or other crimes.

(x) Insufficient Transport Layer Protection: Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communications. When they do, they sometimes support weak algorithms, use expired or invalid certificates, or do not use them correctly. This attack normally occurs when a site does not use SSL/TLS for pages that require authentication, where an attacker can monitor network traffic to steal an authenticated user’s session cookie.

d. The following are the important **Application control and risk mitigation measures** that need to be implemented by banks :

1. Each application should have an owner which will typically be the concerned business function that uses the application
2. 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

3. 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.

4. 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.
5. 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.
6. 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.
7. 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.
8. There should be documented standards/procedures for administering the application, which are approved by the application owner and kept up-to-date.
9. The development, test and production environments need to be properly segregated.
10. 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.
11. There should be controls on updating key 'static' business information like customer master files, parameter changes, etc.
12. 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.
13. Potential security weaknesses / breaches (for example, as a result of analyzing user behaviour or patterns of network traffic) should be identified.
14. 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.
15. 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.
16. 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.
17. Access to the database prompt must be restricted only to the database administrator.

18. Robust input validation controls, processing and output controls needs to be built in to the application.
19. There should be a procedure in place to reduce the reliance on a few key individuals.
20. Alerts regarding use of the same machine for both maker and checker transactions need to be considered.
21. 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.
22. Error / exception reports and logs need to be reviewed and any issues need to be remedied /addressed at the earliest.
23. 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.
24. 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).
25. 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.
26. 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.
27. 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.
28. 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.
29. 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 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.

30. 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.
31. Critical application system logs/audit trails also need to be backed up as part of the application backup policy.
32. 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.

### 12) *Migration controls:*

(i) 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.

(ii) 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.
b. 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)
c. 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
d. 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
e. Continuity—the new application should be able to continue with newer records as addition (or appendage) and help in ensuring seamless business continuity

(iii) 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.

(iv) 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.

(v) 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.

### 13) *Implementation of new technologies:*

(i) 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.

(ii) 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.

### 14) *Encryption*

***(i)*** **<u>Encryption Types:</u>**

**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.

(ii) 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.

(iii) 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

a. Generating keys for different cryptographic systems and different applications
b. Generating and obtaining public keys and distributing keys to intended users, including how keys should be activated when received
c. 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
d. Dealing with compromised keys, revoking keys and specifying how keys should be withdrawn or deactivated
e. Recovering keys that are lost or corrupted as part of business continuity management

f. Archiving, destroying keys
g. Logging the auditing of key management-related activities
h. Instituting defined activation and deactivation dates, limiting the usage period of keys

(iv) Secure key management systems are characterized by the following precautions:
a. Additional physical protection of equipment used to generate, store and archive cryptographic keys
b. Use of cryptographic techniques to maintain cryptographic key confidentiality
c. 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
d. Ensuring key management is fully automated (e.g., personnel do not have the opportunity to expose a key or influence the key creation)
e. Ensuring no key ever appears unencrypted
f. Ensuring keys are randomly chosen from the entire key space, preferably by hardware
g. 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.)
h. 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
i. Ensuring keys are changed frequently.
j. Ensuring keys that are transmitted are sent securely to well-authenticated parties.
k. Ensuring key-generating equipment is physically and logically secure from construction through receipt, installation, operation, and removal from service.

(v) 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.

**15)** ***Data security***

i. 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.
ii. 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.
iii. 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 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.

iv. 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.

v. 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.

vi. 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.

vii. 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.

viii. 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.

ix. 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.

x. 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.

xi. 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.

### 16) *Vulnerability Assessment*

i. 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.

ii. The following are some of the measures suggested:

   a. 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.

   b. 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.

   c. 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.

   d. 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.

   e. 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.

### 17) *Establishing on-going security monitoring processes*

i. 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.

ii. 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.

iii. 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.

iv. 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.

v. 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.

vi. Users, like system administrators, with elevated access privileges should be subjected to a greater level of monitoring in light of the heightened risks involved.

vii. The integrity of the monitoring logs and processes should be safeguarded through appropriate access controls and segregation of duties.

viii. 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 a list of locked out accounts, disabled accounts, accounts with passwords that exceed the maximum password age, and accounts with passwords that never expire.

ix. Banks should establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor.

x. Banks should regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

xi. 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.

xii. 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.

xiii. Banks should monitor attempts to access deactivated accounts through audit logging.

xiv. 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.

xv. 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.

xvi. The following technologies/factors provide capabilities for effective attack detection and analysis:

   a. 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.

   b. 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.

c. 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 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.

d. 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.

xvii. 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.

### 18) *Security measures against Malware:*

i. 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.

ii. 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.

iii. 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.

iv. 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.

v. 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

vi. 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.

vii. Banks should configure systems so that they conduct an automated antimalware scan of removable media when it is inserted.

viii. 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.

ix. **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.

**19)** ***Patch Management:***

i. 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.

ii. 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 eg., based on the information handled, the business processes supported and the environments in which they are used) , recording patches that have been applied (for eg., using an inventory of computer assets including their patch level).

iii. The patch management process should include aspects like:

    a. Determining methods of obtaining and validating patches  for ensuring that the patch is from an authorised source
    b. Identifying vulnerabilities that are applicable to applications and systems used by the organisation
    c. Assessing the business impact of implementing patches (or not implementing a particular patch)
    d. Ensuring patches are tested
    e. Describing methods of deploying patches, for example, through automated manner
    f. Reporting on the status of patch deployment across the organisation
    g. Including methods of dealing with the failed deployment of a patch (for eg., redeployment of the patch).

iv. 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.

v. 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.

vi. 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.

### 20) *Change Management:*

i. 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.

ii. 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.

iii. The following steps should be taken prior to changes being applied to the live environment:

    ➢ Change requests should be documented (for eg., 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 eg., 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 eg., deploying the patch into the live environment)
- ➢ Changes should be reviewed to ensure that they do not compromise security controls (for eg., 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

iv. 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.

### 21) *Audit trails*

i. Banks needs to ensure that audit trails exist for IT assets satisfying the banks 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.

ii. 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.

iii. Some considerations for securing the integrity of log files include :

   a. Encrypting log files that contain sensitive data or that are transmitting over the network
   b. Ensuring adequate storage capacity to avoid gaps in data gathering
   c. Securing back-up and disposal of log files
   d. Logging the data to write-only media like a write-once/read-many (WORM) disk or drive
   e. Setting logging parameters to disallow any modification to previously written data

iv. 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.

v. Other aspects related to logging to be considered include:

   a. All remote access to an internal network, whether through VPN, dial-up, or other mechanism, should be logged verbosely
   b. 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
   c. 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
   d. 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
   e. 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

vi. 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.

vii. 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.

viii. In instances where processing systems and related audit trails are the responsibility of a third-party service provide, 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.

