Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds

Reserve Bank of India
Department of Banking Supervision, Central Office,
Mumbai

Table of Contents

Chapter 1: IT GOVERNANCE

Introduction:

Corporate Governance constitutes the accountability framework of a bank. IT Governance is an integral part of it. It involves leadership support, organizational structure and processes to ensure that a bank's IT sustains and extends business strategies and objectives. Effective IT Governance is the responsibility of the Board of Directors and Executive Management.

Access to reliable information has become an indispensable component of conducting business, indeed, in a growing number of banks, information is business.

Today, almost every commercial bank branch is at some stage of technology adoption: core banking solution (CBS), or alternate delivery channels such as internet banking, mobile banking, phone banking and ATMs.

GUIDANCE FOR BANKS

a) Roles and Responsibilities and Organizational Framework:

Well-defined roles and responsibilities of Board and Senior Management are critical, while implementing IT Governance. Clearly-defined roles enable effective project control. People, when they are aware of others' expectations from them, are able to complete work on time, within budget and to the expected level of quality.

IT Governance Stakeholders include:

- Board of Directors
- IT Strategy Committees
- CEOs
- Business Executives
- CIOs
- IT Steering Committees (operating at an executive level and focusing on priority setting, resource allocation and project tracking)
- Chief Risk Officer
- Risk Committees

b) Organisation Structure:

i). Expertise *at the Board Level:* IT Strategy Committees should have some form of participation at the Board level. This is to ensure that as part of the Corporate Governance initiatives, IT Governance is also addressed, so as to advice on strategic direction on IT and to review IT investments on Board's behalf.

ii). *Qualified and Independent IT Strategy Committee:* A qualified and an independent IT Strategy Committee should be set up with a minimum of two directors as members, one of whom should be an independent director. IT Strategy Committee members should be technically competent. At least one member should have substantial IT expertise in managing technology.

(Explanation1: Technically competent herein will mean the ability to understand and evaluate technology systems.

Explanation 2: A member will be considered to have "substantial IT expertise" if he has a minimum of seven years of experience in managing IT systems and/or leading/guiding technology initiatives/projects. Such a member should also have an understanding of banking processes at a broader level and of the impact of IT on such processes. If not, then the member should be trained on these aspects.)

iii). *Chairman of an IT Strategy Committee shall be an independent director.* Also, the CIO should be a part of this committee, who should be present at Board meetings to help IT strategy align with business goals. The IT Strategy Committee should meet at appropriate frequency as and when needed (at least four times in a year) and not more than four months should elapse between two meetings.

iv). *Powers of IT Strategy Committee:* It is recommended that the committee should have following powers:

- Perform oversight functions over the IT Steering Committee (at a senior management level)
- Investigate activities within this scope
- Seek information from any employee
- Obtain outside legal or professional advice
- Secure attendance of outsiders with relevant expertise, if it considers necessary
- Work in partnership with other Board committees and Senior Management to provide input, review and amend the aligned corporate and IT strategies

c) Recommended Roles and Responsibilities:

Board of Directors/ IT Strategy Committee:

Some of the roles and responsibilities include:

- Approving IT strategy and policy documents
- Ensuring that the management has put an effective strategic planning process in place
- Ratifying that the business strategy is indeed aligned with IT strategy
- Ensuring that the IT organizational structure complements the business model and its direction
- Ascertaining that management has implemented processes and practices that ensure that the IT delivers value to the business
- Ensuring IT investments represent a balance of risks and benefits and that budgets are acceptable
- Monitoring the method that management uses to determine the IT resources needed to achieve strategic goals and provide high-level direction for sourcing and use of IT resources
- Ensuring proper balance of IT investments for sustaining bank's growth
- Becoming aware about exposure towards IT risks and controls. And evaluating effectiveness of management's monitoring of IT risks
- Assessing Senior Management's performance in implementing IT strategies
- Issuing high-level policy guidance (e.g. related to risk, funding, or sourcing tasks)
- Confirming whether IT or business architecture is to be designed, so as to derive the maximum business value from IT

- Overseeing the aggregate funding of IT at a bank-level, and ascertaining if the management has resources to ensure the proper management of IT risks
- Reviewing IT performance measurement and contribution of IT to businesses (i.e., delivering the promised value)

Risk Management Committee*:*

- Promoting an enterprise risk management competence throughout the bank, including facilitating development of IT-related enterprise risk management expertise
- Establishing a common risk management language that includes measures around likelihood and impact and risk categories

Executive Management Level:

Among executives, the responsibility of Senior executive in charge of IT operations/Chief Information officer (CIO) is to ensure implementation from policy to operational level involving IT strategy, value delivery, risk management, IT resource and performance management.

Business Unit Level:

IT Steering Committee*:*

An IT Steering Committee needs to be created with representatives from the IT, HR, legal and business sectors. Its role is to assist the Executive Management in implementing IT strategy that has been approved by the Board. It includes prioritization of IT-enabled investment, reviewing the status of projects (including, resource conflict), monitoring service levels and improvements, IT service delivery and projects. The committee should focus on implementation. Its functions *inter-alia* include:

- Defining project priorities and assessing strategic fit for IT proposals
- Performing portfolio reviews for continuing strategic relevance
- Reviewing, approving and funding initiatives, after assessing value-addition to business process
- Balancing between investment for support and growth
- Ensuring that all critical projects have a component for “project risk management”
- Sponsoring or assisting in governance, risk and control framework, and also directing and monitoring key IT Governance processes
- Defining project success measures and following up progress on IT projects
- Consult and advice on the selection of technology within standards
- Advice on infrastructure products
- Provide direction relating to technology standards and practices
- Ensure that vulnerability assessments of new technology is performed
- Verify compliance with technology standards and guidelines
- Consult and advice on the application of architecture guidelines
- Ensure compliance to regulatory and statutory requirements
- Provide direction to IT architecture design and ensure that the IT architecture reflects the need for legislative and regulatory compliance, the ethical use of information and business continuity

The IT Steering committee should appraise/report to the IT strategy Committee periodically.

IT Line Management and Business Unit Management

Specific roles of IT Line Management and Business Unit Management, with respect to technology, may vary depending upon the bank's approach to risk management and policy enforcement – either a centralized or a decentralized strategy.

d) IT Organizational Structure:

The IT organizational structure should be commensurate with the size, scale and nature of business activities carried out by the bank and the underlying support provided by information systems for the business functions. The broad areas or functions that can be considered for IT organizational structure will include technology and development, IT operations, IT assurance and supplier and resource management, each of which may be headed by suitably experienced and trained senior officials (preferably not less than the rank of AGM).

Illustrative functions of the various divisions may include:

- **Technology:** All IT architecture (systems, software, networks and telecommunications), strategic technology decisions, technology life-cycle management, thought leadership and technology research and prototype development

- **Development:** All IT development initiatives or projects, related budgets, project management, quality of outcomes, managing outsourced IT development, testing all solutions (developed in-house or outsourced)

- **IT Operations:** All IT operations (servers, operating systems, databases, applications and help desks), such as managing IT Infrastructure (facilities, data centres, networks and telecommunication), high availability and reliability of systems, managing outsourced IT operations and services

- **IT Assurance Function:** All quality, risk and compliance management initiatives within the IT vertical such as performance or conformance metrics, reports, dashboards, internal user feedback and analysis, monitoring IT projects, interaction with audit, risk and compliance functions within a bank

Critical Components of IT Governance Framework*:*

The basic principles of value delivery, IT Risk Management, IT resource management (including IT project management) and performance management must form the basis of governance framework. One of the well-known international frameworks in achieving effective control over IT and related risks is the "**Control Objectives for Information Technology"(COBIT**) that is issued by Information Technology Governance Institute (**ITGI)**. The framework provides **five focus areas** for IT Governance. The first two concepts namely Value delivery and IT risk management are outcomes, while the remaining three are drivers: IT strategic alignment, IT resource management and performance measurement (refer Chapter 1 of the Working Group Report). IT Governance has a continuous life-cycle. It's a process in which IT strategy drives the processes, using resources necessary to execute responsibilities. Given the criticality of the IT, banks may follow relevant aspects of such prudential governance standards that have found acceptability in the industry.

Focus Areas for IT Governance:

IT Governance entails number of activities for the Board and Senior Management, such as becoming aware of role and impact of IT on a bank: assigning responsibilities, defining constraints within which to operate, measuring performance, managing risk and obtaining assurance.

Recommendations, Actions on IT Governance practices:

Before adopting these, banks are required to evaluate their nature and scope of activities and the current level of leverage of IT and related controls.

1. **Policies and Procedures:**
   (a) The bank needs to have IT-related strategy and policies that covers areas such as:
      - Existing and proposed hardware and networking architecture for a bank and its rationale
      - Broad strategy for procurement of hardware and software solutions, vendor development and management
      - Standards for hardware or software prescribed by the proposed architecture
      - Strategy for outsourcing, in-sourcing, procuring off-the-shelf software, and in-house development
      - IT Department's Organizational Structure
      - Desired number and level of IT expertise or competencies in bank's human resources, plan to bridge the gap (if any) and requirements relating to training and development
      - Strategy for keeping abreast with technology developments and update systems as and when required
      - Strategies converted into clear IT Initiatives with a broad time frame

   (b) IT strategy and policy needs to be approved by the Board
   (c) Detailed operational procedures may be formulated in relevant areas including for data centre operations
   (d) A bank needs to follow a structured approach for the long-range planning process considering factors such as organizational model and changes to it, geographical distribution, technological evolution, costs, legal and regulatory requirements, requirements of third-parties or market, planning horizon, business process re-engineering, staffing, in- or outsourcing, etc.
   (e) There needs to be an annual review of IT strategy and policies taking into account the changes to the organization's business plans and IT environment
   (f) Long-range IT strategy needs to be converted to short-range plans regularly, for achievability
   (g) The short-range plan, inter-alia, may cover the following: plan for initiatives specified in the long-range plan or initiatives that support the long-range plans, System wise transition strategy, Responsibility and plan for achievement
   (h) Banks need to establish and maintain an enterprise architecture framework or enterprise information model to enable applications development and decision-supporting activities, consistent with IT strategy. The model should facilitate optimal creation, use and sharing of information by a business, in a way that it maintains integrity, and is flexible, functional, cost-effective, timely, secure and resilient to failure
   (i) There is also a need to maintain an "enterprise data dictionary" that

incorporates the organization's data syntax rules. This should enable the sharing of data among applications and systems, promote a common understanding of data among IT and business users and preventing incompatible data elements from being created

(j) Banks need to establish a classification scheme that applies throughout the enterprise, based on the criticality and sensitivity (e.g. public, confidential, or top secret) of enterprise data. This scheme should include details of data ownership; definition of appropriate security levels and protection controls; and a brief description of data retention and destruction requirements (criticality and sensitivity). It should be used as a basis for applying controls such as access controls, archiving or encryption. Banks also need to define and implement procedures to ensure integrity and consistency of data stored in electronic form (read: databases, warehouses and archives). More details are indicated in the "Chapter: Information security".

(k) There is a need for a CIO in banks. He has to be the key business player and a part of the executive decision-making function. His key role would be to be the owner of IT functions: enabling business and technology alignment. The CIO is required to be at a level equivalent to that of the Chief General Manager (CGM) or General Manager (GM), having credible operational experience or proven leadership and awareness and knowledge of IT or having related IT experience

(l) Bank-wide risk management policy or operational risk management policy needs to be incorporate IT-related risks also. The Risk Management Committee periodically reviews and updates the same (at least annually). The IT risk function needs to be integrated into the operational risk management function.

Some of the major issues in respect of control aspects that inter alia may be considered by banks are:

1. Major IT development projects need to be aligned with business strategy
2. IT investments need to be suitably balanced between maintaining the infrastructure that support the bank's "as is" operations, and the infrastructure that transforms the operations and enables the business to grow and compete in new areas
3. IT-enabled investment programmes and other IT assets and services are managed to ascertain that they deliver the greatest possible value in supporting the bank's strategy and objectives:
    - Infrastructure to facilitate creation and sharing of business information
    - Flexibility and ensuring programmes are amenable to maintenance and integration
    - They are functional, timely, secure and resilient to failure
    - Logically extends, maintains and manages disparate legacy systems and new applications
    - Ensures standard, reusable and modular applications and components
4. IT function supports robust and comprehensive Management Information System in respect of various business functions as per the needs of the business that facilitate decision making by management
5. Project management and quality assurance steps should be implemented to ensure systems are delivered on time, to cost and with the necessary level of functionality
6. Project-level steering committees needs to be created for taking responsibility for execution of the project plan, achievement of outcomes and project completion. The various responsibilities include reviewing progress against the project plan, reviewing and approving changes to project resource allocation, time lines, objectives, costs,

keeping the project scope under control and approving changes to the business case, acting on escalated project issues and resolving conflicts between stakeholder groups and assisting in evaluation of project risks, and project risk management approaches

7. Periodical review of all non-performing or irrelevant IT projects in the bank, if any, and taking suitable actions
8. IT management needs to assess IT risks and suitably mitigate them
9. Bank's risk management processes for its e-banking activities are integrated into its overall risk management approach. A process should be in place to have effective management oversight over the risks associated with e-banking activities, including specific accountability, policies and controls to manage these
10. Appropriate measures are implemented to ensure adherence to customer privacy requirements applicable to the jurisdictions to which the bank is providing e-banking products and services, including foreign jurisdictions where the bank operates
11. Appropriate procedures are implemented to comply with legislative, regulatory and contractual requirements on the use of systems and software where IPR, copyrights and on the use of proprietary software products are applicable
12. For managing project risks, a consistent and formally-defined programme and project management approach needs to be applied to IT projects that enable stakeholder participation and monitoring of project risks and progress. Additionally, for major projects, formal project risk assessment needs to be carried out and managed on an ongoing basis
13. Inter-dependencies between risk elements are considered in the risk assessment process, as threats and vulnerabilities have the potential to compromise interconnected and interdependent systems and processes
14. Procedures to assess the integration and interoperability of complex IT processes (such as problem, change and configuration management) exists before committing additional investments
15. Tools such as IT balanced scorecard may be considered for implementation, with approval from key stakeholders, to measure performance along dimensions: financial, customer satisfaction, process effectiveness, future capability and assess IT management performance based on metrics such as scheduled uptime, service levels, transaction throughput and response times and application availability
16. Banks may also consider assessing the maturity level, set a target as per the IT Governance maturity model, design an action plan and subsequently implement it to reach the target maturity level

CHAPTER 2 – INFORMATION SECURITY

Introduction:

Information and the knowledge based on it have increasingly become recognized as 'information assets', which are vital enablers of business operations. Hence, they require organizations to provide adequate levels of protection. For banks, as purveyors of money in physical form or in bits and bytes, reliable information is even more critical and hence information security is a vital area of concern.

Robust information is at the heart of risk management processes in a bank. Inadequate data quality is likely to induce errors in decision making. Data quality requires building processes, procedures and disciplines for managing information and ensuring its integrity, accuracy, completeness and timeliness. The fundamental attributes supporting data quality should include accuracy, integrity, consistency, completeness, validity, timeliness, accessibility, usability and auditability. The data quality provided by various applications depends on the quality and integrity of the data upon which that information is built. Entities that treat information as a critical organizational asset are in a better position to manage it proactively.

Information security not only deals with information in various channels like spoken, written, printed, electronic or any other medium but also information handling in terms of creation, viewing, transportation, storage or destruction .This is in contrast to IT security which is mainly concerned with security of information within the boundaries of the network infrastructure technology domain. From an information security perspective, the nature and type of compromise is not as material as the fact that security has been breached.

To achieve effective information security governance, bank management must establish and maintain a framework to guide the development and maintenance of a comprehensive information security programme.

Basic Principles of Information Security:

For over twenty years, information security has held confidentiality, integrity and availability (known as the CIA triad) to be the core principles. There is continuous debate about extending this classic trio. Other principles such as Authenticity, Non-repudiation and accountability are also now becoming key considerations for practical security installations.

- ***Confidentiality:*** Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred. Breaches of confidentiality take many forms like Hacking, Phishing, Vishing, Email-spoofing, SMS spoofing, and sending malicious code through email or Bot Networks, as discussed earlier.

- ***Integrity:*** In information security, integrity means that data cannot be modified without authorization. This is not the same thing as referential integrity in databases.

Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when he/she is able to modify his own salary in a payroll database, when an employee uses programmes and deducts small amounts of money from all customer accounts and adds it to his/her own account (also called salami technique), when an unauthorized user vandalizes a web site, and so on.
On a larger scale, if an automated process is not written and tested correctly, bulk updates to a database could alter data in an incorrect way, leaving the integrity of the data compromised. Information security professionals are tasked with finding ways to implement controls that prevent errors of integrity.

- ***Availability:*** For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service (DoS) and distributed denial-of service (DDoS) attacks.

- ***Authenticity:*** In computing, e-business and information security it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are.