### 22) *Information security reporting and metrics*

i. 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 (for eg., reviewing the organization’s risk appetite, understanding the information security threat environment and encouraging business and system owners to remedy unacceptable risks).

ii. 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.

iii. 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
- Fraud analysis

iv. 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.

v. 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.

vi. 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.

vii. 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.

viii. 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.

ix. Some illustrative metrics include coverage of anti-malware software and their updation percentage, patch latency, extent of user awareness training, vulnerability related metrics, etc.

### 23) *Information security and Critical service providers/vendors*

i. 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.

ii. 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.

iii. 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).

iv. 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.

v. 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.

vi. 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".

### 24) *Network Security*

i. 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:
(a) Protecting the enclave boundaries or perimeter
(b) Protecting the computing environment.

ii. 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.

iii. 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.

iv. 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 network 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

v. 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.

vi. 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.

vii. A few network protection devices are briefly explained as under:

a) **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*

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, 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 ruleset 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.

### 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.

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 modeled and valid activity in future periods, and the potential for malicious activity to take place while the modeling 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.

"**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 theper ceived attack. Proper tuning is essential to both reliable detection of attacks and the 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 by 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 obviouslya 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 activityto 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 have 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

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.

### viii. 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:

a. Inventory of authorized and unauthorized devices and software.
b. 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.
c. Identifying all connections to critical networks and conducting risk analysis including necessity for each connection. All unnecessary connections to critical networks to be disconnected.
d. Implementation of the security features recommended by device and system vendors.
e. 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.
f. Implementation of internal and external intrusion detection system, incident response system and establishing 24x7 incident monitoring
g. Performing technical audits including vulnerability assessment of critical devices and networks, and any other connected networks, to identify security concerns
h. 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.
i. 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.
j. Documenting network architecture and identifying systems that serve critical functions or contain sensitive information that require additional levels of protection.
k. Establishing a rigorous, ongoing risk management process.
l. 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.
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).
n. 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.

o. 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).

p. 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.

q. Network operation standards and protocols should be documented and made available to the operators, and should be reviewed periodically to ensure compliance.

r. Network access by system engineers should be monitored and reviewed closely to detect unauthorized access to the network.

s. 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.

### 25) *Remote Access:*

i. 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.

ii. 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.

iii. Good controls for remote access include the following actions:

  a. Disallowing remote access by policy and practice unless a compelling business need exists and requiring management approval for remote access

  b. Regularly reviewing remote access approvals and rescind those that no longer have a compelling business justification

  c. Appropriately configuring and securing remote access devices

  d. Appropriately and in a timely manner patching, updating and maintaining all software on remote access devices

  e. Using encryption to protect communications between the access device and the institution and to protect sensitive data residing on the access device

  f. Periodically auditing the access device configurations and patch levels

  g. Using VLANs, network segments, directories, and other techniques to restrict remote access to authorized network areas and applications within the institution

  h. Logging remote access communications, analyzing them in a timely manner, and following up on anomalies

  i. 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

j. Logging and monitoring the date, time, user, user location, duration, and purpose for all remote access including all activities carried out through remote access

k. 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)

l. 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

iv. If remote access is through modems the following steps should be taken:

a. 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

b. Configure modems not to answer inbound calls, if modems are for outbound use only

c. Use automated callback features so the modems only call one number although this is subject to call forwarding schemes

d. 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

v. 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.

vi. 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.

### 26) Distributed Denial of service attacks(DDoS/DoS):

a. 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.

b. 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 review, network design analysis and configuration testing. Addressing these vulnerabilities would improve resilience of the systems.

c. 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.

### 27) *Implementation of ISO 27001 Information Security Management System*

(a) Commercial banks should implement Information Security Management System (ISMS) best practices for their critical functions/processes.

(b) 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.

(c) 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.

(d) 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.

(e) 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.

### 28) *Wireless Security*

i. 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.

ii. 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

iii. 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 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.

iv. 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.

v. Banks should ensure that all wireless access points are manageable using enterprise management tools.

vi. 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.

vii. 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.

viii. 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.

ix. 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.

x. 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.

xi. Banks should ensure all wireless traffic leverages at least AES encryption used with at least WPA2 protection. Organizations should ensure wireless networks use authentication protocols such as EAP/TLS or PEAP, which provide credential protection and mutual authentication.

xii. Banks should ensure wireless clients use strong, multi-factor authentication credentials to mitigate the risk of unauthorized access from compromised credentials.

xiii. Banks should disable peer-to-peer wireless network capabilities on wireless clients, unless such functionality meets a documented business need.

xiv. Banks should disable wireless peripheral access of devices (such as Bluetooth), unless such access is required for a documented business need.

xv. 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.

xvi. 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

### 29) *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.

### 30) *Information security assurance*

a) 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 atleast on an annual basis.

b) 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.

c) Assessment
An assessment is a study to locate security vulnerabilities and identify correctiveactions. 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 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.

### 31) *Security Measures with regard to delivery channels*

(i) 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.

(ii) 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.

(iii) To raise security awareness, banks should sensitize customers on the need to protect their PINs, security tokens, personal details and other confidential data.

(iv) 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.

(v) 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.

A few security measures in respect of delivery channels are indicated below:

**a. ATM related measures**:

- Every ATM may have an unique ID for easy reference, when required.
- Robust tuning and configuration of ATMs
- Cameras - ATM cameras should be so placed as to take a clear picture of the person doing the ATM operations and the lighting inside the ATM centre should facilitate the same. An additional small camera can also be explored by banks to take a snapshot of the customer picking up the money from the bin so as to assist customers when cash disbursement does not take place
- Time out for cash dispensed and swallowing of card (If cardholder has not collected the card in stipulated time)
- Firewall and Antivirus systems
- Security person at ATM location
- One person at a time to operate ATM.
- Controls relating to generation, transmission, loading and destruction of the ATM keys at the time of installation
- The message transmission between the ATM and Switch uses IPSec

***Switch***

- Card/Account authentication and validation using Switch
- PIN based authentication using Hardware Security Module.
- Concept of daily limit for transactions to contain the risk in the event of card misuse
- Activation of new card (PIN verification is must for first transaction at ATM: Card cannot be used for shopping at first time because PIN is not needed presently while shopping)

- Card is blocked if cardholder enters incorrect PIN a certain number of attempts, say three times; this blocked card is not usable for ATM & shopping transactions
- Firewall

***Card Management System***:

• Controls relating to verification of card number

**b) Card based online transactions/E-Commerce**:

• Secured e-commerce transactions through second factor authentication

• Email alerts: After successful registration of the card, email alert can be sent on email-id entered during registration process.