- ***Non-repudiation***: In law, non-repudiation implies one's intention to fulfill one's obligations under a contract / transaction. It also implies that a party to a transaction cannot deny having received or having sent an electronic record. Electronic commerce uses technology such as digital signatures and encryption to establish authenticity and non-repudiation.

In addition to the above, there are other security-related concepts and principles when designing a security policy and deploying a security solution. They include identification, authorization, accountability, and auditing.

- ***Identification:*** Identification is the process by which a subject professes an identity and accountability is initiated. A subject must provide an identity to a system to start the process of authentication, authorization and accountability. Providing an identity can be typing in a username, swiping a smart card, waving a proximity device, speaking a phrase, or positioning face, hand, or finger for a camera or scanning device. Proving a process ID number also represents the identification process. Without an identity, a system has no way to correlate an authentication factor with the subject.

- ***Authorization:*** Once a subject is authenticated, access must be authorized. The process of authorization ensures that the requested activity or access to an object is possible given the rights and privileges assigned to the authenticated identity. In most cases, the system evaluates an access control matrix that compares the subject, the object, and the intended activity. If the specific action is allowed, the subject is authorized. Else, the subject is not authorized.

- ***Accountability and auditability:*** An organization's security policy can be properly enforced only if accountability is maintained, i.e., security can be maintained only if subjects are held accountable for their actions. Effective accountability relies upon the capability to prove a subject's identity and track their activities. Accountability is established by linking a human to the activities of an online identity through the

security services and mechanisms of auditing, authorization, authentication, and identification. Thus, human accountability is ultimately dependent on the strength of the authentication process. Without a reasonably strong authentication process, there is doubt that the correct human associated with a specific user account was the actual entity controlling that user account when an undesired action took place.

Information Security Governance

Information security governance consists of the leadership, organizational structures and processes that protect information and mitigation of growing information security threats like the ones detailed above.
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 and a review on information security needs to be escalated to the Board on a quarterly basis.

Chief information security officer (CISO)

A sufficiently senior level official, of the rank of GM/DGM/AGM, should be designated as Chief Information Security Officer, responsible for articulating and enforcing the policies that banks use to protect their information assets apart from coordinating the security related issues / implementation within the organization as well as relevant external agencies. The CISO needs to report directly to the Head of Risk Management and should not have a direct reporting relationship with the CIO. However, the CISO may have a working relationship with the CIO to develop the required rapport to understand the IT infrastructure and operations, to build effective security in IT across the bank, in tune with business requirements and objectives.

Critical components of information security:

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 and the legal requirements
    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) 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.

4) 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.

5) 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.

6) 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 labelling 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 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. Robust System Security Testing, in respect of critical e-banking systems, needs to incorporate, inter-alia, specifications relating to information leakage, business logic, authentication, authorization, input data validation, exception/error handling, session management, cryptography and detailed logging, as relevant. These need to be carried out atleast on annual basis.

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) **Encryption Types:**

Symmetric encryption is the use of the same key and algorithm by the creator and reader of a file or message. The creator uses the key and algorithm to encrypt, and the reader uses both to decrypt. Symmetric encryption relies on the secrecy of the key. If the key is captured by an attacker, either when it is exchanged between the communicating parties, or while one of the parties uses or stores the key, the attacker can use the key and the algorithm to decrypt messages or to masquerade as a message creator.
Asymmetric encryption lessens the risk of key exposure by using two mathematically related keys, the private key and the public key. When one key is used to encrypt, only the other key can decrypt. Therefore, only one key (the private key) must be kept secret. The key that is exchanged (the public key) poses no risk if it becomes known. For instance, if individual A has a private key and publishes the public key, individual B can obtain the public key, encrypt a message to individual A, and send it. As long as an individual keeps his private key secure from disclosure, only individual A will be able to decrypt the message.

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

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 e.g., based on the information handled, the business processes supported and the environments in which they are used) , recording patches that have been applied (for e.g., using an inventory of computer assets including their patch level).
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 (e.g., 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 (e.g., on a change request form) and accepted only from authorised individuals and changes should be approved by an appropriate authority
   - The potential business impacts of changes should be assessed (for e.g., in terms of the overall risk and impact on other components of the application)
   - Changes should be tested to help determine the expected results (for e.g., deploying the patch into the live environment)
   - Changes should be reviewed to ensure that they do not compromise security controls (e.g., by checking software to ensure it does not contain malicious code, such as a trojan horse or a virus)
   - Back-out positions should be established so that the application can recover from failed changes or unexpected results

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 provider, the bank should ensure that it has access to relevant audit trails maintained by the service provider apart from ensuring that the audit trails maintained by the service provider meet the bank's standards.

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 (e.g., 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 rule set that disallows all inbound and outbound traffic that is not specifically allowed
- Using NAT and split DNS to hide internal system names and addresses from external networks
- Using proxy connections for outbound HTTP connections and filtering malicious code

- Hardening the firewall by removing all unnecessary services and appropriately patching, enhancing, and maintaining all software on the firewall unit
- Restricting network mapping capabilities through the firewall, primarily by blocking inbound ICMP (Internet Control Messaging Protocol) traffic
- Backing up firewalls to internal media and not backing up the firewall to servers on protected networks
- Logging activity, with daily administrator review and limiting administrative access to few individuals
- Using security monitoring devices and practices to monitor actions on the firewall and to monitor communications allowed through the firewall
- Administering the firewall using encrypted communications and strong authentication, accessing the firewall only from secure devices, and monitoring all administrative access
- Making changes only through well-administered change control procedures.

The firewall also needs to be configured for authorized outbound network traffic. In the case of a compromised host inside the network, outbound or egress filtering can contain that system and prevent it from communicating outbound to their controller – as in the case with botnets. Often times, firewalls default to allowing any outbound traffic, therefore, organizations may need to explicitly define the acceptable outbound communication policies for their networks. In most cases the acceptable outbound connections would include SMTP to any address from only your SMTP mail gateway(s), DNS to any address from an internal DNS server to resolve external host names, HTTP and HTTPS from an internal proxy server for users to browse web sites, NTP to specific time server addresses from an internal time server(s), any ports required by Anti-Virus, spam filtering, web filtering or patch management software to only the appropriate vendor address(es) to pull down updates and any other rule where the business case is documented and signed off by appropriate management.

Perimeters may contain proxy firewalls or other servers that act as a control point for Web browsing, e-mail, P2P, and other communications. Those firewalls and servers frequently are used to enforce the institution's security policy over incoming communications. Enforcement is through anti-virus, anti-spyware, and anti-spam filtering, the blocking of downloading of executable files, and other actions. To the extent that filtering is done on a signature basis, frequent updating of the signatures may be required, as had been explained earlier.

Perimeter servers also serve to inspect outbound communications for compliance with the institution's security policy. Perimeter routers and firewalls can be configured to enforce policies that forbid the origination of outbound communications from certain computers. Additionally, proxy servers could be configured to identify and block customer data and other data that should not be transmitted outside the security domain.

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 modelled and valid activity in future periods, and the potential for malicious activity to take place while the modelling is performed. This method is best employed in environments with predictable, stable activity.

Anomaly detection can be an effective supplement to signature-based methods by signalling attacks for which no signature yet exists. Proper placement of NIDS sensors is a strategic decision determined by the information the bank is trying to obtain. Placement outside the firewall will deliver IDS alarms related to all attacks, even those that are blocked by the firewall. With this information, an institution can develop a picture of potential adversaries and their expertise based on the probes they issue against the network.

Because the placement is meant to gain intelligence on attackers rather than to alert on attacks, tuning generally makes the NIDS less sensitive than if it is placed inside the firewall. A NIDS outside the firewall will generally alert on the greatest number of unsuccessful attacks while NIDS monitoring behind the firewall is meant to detect and alert on hostile intrusions. Multiple NIDS units can be used, with placement determined by the expected attack paths to sensitive data. In general, the closer the NIDS is to sensitive data, the more important the tuning, monitoring, and response to NIDS alerts. It is generally recommended that NIDS can be placed at any location where network traffic from external entities is allowed to enter controlled or private networks.

"**Tuning**" refers to the creation of signatures and alert filters that can distinguish between normal network traffic and potentially malicious traffic apart from involving creation and implementation of different alerting and logging actions based on the severity of the perceived attack. Proper tuning is essential to both reliable detection of attacks and the

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 obviously a concern, false positives can also hinder detection. When security personnel are overwhelmed with the number of false positives, their review of NIDS reports may be less effective thereby allowing real attacks to be reported by the NIDS but not suitably acted upon. Additionally, they may tune the NIDS to reduce the number of false positives, which may increase the number of false negatives. Risk-based testing is necessary in this regard to ensure the detection capability is adequate.

c) Network Intrusion Prevention Systems

Network Intrusion Prevention Systems (NIPS) are an access control mechanism that allow or disallow access based on an analysis of packet headers and packet payloads. They are similar to firewalls because they are located in the communications line, compare activity to pre-configured decisions of the type of packets to filter or block, and respond with pre-configured actions. The IPS units generally detect security events in a manner similar to IDS units and are subject to the same limitations. After detection, however, the IPS unit 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. Banks 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 at least 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 corrective actions. An assessment differs from an audit by not having a set of standards to test against. It differs from a penetration test by providing the tester with full access to the systems being tested. Assessments may be focused on the security process or the information system. They may also focus on different aspects of the information system, such as one or more hosts or networks. Vulnerability assessment was explained earlier in the chapter.

The assurance work needs to be performed by appropriately trained and independent information security experts/auditors. The strengths and weaknesses of critical internet-based applications, other critical systems and networks needs to be carried out before each initial implementation, and at least annually thereafter. Any findings needs to be reported and monitored using a systematic audit remediation or compliance tracking methodology.

A bank needs to regularly assess information security vulnerabilities and evaluate the effectiveness of the existing IT security risk management framework, making any necessary adjustments to ensure 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) *General information regarding 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.

(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 at least SSL v3 or Extended Validation –SSL / TLS 1.0 128 bit encryption level for all online activity.
iii.Re-establishment of any session after interruption should require normal user

identification, authentication, and authorization. Moreover, strong server side validation should be enabled.
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.

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. There is a legal risk in not using the asymmetric cryptosystem and hash function for authenticating electronic transactions. However, it is observed that some banks still use weak user id/password based authentication for fund transfers using internet banking. For carrying out critical transactions like fund transfers, the banks, at the least, need to implement robust and dynamic two-factor authentication through user id/password combination and second factor like (a) a digital signature (through a token containing digital certificate and associated private key) (preferably for the corporate customers) or (b) OTP/dynamic access code through various modes (like SMS over mobile phones or hardware token).
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.

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.

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: Computing environment owned by a company is shared with client companies through web-based service over Internet which hosts all the programs to run everything from e-mail to word processing to complex data analysis programs. This is called cloud computing.
The term cloud computing probably comes from the use of a cloud image to represent the Internet or some large networked environment. We don’t care much what’s in the cloud or what goes on there except that we get the services we require. Service may include software, platform or infrastructure.
At the backend, cloud computing can make use of virtualization and grid computing. In grid computing, networked computers are able to access and use the resources of every other computer on the network.

Cloud Computing Concerns

Perhaps the biggest concerns about cloud computing are security and privacy. The idea of handing over important data to another company worries some people. Corporate executives might hesitate to take advantage of a cloud computing system because they can't keep their company's information under lock and key.

Privacy is another matter. If a client can log in from any location to access data and applications, it's possible the client's privacy could be compromised. Cloud computing companies will need to find ways to protect client privacy by implementing reliable authentication techniques.

A cloud computing system must ensure backup of all its clients' information.

Some questions regarding cloud computing are more legal. Does the user or company subscribing to the cloud computing service own the data? Does the cloud computing system, which provides the actual storage space, own it? Is it possible for a cloud computing company to deny a client access to that client's data? Several companies, law firms and universities are debating these and other questions about the nature of cloud computing. Thus, there are issues relating to data security and privacy, compliance and legal/contractual issues.

A few examples of cloud computing risks that need to be managed include:

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 centre. 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.

ANNEXURE:

ANNEX A – Provides an illustrative information security related checklist

CHAPTER 3: IT OPERATIONS

Introduction:

For banks in which information technology (IT) systems are used to manage information, IT Operations should support processing and storage of information, such that the required information is available in a timely, reliable, secure and resilient manner.

IT Operations are a set of specialized organizational capabilities that provide value to customers (internal or external) in form of IT services. Capabilities take the form of functions and processes for managing services over technology lifecycle. IT Operations should ensure effectiveness and efficiency in delivery and support of these services to ensure value for customers.

Scope:

Functions covered as a part of IT Operations are:

- IT Service Management
- Infrastructure Management
- Application Lifecycle Management
- IT Operations Risk Framework

The Board, Senior Management:

- Roles and Responsibilities:

Bank's Board of Directors has ultimate responsibility for oversight over effective functioning of IT operational functions. Senior management should ensure the implementation of a safe IT Operation environment. Policies and procedures defined as a part of IT Operations should support bank's goals and objectives, as well as statutory requirements.

- Functional areas, within the preview of these roles, are*:*

- Core IT Operations
- Business Line-specific IT Operations
- Any Affiliates-related IT Operations
- Business Partners' Operations (including that of IT support vendors if any)

The Board or Senior Management should take into consideration the risk associated with existing and planned IT operations and the risk tolerance and then establish and monitor policies for risk management.

Organisational Structure*:*

IT Operations include business services that are available to internal or external customers using IT as a service delivery component–such as mobile or internet banking. IT Operations include components that are used to support IT Operations: service desk application, ticketing and event management tools, etc. Banks may consider including Test and Quality Assurance Environment (besides, Production Environment) within the scope of IT Operations.

a) **Service Desk*:*** The service desk is the primary point of contact (Single Point of Contact or SPOC) for internal and external customers. Besides handling incidents

and problems, it also provides interface to other IT operation processes, such as Request For Change (RFC), Request Fulfillment, Configuration Management, Service Level Management and Availability Management, etc. It can have the following functions:

- Interacting with customers (e-mail, voice or chat): first-line customer liaison
- Recording and tracking incidents and problems or requests for change
- Keeping customers informed on request status and progress
- Making an initial assessment of requests, attempting to resolve them via knowledge management or escalating, based on agreed service levels
- Monitoring and escalation procedures relative to the appropriate SLA
- Managing the request life-cycle, including closure and verification
- Coordinating second-line and third-party support groups
- Providing management information for service improvement
- Identifying problems
- Closing incidents and confirmation with the customer
- Contributing to problem identification
- Performing user satisfaction surveys

A structure for the Service Desk that allows optimum resource utilization would include*:*

- Local Service Desk
- Central Service Desk
- Virtual Service Desk
- Follow the Sun i.e. in time zones such that service desk is available for assistance and recording of incidents round the clock
- Specialized Service Desk Groups

b) **<u>IT Operations Management</u>**

i. IT Operations management is a function which is primarily responsible for the day-to-day management and maintenance of an organisation's IT infrastructure, ensuring service delivery to the agreed level as defined by Service Level Agreement (SLA).

ii. IT Operations management can have following functions:

- **Operational Control:** Oversee the execution and monitoring of operational activities and events in IT infrastructure which is within the preview of IT operations. Operational control activities are normally carried out by Network Operations Centre (NOC) or Operations Bridge. Beside execution and monitoring of routine tasks operation control also involve the following activities :

- *Console Management*
- *Job Scheduling*
- *Backup and Restoration*
- *Print and Output Management*
- *General Maintenance Activities*

- **Facility Management:** It refers to management of physical IT environment of data centre, computers rooms and recovery sites

iii. Operations Management Structure: For all practical reasons, application management and infrastructure management teams should be part of IT operations. As, these functions manage and execute operational activities, whereas others delegate these to dedicate IT operations function.

c) **<u>Application Management:</u>**

It involves handling and management of application as it goes through the entire life-cycle. The life-cycle encompasses both application development and application management activities. Sub-activities that can be defined for application management functions are:

- **Application Development:** It is concerned with activities needed to plan, design and build an application that ultimately is used by a part of the organisation to address a business requirement. This also includes application acquisition, purchase, hosting and provisioning
- **Application Maintenance/Management:** It focuses on activities that are involved with the deployment, operation, support and optimisation of the application

Application Management related functions may include the following:

- Managing operational applications, whether vendor developed, or off-the-shelf or in-house
- It acts as a custodian of technical knowledge and expertise related to managing and supporting applications. It ensures that the technical knowledge and expertise required to design, develop, test, manage and improve IT services are identified, developed and refined. Therefore, it participates in IT operation management
- It ensures that appropriate resources are effectively trained and deployed to deliver, build, transit, operate and improve the technology required to manage and support IT services
- It defines and executes training programmes
- It documents skill sets available within an organisation and skills that need to be developed to manage application management as function
- It defines standards to be adapted when defining new application architecture and involvement in design and build of new services
- It assesses the risk involved in an application architecture
- It records feedbacks on availability and capacity management activities
- It designs and performs tests for functionality, performance and manageability of IT services
- It defines and manages event management tools
- It participates in incident, problem, performance, change and release management, and in resource fulfillment
- It provides information on the Configuration Management System

Application Management Structure: Though activities to manage applications are generic and consistent across applications; application management function, for all practical reasons, is not performed by a single department or group. It consists of technical areas as per technical skill sets and expertise. Some of these can be:

- Financial application
- Infrastructure applications
- Messaging and collaborative applications
- Web portal or web applications
- Contact centre applications
- Function-specific applications

d) **Infrastructure Management**

It is the function primarily responsible for providing technical expertise and overall management of the IT infrastructure. Its primary objective is to assist in plan, implement and maintenance of a stable technical infrastructure in order to support an organisation's business processes.