**c) Phone Banking**:

- Suitable security measures for authenticating customers through phone banking.
- As a part of the security measures, no customer data like account number, status, etc. is stored in cache memory. Information provided by the customer on the IVR is sent to back-end host directly after encryption. Information received from the host is sent back to application and when the caller disconnects the call all the information inputted by the caller is deleted automatically.
- Critical details like change in phone details and address details should not be allowed through phone banking but only through a branch after due verification.
- From January 01, 2011, RBI has made it applicable for providing for additional authentication/validation based on information not visible on the cards for all on-line card not present transactions including through IVR mode. Subsequently, deadline has been extended in view of the requests received by RBI.

**d) <u>Mobile Banking:</u>**

Technically speaking most of these services can be deployed using more than one channel. At present, Mobile Banking is being deployed using mobile applications developed on one of the following channels.

• SMS (Short Messaging Service)<br>
• WAP (Wireless Access Protocol)<br>
• Web Browser Based<br>
• Mobile Application Client<br>
• USSD<br>
• IVR (Interactive Voice Response)

➢ **SMS (Short Messaging Service)**

SMS uses the popular text-messaging standard to enable mobile application based banking. The main advantage of deploying mobile applications over SMS is that almost all mobile phones, including the low end, cheaper ones, which are most popular in countries like India and China are SMS enabled. An SMS based service is hosted on a SMS gateway that further connects to the Mobile service providers SMS Centre.

➢ **WAP (Wireless Access Protocol)**

WAP uses a concept similar to that used in Internet banking. Banks maintain WAP sites which customer's access using a WAP compatible browser on their mobile phones.

WAP sites offer the familiar form based interface and can also implement security quite effectively. A bank's customers can now have an anytime, anywhere access to a secure reliable service that allows them to access all enquiry and transaction based services and also more complex transaction like trade in securities through their phone. A WAP based service requires hosting a WAP gateway. Mobile Application users access the bank's site through the WAP gateway to carry out transactions, much like internet users access a web portal for accessing the banks services.

- **Web Browser Based**

For years, this solution has been shunned as slow, insecure and impossible to develop because of rendering. This is no longer the case, with the launch of high end phones with browsers supporting HTML and support of HTTPS this channel has now become secure and easy to use. The speed of download has also increased with GPRS and 3G coming into picture. In fact, after implementation of 3G it will be better than a standard internet connection on PC. The main advantage of this solution will be the bank can use the same infrastructure which is used for hosting its online banking solution. All the features of online banking can be extended to the customer with minimal efforts for customization of the site for mobile phones. As the solution is browser based, it will be accessible on both GSM and CDMA phones without any changes required.

- **Mobile Application Client**

Mobile applications are the ones that hold out the most promise, as they are most suitable to implement complex transactions like trading in securities. They can be easily customized according to the user interface complexity supported by the mobile. In addition, mobile applications enable the implementation of a very secure and reliable channel of communication. One requirement of mobile applications clients is that they require to be downloaded on the client device before they can be used, which further requires the mobile device to support one of the many development environments like J2ME or BREW. J2ME is fast becoming an industry standard to deploy mobile applications and requires the mobile phone to support Java.

- **Unstructured Supplementary Services Data (USSD)**

USSD stands for Unstructured Supplementary Services Data and is only available on GSM carrier networks. This communication protocol can be used for many mobile banking processes such as balance inquiry, money transfer, bill payment and airtime top up. USSD is similar to SMS technology only in that it too has data payload limits between 160 – 182 alphanumeric characters in a single transmission. However, USSD has a number of advantages over SMS technology.

- **Interactive Voice Response IVR)** service operates through pre-specified numbers that banks advertise to their customers. The most commonly used technologies across banking domain are Mobile Application Client, SMS, WAP and Web Browser Based Applications. Most financial institutions around the world have initiated basic mobile banking programs; others are contemplating more advanced & secure mobile banking options.

*Security measures in Mobile Banking*

Security of financial transactions, being executed from some remote location and transmission of financial information over the air, is the most complicated challenges that need to be addressed jointly by mobile application developers, wireless network service providers and the bank.

The following aspects are among the security measures in respect of mobile banking :

- Security of any thick-client application running on the device. In case the device is stolen, the hacker should require at least an ID/Password to access the application

- Authentication of the device with a service provider before initiating a transaction. This would ensure that unauthorized devices are not connected to perform financial transactions
- User ID / Password authentication of bank's customer
- Two-factor authentication through mPIN or higher standard and end-to-end encryption of mPIN is desirable
- The mPIN shall be stored in a secure environment.
- Encryption of the data being transmitted over the air.

### *e) DEBIT CARD SECURITY MEASURES*

1. Personalization of card, generation of card through a specific algorithm and verification of the same at switch level.
2. Delivering securely to customer after customer identification
3. Controls around activation of card
4. Blocking of cards after certain number of attempts with wrong PINs
5. An instant SMS message is sent to the customer's registered mobile number with the bank on usage of card at any ATM, POS or E Commerce site.

### *(f) Anti-skimming Measures:*

'Card skimming' is the illegal copying of information from the magnetic strip of a credit or ATM card. It is a more direct version of a phishing scam.

The scammers try to steal a customer's details so that they can access the relative accounts. Once scammers have skimmed the card, they can create a fake or 'cloned' card with details from the skimmed card on it. The scammer is then able to run up charges on your account.

There are a variety of methods that may be employed to deter card skimming.

a. Awareness among consumers, branch personnel, and ATM service technicians can result in the detection of devices added to an ATM fascia. Visual clues such as tape residue near on a card reader may indicate the former presence of a skimming device.

b. Any servicing in onsite ATMs by external service personnel may be done in the presence of a bank official and in respect of off-site ATMs random checks by bank officials may be conducted.

c. All ATMs including offsite ATMs need to be manned by security guards

d. Physically inspecting the ATMs once a day. Best practices include doing a physical inspection during maintenance or cash replacement etc. by the bank or outsourced agency managing the ATM network for the bank.

e. Enforce standards for the appearance of ATMs. Adopt visual standards for ATMs so all ATMs should look alike.

f. Banks can ask the customers to provide / register their mobile numbers for sending an alert message for transactions done on alternate channels.

g. Looking for anomalous activity in customer accounts. Fraud detection software isn't foolproof, but it can detect some behaviors associated with a fraudulent transaction. Updated customer contact information is critical for quickly verifying the legitimacy of transactions or stopping fraud. Deploying fraud monitoring system especially in on-line environment may be difficult and expensive but will be useful in fraud detection and timely action.

h. The banks may consider dynamic scoring models and related processes to trigger or alert transactions which are not normal to improve preventive/detective capability. Study of customer transaction behavioral patterns and stopping irregular transactions or getting confirmation from customers for outlier transactions may be part of the process.

i. Network with other bank security / branch officers by participating in electronic security taskforces, or even casual cooperative agreements with other local banks, can help ensure that bank's branch managers / ATM officers are the first to know when a skimmer is targeting his area.

j. All ATM/Debit cards by default may be payable only in India, Nepal and Bhutan and if any card holder wants to use his ATM/Debit cards abroad he should either obtain separate PIN before he leaves India or international usage may be separately activated either online or through call centre.

k. Banks may also explore usage of biometric ATM cards to illiterate customers who may not be at ease while using ordinary ATM cards.

Further, the following anti-skimming solutions can be introduced:

*Jittering*: Jittering is a process that controls and varies the speed of movement of a card as it's swiped through a card reader, making it difficult – if not impossible – to read card data by the external device.

*Chip-based cards*: These cards house data on microchips instead of magnetic stripes, making data difficult to be cloned. It is recommended that RBI may consider moving over to chip based cards along with upgradation of necessary infrastructure like ATMs/POS terminals in this regard in a phased manner.

PIN based authorization: For debit / credit card transactions at the POS terminals, PIN based authorization system needs to be put in place (without any looping) in place of the existing signature based system and the non-PIN based POS terminals need to be withdrawn in a phased manner.

***(g) Internet banking:***

i. 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 atleast 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.
iv. Banks need to follow a defense in depth strategy by applying robust security measures across various technology layers

***Authentication practices for internet banking:***

1) 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).

2) 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.

iii. The various major two- factor techniques/methodologies include the following:

Tokens: Tokens are physical devices (something the person has) and may be part of a multifactor authentication scheme. Three types of tokens are the USB token device, the smart card, and the password-generating token.

USB Token Device: The USB token device typically plugs directly into a computer’s USB port and therefore does not require the installation of any special hardware on the user’s computer. Once the USB token is recognized, the customer is prompted to enter his or her password (the second authenticating factor) in order to gain access to the computer system. USB tokens are one-piece, injection-molded devices. USB tokens are hard to duplicate and are tamper resistant; thus, they are a relatively secure vehicle for storing sensitive data and credentials. The device has the ability to store digital certificates that can be used in a public key infrastructure (PKI) environment. The USB token is generally considered to be user-friendly. Its small size makes it easy for the user to carry and there is no need for additional hardware is eliminated. However there are logistics issues in managing USB token devices for large retail customer base.

Smart Card: *A* smart card is the size of a credit card and contains a microprocessor that enables it to store and process data. Inclusion of the microprocessor enables software developers to use more robust authentication schemes. To be used, a smart card must be inserted into a compatible reader attached to the customer’s computer. If the smart card is recognized as valid (first factor), the customer is prompted to enter his or her password (second factor) to complete the authentication process. Smart cards are hard to duplicate and are tamper resistant; thus, they are a relatively secure vehicle for storing sensitive data and credentials. Smart cards are easy to carry and easy to use. Their primary disadvantage as a consumer authentication device is that they require the installation of a hardware reader and associated software drivers on the consumer’s home computer. Thus may not be the preferred option for the bank as well as customers.

*Password-Generating Token: A* password-generating token produces a unique pass-code, also known as a one-time password (OTP) each time it is used. The token ensures that the same OTP is not used consecutively. The OTP is displayed on a small screen on the token, consisting of 6 or more alphanumeric characters (sometimes numbers, sometimes combinations of letters and numbers, depending upon vendor and model). The customer first enters his or her user name and regular password (first factor), followed by the OTP generated by the token (second factor) into the banks website. The customer is authenticated if (a) the regular password matches and (b) the OTP generated by the token matches the password on the authentication server. A new OTP is typically generated every 60 seconds—in some systems, every 30 seconds. This very brief period is the life span of that password. OTP tokens generally last 4 to 5 years before they need to be replaced.

Password-generating tokens are secure because of the time-sensitive, synchronized nature of the authentication. The randomness, unpredictability, and uniqueness of the OTPs substantially increase the difficulty of a cyber fraudster from capturing and using OTPs gained from keyboard logging. However, it has the same logistics issues as highlighted in case of USB token devices.

*SMS based One Time Password :*In this method, the one-time password sent in an SMS to the user, is used in the bank's website. The user enters this code into the website to prove their identity and to authenticate transactions, and if the PIN code entered is correct, the user will be granted access to their account. This process provides an extra layer of online security beyond merely a username and password. These solutions can be used with any telephone, not just mobile devices. As with any out-of-band authentication method, SMS one time password methods are also vulnerable to man-in-the-middle attacks.

*Biometrics: Biometric* technologies identify or authenticate the identity of a living person on the basis of a physiological or physical characteristic (something a person is). Physiological characteristics include fingerprints, iris configuration, and facial structure. Fingerprints are unique and complex enough to provide a robust template for authentication. Using multiple fingerprints from the same individual affords a greater degree of accuracy. Fingerprint identification technologies are among the most mature and accurate of the various biometric methods of identification. Although end users should have little trouble using a fingerprint-scanning device, special hardware and software may need to be installed on the user's computer. At this junction it is not feasible to implement this technology for applications like Internet banking, Mobile etc at large scale as technology required to minimize error free authentication is very complex and expensive.

*Digital Signature certificates :*Digital Client certificates are a PKI solution for enabling the user identification and access controls needed to protect sensitive online information. Digital certificates can also be stored and transported on smart cards or USB tokens. Each certificate can only be used to authenticate one particular user because only that user's computer/token has the corresponding and unique private key needed to complete the authentication process. However, there are issues with deployment and support of digital certificates.

In the Indian context, the following are some of the operational issues in case banks are required to act as Registration Authority / Certifying Authority:

a. The digital certificates issued could be used for any purpose other than internet banking transactions also.
b. If a customer has accounts with more than one bank, the customer may need to carry as many number of certificates as the number of accounts he/she is having in case bank chooses to issue bank / application specific certificates.
c. If Certifying Authority performs Registration Authority's role, cost involved may be high and if a bank is to act as a Registration Authority, it will give rise to logistic issues for maintaining documentation and other processes required as part of RA.
d. The costs involved may be high in acquiring digital certificates for customers/banks. Another critical factor would be who will bear the cost of DC as this will not only

increase the transaction cost but will also make the channel less attractive and more expensive.

e. The responsibility for the safe custody of the digital certificates, backups, key compromise, timely renewal, accidental erase, etc. are a challenge with the customers. Further, banks would not be in a position to assume any onerous responsibilities in this regard.
f. Renewal of digital certificates at periodical intervals may be a repetitive job for banks or users.
g. There may be higher effort involved in installation of hardware or card reader at client's or customer's end.
h. Tremendous efforts would be required towards customer education and certificate helpdesk.
i. The need for suitable integration of PKI algorithms/technology with Internet Banking and provision for automated online validation and verification through linkage with Certificate Revocation Lists may be a key requirement.
j. A secure way of handling the digital certificates by customers is an issue and lapses in this regard may actually reduce overall security.
k. One of the most effective methods in combating MITM, MITB and similar session hijack attacks is by signing transactions. Till recently, the only way to sign transactions digitally was by using PKI. Now there are technologies available to sign transactions using software tokens which involve generating a transaction signature corresponding to the values of the transaction and then entering the signatures on the online application (which can also support non-repudiation in respect of the transaction.)