Infrastructure Management can have following functions:

i. Manage IT infrastructure components for an environment, which falls within the preview of IT operations

ii. It acts as a custodian of technical knowledge and expertise, related to the management of IT infrastructure. It ensures that technical knowledge and expertise required to design, develop, test, manage and improve IT services are identified, developed and refined

iii. It ensures appropriate resources are effectively trained and deployed to deliver, build, transit, operate and improve the technology required to deliver and support IT infrastructure

iv. It helps define and execute training programmes

v. It helps document skill sets available within an organisation and skills needed to be developed to manage infrastructure management as function

vi. Definition of standards to be adapted when defining new IT architecture and involvement in the design and build of new services

vii. Risk assessment for IT infrastructure architecture

viii. Feedbacks to availability and capacity management activities

ix. Designing and performing tests for functionality, performance and manageability of IT services

x. Definition and management of event management tools

xi. Participation in incident, problem, performance, change and release management and resource fulfillment

xii. Infrastructure management function should provide information or manage for configuration Management System

Infrastructure Management Structure**:** For all practical reasons, infrastructure management function is not performed by a single department or group, it consist of technical areas as per the technical skill sets and expertise, some of these are:

- Mainframe management team
- Server management team
- Storage management team
- Network support team
- Desktop support team

- Database management team
- Middleware management team
- Directory services team
- Internet team
- Messaging team
- IP-based telephony team

Components of IT operations framework:

a) Risk Management

Banks should analyse their IT Operation environment, including technology, human resources and implemented processes, to identify threats and vulnerabilities. They should conduct a periodic risk assessment which should identify:

- *Internal and external risks*
- *Risks associated with individual platforms, systems, or processes, as well as automated processing units*

While identifying the risks, a risk assessment process should quantify the probability of a threat and vulnerability, and the financial consequences of such an event. Banks should also consider the inter-dependencies between risk elements, as threats and vulnerabilities have the potential to quickly compromise inter-connected and inter-dependent systems and processes.

Banks should implement a cost-effective and risk-focused environment. The risk control environment should provide guidance, accountability and enforceability, while mitigating risks.

Risk Categorisation**:** As a part of risk identification and assessment, banks should identify events or activities that could disrupt operations, or negatively affect the reputation or earnings, and assess compliance to regulatory requirements. Risks identified can be broadly categorised into following categories:

- *Strategic Failures:* That might include improper implementation, failure of supplier, inappropriate definition of requirements, incompatibility with existing application infrastructure etc. It will also include regulatory compliance
- *Design Failures:* It might include inadequate project management, cost and time overruns, programming errors and data migration failures among others
- *Transition Failures:* It might include inadequate capacity planning, inappropriately defined availability requirements, SLA / OLA / Underpinning contracts not appropriately defined and information security breaches, among others

Risk Mitigation**:** Once the organisation has identified, analyzed and categorized the risks, organisation should define following attributes for each risk component:

- Probability of Occurrence;
- Financial Impact;
- Reputational Impact;
- Regulatory Compliance Impact;
- Legal Impact.

Beside above specified attributes, an organisation should also consider these:

- Lost revenues
- Loss of market share
- Non-compliance of regulatory requirements
- Litigation probability
- Data recovery expenses
- Reconstruction expenses

These, along with the business process involved, should be used to prioritise risk mitigation actions and control framework.

b) IT Operations Processes

i) IT Strategy

Processes within IT Strategy provide guidance to identify, select and prioritise services that are aligned to business requirements. IT strategy, as a framework, provides feedback to IT Operations on the services to be supported and their underlying business processes and prioritisation of these services, etc.

A well-defined IT Strategy framework will assist IT Operations in supporting IT services as required by the business and defined in OLA / SLAs.

IT Strategy processes provide guidelines that can be used by the banks to design, develop, and implement IT Operation not only as an organisational capability but as a strategic asset.

a) Financial Management: It provides mechanism and techniques to IT operations to quantify in financial terms, value of IT services it supports, value of assets underlying the provisioning of these services, and qualification of operational forecasting.

Advantages of implementing Financial Management process are:

- Assists in decision-making
- Speed of changes
- Service Portfolio Management
- Financial compliance and control
- Operational control
- Value capture and creation

b) Service Valuation

It is the mechanism that can be considered by banks to quantify services, which are available to customers (internal or external) and supported by IT operations in financial terms. It assists IT Operation functions to showcase the involvement of function in supporting the bank's core business.

Financial Management uses Service Valuation to quantify financial terms, value of IT services supported by IT Operations. It provides a blueprint from which businesses can comprehend what is actually delivered to them from IT. Combined with Service Level Management, Service Valuation is the means to a mutual agreement with businesses, regarding what a service is, what its components are, and its cost and worth.

Service Valuation quantifies, in financial terms, funding sought by a business and IT for services delivered, based on the agreed value of those services. The activity involves identifying cost baseline for services and then quantifying the perceived valued, added by the provider’s service assets in order to conclude a final service value.

Service Valuation will have two components, these being:

i) **Provisioning Value:** The actual underlying cost of IT, related to provisioning a service, including all fulfillment elements–tangible and intangible. Input comes from financial systems and consists of payment of actual resources consumed by the IT in the provisioning of services. This cost element includes items such as:

- *Hardware and software license cost*
- *Annual maintenance fees for hardware and software*
- *Personnel resources used in the support or maintenance of the services*
- *Utilities, data centre or other facilities charge*
- *Taxes, capital or interest charges*
- *Compliance costs*

ii) **Service Value Potential:** Is the value-added component based on a customer's perception of value from the service or expected marginal utility and warranty from using the services in comparison with what is possible using the customer's own assets.

c) Portfolio Management

It provides guidelines that can be considered by banks for governing investments in service management across an enterprise and managing them for value. Portfolio management contains information for all existing services, as well as every proposed service–those that are in conceptual phase.

Every service, which is a part of service portfolio, should include a business case, which is a model of what a service is expected to achieve. It is the justification for pursuing a course of action to meet stated organisational goals. Business case links back to service strategy and funding. It is the assessment of a service management in terms of potential benefits and the resources and capabilities required to provision and maintain the service. Portfolio Management framework defined by the banks should highlight controls, which are defined to develop an IT Service from conceptual phase to go-live phase and then to transition to production environment. During the development of IT services financial impact of the new service on IT Operation should also be ascertained which will assist IT Operations in Service Validation.

d) Demand Management

Demand Management process provides guidelines which can be used by banks to understand the business processes IT operations supports to identify, analyse, and codify Patterns of business activities (PBA) to provide sufficient basic for capacity requirement. Analysing and tracking the activity patterns of the business process makes it possible to predict demand for services. It is also possible to predict demand for underlying service assets that support these services.

Demand Management guidelines should also take into consideration IT Operations involvement in development of service from conceptual phase to go to the live phase, so that there is a transparency of demand of new service in IT Operations.

Ii) Design

The design phase of the IT operations provides the guidelines and processes, which can be used by the banks to manage the change in the business landscape. Components which should be considered when designing a new IT service or making a change to the existing IT service are:

- Business Processes
- IT Services
- Service-level Agreements

- IT Infrastructure
- IT Environment
- Information Data
- Applications
- Support Services
- Support Teams
- Suppliers

i) **Service design:** This should not consider components in isolation, but must also consider the relationship between each of the components and their dependencies on any other component or service.

ii) **Design phase:** Provides a set of processes and guidelines that can be used by banks to design IT services, supported by IT operations, that satisfies business objectives, compliance requirements and risk and security requirements. The processes also provide guidelines to identify and manage risks and to design secure and resilient IT services.

e) <u>Service Catalogue Management</u>

Over the years, banks' IT infrastructure has grown and developed. In order to establish an accurate IT landscape, it is recommended that an *IT Service Catalogue* is defined, produced and maintained. It can be considered as a repository that provides information on all IT services supported by IT Operations framework.

The Service Catalogue Management process provides guidelines, used by banks to define and manage service catalogue, which provides a consistent and accurate information on all IT services available to customers (internal or external). It also ensures that the service catalogue is available to users, who are approved to access it. It should contain details of all services that are in production, as well as the services that are being prepared for transition. Banks may consider following attributes to be included into the service catalogue:

1. Definition of Service
2. Categorization of Service (business application and IT support)
3. Service Criticality
4. Disaster Recovery Class
5. Service-level Agreement Parameters
6. Service Environment (Production, Testing, Quality Assurance, Staging, etc.)
7. IT Support Status (Operational and Transaction, etc.)
8. Configuration Management Group
9. Incident Management Group
10. Problem Management Group
11. Change and Release Management Group
12. Service Owner
13. Service-level Manager
14. Principal Business Activities Details
15. Interdependency on Configuration Items
16. Interdependency on Service Portfolio

Service catalogue provides details of services available to customers such as intended use,

business processes they enable and the level and quality of service the customer can expect from each service. Banks can also consider incorporating "charge back mechanism", as defined in financial management into the service catalogue.

A Service catalogue has two aspects:

i) **Business Service Catalogue:** It contains details of all IT services delivered to a customer, together with relationships with business units and business processes that rely on IT services. This is the customer view of the catalogue. Business Service Catalogue facilitates development of robust Service Level Management process.

ii) **Technical Service Catalogue:** It contains details of all IT services delivered to a customer, together with his or her relationship with supporting and shared services, relationship to configuration items (CIs). CIs can be a service asset or component, or any other item that is under control of configuration management. Depending on established strategy configuration, an item may vary widely in complexity, size and type. It can range from entire services or systems to a single software module or a minor software component. (Configuration Items are explained in details in "Service Assets and Configuration Management" section of the guidelines.) It facilitates the development of the relationship between services, underlying CIs, SLAs and OLAs, and the support groups, which support services throughout its life-cycle.

f) Service Level Management

This process defines the framework that can be used by banks to plan, co-ordinate and draft, agree, monitor and report service attributes used to measure the service quality. Its framework also includes guidelines for ongoing review of service achievements to ensure that the required and cost-justifiable service quality is maintained and improved. Beside current services and SLAs, this management provides guidelines to ensure that new requirements are captured. That new or changed services and SLAs are developed to match the business needs and expectations.

i) Service Level Management process should be able to meet the following objectives:

- Define, document, agree, monitor, measure, report and review the level of IT services
- Ensure specific and quantifiable targets are defined for IT services
- Ensure that IT Operations and consumers have clear, unambiguous expectations of the level of services to be delivered
- Ensure that pro-active measures, to improve the level of service delivered, are implemented if cost-justified

ii) While defining SLM framework for banks, the following aspects should also be considered

- Operational-level agreement to ensure that Operational Level Agreements (OLAs) with other support groups are defined and developed; these OLAs should be in line with SLAs which it supports
- Underpinning supplier contract to ensure all underpinning supplier contracts with the vendors or suppliers are defined and developed: these contracts should be in line with SLAs, which it supports

iii) While defining Service Level Agreement as a part of Service Level Management framework, the following options can be considered:

- **Service based SLA:** Its structure covers attributes for single service across an organisation. For instance, SLA for internet banking service
- **Customer based SLA:** The structure covers attributes for all services for a defined set of customers. For instance, SLA for SMEs customers

- **Multi-Level SLA:** Multi-level SLA structure can be defined as per the organizational hierarchy. For instance, SLA for corporate offices, branches and head offices

Attributes that are included in SLAs should be ones which can effectively be monitored and measured. Attributes which are included in the SLAs can be categorised into operational, response, availability and security attributes. Service Level Management framework should also define guidelines for reviews of Service Level Agreements, Operational Level Agreements, and underpinning contracts to ensure that they are aligned to business needs and strategy. These should ensure that services covered, and targets for each, are relevant. And that nothing significant is changed that invalidates the agreement in any way. Service Level Management framework defined should also have guidelines defined for logging and management, including escalation of complaints and compliments.

g) Capacity Management

The process provides the framework and guidelines that can be adapted by banks to ensure that cost-justifiable IT capacity exists and matches to current- and future-agreed business requirements as identified in Service Level Agreement.

The Capacity Management process provides guidelines to:

- Produce and maintain capacity plan that reflects the current and future business requirements
- Manage service performance so that it meets or exceeds the agreed performance targets
- Diagnosis and resolution of performance and capacity-related incidents and problems
- Assess impact of all changes on capacity plan and performance of IT services supported by IT Operations
- Ensure that pro-active measures are undertaken to improve the performance of services, whenever it is cost-justifiable.

One of the key activities defined as a part of capacity management process is to produce and maintain, at an ongoing basis, the capacity plan, which depicts current level of resource utilization and service performance. Capacity plans can also include forecasting future requirements to support business activities. *The process can be subdivided into three:*

i. **Business Capacity Management:** Defines guidelines for translating business-need plans into requirements for IT services and supporting infrastructure, ensuring that the future business requirements for IT services are quantified, designed, planned and implemented. Inputs for future IT requirements come from the Service Portfolio and Demand Management.

ii. **Service Capacity Management:** This defines guidelines for management, control and prediction of end-to-end performance and capacity of live and operational IT service usage and workloads. It provides guidelines to ensure that the performance of IT services is monitored and measured.

iii. **Component Capacity Management:** It defines guidelines to identify and understand the performance, capacity and utilization of each individual component within a technology used to support IT services, including infrastructure, environment, data and applications.

A major difference between sub-processes is in the data that is being monitored and collected. For example, the level of utilization of individual components in the infrastructure: processors, disks and network links will be under Component Capacity Management. While transaction throughput rates and response times will be under Service Capacity Management. Business Capacity Management will be concerned with data, specific to

business volumes. Banks adapting capacity management process should ensure that its framework encompass all areas of technology (hardware, software, human resource, facilities, etc.)

h) Availability Management

Availability and reliability of IT services can directly influence customer satisfaction and reputation of banks. Therefore Availability Management is essential in ensuring that the IT delivers the "right level" of service required by the business to satisfy its objectives. The process provides framework and guidelines that can be adapted by banks to ensure that the level of service availability (for all services) is matched, or exceeds the current and future requirements, as defined in the Service Level Agreement.

Availability Management process provides guidelines so that banks can:

- Produce and maintain an appropriate up-to-date Availability Plan that reflects the current and future needs of the business
- Ensure that service availability achievements meet or exceed agreed targets, by managing services and resources-related availability targets
- Assist with diagnosis and resolution of availability-related incidents and problems
- Ensure that pro-active measures to improve the availability of services are implemented wherever it is cost justifiable to do so

When implementing Availability Management processes, banks should consider including the following:

i. All operational services and technology, supported by IT Operations function and for which there is a formal SLA

ii. New services where Service Level Requirement and Agreement have been established

iii. Aspects of IT's services and components that may impact availability, which may include training, skills, process effectiveness, procedures and tools

Availability Management process has two key elements:

i. **Reactive activities:** The reactive aspect of availability management involves monitoring, measuring, analysis and management of events, incidents, problems and changes, involving unavailability

ii. **Proactive activities:** This aspect involves planning, design and improvement of availability

Attributes that can be used by the banks for reporting availability of IT services, can be:

- **Availability:** The ability of a service, component or CI, to perform the agreed function when required.

- **Availability (%)** = $\frac{\text{Agreed Service Time - Downtime}}{\text{Agreed Service Time}} \times 100$

  Downtime should only be included in the above calculation, when it occurs within the "Agreed Service Time".

- **Mean Time Between Service Incidents (MTBSI):** MTBSI refers to how long a service; component or CI can perform its agreed function without interruption.

- MTBSI = $\frac{\text{Available time in hours}}{\text{}}$

Number of Breaks

- **Mean Time Between Failures (MTBF):** MTBF refers to how long a service; component or CI can perform its agreed function without reporting a failure.

Available time in hours – Total downtime in Hours

MTBF = ----------

Number of breaks

Mean Time Between Failures (MTBF): is the mean time between the recovery from one incident and occurrence of the next incident, it is also known as uptime. This metric relates to the reliability of the IT Service supported by IT Operations.

- **Mean Time to Repair (MTTR):** MTTR refers to how quickly and effectively a service, component or CI can be restored to normal working after failure.

Total downtime in Hours

MTTR = ----------

Number of breaks

Mean Time to Repair (MTTR): This is the average time between occurrence of a fault and service recovery. It is also known as downtime. This metric relates to the recoverability and serviceability of the IT Services supported by IT Operations.

Vital Business Functions

When defining availability targets for a business service, banks should consider identifying Vital Business Function (VBF). VBF represents critical business elements of a process supported by IT services. For example, an ATM will have following business functions:

i. Cash dispensing
ii. Reconciliation with the relevant account
iii. Statement printing.

Out of these three, cash dispensing and reconciliation should be considered as vital business functions, influencing the availability design and associated costs.

i) Supplier Management

Complex business demands require extensive skills and capabilities from IT to support business processes, therefore collaboration with service providers and value networks are an integral part of end-to-end business solution. Supplier Management process provides framework and guidelines that can be used by banks to manage relationships with vendors, suppliers and contractors. This framework ensures that suppliers and services they provide are managed to support IT service targets and business expectations. The purpose of this management process is to obtain value for money from suppliers, and to ensure that suppliers perform to the targets contained within contracts and agreements, while conforming to all terms and conditions.

Supplier Management process provides guidelines which can be used by the banks to:

- Implement and enforce supplier policies
- Maintenance of supplier and contact database

- Suppler and contact categorization and risk assessment
- Supplier and contract evaluation and selection
- Development, negotiation and agreement of contracts
- Contract review, renewal and termination
- Management of suppliers and supplier performance
- Agreement and implementation of service and supplier improvement plans
- Maintenance of standard contracts, terms and conditions
- Management of contractual dispute resolution
- Management of sub-contracted suppliers

iii) Transition

The transition phase provides frameworks and processes that may be utilised by banks to:

- Evaluate service capabilities and risk profile of new or changes service before it is released into production environment
- Evaluate and maintain integrity of all identified service assets and configuration items required to support the service

Service Asset and Configuration Management

Service Asset and Configuration Management process provides framework and guidelines that can be used by the banks to manage service assets and configuration items that supports business services.

The framework provides guidelines to:

- Identify, control, record, audit and verify service assets and configuration items, including service baseline version controls their attributes and relationships.
- Manage and protect integrity of service assets and configuration items through the service lifecycle by ensuring only authorised assets are used and only authorised changes are made.
- Ensure integrity of configuration items required to support business services and IT infrastructure by establishing and maintaining an accurate and complete Configuration Management System.
- Provide accurate information of configuration items to assist in change and release management process.

Service asset management manages assets across its lifecycle from acquisition through disposal. Implementation of Service Asset and Configuration Management framework has cost and resources implications and therefore strategic discussions needs to be made about the priorities to be addressed. For instance banks can decide on initially focusing on the basic IT assets (hardware and software) and the services and assets that are business critical or covered by legal regulatory compliance.

Components that can be considered as part of Service Asset and Configuration Management are:

i. **Configuration Items:** These can be a service asset or component, or any item that is under the control of configuration management. Depending on established strategy

configuration, the item may vary widely in complexity, size and type. It can range from an entire service or system to a single software module or a minor software component.

If desired, banks can define a hierarchical structure for configuration items. For instance banks can define Core Banking as a configuration item which can have different application as a subset Configuration Item of the Core Banking configuration item. Each configuration item can have modules as sub set which can have two configuration item, these being hosting and application support. Hosting can then be further sub-divided into configuration item that can be servers, operating systems, databases, network components.

ii. **Configuration Management System:** To manage large and complex IT environment banks may consider implementation of supporting system known as Configuration Management System. Beside holding information about configuration items, their components and relationship between configuration items Configuration Management System can also be used to correlate services and configuration items; this kind of snapshot will assist in proactively identifying incidents, events etc.

iii. **Secure libraries:** Secure library is a collection of software, electronic or document CIs. Access to items in a secure library is restricted. The secure library is used for controlling and releasing components throughout the service lifecycle.

iv. **Definitive Media Library:** Definitive media library (DML) is a secure library that may be used to store definitive authorised versions of all media CIs. It stores master copies of versions that have passed quality assurance checks.

v. **Configuration Baseline:** This baseline is the configuration of a service, product or infrastructure that has been formally reviewed and agreed on, that thereafter serves as the basis for further activities and that can be changed only through formal change procedure. Configuration baseline captures and represents a set of configuration items that are related to each other.

vi. **Snapshot:** It defines the current state of configuration items or an environment.

vii. **Change Management:** This process provides guidelines which can be used by the banks for handling changes to ensure that the changes are recorded, assessed, authorised, prioritised, planned, tested, implemented, documented and reviewed in a controlled manner and environment. The primary objective of the change management procedures is to ensure assessment of:

- Risks
- Change authorization
- Business Continuity
- Change impact

iv) Operations

This phase, as a part of Service Management lifecycle, is responsible for executing and performing processes that optimise the cost of the quality of services. As a part of the organisation, it's responsible for enabling businesses to meets objectives. As a part of technology, it's responsible for effective functioning of components that support business services.

Event Management

Event Management process provides the guidelines which can be used by the banks to define the framework for monitoring all the relevant events that occurs through the IT

infrastructure. It provides the entry point for the execution of many Service Operations processes and activities.

Event can be defined as any detectable or discernible occurrence that has significance for the management of the IT infrastructure, or delivery of IT services. *Event Management framework when defined will have two mechanisms for monitoring, these are:*

- **Active Monitoring:** Active monitoring is related to polling of business significant Configuration Items to determine their status and availability. Any diversion from normal status should be reported to appropriate team for action.
- **Passive Monitoring:** Passive monitoring detects and correlate operational alerts or communications generated by Configuration Items.

Event Management can be applied to any aspect of Service Management that needs to be controlled. These components can be:

- Configuration Items
- Environment conditions
- Software licence monitoring
- Security breaches

Event Management portfolio can have different kind of event, some of these are:

- **Informational:** Events signifying regular operations for instance notification that a scheduled job has completed
- **Warning:** Events signifying diversion from normal course of action, for instance a user attempting to login with incorrect password. Exceptional events will require further investigation to determine an environment which may have led to an exception
- **Exceptions:** Events, which are unusual. Events may require closer monitoring. In some case the condition will resolve itself. For instance, unusual combinations of workloads as they are completed, normal operations will restore. In other cases, operations intervention will be required if the situation is repeated

Incident Management

An incident is an unplanned interruption to an IT service, or the reduction in the quality of an IT service. Failure of a configuration item that has not yet impacted service shall also be an incident.

Incident Management process provides guidelines that can be implemented by the banks for the management of incidents so that restoration of service operations as quickly as possible and to minimise adverse impact on business operations. The primary objective of the Incident Management procedures is to ensure best possible level of service quality and availability.

Problem Management

Problem Management process provides a framework, which can be implemented by banks to minimise the adverse impact of incidents on the IT Infrastructure and the business by identifying root cause, logging known errors, providing and communicating workarounds, finding permanent solutions, and preventing recurrence of incidents related to these errors. Problem Management increases stability and integrity of the infrastructure.

Problem Management process includes activities required to carry out the root causes of incidents and to determine the resolution to these underlying problems. Problem management procedures also include implementation of the resolution through Change

Management procedures and Release Management procedures. This also includes appropriate turnaround and resolutions to incidents that cannot be resolved due to business cases, or technical short falls. Periodic trend analysis of the problems in respect of systems or customer facing channels may be carried out and appropriate action taken.

Access Management

Access Management process provides the guidelines, which can be implemented by banks to limit access to IT services only to those individuals and applications that are duly authorised based on organisational policies and standards. Access Management enables the organisation to manage confidentiality, integrity of the organisation's data, IT infrastructure, and applications. *(Details have been provided in the "Information Security" chapter.)*

CHAPTER 4 – IT SERVICES OUTSOURCING

Introduction

In India, as banks augment growth and expand business, there is an increasing reliance on external service providers as partners in achieving the growth targets and as effective cost alternatives.

'Outsourcing' may be defined as a bank's use of a third party (either an affiliated entity within a corporate group or an entity that is external to the corporate group) to perform activities on a continuing basis that would normally be undertaken by the bank itself, now or in the future. 'Continuing basis' includes agreements for a limited period.

The benefits of outsourcing include efficiencies in operations, increased ability to acquire and support current technology and tide over the risk of obsolescence, increased time availability for management to focus on key management functions, shorter lead time in delivering services to customers, better quality of services, and stronger controls among others.

Common areas for Outsourcing

Outsourcing has been a constant theme in banking technology over at least the past ten years, as banking has become more technology intensive and the required scale of investment has grown exponentially. Many operations have been outsourced to Third party vendors comprising external vendors and specialized subsidiaries. Service providers today may be a technology company or specialist outsourcing manager. This decision to outsource should fit into the institution's overall strategic plan and corporate objectives.

Common areas where Banks have outsourced functions include:

- Technology Operations
    - Technology Infrastructure Management, Maintenance and Support
    - Application Development, Maintenance and Testing
- Banking Operations
    - Sourcing, Leads Generation
    - Cash Management and Collections
    - Customer Service helpdesk / call center services
    - Transaction Processing including payments, loans, deposits
    - Activities such as Debit card printing and dispatch, verifications, etc.
- Marketing and Research
- Fiduciary and Trading activities

Role of the Board and Senior Management

The Board and senior management are ultimately responsible for 'outsourcing operations' and for managing risks inherent in such outsourcing relationships. Whereas an institution may delegate its day-to-day operational duties to a service provider, responsibilities for effective due diligence, oversight and management of outsourcing and accountability for all outsourcing decisions continue to rest with the Bank, Board and senior management. Board and senior management have the responsibility to institute an effective governance mechanism and risk management process for all outsourced operations.

The Board is responsible for:

- Instituting an appropriate governance mechanism for outsourced processes, comprising of risk based policies and procedures, to effectively identify, measure, monitor and control risks associated with outsourcing in an end to end manner
- Defining approval authorities for outsourcing depending on nature of risks in and materiality of outsourcing
- Assessing management competencies to develop sound and responsive outsourcing risk management policies and procedures commensurate with the nature, scope, and complexity of outsourcing arrangements
- Undertaking a periodic review of outsourcing strategies and all existing material outsourcing arrangements

Senior management is responsible for:

- Evaluating the risks and materiality of all prospective outsourcing based on the framework developed by the Board
- Developing sound outsourcing policies and procedures for implementation by Line Managers
- Periodically reviewing the effectiveness of policies and procedures
- Communicating significant risks in outsourcing to the Board on a periodic basis
- Ensuring an independent review and audit in accordance with approved policies and procedures
- Ensuring contingency plans have been developed and tested adequately

Various components/aspects relating to outsourcing:

A reference may also be made to "Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks" (*circular no: DBOD.NO.BP.40/21.04.158/ 2006-07 dated November 3, 2006)* issued by RBI. Aspects relating to IT services outsourcing may also be incorporated as part of outsourcing policy of a bank.

1. 'Material' Outsourcing

Banks need to assess the degree of 'materiality' inherent in the outsourced functions. Whether an outsourcing arrangement is 'material' to the business context or not is a qualitative judgment and may be determined on the basis criticality of service, process, or technology to the overall business objectives.

Outsourcing of non-financial processes, such as technology operations, is 'material' and if disrupted has the potential to significantly impact business operations, reputation and stability of the Bank. Where a Bank relies on third party employees to perform key banking functions such as applications processing, verifications, approvals, etc., on a continuous basis, such outsourcing may also be construed as 'material', whether or not the personnel are located within the premises of the Bank. However, extant RBI guidelines on outsourcing indicate activities which cannot be outsourced and need to be carried out by the bank. These include Internal Audit, Compliance function, and decision making functions like KYC compliance, loans sanctioning, and managing investment portfolio. These need to be kept in view.

Criteria that may be considered in determining the materiality of proposed outsourcing include the following:

- Size and scale of operations which are outsourced

- Potential impact of outsourcing on parameters such as cost of outsourcing as a proportion of total operating costs, earnings, liquidity, solvency, funding capital, risk profile, among others, for the Bank
- Nature of functions outsourced
- Nature and extent of data sharing involved. For e.g., where outsourcing involves sharing of customer data, the engagement may be 'material'
- Degree/extent of control and oversight exercised by the bank on vendor managed processes. For e.g., the ability of bank staff to design and influence day to day operations and decision making, whether bank staff is able to exercise sufficient oversight over the day to day activities performed by outsourced agencies
- Degree of control exercised by banks on outsourced entities, regardless of a conglomerate entity structure
- Impact on data privacy and security. For e.g., whether access to customer data has to be extended to staff of the service provider
- Whether the bank has adequate flexibility to switch service providers, so that the risk of being attached to a single service provider is adequately mitigated, and the aggregate exposure to a single service provider

Banks should undertake a periodic review of their outsourced processes to identify new outsourcing risks as they arise. For e.g. when the service provider has further sub-contracted work to other service providers or has undergone a significant change in processes, infrastructure, or management.

Materiality should be considered both at an institution level and on a consolidated basis i.e. together with the institution's branches and corporations/entities under its control.

2. Risk Management in outsourcing arrangements

Risk management is the process of identifying, measuring, monitoring and managing risk. Risks inherent to process outsourcing, include Strategic risk, Reputation risk, Operational risk, Compliance risk, Legal risk, Counter party risk, Country risk, Contractual risk, Access risk, Concentration and systemic risk, and Exit strategy risk. Failure of a service provider in providing a specified service, a breach in security/ confidentiality, or non-compliance with legal and regulatory requirements, among others may lead to reputation / financial losses for the bank and may also result in systemic risks within the banking system in the country. Pervasive use of technology in banking operations further amplifies the risk impact.

(i) Risk Evaluation and Measurement

Risk evaluation should be performed prior to entering into an outsourcing agreement and reviewed periodically in the light of known and expected changes, as part of the strategic planning or review processes.

The framework for risk evaluation should include the following steps:

- Identification of the role of outsourcing in the overall business strategy and objectives, and inter-linkages with corporate strategic goals
- Comprehensive due diligence on the nature, scope and complexity of the outsourcing to identify the key risks and risk mitigation strategies For e.g. in case of technology outsourcing, state of security practices and controls environment offered by the service provider is a key factor
- Analysis of the impact of such arrangement on the overall risk profile of the bank, and whether adequate internal expertise and resources exist to mitigate the risks identified
- Analysis of risk-return on the potential benefits of outsourcing vis-à-vis the vulnerabilities that may arise

Banks should evaluate vendor managed processes or specific vendor relationships as they relate to information systems and technology. All outsourced information systems and operations may be subject to risk management and security and privacy policies that meet the Bank's own standards.

(ii) Service provider selection

Management should identify functions to be outsourced along with necessary controls and solicit responses from prospective bidders via an RFP process. Proposals submitted by service providers should be evaluated in the light of the organisation's needs, and any differences in the service provider proposals as compared to the solicitation should be analyzed carefully. Selection of affiliated parties as service providers should be done at arm's length in accordance with this guideline.

Due Diligence

In negotiating / renewing an Outsourcing arrangement, due diligence should be performed to assess the capability of the technology service provider to comply with obligations in the outsourcing agreement. Due diligence should involve an evaluation of all information about the service provider including qualitative, quantitative, financial, operational and reputational factors, as follows:

- Past experience and competence to implement and support proposed activities over the contractual period
- Financial soundness and ability to service commitments even under adverse conditions
- Business reputation and culture, compliance, complaints and outstanding or potential litigations
- Security and internal control, audit coverage reporting and monitoring environment, business continuity management
- External factors like political, economic, social and legal environment of jurisdiction in which the service provider operates and other events that may impact service performance
- Business continuity arrangements in case of technology outsourcing
- Due diligence for sub-service providers
- Risk management, framework, alignment to applicable international standards on quality / security / environment, etc., may be considered
- Secure infrastructure facilities
- Employee training, knowledge transfer
- Reliance on and ability to deal with sub-contractors

Extent of due diligence reviews may vary based on risk inherent in the outsourcing arrangements. Due diligence undertaken during the selection process should be documented and re-performed periodically as part of the monitoring and control processes of outsourcing.

Maintaining Caution lists and scoring for service providers (bureau services)

Where possible the bank may obtain independent reviews and market feedback to supplement internal findings. Banks should ensure that information used for due diligence is current and not more than 12 months old.

Reporting to the regulator

Banks must be required to report to the regulator, where the scale and nature of functions outsourced are significant, or extensive data sharing is involved across geographic locations

as part of technology / process outsourcing and when data pertaining to Indian operations are stored/processed abroad.

Multiple Service provider relationships

A multiple service provider relationship is one where two or more service providers collaborate to deliver an end to end solution to the financial institution. Multiple contracting scenarios are possible:

- One service provider may be designated as the 'Lead Service Provider', to manage the other service providers
- Bank may independently enter into stand-alone contracts with each service provider

An institution selects from the above or any other contractual relationship, however, remains responsible for understanding and monitoring the control environment of all service providers that have access to the banks systems, records or resources.