Further, it would not be ideal to mandate a specific technology for all online internet banking transactions.

'**Electronic Signature**' has been defined in Section 2(ta) of the IT Act (vide 2008 Amendment). However, in terms of the definition, the electronic techniques through which an electronic record is to be authenticated is to be specified in the Second Schedule. The 'techniques' have so far not been specified in the Second Schedule of the Act. Though the current legal position favours a specific technology for authenticating records/transactions i.e. asymmetric crypto-system and hash function, the amendment to IT Act has also allowed for 'electronic signatures' (which are to be notified by the Government in Second Schedule to the Act) where more options may be provided in future. There are also operational issues relating to widespread use of digital signatures as detailed earlier which require further assessment and clarification before being widely used. Hence, it is felt that any stringent prescription regarding digital signature or big bang approach to use of digital signatures may be counter-productive. Detailed discussion on the legal aspects, in this regard, is available in the "Legal issues" chapter later in the report.

*Implementation of two-factor authentication and other security measures for internet banking:*

1. In view of the proliferation of cyber attacks and their potential consequences, banks should implement two-factor authentication for fund transfers through internet banking.
2. 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.

3. 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.
4. While not using the asymmetric cryptosystem and hash function is a source of legal risk, keeping in view the various methods and issues discussed above, for carrying out critical transactions like fund transfers, the banks, at the least, need to implement dynamic two-factor authentication through user id/password combination and second factor like (a) OTP/dynamic access code through various modes (like SMS over mobile phones or hardware token) or (b) a digital signature (through a token containing digital certificate and associated private key) (preferably for the corporate customers) .
5. 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.
6. 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.
7. 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.
8. Changes in mobile phone number may be done through request from a branch only
9. Implementation of virtual keyboard
10. A cooling period for beneficiary addition and SMS and E-mail alerts when new beneficiaries are added
11. 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.
12. Risk based transaction monitoring or surveillance process needs to be considered as an adjunct.
13. 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.
14. 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.
15. 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:

a. 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.

b. 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.

c. 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 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.

d. 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.

e. 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.

f. 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.

g. 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. Some such concerns were considered by the Group are indicated below:

### 1. 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.

*Types of Virtualization*

Virtualization is the creation of a virtual environment of the server, operating system, storage, network resources and desktops.

a. Server virtualization means masking of server physical resources from server users.
b. Operating system virtualization is the use of software to allow a piece of hardware to run multiple operating system images at the same time.
c. Storage virtualization means pooling of physical storage from multiple storage devices into what appears to be a single storage device.
d. Network virtualization is a method of combining the available resources in a network by splitting up the available bandwidth into channels, each of which can be assigned to a particular connectivity. Also, using VLAN and switch technology, the system administrator can configure systems physically attached to the same local network into different virtual networks.
e. Desktop virtualization enables a centralized server to deliver and manage individualized desktops remotely. This gives users a full client experience, but lets IT staff provision, manage, upgrade and patch them virtually, instead of physically.

Virtualization enables the IT environment to manage itself based on perceived activity, and utility computing, in which computer processing power is seen as a utility that clients can pay for only as needed. The usual goal of virtualization is to centralize administrative tasks while improving scalability and workloads.

Virtualization technology enables us to move towards server consolidation where in many small physical servers are replaced by one larger physical server, which is partitioned into several virtual servers to increase the utilization of costly hardware resources such as CPU, memory etc. Different virtual machines can run different operating systems and multiple applications while sharing the resources of a single physical computer.

A virtual machine can be more easily controlled and inspected from outside than a physical one, and its configuration is more flexible. It can be provisioned as needed without the need for an up-front hardware purchase. Also, it can easily be relocated from one physical machine to another as needed. For example, a salesperson going to a customer can copy a virtual machine with the demonstration software to his laptop, without the need to transport the physical computer.

*Challenges of Virtualization*

a. Compatibility and support – Often software developers are not ready to guarantee fail-safe operation of all their programs in virtual machines.
b. 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.

c. 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.

d. 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.

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 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).

## 2. Cloud Computing

**Background :**Remote machines owned by a company are 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.
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.

### *Benefits of cloud computing*

Clients would be able to access their applications and data from anywhere at any time. They could access the cloud computing system using any computer linked to the Internet. Data wouldn't be confined to a hard drive on one user's computer or even a corporation's internal network.

It could bring hardware costs down. Cloud computing systems would reduce the need for advanced hardware on the client side. You wouldn't need to buy the fastest computer with the most memory, because the cloud system would take care of those needs for you. Instead, you could buy an inexpensive computer terminal. The terminal could include a monitor, input devices like a keyboard and mouse and just enough processing power to run the middleware necessary to connect to the cloud system.

Corporations that rely on computers have to make sure they have the right software in place to achieve goals. Cloud computing systems give these organizations company-wide access to computer applications. The companies don't have to buy a set of software or software licenses for every employee. Instead, the company could pay a metered fee to a cloud computing company.

Servers and digital storage devices take up space. Some companies rent physical space to store servers and databases because they don't have it available on site. Cloud computing gives these companies the option of storing data on someone else's hardware, removing the need for physical space on the front end. Corporations might save money on IT support as the infrastructure is not owned by them.

If the cloud computing system's back end is a grid computing system, then the client could take advantage of the entire network's processing power.

*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:

a. 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.
b. 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.
c. 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.
d. The geographical location of data storage and processing is not definite unlike traditional data centres. Trans-border data flows, business continuity requirements, log retention, data retention, audit trails are among the issues that contribute to compliance challenges in Cloud Computing environment.
e. 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.

f. 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.
g. 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.
h. 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?

Given that control, security, legal issues on cloud computing are still evolving, a bank needs to exercise caution and carry out necessary due diligence and assess the risks comprehensively while considering cloud computing.

### 3. Multiprotocol Label Switching (MPLS)

**Background :**Multiprotocol Label Switching (MPLS) is a technology typically offered by a service provider (SP) as a managed service to the customers. MPLS is an effective way of expanding to establish connectivity from any point and path. It offers the advantage of replacing traditional leased line and point to point links, and this helps in reducing costs. Enterprises can use the service provider’s shared MPLS backbone to connect its multiple locations using this technology.