(iii) Contracting

The terms and conditions governing the contract between the bank and the service provider should be carefully defined in written agreements and vetted by bank's legal counsel on their legal effect and enforceability.

Banks should ensure that the contract brings out nature of legal relationship between the parties (agent, principal or otherwise), and addresses risks and mitigation strategies identified at the risk evaluation and due diligence stages. Contracts should clearly define the roles and responsibilities of the parties to the contract and include suitable indemnification clauses. Any 'limitation of liability' consideration incorporated by the service provider should be assessed in consultation with the legal department.

Contracts should provide for periodic renewal and re-negotiation to enable the institution to retain an appropriate level of control over the outsourcing and should include the right to intervene with appropriate measure to meet the Banks' legal and regulatory obligations.

Contractual agreements should, in the very least, have provisions for the following:

- *Scope:* Agreements should state the activities that are to be outsourced
- *Performance Standards:* Key performance metrics should be defined for each activity to be outsourced, as part of the overall Service Level Agreement
- *Monitoring and Oversight:* Provide for continuous monitoring and assessment by the bank of the service provider so that any necessary corrective measure can be taken immediately
- *Access to books and records / Audit and Inspection:* This would include :

✓ Ensure that the bank has the ability to access all books, records and information relevant to the outsourced activity available with the service provider. For technology outsourcing, requisite audit trails and logs for administrative activities should be retained and accessible to the Bank based on approved requests

✓ Provide the bank with the right to conduct audits on the service provider whether by its internal or external auditors, or by external specialists appointed to act on its behalf and to obtain copies of any audit or review reports and findings made on the service provider in conjunction with the services performed for the bank

✓ Include clauses to allow the Reserve Bank of India or persons authorized by it to access the bank's documents, records of transactions, and other necessary information given to, stored or processed by the service provider within a reasonable time. This includes information maintained in paper and electronic formats

- ✓ Recognize the right of the Reserve Bank to cause an inspection to be made of a service provider of a bank and its books and account by one or more of its officers or employees or other persons
- ✓ Where the controlling/Head offices of foreign banks operating in India outsource the activities related to the Indian operations, the Agreement should include clauses to allow the RBI or persons authorized by it to access the bank's documents, records of transactions and other necessary information given or stored or processed by the service provider within a reasonable time as also clauses to recognize the right of RBI to cause an inspection to be made of a service provider and its books and accounts by one or more of its officers or employees or other persons

- *Include termination clause :*

  - ✓ Contracts should include a termination clause and minimum periods to execute a termination provision, as deemed necessary
  - ✓ Agreements should provide for maintaining confidentiality of customer's information even after the contract expires or is terminated by either party
  - ✓ Contract should include conditions for default termination / early exit option for contracts. This may include circumstances when the service provider undergoes a change in ownership, becomes insolvent or goes under liquidation, received judicial indictment (whether within India or any other location), or when there has been a breach of confidentiality, security, or demonstrable deterioration in quality of services rendered
  - ✓ In all cases of termination (early or otherwise), an appropriate handover process for data and process needs to be agreed with the service provider

- *Confidentiality and security :*

- ✓ Mandate controls to ensure customer data confidentiality and service providers' liability in case of breach of security and leakage of confidential customer related information. For e.g. use of transaction-enabled mobile banking channels necessitates encryption controls to ensure security of data in transmission
- ✓ Provide for the preservation of documents and data by the service provider in accordance with the legal/regulatory obligation of the bank in this regard

- *Business Continuity:* The contract should contain clauses for contingency plans and testing thereof, to maintain business continuity.

- *Sub-contracting:* Agreements may include covenants limiting further sub-contracting. Agreements should provide for due prior approval/consent by the bank of the use of subcontractors by the service provider for all or part of an outsourced activity. The bank should retain the ability of similar control and oversight over the sub service provider as the service provider.

- *Dispute resolution:* Agreements should specify the resolution process, the event of default, indemnities involved and the remedies and recourse of the respective parties to the agreement.

- *Applicable laws:* Agreements should include choice of law provisions, based on the regulations as applicable to the bank. An agreement should be tailored to provide for specific risks relating to cross border businesses and operations, data privacy and ownership aspects, among others.

(iv) Monitoring and Control of outsourced activities

Banks should establish a structure for management and control of outsourcing, based on the nature, scope, complexity and inherent risk of the outsourced activity.

A structure for monitoring and control of outsourced activities should comprise of the following:

- A central record of all material outsourcing, including technology outsourcing and sub service provider relationships, that is readily accessible for review by the Board and senior management of the bank should be maintained. The records should be updated promptly and half yearly reviews should be placed before the Board.
- Banks should at least on an annual basis, review the financial and operational condition of the service provider to assess its ability to continue to meet its outsourcing obligations. Such due diligence reviews, which can be based on all available information about the service provider should highlight any deterioration or breach in performance standards, confidentiality and security, and in business continuity preparedness.
- Banks should review and monitor the security practices and control processes of the service provider on a regular basis and require the service provider to disclose security breaches.
- Banks should pro-actively intimate RBI of any adverse developments or non – compliance with legal and regulatory requirements in an outsourcing arrangement.
- In the event of outsourcing of technology operations, the banks should subject the same to enhanced and rigorous change management and monitoring controls since ultimate responsibility and accountability rests with the bank. It may be desirable if banks control the management of user ids created for use of external vendor personnel. As a contingency measure, banks may also endeavor to develop, over a period of time, reasonable level of skills/knowledge in various technology related areas like system administration, database administration, network architecture and administration, etc., to effectively engage with the vendors and also to take over these functions in the event of any contingency.

Service Level Agreements and performance metrics

Management should include SLAs in the outsourcing contracts to agree and establish accountability for performance expectations. SLAs must clearly formalize the performance criteria to measure the quality and quantity of service levels. Banks should develop the following towards establishing an effective oversight program:

- Formal policy that defines the SLA program
- SLA monitoring process
- Recourse in case of non-performance
- Escalation process
- Dispute resolution process
- Conditions in which the contract may be terminated by either party

For outsourced technology operations, specific metrics may be defined around the service availability, business continuity and transaction security, in order to measure services rendered by the external vendor organization. Please refer to the chapter on '*IT Operations*' for details on the SLA and performance metrics for technology operations.

Performance expectations, under both normal and contingency circumstances, need to be defined. Provisions need to be in place for timely and orderly intervention and rectification in the event of substandard performance by the service provider.

Control environment offered by the Service Provider

Banks should evaluate the adequacy of internal controls environment offered by the service provider. Due consideration should be given to the implementation of following by the service provider:

- Information security policies and employee awareness of the same
- Controls for logical access to customer information by service provider staff, so that information may be accessed on a need-to-know basis only
- Physical and environmental security and controls
- Network security and controls
- Formal process for tracking and monitoring program changes and projects
- Process for incident reporting and problem management
- Special control considerations for service providers using cloud computing as part of service
- Control considerations for handling of customer information and personally identifiable information
- Data classification and controls for handling data

Periodic Risk Assessment, Audit and Reviews

Outsourcing should not impede or interfere with the ability of the Bank or the Regulator in performing its supervisory functions and objectives.

As a practice, institutions should conduct pre- and post- outsourcing implementation reviews. An institution should also review its outsourcing arrangements periodically to ensure that its outsourcing risk management policies and procedures, and these Guidelines, are effectively complied with.

An institution should, at least on an annual basis, review the financial and operational condition of the service provider to assess its ability to continue to meet outsourcing obligations. Such due diligence reviews, which can be based on all available information about the service provider including reports by the service provider's external auditors, should highlight any deterioration or breach in performance standards, confidentiality and security, and in business continuity preparedness.

Banks should also periodically commission independent audit and expert assessments on the security and control environment of the service provider. Such assessments and reports on the service provider may be performed and prepared by the institution's internal or external auditors, or by agents appointed by the institution.

Such reviews should take adequate cognizance of historical violations or issue remediation during previous audits and assessments. Copies of previous audits and assessments should be shared during RBI inspections.

Business Continuity Planning

Banks should ensure that their business continuity preparedness is not adversely compromised on account of outsourcing. Banks are expected to adopt sound business continuity management practices as issued by RBI and seek proactive assurance that the outsourced service provider maintains readiness and preparedness for business continuity on an ongoing basis.

Banks, while framing the viable contingency plan, need to consider the availability of alternative service providers or the possibility of bringing the outsourced activity back-in-house in an emergency(for example, where number of vendors for a particular service is

extremely limited) and the costs, time and resources that would be involved and take suitable preparatory action.

(v) Confidentiality and Security

Public confidence is a cornerstone in the stability and reputability of a bank. Banks should be proactive to identify and specify the minimum security baselines to be adhered to by the service providers to ensure confidentiality and security of data. This is particularly applicable where third party service providers have access to personally identifiable information and critical customer data.

An institution may take the following steps to ensure that risks with respect to confidentiality and security of data are adequately mitigated:

- Address, agree and document specific responsibilities of the respective parties in outsourcing to ensure adequacy and effectiveness of security practices, including identifying obligations and liability in the event of a breach or default
- Discuss and agree on the instances where customer data shall be accessed and the user groups who will have access to the same. Access to a Bank's data should be strictly on a need to know basis
- Ensure that service provider employees are adequately aware and informed on the security and privacy policies

(vi)Outsourcing to Foreign Service providers

The engagement of service providers across multiple geographies exposes the organization to country risk – economic, social and political reasons in the country that may adversely affect the Banks business and operations. Banks should proactively evaluate such risk as part of the due diligence process and develop appropriate mitigating controls and as required, an effective exit strategy.

Outsourcing outside India should be agreed, in a manner that does not obstruct or hinder the ability of the bank or regulatory authorities to perform periodic audits/inspections and assessments, supervise or reconstruct activities of the bank based on books, records and necessary documentation, in a timely manner. Banks should ensure the following:

- Banks should principally enter into arrangements with parties operating in jurisdictions that generally uphold confidentiality clauses and agreements
- Banks may not outsource within jurisdictions where access to books, records and any other information required for audit and review purposes may be impeded due to regulatory or administrative constraints
- Banks should notify the Regulator where the rights of access for the Bank and / or the Regulator are likely to be impeded
- Emerging technologies such as data center hosting, applications as a service, cloud computing have given rise to unique legal jurisdictions for data and cross border regulations. Banks should clarify the jurisdiction for their data and applicable regulations at the outset of an outsourcing arrangement. This information should be reviewed periodically and in case of significant changes performed by the service provider

(vii) Outsourcing within a Group

These guidelines are generally applicable to outsourcing within a group conglomerate, including parent or Head Office, branch or a group company, whether located within or outside India. These requirements may be addressed as part of group wide risk assessment and management procedures.

Due diligence on an intra-group service provider may take the form of evaluating qualitative aspects on the ability of the service provider to address risks specific to the institution, particularly those relating to business continuity management, monitoring and control, and audit and inspection, including confirmation on the right of access to be provided to RBI to retain effective supervision over the institution, and compliance with local regulatory standards. The respective roles and responsibilities of each office in the outsourcing arrangement should be documented in writing in a formal Service Level Agreement.

(viii) Handling customer grievances and complaints

The Board and senior management are responsible for ensuring that quality and availability of banking services to customers are not adversely affected due to the outsourcing arrangements entered into by the Bank. Banks need to institute a robust grievance redressal mechanism, which should not be compromised in any way due to outsourcing.

The name and contact number of designated grievance redressal officer of the bank should be made known and widely publicized. The designated officer should ensure that genuine grievances of customers are redressed promptly without involving delay. It should be clearly indicated that banks' Grievance Redressal Machinery will also deal with the issue relating to services provided by the outsourced agency.

Generally, a time limit of 30 days may be given to the customers for forwarding their complaints / grievances. The grievance redressal procedure of the bank and the time frame fixed for responding to the complaints should be placed on the bank's website. If a complainant does not get satisfactory response from the bank within 60 days from the date of his lodging the complaint, he will have the option to approach the Office of the concerned Banking Ombudsman for redressal of his grievance/s.

CHAPTER 5: IS AUDIT

Introduction:
In the past decade, with the increased technology adoption by Banks, the complexities within the IT environment have given rise to considerable technology related risks requiring effective management.

This led the Banks to implement an Internal Control framework, based on various standards and its own control requirements and the current RBI guidelines. As a result, Bank's management and RBI, need an assurance on the effectiveness of internal controls implemented and expect the IS Audit to provide an independent and objective view of the extent to which the risks are managed.

As a consequence, the nature of the Internal Audit department has undergone a major transformation and IS audits are gaining importance as key processes are automated, or enabled by technology. Hence, there is a need for banks to re-assess the IS Audit processes and ensure that IS Audit objectives are effectively met.

The scope of IS Audit includes:

- Determining effectiveness of planning and oversight of IT activities
- Evaluating adequacy of operating processes and internal controls
- Determining adequacy of enterprise-wide compliance efforts, related to IT policies and internal control procedures
- Identifying areas with deficient internal controls, recommend corrective action to address deficiencies and follow-up, to ensure that the management effectively implements the required actions

Following areas have been covered under this chapter:

- *IS Audit:* The organisation's structure, roles and responsibilities. The chapter identifies the IS Audit stakeholders, defines their roles, responsibilities and competencies required to adequately support the IS Audit function
- *Audit Charter or Policy (to be included in the IS Audit):* This point addresses the need to include IS Audit as a part of the Audit Charter or Policy
- *Planning an IS Audit:* This point addresses planning for an IS Audit, using Risk Based Audit Approach. It begins with an understanding of IT risk assessment concepts, methodology and defines the IS Audit Universe, scoping and planning an audit execution
- *Executing an IS Audit:* This describes steps for executing the audit, covering activities such as understanding the business process and IT environment, refining the scope and identifying internal controls, testing for control design and control objectives, appropriate audit evidence, documentation of work papers and conclusions of tests performed
- *Reporting and Follow-up:* Describes the audit summary and memorandum, the requirements for discussing findings with the management, finalising and submitting reports, carrying out follow-up procedures, archiving documents and ensuring continuous auditing
- *Quality Review:* This addresses the quality aspects which ensures supervision and exercising due care.

1) Role and Responsibilities / Organisational structure

Board of Directors and Senior Management
Board of Directors and senior management are responsible for ensuring that an institution's system of internal controls operates effectively. One important element of an effective

internal control system is an internal audit function that includes adequate IT coverage. To meet its responsibility of providing an independent audit function with sufficient resources to ensure adequate IT coverage, the Board, or its Audit Committee, should enable an internal audit function, capable of evaluating IT controls adequately.

Audit Committee of the Board

An institution's board of directors establishes an "Audit Committee" to oversee audit functions and to report on audit matters periodically to the Board of Directors. Banks should enable adequately skilled Audit Committee composition to manage the complexity of the IS Audit oversight.

A designated member of an Audit Committee needs to possess the knowledge of Information Systems, related controls and audit issues. Designated member should also have competencies to understand the ultimate impact of deficiencies identified in IT internal control framework by the IS Audit. The committee should devote appropriate time to IS audit findings identified during IS Audits and members of the Audit Committee need to review critical issues highlighted and provide appropriate guidance to a bank's management.

As a part of its overall responsibilities, the committee should also be ultimately responsible for the following IS Audit areas:

- Bank's compliance with legal and regulatory requirements such as (among others) Information Technology Act-2000, Information Technology (Amendment) Act-2008, Banker's Books (Evidence) Act-1891, The Banking Regulation Act-1949, Reserve Bank of India Act-1934 and RBI circulars and guidelines
- Appointment of the IS Audit Head
- Performance of IS Audit
- Evaluation of significant IS Audit issues

(A Board or its Audit Committee members should seek training to fill any gaps in the knowledge, related to IT risks and controls.)

Internal Audit/Information System Audit function

Internal Audit is a part of the Board's assurance process with regard to the integrity and effectiveness of systems and controls. It is an independent group that reports directly to the Audit Committee or the Board of Directors. IS Audit, being an integral part of Internal Audit, requires an organisation structure with well-defined roles which needs to function in alignment with the Internal Audit, and provide technical audit support on key focus areas of audit or its universe, identified by an Internal Audit department. A well-defined IS Audit organisation structure ensures that the tasks performed fulfill a bank's overall audit objective, while preserving its independence, objectivity and competence.

In this regard, banks require a separate IS Audit function within an Internal Audit department led by an IS Audit Head reporting to the Head of Internal Audit or Chief Audit Executive (CAE). The personnel needs to assume overall responsibility and accountability of IS Audit functions. Where the bank leverages external resources for conducting IS Audit on areas where skills are lacking, the responsibility and accountability for such external IS Audits still remain with the IS Audit Head and CAE.

Critical Components and Processes

(i) Because the IS Audit is an integral part of the Internal Auditors, auditors will also be required to be independent, competent and exercise due professional care.

Independence: IS Auditors should act independently of the bank's management. In matters

related to the audit, the IS Audit should be independent of the auditee, both in attitude and appearance. The Audit Charter or Policy, or engagement letter (in case of external professional service provider), should address independence and accountability of the audit function. In case independence is impaired (in fact or appearance), details of the impairment should be disclosed to the Audit Committee or Board. Independence should be regularly assessed by the Audit Committee. In case of rotation of audit staff members from IT department to the IS Audit, care should be taken to ensure that the past role of such individuals do not impact their independence and objectivity as an IS Auditor.
Additionally, to ensure independence for the IS Auditors, Banks should make sure that:

- Auditors have access to information and applications
- Auditors have the right to conduct independent data inspection and analysis

Competence: IS Auditors should be professionally competent, having skills, knowledge, training and relevant experience. They should be appropriately qualified, have professional certifications and maintain professional competence through professional education and training. As IT encompasses a wide range of technologies, IS Auditors should possess skills that are commensurate with the technology used by a bank. They should be competent audit professionals with sufficient and relevant experience. Qualifications such as CISA (offered by ISACA), DISA (offered by ICAI), or CISSP (offered by ISC2), along with two or more years of IS Audit experience, are desirable. Similar qualification criteria should also be insisted upon, in case of outsourced professional service providers.

Due Professional Care: IS Auditors should exercise due professional care, which includes following the professional auditing standards in conducting the audit. The IS Audit Head should deal with any concerns in applying them during the audit. IS Auditors should maintain the highest degree of integrity and conduct. They should not adopt methods that could be seen as unlawful, unethical or unprofessional to obtain or execute an audit.

(ii) Outsourcing relating to IS Audit

Banks may decide to outsource execution of segments of audit plan to external professional service providers, as per the overall audit strategy decided in co-ordination with the CAE and the Audit Committee. This may be due to inadequate staff available internally within the bank to conduct audits, or insufficient levels of skilled staff. The work outsourced shall be restricted to execution of audits identified in the plan. Banks need to ensure that the overall ownership and responsibility of the IS Audit, including the audit planning process, risk assessment and follow-up of compliance remains within the bank. External assistance may be obtained initially to put in place necessary processes in this regard.

Both the CAE and Audit Committee should ensure that the external professional service providers appointed should be competent in the area of work that is outsourced and should have relevant prior experience in that area.

2) Audit Charter, Audit Policy to include IS Audit

Audit Charter or Policy is a document, which guides and directs activities of an internal audit function. IS Audit, being integral part of an Internal Audit department, should also be governed by the same charter or policy. The charter should be documented to contain a clear description of its mandate, purpose, responsibility, authority and accountability of relevant members or officials in respect of the IS Audit (namely the IS Auditors, management and Audit Committee) apart from the operating principles. The IS Auditor will have to determine how to achieve the implementation of the applicable IS Audit standards, use professional judgment in their application, and be prepared to justify any departure therefrom.

(a) Contents of the Audit Policy

The Policy should clearly address the aspects of responsibility, authority and accountability

of the IS auditor. *Aspects to be considered:*

Responsibility:
Some of the aspects include:
1. Mission Statement
2. Scope or Coverage
3. Audit Methodology
4. Objectives
5. Independence
6. Relationship with External Audit
7. Auditee's Requirements
8. Critical Success Factors
9. Key Performance Indicators
10. Other Measures of Performance
11. Providing Assurance on Control Environment
12. Reviewing Controls on Confidentiality, Integrity and Availability of Data or Systems

Authority:
Includes the following:
1. Risk Assessment
2. Mandate to perform an IS Audit
3. Allocation of resources
4. Right to access the relevant information, personnel, locations and systems
5. Scope or limitations of scope
6. Functions to be audited
7. Auditee's expectations
8. Organizational structure
9. Gradation of IS Audit Officials or Staff

Accountability: Some of the aspects in this regard include the following:
1. Reporting Lines to Senior Management, Board of Directors or Designated Authority
2. Assignment Performance Appraisals
3. Personnel Performance Appraisals
4. Staffing or Career Development
5. Training and Development of Skills including maintenance of professional certification/s, continuing professional education
6. Auditees' Rights
7. Independent Quality Reviews
8. Assessment of Compliance with Standards
9. Benchmarking Performance and Functions
10. Assessment of Completion of the Audit Plan
11. Agreed Actions (e.g. penalties when either party fails to carry out responsibilities)
12. Co-ordinate with and provide Oversight over other control functions like risk management, security and compliance

The policy should also cover Audit Rating Methodology and Quality Assurance Reviews. There should also be annual review of IS Audit Policy or Charter to ensure continued relevance.

(b) Communication with the Auditees

Effective communication with the auditees involves considering the following:

- Describing a service, its scope, availability and timeliness of delivery
- Providing cost estimates or budgets, if needed
- Describing problems and possible resolutions

- Providing adequate and accessible facilities for effective communication
- Determining relationship between the service offered, and the needs of the auditee

The Audit Charter forms a basis for communication with an auditee. It should include relevant references to service-level agreements for aspects like the following, as applicable:

- Availability for Unplanned Work
- Delivery of reports
- Costs
- Response to Auditee's Complaints
- Quality of Service
- Review of Performance
- Communication with the Auditee
- Needs Assessment
- Control Risk Self-assessment
- Agreement of Terms of Reference for Audit
- Reporting Process
- Agreement of Findings

(c) Quality Assurance Process

The IS Auditor should consider establishing a quality assurance process (e.g., interviews, customer satisfaction surveys, or assignment performance surveys) to understand his expectations relevant to the function. These needs should be evaluated against the Charter, to improve the service or change the service delivery or Audit Charter, if necessary.

(d) Engagement Letter

Engagement letters are often used for individual assignments. They set out the scope and objectives of a relationship between an external IS audit agency and an organisation. The letter should address the three aspects of responsibility, authority and accountability.

Following aspects needs to be considered:

Responsibility: The aspects addressed includes scope, objectives, independence, risk assessment, specific auditee requirements and deliverables

Authority: The aspects to be addressed include right of access to information, personnel, locations and systems relevant to the performance of the assignment, scope or any limitations of scope and documentary evidence or information of agreement to the terms and conditions of the engagement

Accountability: Areas addressed include designated or intended recipients of reports, auditees' rights, quality reviews, agreed completion dates and agreed budgets or fees if available

3) Planning an IS Audit

(a) Introduction

An effective IS Audit programme addresses IT risk exposures throughout a bank, including areas of IT management and strategic planning, data centre operations, client or server architecture, local and wide-area networks, telecommunications, physical and information security, electronic banking, applications used in banking operations, systems development, and business continuity planning.

A well-planned, properly structured audit programme is essential to evaluate risk management practices, internal control systems and compliance with policies concerning IT-related risks of every size and complexity. Effective programmes are risk-focused, promote sound IT controls, ensure timely resolution of audit deficiencies, and inform the Audit Committee of the effectiveness of Risk Management practices and internal control systems.

In the past, the Internal Audit concentrated on transaction testing, testing of accuracy and reliability of accounting records and financial reports, integrity, reliability and timeliness of control reports, and adherence to legal and regulatory requirements.

However, in the changing scenario, there is an increased need for widening, as well as redirecting, the scope of Internal Audit to evaluate the adequacy of IT Risk Management procedures and internal control systems. To achieve these, banks are moving towards risk-based internal audit, which include, in addition to selective transaction testing, an evaluation of the Risk Management systems and control procedures prevailing in a bank's operations.

Risk-based Internal Audit (RBIA) approach helps in planning the IS Audit.
It includes the following components:

- Understanding IT Risk Assessment Concepts
- Adopting a suitable IT Risk Assessment Methodology–used to examine auditable units in the IS audit universe and select areas for review to include in the IS Annual Plan that have the greatest risk exposure

  Steps involved are:
  - **Step 1:** System Characterisation
  - **Step 2:** Threat Identification
  - **Step 3:** Vulnerability Identification
  - **Step 4:** Control Analysis
  - **Step 5:** Likelihood Determination
  - **Step 6:** Impact Analysis
  - **Step 7:** Risk Determination

As a part of RBIA, planning the IS Audit involves the following:

- **Defining the IS Audit Universe:** This covers the IS Audit Universe, which defines the areas to be covered
- **Scoping for IS Audit:** This addresses the scoping requirements and includes:
  - *Defining control objectives and activities*
  - *Considering materiality*
  - *Building a fraud risk perspective*
- **Planning Execution of an Audit:** This describes the steps of a planning process before IS Audit starts execution of the plan
  - *Documenting an audit plan*
  - *Nature and extent of test of control*
  - *Sampling techniques*
  - *Standards and frameworks*
  - *Resource management*

The above components are clarified in the sub-sections below:

(b) Risk Based IS Audit

This internal audit approach is aimed at developing a risk-based audit plan keeping in mind th inherent risks of a business or location and effectiveness of control systems managing inherent risks. In this approach, every bank business or location, including risk management function, undergoes a risk assessment by the internal audit function.

RBI issued the "Guidance Note on Risk-based Internal Audit" in 2002 to all scheduled commercial banks, introducing the system of "risk-based internal audit".

The guidance note at a broad-level provided the following aspects:

- Development of a well-defined policy for risk-based internal audit

- Adoption of a risk assessment methodology for formulating risk based audit plan
- Development of risk profile and drawing up of risk matrix taking inherent business risk and effectiveness of the control system for monitoring the risk
- Preparation of annual audit plan, covering risks and prioritization, based on level and direction of each risk
- Setting up of communication channels between audit staff and management, for reporting issues that pose a threat to a bank's business
- Periodic evaluation of the risk assessment methodology
- Identification of appropriate personnel to undertake risk-based audit, and imparting them with relevant training
- Addressing transitional and change management issues

The overall plan, arrived at, using the risk assessment approach enables the Internal Audit to identify and examine key business areas that have highest exposure and enables effective allocation of Audit resources. As stated earlier, IS Audit, being an integral part of the Internal Audit, there is a need for IS Auditors to focus on the IT risks, related to the high-risk business areas identified by the Internal Audit for review during a year. This enables the IS Audit to provide an assurance to the management on the effectiveness of risk management and internal controls underlying the high-risk business processes, which when read in conjunction with the Internal Audit reports, provides a holistic view of the effectiveness.

Risk-based IS Audit needs to consider the following:

- Identification of an institution's data, application, technology, facilities, and personnel
- Identification of business activities and processes within each of those categories
- Profiles of significant business units, departments and product lines and systems, and their associated business risks and control features, resulting in a document describing the structure of risk and controls throughout the institution
- Use a measurement or scoring system that ranks and evaluates business and control risks for business units, departments and products
- Includes Board or Audit Committee approval of risk assessments and annual Risk-based Audit Plans that establish audit schedules, cycles, work programme scope and resource allocation for each area audited
- Implementation of the Audit Plan

Further, while identifying IT risks, an IS Auditor must consider the impact of non-alignment with any information security-related guidelines issued by RBI based on recommendations in Chapter 2 of this report. It should also be ensured that all systems, domains and processes, irrespective of their risk-levels, are covered within a period of **three** years.

(c) Adopting a Suitable Risk Assessment Methodology

The IS Auditor must define, adopt and follow a suitable risk assessment methodology. This should be in consonance with the focus on risks, to be addressed as a part of the overall Internal Audit Strategy.
A successful risk-based IS Audit Programme can be based on an effective scoring system arrived at by considering all relevant risk factors.

Major risk factors used in scoring systems include: Adequacy of internal controls, business criticality, regulatory requirements, amount or value of transactions processed, if a key customer information is held, customer facing systems, financial loss potential, number

of transactions processed, availability requirements, experience of management and staff, turnover, technical competence, degree of delegation, technical and process complexity, stability of application, age of system, training of users, number of interfaces, availability of documentation, extent of dependence on the IT system, confidentiality requirements, major changes carried out, previous audit observations and senior management oversight.

On the basis of risk matrix of business criticality and system or residual risk, applications or systems can be graded, based on where they fall on the "risk map" and accordingly their audit frequency can be decided. Banks should develop written guidelines on the use of risk assessment tools and risk factors and review these with the Audit Committee or the Board. Risk assessment guidelines will vary for banks depending on size, complexity, scope of activities, geographic diversity and technology systems used. Auditors should use the guidelines to grade major risk areas and define range of scores or assessments (e.g., groupings such as low, medium, or high risk or a numerical sequence such as 1 to 5).

The written risk assessment guidelines should specify the following elements:

- **Maximum length for audit cycles based on the risk assessment process:** For example, very high to high risk applications audit cycle can be at a frequency ranging from six months upto 12, medium risk applications can be 18 months (or below) and up to 36 months for low-risk areas. Audit cycles should not be open-ended.
- **Timing of risk assessments for each business area or department:** While risk assessment is expected to be on an annual basis, frequent assessments may be needed if an institution experiences rapid growth or change in operation or activities.
- **Documentation requirements to support risk assessment and scoring decisions**
- **Guidelines for overriding risk assessments in special cases and the circumstances under which they can be overridden:** Example: due to major changes in system, additional regulatory or legal requirements, a medium risk application may have to be audited more frequently.

Notwithstanding the above, IT governance, information security governance-related aspects, critical IT general controls such as data centre controls and processes and critical business applications/systems having financial/compliance implications, including regulatory reporting, risk management, customer access (delivery channels) and MIS systems, needs to be subjected to IS Audit at least once a year (or more frequently, if warranted by the risk assessment).

IS Auditors should periodically review results of internal control processes and analyse financial or operational data for any impact on a risk assessment or scoring. Accordingly, auditee units should be required to keep auditors up-to-date on major changes, such as introduction of a new product, implementation of a new system, application conversions, significant changes in organisation or staff, regulatory and legal requirements, security incidents.

(d) Defining the IS Audit Universe

An Audit Universe is an outcome of the risk assessment process. It defines the audit areas to be covered by the IS Auditor. It is usually a high-level structure that identifies processes, resources, risks and controls related to IT, allowing for a risk-based selection of the audit areas. The IT risks faced by banks due to emerging technologies, prioritisation of IS Audit Universe, selection of types of audits that need to be performed, optimisation of available resources, and ensuring quality of findings, are challenges faced by IS Audit.

The IS Audit Universe can be built around the four types of IT resources and processes: Such as application systems, information or data, infrastructure (technology and facilities

such as hardware, operating systems, database management systems, networking, multimedia, and the environment that houses and supports them and enable processing of applications) and people (internal or outsourced personnel required to plan, organise, acquire, implement, deliver, support, monitor and evaluate the information systems and services).

The challenge is to provide the "right level of granularity" in the definition of the universe, so as to make it effective and efficient.
Though this is different for every bank, below are some of the considerations for defining IS Audits:

- **Using overly-broad definitions for IS Audits (e.g. IT general controls) will ensure a scope creep in audit procedures.** The IS Audit Head should make sure that the definition of each IS Audit is an accurate description of what is being reviewed.
- **Audit Universe for a year should touch upon all layers in the IT environment.** Though each IT environment is different, layers tend to be the same. If an IS Audit plan does not include some review for each of the layers, odds are that the plan, as a whole, is deficient.
- **IS Audits should be structured in such a way as to provide for effective and logical reporting**. For example: IS Audits of pervasive technologies (e.g. networks or processes) are more effective when audited at an enterprise level.
- **IS Audits should address appropriate risks.** In many cases, IS Audit budgets are determined before the IT risk assessment is performed. This inevitably leads to one of two situations:

An inadequate number of audit hours are spread over too many audits, which results in consistently poor quality audits, because there is not enough time.
Audits that should be performed are not performed because the budget does not allow it.

(e) Scoping for IS Audit

Information gathered by the IS Auditors during IT risk assessment about the IT system processing and operational environment, threats, vulnerabilities, impact and controls, enables identification of the control objectives and activities to be tested for design and implementation effectiveness and its operating effectiveness.

Scoping plays a crucial role in overall effectiveness. This is exacerbated by the need for the IS Auditors to integrate with the process, operational or financial auditors, and the procedures they are performing, particularly in environments with large integrated CBS applications, where a high number of key process controls are contained within the systems.
(An illustrative list of areas which can form a part of IS Audit scope are given in Annex-B.)

IS Audits should also cover branches, with focus on large and medium branches, in areas such as control of passwords, user ids, operating system security, anti-malware, maker-checker, segregation of duties, physical security, review of exception reports or audit trails, BCP policy and or testing.

Reports and circulars issued by RBI for specific areas which also need to be covered in the IS Audit Scope:

Report of the Committee on Computer Audit (dated: April 2, 2002)
Circular on Information System Audit–A Review of Policies and Practices
(dated: April 30, 2004 (RBI/2004/191 DBS.CO.OSMOS.BC/ 11 /33.01.029/2003-04)

(i) Defining Control Objectives and Activities

IT control objectives, based on well known frameworks can be included in the scope.