*Challenges with Traditional Point to Point Network*

a) Upgrading of bandwidth is time-consuming.
b) Scalability issues with regard to increases in bandwidth on demand
c) As the organization grows, the number of links increase and it becomes a complex task to maintain and manage these links
d) There are scalability issues with regard to existing network infrastructure requirements
e) Networking solution becomes costly due to investment in multiple links and networking equipment
f) With various kinds of connectivity available viz. Leased Line, Metro Ethernet, ISDN, RF and Wi-Max, they have their own limitations
g) It might happen that the primary leased line and backup line fail at the same time due to local exchange problem
h) Provisioning and commissioning is time consuming
i) There can be issues with remote branch network connectivity

j) In case of expansion, availability of links depends on the presence of service provider at the desired location

k) It is difficult to implement traffic management for audio, video, data and business critical applications

*Best Practices for MPLS-based networks*

(a) Service Provider selection: Selection of Service Providers requires consideration of factors such as:

- Multiple Service Providers to ensure last mile redundancy
- Fallback mechanism for backup connectivity using different media connectivity and if required from other service provider
- Real-time network monitoring and managed service portal at customer end
- Level 3 IP VPN service
- SP should have experience in designing and implementing MPLS based solution in the BFSI sector
- Support Multicast, Quality of Service (QoS) and Classes of Service(CoS)
- Network connectivity with secure encryption techniques

(b) QoS/ CoS support: The MPLS solution should support end-to-end Quality of Service with inter-CoS burstability. There should be a facility to prioritize/ configure quality/ class of service parameters on the MPLS network. Enterprise can configure to provide high priority for business and critical applications. This will save bandwidth usage during business hours and ensure increased availability for business applications.

(c) Data encryption: In MPLS, the Service Provider can provide data encryption throughout their network using IP Tunnel and different encryption methods. Considering encryption overhead, enterprise needs to resize their bandwidth requirements. Enterprise should use IPSEC encryption technology for secure, confidentiality and integrity of data across MPLS shared network.

(d) Managed services: A bank should ensure that SP should provide access to management portal at its hosting site (Data Centre). Enterprise should ask for daily, weekly, monthly reports showing peak and average usage for network from SP. Enterprise should ensure Standard Operating Procedures for service delivery, change/release management, and issue resolution.

(e) Remote and central site connectivity: Bank should ensure that Service Provider should provide connectivity with dual POP redundant path which will ensure higher uptime.

(f) Business application considerations: MPLS enables enterprises to design and deploy network with the support of applications used in critical business environment. MPLS connectivity should be configured with correct policy, security, and network-based performance in mind to support business applications.

(g) Redundancy: Enterprise should select multiple SPs in order to maintain redundancy of network and avoid business outage.

(h) Service level agreement:SLA plays a very crucial role in MPLS. Enterprise should request SLAs for availability, latency, RTD (Round Trip Delay), and delay variance or jitter and commissioning timelines.

(i) Configuration Management: To ensure adherence to information security policy, enterprise should maintain configuration management of network devices instead of outsourcing it to SP.

(j) Migration: Migrating from traditional point to point WAN to MPLS should be done phase-wise.

(k) Last mile and backhaul connectivity: Bank should ensure that SP provides last mile connectivity preferably on wired media. SP should provide dual last mile and dual POP backhaul connectivity at the central location.

## B. INFORMATION SECURITY – INDUSTRY WIDE RECOMMENDATIONS:

i. There needs to be forum of CISOs who can periodically interact and share experiences regarding any information security threats. It is reported that a CISO forum is already functional under IDRBT. The forum may among other functions endeavour to share good practices and identify any specific information security issues and flag them to appropriate stakeholders like regulator, IBA etc. A member from the regulator can also be part of the meeting.

ii. There is a need for a system of information sharing akin to the functions performed by FS-ISAC (Financial Services Information Sharing Agency) in the US. IDRBT as a sub-CERT to the banking system can function as a nodal point for information sharing and can perform the following functions:

   a. Working closely with other GoI as well as private sector agencies for critical infrastructure protection in respect of banking sector
   b. Providing a forum for exchange of information and best practices on information/cyber security to the banks through alert system, training programmes,seminars, conferences etc.
   c. Based on the incidents reported by the banks and information received from other agencies like CERT-In, generating information on current threat levels as well as intelligence reports
   d. Assisting constituents of banking sector in rapidly remediating major cyber incidents
   e. Implementing a crisis communication system to notify all of its members within certain time-frame (say, one hour).
   f. Developing searchable database of past and current incidents, vulnerabilities and threat data along with extensive e-library of important security and infrastructure protection documents
   g. Developing threat vulnerability and incident management best practices for the financial sector
   h. Coordinating with CERT-IN and assisting in conduct of system-wide cyber crisis related stress testing
   i. Periodically sharing issues of concern to supervisory authorities like RBI
   j. IDRBT can consider developing an internet portal for facilitating reporting of incidents.

iii. In order to reduce the time, cost, and complexity of software assurance and to ensure its security, resiliency, sustainability and integrity and increase the effectiveness of the methods used by the banking industry for Software Assurance, an initiative similar to FSTC Software Assurance Initiative (SAI) in US can be considered in India possibly under the aegis of IDRBT along with various stakeholders like banks, vendors and their associations, government agencies and with regulator as observer. A few areas that can be considered includes areas like security architecture and principles, application security, software testing and evaluation. Under the initiative, product certification program can also be developed involving testing of technology products used to deliver financial services against minimum-security criteria. The criteria developed in this regard can represent the minimum baseline security features and functionality of various types of commercial banking software products. Criteria can be developed for certain classifications of products based on function and application. The detailed product security requirements could include areas relating to: identification, non-repudiation, authorization, confidentiality, data and system integrity, data disposal, audit, authentication, security administration, guidance documentation, security functionality and scalability.

iv. Accreditation and empanelment of security audit qualifications/certifications and security audit vendors can be considered at a wider level by Government of India/CERT-In or by IDRBT for the banking sector.

v. Collaborative efforts may also be made by reputed bodies like IDRBT, IIBF and DSCI coordinated by IBA to create customized indigenous certification courses to certify specific knowledge and skillsets in IT/information security areas for various categories of bank personnel like operational and managerial levels so as to create a large and diverse pool of requisite talent within the banking system.

vi. There is a need for IBA, IDRBT and reputed institutions like DSCI to collaborate and develop security frameworks and detailed implementation methodologies for the benefit of the banking sector.

vii. There is an increasing need for specific detailed research in security of banking technology and bringing out innovative and secure banking products in collaboration with reputed academic bodies like the IITs. IDRBT can take necessary initiatives in this regard.

viii. Given the nature of problem of cyber security, there needs to be engagement at wider level nationally and internationally, with Government, law enforcement agencies, various sectoral associations and academic institutions.

ix. RBI can consider having a multi-disciplinary Standing Committee on Information Security with representation from various stakeholders to consider new security related developments and also legal developments and based on the same to provide recommendations for suitable updation of the guidelines.