(ii) Materiality

When conducting financial statement audits, Internal Auditors measure materiality in monetary terms, since areas that are audited are also measured and reported in monetary terms. However, since IS Auditors conduct audit on non-financial items, alternative measures are required to assess materiality. Such assessments are a matter of professional judgment. They include consideration of its effect on a bank as a whole, of errors, omissions, irregularities and illegal acts, which may have happened as a result of "internal control weaknesses" in an area being audited. ISACA IS Auditing Guideline G6: specifies that if the IS Audit focus relates to systems or operations that process financial transactions, the value of assets controlled by the system(s), or the value of transactions processed per day/week/month/year, should be considered in assessing materiality. In case, the focus is on systems that do not process financial transactions, then following measures should be considered:

- Criticality of the business processes supported by the system or operation
- Cost of system or operation (hardware, software, staff, third-party services, overheads or a combination of these)
- Potential cost of errors (possibly in terms of irrecoverable development costs, cost of publicity required for warnings, rectification costs, health and safety costs, high wastage, etc.)
- Number of accesses/transactions/inquiries processed per period
- Nature, timing and extent of reports prepared, and files maintained
- Service-level agreement requirements and cost of potential penalties
- Penalties for failure to comply with legal and contractual requirements

IS Auditors should review the following additional areas that are critical and high risk such as:

- IT Governance and information security governance structures and practices implemented by the Bank
- Testing the controls on new development systems before implementing them in live environment.
- A pre-implementation review of application controls, including security features and controls over change management process, should be performed to confirm that:
    - Controls in existing application are not diluted, while migrating data to the new application
    - Controls are designed and implemented to meet requirements of a bank's policies and procedures, apart from regulatory and legal requirements
    - Functionality offered by the application is used to meet appropriate control objectives

- A post implementation review of application controls should be carried out to confirm if the controls as designed are implemented, and are operating, effectively. Periodic review of application controls should be a part of an IS audit scope, in order to detect the impact of application changes on controls. This should be coupled with review of underlying environment–operating system, database, middleware, etc.–as weaknesses in the underlying environment can negate the effectiveness of controls at the application layer. Due care should be taken to ensure that IS Auditors have access only to the test environment for performing the procedures and data used for testing should be, as far as practical, be a replica of live environment.

- Detailed audit of SDLC process to confirm that security features are incorporated into a new system, or while modifying an existing system, should be carried out.
- A review of processes followed by an implementation team to ensure data integrity after implementation of a new application or system, and a review of data migration from legacy systems to the new system where applicable, should be followed.
- IS Auditors may validate IT risks (identified by business teams) before launching a product or service. Review by IS Auditor may enable the business teams to incorporate additional controls, if required, in the system before the launch.

(iii) Building Fraud Risk Perspective

In planning and performing an audit to reduce risks to a low level, the auditor should consider the risk of irregularities and illegal acts. He should maintain professional skepticism during an audit, recognising the possibility that "material mis-statements due to irregularities and illegal acts" could exist, irrespective of their evaluation of risk of irregularities and illegal acts.

IS Auditors are also required to consider and assess the risk of fraud, while performing an audit. They should design appropriate plans, procedures and tests, to detect irregularities, which can have a material effect on either a specific area under an audit, or the bank as a whole. IS Auditors should consider whether internal control weaknesses could result in material irregularities, not being prevented or detected. The auditor should design and perform procedures to test the appropriateness of internal control and risk of override of controls. They should be reasonably conversant with fraud risk factors and indicators, and assess the risk of irregularities connected with the area under audit.

In pursuance to the understanding gathered during threat identification step of the IT Risk Assessment process, the auditors should identify control objectives and activities. These are required to be tested to address fraud risk. He should consider "fraud vulnerability assessments" undertaken by the "Fraud Risk Management Group", while identifying fraud risk factors in the IT risk assessment process. He should be aware that certain situations may increase a bank's vulnerability to fraud risk (e.g. introduction of a new line of business, new products, new delivery channels and new applications or systems.)

In preparing an audit scope, auditors should consider fraud risk factors including these*:*

1. Irregularities and illegal acts that are common to banking industry
2. Corporate ethics, organisational structure, adequacy of supervision, compensation and reward structures, the extent of performance pressures
3. Management's behavior with regard to ethics
4. Employee dissatisfaction resulting from potential layoffs, outsourcing, divestiture or restructuring
5. Poor financial or operational performance
6. Risk arising out of introduction of new products and processes
7. Bank's history of fraud
8. Recent changes in management teams, operations or IT systems
9. Existence of assets held, or services offered, and their susceptibility to irregularities
10. Strength of relevant controls implemented
11. Applicable regulatory or legal requirements
12. History of findings from previous audits
13. Findings of reviews, carried out outside the audit, such as the findings from external auditors, consultants, quality assurance teams, or specific investigations
14. Findings reported by management, which have arisen during the day-to-day course of

business
15. Technical sophistication and complexity of the information system(s) supporting the area under audit
16. Existence of in-house (developed or maintained) application systems, as compared with the packaged software for core business systems

Instances of fraud should be reported to appropriate bank stakeholders*:*
1. Frauds involving amounts of Rs 1 crore (and above) should be reported to Special Committee formed to monitor and follow up large fraud cases
2. Other fraud cases should be reported to Fraud Review Councils or independent groups formed to manage frauds
3. The status of fraud cases should be reported to Audit Committee as a part of their review of IS audit
4. IS Auditors should also extend necessary support to Fraud Review Councils or independent groups or Special Committees in their investigations

(f) Planning the Execution

The IS Audit Head is responsible for the annual IS Audit Plan, prepared after considering the risk assessment and scoping document. The plan covers overall audit strategy, scoped areas, details of control objectives identified in the scoping stage, sample sizes, frequency or timing of an audit based on risk assessment, nature and extent of audit and IT resource skills availability, deployment and need for any external expertise. A report on the status of planned versus actual audits, and any changes to the annual audit plan, needs to be periodically presented to Audit Committee and Senior Management on a periodic basis.
There are well-known guidance on IS Audit. The Institute of Chartered Accountants of India (ICAI), in March 2009, published the "Standard on Internal Audit (SIA) 14: Internal Audit in an Information Technology Environment" covering requirements of the planning stage, which an auditor should follow. IIA has provided guidance on defining the IS Audit Universe, through the guide issued on "Management of IS Auditing" under the "Global Technology Audit Guide" series. ITGI has provided guidance on audit planning in its "IT Assurance Guide using COBIT".

Suggested guidelines for implementation by banks are as follows:

i. Documenting the Audit Plan

The plan (either separately or as part of overall internal audit plan) should be a formal document, approved by the Audit Committee initially and during any subsequent major changes. The plan should be prepared so that it is in compliance with any appropriate external requirements in addition to well-known IS Auditing Standards.

Audit Plan Components include:

- **Internal Audit Subject:** Name of the Audit Subject
- **Nature of Audit:** Compliance with legal, regulatory or standards, performance metrics assessment or security configuration testing
- **Schedule:** Period of audit and its expected duration
- **Scoped Systems:** Identified IT resources that are in the scope based on the risk assessment process
- **System Overview:** Details of System Environment based on the risk assessment process
- **Audit Details:** Details of risks and controls identified, based on the risk assessment process
- **Nature and Extent of Tests:** Controls testing for effectiveness of design and implementation of controls, substantive testing for operating effectiveness of controls implemented

- **Method of Internal Audit:** Brief audit approach and methodology
- **Team and Roles and Responsibilities:** Identified skills and names of IS Auditors including their roles and responsibilities
- **Points of Contact:** Contact names of auditee department
- **Co-ordination:** Names of the project lead and higher official for escalation of issues
- **Information:** Report details of past audits on the subject

ii. Nature and Extent of Tests of Control

Types of testing that can be performed are as below:

- **Test of Control Design:** Controls that have been identified are evaluated for appropriateness in mitigating the risks
- **Test of Control Implementation:** Tests are performed to confirm that the control that has been appropriately designed is implemented and is operating at the time of testing. Mitigating or compensating controls are also reviewed wherever necessary
- **Assessing Operational Effectiveness of Controls:** Wherever the controls designed are found to be in operation, additional testing is performed for the period of reliance (audit period) to confirm if they are operating effectively and consistently

On case-to-case basis, the auditor should exercise professional judgment and decide the nature and extent of procedures that need to be adopted for conclusions. **ISA 330** gives guidance on the nature, timing and extent of procedures.

iii. Sampling techniques

During an audit, auditors should obtain sufficient, reliable and relevant evidence to achieve their objectives. Findings and conclusions should be supported by appropriate analysis and interpretation. Auditors should consider sample selection techniques, which result in a statistically-based representative sample for performing compliance or substantive testing. Statistical sampling involves the use of techniques from which mathematically-constructed conclusions regarding the population can be drawn. Non-statistical sampling is not statistically-based. Its results should not be extrapolated over the population as a sample is unlikely to be representative of the population. Examples of compliance testing of controls where sampling could be considered, include user-access rights, programme change control procedures, procedures documentation, programme documentation, follow-up of exceptions, review of logs and software licences audits. Examples of substantive tests where sampling could be considered, include re-performance of a complex calculation (e.g., interest applied), on a sample of accounts, sample of transactions to vouch to supporting documentation, etc.

Design of A Sample

While designing the size and structure of an audit sample, auditors may consider the following guidelines:

– **Sampling Unit:** The unit will depend on the sample purpose. For compliance testing of controls, attribute sampling is typically used, where the unit is an event or transaction (e.g., a control such as an authorisation of transaction).

– **Audit objectives:** IS Auditors should consider the audit objectives to be achieved and the audit procedures, which are most likely to achieve those objectives. In addition, when sampling is appropriate, consideration should be given to the nature of the audit evidence sought, and possible error conditions.

– Population: Population is an entire set of data from which auditors wish to sample, in order to reach a conclusion. Hence, the population from which a sample is drawn, has to be appropriate and verified as a “complete” for audit objective.

– **Stratification:** To assist in efficient and effective design of a sample, stratification may be appropriate. Stratification is a process of dividing a population into “sub-populations” with

similar characteristics, explicitly defined, so that each sample unit can belong to only one stratum.

Selection of A Sample

IS Auditors should use statistical sampling methods. They may consider using the following:

– **Random Sampling:** It ensures that all combinations of units in the population have an equal chance of selection

– **Systematic Sampling:** It involves selecting units using a fixed interval between selections, the first interval having a random start. Examples include “Monetary Unit Sampling” or “Value Weighted Selection”, where each individual monetary value (e.g., Rs 100) in the population, is given an equal chance of selection. As an individual monetary unit cannot ordinarily be examined separately, the item which includes that monetary unit is selected for examination. This method systematically weighs the selection in favour of the larger amounts, but gives every monetary value an equal opportunity for selection. Another example includes selecting every ‘nth sampling unit”.

iv. Standards and Frameworks

One challenge that the IS Auditors face is knowing what to audit against as a fully-developed IT control baselines for applications and technologies that may not have been developed. Rapid evolution of technology is likely to render baselines useless, after a period of time. However, this does not detract from the concept of control objectives.

Control objectives, by definition, should remain more or less constant (from environment to environment). Consider the objective that critical business data and programmes should be backed up and recoverable. Now, each environment may do that differently; backups could be manual, or automated, or a tool may be used. They could be incremental only, or there may be complete backups of everything. Backups could be done daily, weekly, or monthly. Storage of backups could be onsite in a fireproof safe, off-site at another company facility, or outsourced to a third party. Method used by the organisation to manage backups would certainly impact the audit procedures and budget, but the control objective will not change. IS Auditor should be able to start with a set of IT control objectives, and though not specific to particular environments, select an appropriate framework.

v. Resource Management

A bank’s auditors play a critical role in efficiency and effectiveness of audits. IT encompasses a wide range of technology and sophistication—the skill set needed to audit a Firewall configuration is vastly different from the skill set needed to audit application controls. It is critical to match the skills needed to perform a particular IS Audit, with the appropriate auditor. IS Auditors should also have the appropriate analytical skills to determine and report the root cause of deficiencies. Bank’s hiring and training practices should ensure that it has qualified IS Auditors where education and experience should be consistent with job responsibilities. Audit management should also provide an effective programme of continuing education and development.

The main issue is having staff with the requisite range of IS Audit skills, needed to audit an IS Audit universe, effectively. If internal expertise is inadequate, the Board should consider using qualified external sources, such as management consultants, independent auditors, or professionals, to supplement internal resources and support bank's objectives.

4) Executing IS Audit

As mentioned earlier, auditors must understand the business and IT environment, risks and internal control framework. During audit, auditors should obtain evidences, perform test

procedures, appropriately document findings, and conclude a report. This section provides guidance on matters that IS Auditor should consider while executing the Plan.

ICAI, in March 2009, had published a "Standard on Internal Audit (SIA) 14: Internal Audit in an Information Technology Environment" covering the requirements of executing a plan that an IS Auditor should follow. Additionally, IIA has also provided guidance in their "Management of IS Auditing" under their "Global Technology Audit Guide" series. The ITGI has also provided guidance on execution of assurance initiative in its "IT Assurance Guide Using COBIT".

Guidance on executing the IS Audit entails the following steps:

- Refining the understanding of business process and IT environment
- Refining the scope and identifying internal controls
- Testing Control Design
- Testing the outcome of the control objectives
- Collecting audit evidence
- Documenting test results
- Concluding tests performed
- Considering use of audit accelerators
- Considering the use of Computer-Aided Automated Tools (CAATs)
- Considering the work of others
- Considering third-party review by service providers

The above are covered in the following sections:

(a) Refine understanding of the business process and IT environment:

The first step of the execution stage is refining the understanding of an IT environment, in which a review is being planned. This implies understanding of a bank's business processes to confirm the correct scope and control objectives. The scope of the IS Audit need to be communicated to and agreed upon by stakeholders.

Output from this step consists of documented evidence regarding:

– Who performs the task(s), where it is performed and when
– Inputs required to perform the task and outputs generated by it
– Automated tasks performed by systems and system configurations
– System-generated information used by business
– Stated procedures for performing tasks

The IS Auditor can structure this step along the following lines:

- Interview and use activity lists and RACI charts
- Collect and read process description, policies, input or output, issues, meeting minutes, past audit reports, past audit recommendations, business reports
- Prepare a scoping task (process objective, goals and metrics)
- Build an understanding of enterprise IT architecture

(b) Refining Scope and Identifying Internal Controls:

While understanding and evaluating internal controls of a bank, areas mentioned under "Scope of IS Audit" needs to be covered. However, the nature and extent of control risks may vary, depending on nature and characteristics of a bank's information system:

- Reliance on systems or programmes that are inaccurately processing data, or processing inaccurate data, or both
- Unauthorised access to data which may result in destruction of data, or improper changes to data, including recording of unauthorised or non-existent transactions, or inaccurate recording of transactions
- Possibility of IT personnel gaining access to privileges, beyond those necessary, to

perform their assigned duties, thereby breaking down segregation of duties
- Unauthorised changes to data in master files
- Unauthorised changes to systems or programmes
- Failure to make necessary changes to systems or programmes
- Inappropriate manual intervention
- Potential loss of data or inability to access data

(c) Testing Control Design:

This section lists the different techniques that will be used in detailed audit steps. Testing of controls is performed covering the main test objectives:

- Evaluation of control design
- Confirmation that controls are in place within the operation
- Assess the operational effectiveness of controls
- Additionally, control efficiency could be tested

In the testing phase, different types of testing can be applied. Five generic testing methods include enquire and confirm, inspect, compare actual with expected findings, re-perform or re-calculate and review automated evidence collection through analyzing date using computer assisted audit techniques and extracting exceptions or key transactions.

To assess the adequacy of the design of controls the following steps should be performed:

– Observe, inspect and review control approach. Test the design for completeness, relevance, timeliness and measurability

– Enquire whether, or confirm that, the responsibilities for control practices and overall accountability have been assigned

– Test whether accountability and responsibilities are understood and accepted. Verify that the right skills and the necessary resources are available

– Enquire through interviews with key staff involved whether they understand the control mechanism, its purpose and the accountability and responsibilities.

IS Auditor must determine whether:

- Documented control processes exist
- Appropriate evidence of control processes exists
- Responsibility and accountability are clear and effective
- Compensating controls exist, where necessary

Additionally, specifically in internal audit assignments, cost-effectiveness of a control design may also be verified, with the following audit steps:

– **If the control design is effective:** Investigate whether it can be made more efficient by optimising steps, looking for synergies with other mechanisms, and reconsidering the balance of prevention versus detection and correction. Consider the effort spent in maintaining the control practices

– **If the control is operating effectively:** Investigate whether it can be made more cost-effective. Consider analysing performance metrics of activities associated, automation opportunities or skill level

(d) Test the Outcome of Control Objectives

Audit steps performed ensure that control measures established are working as prescribed and conclude on the appropriateness of the control environment. To test the effectiveness of a control, the auditor needs to look for direct and indirect evidence of the control's impact on the process outputs. This implies the direct and indirect substantiation of measurable contribution of the control to the IT, process and activity goals, thereby recording direct and indirect evidence of actually achieving the outcomes or various control objectives (based on those documented in standards like COBIT, as relevant).