## KEY RECOMMENDATIONS:

1. Robust information security governance needs to be instituted consisting of leadership, organizational structures and processes to mitigate the growing information security threats.
2. The role of Board is to approve information security policy and provide effective oversight over the performance of the top management regarding information security. The major role of top management involves implementing Board approved information security policy, establishing necessary organizational processes/functions for information security and providing necessary resources for success of information security.
3. Each bank needs to create a separate information security function for exclusively focusing on information security management. The organization of information security function should be commensurate with the nature and size of activities of a bank including 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, their range and level of skills, and tools or techniques.
4. A sufficiently senior level official of the rank of GM/DGM/AGM needs to be designated as the Chief Information Security Officer(CISO) responsible for articulating and enforcing the policies that a bank uses to protect their information assets apart from coordinating the information security related issues / implementation within the organization as well as relevant external agencies.

5. An information security steering committee of executives should be formed with a formal terms of reference. Members of such a committee may include, amongst others, the chief executive officer (CEO) or designee, business unit executives, chief financial officer (CFO), chief information officer (CIO)/ IT Head, chief security officer (CSO), CISO (who would be the member secretary to the Committee), human resources, legal, risk management, audit, operations and public relations.
6. The CISO needs to report directly to the Head of Risk Management and should not have a direct reporting relationship with the CIO. However, CISO may have a working relationship with the CIO to develop the required rapport for understanding the IT infrastructure and operations, to build effective security in IT across the bank, in tune with the business requirements and objectives.
7. A Board approved Information security policy needs to be in place and reviewed atleast annually and in the event of any significant changes necessitating revision. The policy framework would, incorporate/take into consideration,inter-alia, aspects like alignment with business objectives; the objectives, scope, ownership and responsibility for the policy; information security organizational structure; Information security roles and responsibilities; exceptions; knowledge and skill sets required; periodic training and continuous professional education; compliance review and penal measures for non-compliance of policies.
8. Job descriptions, employment agreements, and policy awareness acknowledgements increase accountability for security. Management can communicate general and specific security roles and responsibilities for all employees within their job descriptions. Management should expect all employees, officers, and contractors to comply with security and acceptable-use policies and protect the institution's assets, including information. The job descriptions for security personnel should describe the systems and processes they will protect and the control processes for which they are responsible. Management can take similar steps to ensure contractors and consultants understand their security responsibilities as well.
9. 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 the concerned personnel. A policy needs to be in place in this regard.
10. Given the critical role of security technologies used as part of the information security framework, banks need to subject them to suitable controls across their lifecycle.
11. Risk assessment is the core competence of information security management for a bank. The risk assessment must, for each asset within 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.
12. Maintaining detailed inventory of information assets, classification of information/data and defining information security related roles and responsibilities are among the key steps of information security management.
13. An effective process towards access to information assets is one of critical requirement of information security. A bank needs to authorise access to information assets only where a valid business need exists and only for a specific time-period that the access is required. A bank should take appropriate measures to identify and authenticate users or IT assets, commensurate with risk involved. Further, for accountability purposes, a bank should ensure that users/IT assets are uniquely identified and their actions are auditable.
14. Personnel with elevated system access privileges should be closely supervised with all their systems activities logged as they have the inside knowledge and the resources to circumvent systems controls and security procedures.

15. 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.
16. 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.
17. Banks should implement suitable physical and environment controls taking into consideration 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 applicable based on the entity's unique geographical location, building configuration, neighboring entities, etc.
18. There is a vital need for initial, and ongoing, training and information security awareness program. The program 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 mechanism of tracking the effectiveness of the training programmes through an assessment/testing process, both initially as well as periodically. The matter also needs to be important agenda item during Information Security Committee meetings.
19. Robust Incident management process needs to be in place for maintaining the capability to manage incidents within an enterprise so that exposure can be 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.
20. A bank needs to have clear accountability and communication strategies to limit the impact of IT security incidents. This would require 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.
21. A bank needs to incorporate information security at all stages of software development. This would assist in improving software quality and minimising exposure to vulnerabilities.
22. Rigorous implementation of application control and security features is required. Each application should have an owner which will typically be the concerned business function that uses the application. There should be documented standards / procedures for administering the application, which are approved by the application owner and kept up-to-date.
23. All the 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, 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 audit trail or log monitoring process/procedure.
24. Critical functions , for example relating to/dealing with financial, regulatory and legal, MIS and risk assessment/management, needs to be done through proper application systems and not manually or semi-automated manner through spreadsheets which poses 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 defined time-frame.
25. 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 IP address of client machine, terminal identity or location may also be considered. Alerts regarding use of same machine for both maker and checker transactions need to be considered. The logs/alerts/exception reports need to be analyzed and any issues need to remediated at the earliest.

26. Access to application 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.
27. 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 be reversing the original authorized entry and passing a fresh entry.
28. Direct back-end updates to database should not be allowed except during exigencies with genuine business need and after due authorization as per relevant policy.
29. Banks need to ensure that application integrity statements are obtained in writing from the vendor relating to the application being free of malware at the time of sale, free of any obvious bugs, and is free of any covert channels in the code being provided and any subsequent modifications to be done on them.
30. Any changes to an application system/data needs to be justified by genuine business need and approvals supported by documentation and subjected to a robust change management process.
31. For all critical applications, either a source code must be received from the vendor or a software escrow agreement needs to 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 program fixes are also included in the escrow agreement.
32. Data transfer from one process to another or from one application to another should not have any manual intervention 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".
33. Robust system security testing needs to be carried out. It should also be ensured that web applications adequately address various vulnerabilities that lead to exploitation by fraudsters leading to undesirable consequences.
34. Multi-tier application architecture needs to be implemented for critical systems which differentiate session control, presentation logic, server side input validation, business logic and database access.
35. A bank needs to have documented Migration policy specifying systematic process for data migration and ensuring data integrity, completeness and consistency. Explicit sign offs from users/application owners needs to be obtained after each stage of migration and also after complete migration process. Audit trails need to be available to document the conversion, including data mappings and transformations.
36. Banks need to carry out necessary due diligence in respect of new technologies since they can potentially introduce additional risk exposures.
37. Any new business products introduced and along with the underlying information systems needs 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.
38. Cryptographic techniques need to be used to control access to critical/sensitive data/information in transit and storage. Banks need to deploy strong cryptography and end-to-end application layer encryption to protect customer PINs, user passwords and other sensitive data in networks and in storage.
39. There is a need for encrypting 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.

40. Constant advances in computer hardware, computational number theory, cryptanalysis and distributed brute force techniques may induce use of larger key lengths in future. It is expected that banks will properly evaluate security requirements associated with their internet 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 community of cryptographers or approved by authoritative professional bodies, reputable security vendors or government agencies.
41. Data security measures need to be in place.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.
42. Policies regarding media handling, disposal, and transit should be implemented to enable the use of protection profiles and mitigate risks to data. More sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration like integrity checkers, cryptographic hashes.
43. Banks need to frequently scan for vulnerabilities and address discovered flaws proactively to avoid significant likelihood of having their computer systems compromised. 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. Where feasible, vulnerability scanning should occur on a daily basis using an up-to-date vulnerability scanning tool.
44. A bank needs to have 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.
45. A bank would need to establish a clear allocation of responsibility for regular monitoring, with appropriate processes and tools in place to manage the volume of monitoring required, thereby reducing the risk of an incident going undetected.
46. Highly sensitive and/or critical IT assets would need to have logging enabled to record events and monitored at a level commensurate with the level of risk.
47. Banks need to employ suitable technologies that provide capabilities for effective attack detection and analysis.
48. Robust processes need to be in place for effective malware control. Anti-virus and anti-spyware software, collectively referred to as anti-malware tools, help defend against the malware threats by attempting to detect malware and block its execution.
49. An effective patch management process should 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.
50. 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.
51. Banks needs to ensure that audit trails exist for IT assets satisfying the banks business requirements including regulatory and legal requirements, facilitating audit, serving as forensic evidence when required and assisting in dispute resolution including for non-repudiation purposes. Audit trails should be secured to ensure the integrity of the information captured and preservation of evidence.
52. There should be arrangements for monitoring and reporting of the information security condition of the organisation, which are documented, agreed with top management and performed regularly. Security related metrics can be used to measure security policy implementation, the effectiveness and efficiency of security services delivery, and the impact of security events on business processes.

53. Given the multiplicity of devices and systems, banks should consider deploying suitable automated tools for log aggregation and consolidation from multiple machines/systems and for log correlation and analysis.
54. Security and Audit Processes of Critical service providers/vendors needs to be regularly assessed since ineffective third-party controls can weaken the ability of a bank to achieve its control objectives.
55. 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. There is a need to utilize technical and administrative controls to mitigate threats from identified risks to as great a degree as possible at all levels of the network. Various measures in this regard have been indicated in the report.
56. Strong controls need to initiated against any remote access facility provided by banks. The relevant controls need to be consistent with the sensitivity of remote use. For example, remote use to administer sensitive systems or databases during exigencies may include highest level of controls and monitoring processes.
57. Commercial banks should implement ISO 27001 based Information Security Management System (ISMS) Best Practices for their critical functions/processes.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. Such an ISMS offers the opportunity to define and monitor service levels internally as well as in contractor/partner organizations, thus demonstrating the extent to which there is effective control of security risks.Banks may also additionally consider other reputed security frameworks and standards from well-known institutions like ISACA, DSCI, IDRBT etc.
58. If a bank uses a wireless network, it should carefully evaluate the risks and implement appropriate additional controls.
59. Events that trigger the implementation of a business continuity plan may have significant security implications. Risk assessments should consider the changing risks that appear in business continuity scenarios and the different security posture that may be established.
60. Information security assurance needs to be obtained through periodic penetration testing exercises, audits and vulnerability assessments. 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.
61. A bank needs to engage independent security specialists to assess the strengths and weaknesses of critical internet-based applications, systems and networks before initial implementation, and at least annually thereafter.
62. A bank should manage the information security risk management framework on an ongoing basis as a security programme in a systematic manner.
63. Various important security measures have been suggested in respect of debit cards, ATMs, internet banking, phone banking and mobile banking.
64. RBI may consider moving over to chip based cards along with upgradation of necessary infrastructure like ATMs/POS terminals in this regard in a phased manner.
65. For debit / credit card transactions at the POS terminals, PIN based authorization system may be put in place (without any looping) in place of the existing signature based system and the non-PIN based POS terminals need to be withdrawn in a phased manner.

66. In view of the proliferation of cyber attacks and their potential consequences, banks should implement two-factor authentication for fund transfers and critical activities like changing customer related details through internet banking.
67. 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.
68. While not using the asymmetric cryptosystem and hash function is a source of legal risk, keeping in view the various methods and issues discussed above, for carrying out critical transactions like fund transfers, the banks, at the least, need to implement two-factor authentication through user id/password combination and second factor like (a) OTP/dynamic access code through various modes like SMS over mobile phones or hardware token or (b) a digital signature (through a token containing digital certificate and associated private key), preferably for the corporate customers .
69. 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.
70. 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. 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.
71. Risk based transaction monitoring /surveillance process needs to be instituted by banks as an effective alert system to enhance capability to identify anomalous/suspicious transactions.
72. 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 before they choose to subscribe to such services.
73. 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.
74. A few security issues and best practices in respect of emerging/new technologies like virtualization, cloud computing and MPLS have been indicated.
75. Given that control, security, legal issues on cloud computing are still evolving, a bank needs to be cautious and carry out necessary due diligence and assess the risks comprehensively before considering cloud computing.
76. There needs to be forum of CISOs who can periodically interact and share experiences regarding any information security threats. It is reported that a CISO forum is already functional under IDRBT. The forum may among other functions endeavour to share good practices and identify any specific information security issues and flag them to appropriate stakeholders like regulator, IBA etc. A member from the regulator can also be part of the meetings of the forum.

77. There is a need for a system of information sharing akin to the functions performed by FS-ISAC (Financial Services Information Sharing Agency) in the US. IDRBT as a sub-CERT to the banking system can function as a nodal point for information sharing.
78. Collaborative efforts may also be made by reputed bodies like IDRBT, IIBF and DSCI coordinated by IBA to create customized indigenous certification courses to certify specific knowledge and skillsets in IT/information security areas for various categories of bank personnel like operational and managerial levels so as to create a large and diverse pool of requisite talent within the banking system.
79. In order to reduce the time, cost, and complexity of software assurance and to ensure its security, resiliency, sustainability and integrity and increase the effectiveness of the methods used by the banking industry for Software Assurance, an initiative similar to FSTC Software Assurance Initiative (SAI) in US can be considered in India possibly under the aegis of IDRBT along with various stakeholders like banks, vendors and their associations, government agencies and with regulator as observer.
80. Accreditation and empanelment of security audit qualifications/certifications and security audit vendors can be considered at a wider level by Government of India/CERT-In or by IDRBT for the banking sector.
81. There is a need for IBA, IDRBT and reputed institutions like DSCI to collaborate and develop security frameworks and detailed implementation methodologies for the benefit of the banking sector.
82. There is an increasing need for specific detailed research in security of banking technology and bringing out innovative and secure banking products in collaboration with reputed academic bodies like the IITs. IDRBT can take necessary initiatives in this regard.
83. Given the nature of problem of cyber security, there needs to be engagement at wider level nationally and internationally, with Government, law enforcement agencies, various industrial sector associations and academic institutions.
84. RBI can consider having a multi-disciplinary Standing Committee on Information Security with representation from various stakeholders to consider new security related developments and also legal developments and based on the same to provide recommendations for suitable updating of the guidelines.