The auditor should obtain direct or indirect evidence for selected items or periods to ensure that the control under review is working effectively by applying a selection of testing techniques as presented in step on test of control design. The IS Auditor should also perform a limited review of the adequacy of the process deliverables, determine the level of substantive testing and additional work needed to provide assurance that the IT process is adequate. Substantive testing would involve performing analytical procedures and tests of details, to gain assurance on areas where control weaknesses are observed. Substantive testing is performed to ascertain the actual impact of control weaknesses.

(e) Audit Evidence

IS Auditors should obtain sufficient and reliable audit evidence to draw reasonable conclusions on which to base the audit results.

Sufficient Evidence: Evidence can be considered sufficient if it supports all material questions in the audit objective and scope. Evidence should be objective and sufficient to enable a qualified independent party to re-perform tests and obtain the same results. The evidence should be commensurate with the materiality of an item and risks involved. In instances where IS Auditor believes sufficient audit evidence cannot be obtained, they should disclose this in a manner consistent with the communication of the audit results.

Appropriate Evidence: Appropriate evidence shall include the following indicative criteria:

- Procedures as performed by the IS Auditor
- Results of procedures performed by the IS Auditor
- Source documents (electronic or paper), records and corroborating information used to support the audit
- Findings and results of an audit

When obtaining evidence from a test of control design, auditors should consider the completeness of an audit evidence to support the assessed level of control risk.

Reliable Evidence: IS Auditors should take note of following examples of evidence that is more reliable when it is:

– Written form and not oral expressions
– Obtained from independent sources
– Obtained by IS Auditors, rather than from the bank being audited
– Certified by an independent party

Procedures used to gather evidence can be applied through the use of manual audit procedures, computer-assisted techniques, or a combination of both. For example: a system, which uses manual control totals to balance data entry operations might provide audit evidence that the control procedure is in place by way of an appropriately reconciled and annotated report. IS Auditors should obtain audit evidence by reviewing and testing this report. Detailed transaction records may only be available in machine-readable format, requiring IS Auditors to obtain evidence using computer-assisted techniques.

When information produced by a bank is used by auditors, they should obtain evidence about the completeness and accuracy by the following means:

- Performing tests of the operating effectiveness of controls over the production and maintenance of information, to be used as audit evidence
- Performing audit procedures directly on information to be used as audit evidence

Auditors should consider the following controls over production and maintenance of information produced by a bank:

– Controls over the integrity, accuracy, and completeness of the source data
– Controls over the creation and modification of the applicable report logic and parameters

(f) Documentation

Audit evidence gathered should be documented and organised to support findings and conclusions. IS Audit documentation is a record of the work performed and evidence supporting findings and conclusions.

***The potential uses of documentation**:*

- Demonstration of the extent to which the auditor has complied with professional standards related to IS auditing
- Assistance with audit planning, performance and review
- Facilitation of third-party reviews
- Evaluation of the auditors' quality assurance programme
- Support in circumstances such as insurance claims, fraud cases and lawsuits
- Assistance with professional development of the staff

Documentation should include, at a minimum, a record of:

– Planning and preparation of the audit scope and objectives
– Audit steps performed and audit evidence gathered
– Audit findings, conclusions and recommendations
– Reports issued as a result of the audit work
– Supervisory review

Extent of an IS Auditor's documentation may depend on needs for a particular audit and should include such things as:

- IS Auditor's understanding of an area to be audited, and its environment
- His understanding of the information processing systems and internal control environment
- Audit evidence, source of audit documentation and date of completion
- Bank's response to recommendations

Documentation should include audit information, required by law, government regulations, or by applicable professional standards. Documentation should be clear, complete and understandable, by a reviewer. IS Audit owns evidences documented by them, in order to substantiate conclusions on tests performed and specific observations reported to management and Audit Committee.

(g) Conclusion on Tests Performed

IS Auditors should evaluate conclusions drawn as a basis for forming an opinion on the audit. Conclusions should be substantiated by evidences, collected and documented. The IS Audit Team may be required to provide and maintain evidences in respect of observations reported by them.

IS Auditors may perform following activities required to conclude on tests performed based on nature and amount of identified control failures and likelihood of undetected errors:

– Decide whether the scope of IS Audit was sufficient to enable the auditors to draw reasonable conclusions on which to base audit opinion

- Perform audit procedures designed to obtain sufficient appropriate audit evidence: events upto the date of audit report may be included and identified in the report
- Prepare an audit summary memorandum documenting findings and conclusions on important issues of IS Auditing and reporting, including judgments made by an IS Audit team
- Obtain appropriate representations from bank management
- Prepare a report appropriate to circumstances, and in conformity with, applicable professional standards and regulatory and legal requirements

- Communicate, as necessary, with Audit Committee or Senior Management
- Maintain effective controls over processing and distribution of reports relating to the IS Audit

If audit evidence or information indicate that irregularities could have occurred, IS auditors should recommend the bank management on matters that require detailed investigation to enable the management to initiate appropriate investigative actions. The auditors should also consider consulting the Audit Committee and legal counsel about the advisability and risks of reporting the findings outside the Bank.

RBI (vide its circular DBS.CO.FrMC.BC.No.7/23.04.001/ 2009-10, dated: September 16, 2009) requires that fraud cases should be reported to law enforcement agencies and to the RBI. Banks should appropriately include requirements for reporting to RBI, of such instances, in engagement letters issued to external IS Auditors.

(h) Audit Accelerators

Since IS Audit budgets can be difficult to estimate and manage, CAEs can consider using testing accelerators—tools or techniques that help support procedures that the IS Auditors will be performing —to increase efficiency and effectiveness. CAEs can use an accelerator to do the same audit in less time, or do more detailed audit procedures in the same amount of time. Audit accelerators can be divided into two categories:

– Audit Facilitators: Tools that help support the overall management of an audit (e.g., an electronic workpaper management tool)

– **Testing Accelerators**: Tools that automate the performance of audit tests (e.g., data analysis tools).

Audit Facilitators

These include Electronic Workpapers, project management software, flow charting software and open issue tracking software.

Testing Accelerators

Testing accelerators can automate time-consuming audit tasks, such as reviewing large populations of data. Also, using a tool to perform audit procedures helps establish consistency. For example, if a tool is used to assess server security configuration, servers tested with that tool will be assessed along the same baselines. Performing these procedures manually allows for a degree of interpretation on the part of the IS Auditor. Lastly, the use of tools enables IS Auditors to test an entire population of data, rather than just a sample of transactions. This provides for a much higher degree of audit assurance.

Data Analysis Software: These allow an auditor to perform robust statistical analysis of large data sets. They can also be used to support process or operational audits like KYC reviews. They can support types of testing. One consideration when using a data analysis tool is that it may be difficult to extract the data from the original source. It is critical that audit procedures be performed to ensure the completeness and accuracy of the source data.

Security Analysis Tools: These are a broad set of tools that can review a large population of devices or users and identify security exposures. There are different types of security analysis tools. Generally they can be categorised as follows:

- *Network Analysis Tools:* These consist of software programmes that can be run on a network and gather information about it. IS Auditors can use these tools for a variety of audit procedures, including:

Verifying the accuracy of network diagrams by mapping corporate network
Identifying key network devices that may warrant additional audit attention
Gathering information about what traffic is permitted across a network (which would directly support the IT risk assessment process).

- *Hacking Tools:* Most technologies have a number of standard vulnerabilities, such as the existence of default IDs and passwords or default settings when the technology is installed out-of-the-box. Hacking tools provide for an automated method of checking for these. Such tools can be targeted against Firewalls, servers, networks and operating systems.
- *Application Security Analysis Tools:* If an organisation is using large integrated business application, key internal controls are highly security dependent. Application-level security must be well-designed and built in conjunction with the application's processes and controls.

The CAE should be aware that most of these come with a set of pre-configured rules, or vendor-touted "best practices". Implementation of one will need to be accompanied by a substantive project to create a rule set that is relevant for that particular organisation. Failure to do so will result in audit reports that contain a number of either false-positives or false-negatives.

CAEs should be aware of the following considerations, with respect to IS Audit Accelerators:

- Tools cost money. The CAE should be sure that the benefits outweigh the costs
- That IS Auditors will need to be trained on the new tool. It is not uncommon that a tool sits unused in an Internal Audit Department
- That the tool will need support, patch management and upgrades. Depending on the quality, it may require a standalone server, as well. For this, any tool selection should be managed with the IT department's assistance

Sometimes, IT management or third-party service providers are not allowed tools to access the production environment directly. They are instead asked to do so from a copy of data from an alternative site, or standby server. Any use of tools or scripts should be thoroughly discussed with and approved by IT management and be tested fully before deploying.

(i) Computer-Assisted Audit Techniques (CAATS)

IS Auditors can use an appropriate combination of manual techniques and CAATs. IS Audit function needs to enhance the use of CAATs, particularly for critical functions or processes carrying financial or regulatory or legal implications. The extent to which CAATs can be used will depend on factors such as efficiency and effectiveness of CAATs over manual techniques, time constraints, integrity of the Information System and IT environment and level of audit risk.

CAATs may be used in critical areas (like detection of revenue leakage, treasury functions, assessing impact of control weaknesses, monitoring customer transactions under AML requirements and generally in areas where a large volume of transactions are reported).

Process involved in using CAATs involve the following steps:

- Set audit objectives of CAATs
- Determine accessibility and availability of a bank's IS facilities, programs, systems and data
- Define procedures to be undertaken (e.g., statistical sampling, recalculation, or confirmation)
- Define output requirements
- Determine resource requirements: i.e. personnel, CAATs, processing environment, bank's IS facilities or audit IS facilities
- Obtain access to the bank's IS facilities, programmes, systems and data, including file definitions
- Document CAATs to be used, including objectives, high-level flowcharts, and run instructions

CAATs may be used to perform the following audit procedures among others:

– Test of transactions and balances, such as recalculating interest
– Analytical review procedures, such as identifying inconsistencies or significant fluctuations
– Compliance tests of general controls: testing set-up or configuration of the operating system, or access procedures to the programme libraries
– Sampling programmes to extract data for audit testing
– Compliance tests of application controls such as testing functioning of a programmed control
– Re-calculating entries performed by the entity's accounting systems
– Penetration testing

In instances, where CAATs may be used to extract sensitive programmes, system information or production data, IS Auditors should safeguard the programme, system information or production data, with an appropriate level of confidentiality and security. In doing so, IS Auditors should consider the level of confidentiality and security required by the bank, owning the data and any relevant legislation. IS Auditors should be provided with "view access" to systems and data. In case audit procedures cannot be performed in the live environment, appropriate test environment should be made available to IS Auditors. Systems and data under test environment should be synchronised to the live environment.

IS Auditors should use and document results of appropriate procedures to provide for ongoing integrity, reliability, usefulness and security of the CAATs. Example: this should include a review of programme maintenance and change controls over embedded audit software to determine that only authorised changes were made to the CAATs.

In instances where CAATs reside in an environment not under the control of the IS Auditor, an appropriate level of control should, in effect, be placed to identify changes. When the CAATs are changed, IS Auditors should obtain assurance of their integrity, reliability, usefulness and security, through appropriate planning, design, testing, processing and review of documentation, before placing their reliance.

(j) Continuous Auditing

Traditionally, testing of controls performed by an internal audit team was on a retrospective and cyclical basis, often many months after business activities have occurred. The testing procedures have often been based on a sampling approach. They included activities such as reviews of policies, procedures, approvals and reconciliations. Today, however, it is recognised that this approach only affords internal auditors a narrow scope, and is often too late to be of "real value" to business performance or regulatory compliance.

Continuous auditing is a method used to perform control and risk assessments automatically on a more frequent basis using technology which is key to enabling such an approach. Continuous auditing changes the audit paradigm from periodic reviews of a sample of transactions to ongoing audit testing of 100 percent of transactions. It becomes an integral part of modern auditing at many levels. It also should be closely tied to management activities such as performance monitoring, scorecard or dashboard and enterprise risk management.

A continuous audit approach allows internal auditors to fully understand critical control points, rules, and exceptions. With automated, frequent analyses of data, they are able to perform control and risk assessments in real time or near real time. They can analyse key business systems for both anomalies at the transaction level and for data-driven indicators of control deficiencies and emerging risk.

Finally, with continuous auditing, the analysis results are integrated into all aspects of the audit process, from the development and maintenance of the enterprise audit plan to the conduct and follow-up of specific audits. Depending on the level of implementation and

sustenance of risk-based IS Audit approach; banks may explore implementation of continuous auditing in critical areas in a phased manner.

(k) Application Control Audit:

Detailed pre-implementation application control audits and data migration audits in respect of critical systems needs to be subjected to independent external audit. Banks also need to conduct a post-implementation detailed application control audit. Furthermore, banks should also include application control audits in a risk based manner as part of the regular Internal Audit/IS Audit plans with focus on data integrity (among other factors). General internal auditors with requisite functional knowledge need to be involved along with the IS Auditors in the exercise to provide the requisite domain expertise.

Some of the considerations in application control audit (based on ISACA guidelines) include:

i. An IS Auditor should understand the IS environment to determine the size and complexity of the systems, and the extent of dependence on information systems by the bank
ii. Application-level risks at system and data-level include, system integrity risks relating to the incomplete, inaccurate, untimely or unauthorized processing of data; system-security risks relating to unauthorized access to systems or data; data risks relating to its completeness, integrity, confidentiality and accuracy; system-availability risks relating to the lack of system operational capability; and system maintainability risks in terms of adequate change control procedures.
iii. Application controls to address the application-level risks may be in the form of computerized controls built into the system, manually performed controls, or a combination of both. Risks of manual controls in critical areas need to be considered. Where the option to place reliance on programmed controls is taken, relevant general IT controls should be considered, as well as controls specifically relevant to the audit objective. Objectives should be developed to address criteria such as integrity, availability, compliance, reliability and confidentiality. Effectiveness and efficiency can also be additional criteria.
iv. As part of documenting the flow of transactions, information gathered should include both computerized and manual aspects of the system. Focus should be on data input (electronic or manual), processing, storage and output which are of significance to the audit objective.
v. Consideration should also be given to documenting application interfaces with other systems. The auditor may confirm the documentation by performing procedures such as a walk-through test.
vi. Specific controls to mitigate application risks may be identified. Sufficient audit evidence obtained to assure the auditor that controls are operating as intended through procedures such as inquiry and observation, review of documentation and testing of the application system controls, where programmed controls are being tested. Use of computer-assisted audit techniques (CAATs) also needs to be considered.
vii. Nature, timing and extent of testing should be based on the level of risk to the area under review and audit objectives. In absence of strong general IT controls, an IS auditor may make an assessment of the effect of this weakness on the reliability of the computerized application controls.
viii. If an IS auditor finds significant weaknesses in the computerized application controls, assurance should be obtained (depending on the audit objective), if possible, from the manually performed processing controls.
ix. Effectiveness of computerized controls is dependent on general IT controls. Therefore, if general IT controls are not reviewed, ability to place reliance on controls may be limited. Then the IS Auditor should consider alternative procedures.
x. Where weaknesses identified during the application systems review are considered

to be significant or material, appropriate level of management should be advised to undertake immediate corrective action.

(l) Using the Work of Others

Purpose of an IS Audit standard is to establish and provide a guidance to auditors who can use the work of experts on an audit. The following are standards, to test the reliability of the work of an expert:

i. IS Auditors should, where appropriate, consider using the work of other experts for audit
ii. They should assess, and then be satisfied with professional qualifications, competencies, relevant experience, resources, independence and quality control processes, prior to engagement

- They should assess, review and evaluate work of experts, as a part of an audit, and then conclude the extent of use and reliance of the work
- They should determine and conclude whether the work of experts is adequate and competent to enable them to conclude on current audit objectives. Such conclusion should be documented
- They should apply additional test procedures to gain and include scope limitation, where required evidence is not obtained through additional test procedures
- An expert could be an IS Auditor from external auditing firm, a management consultant, an IT domain expert, or an expert in the area of audit, who has been appointed by management or by the IS Audit Team
- An expert could be internal or external to the bank. If an expert is engaged by another part of the organisation, reliance may be place on the banks' report. In some cases, this may reduce the need of an IS Audit coverage, though IS Auditors do not have supporting documentation and work papers. IS Auditors should be cautious in providing an opinion on such cases
- An IS Auditor should have access to all papers, supporting documents and reports of other experts, where such access does not create legal issues. Where access creates legal issues, or such papers are not accessible, auditors should determine and conclude on the extent of use and reliance on expert's work
- The IS Auditor's views, relevance and comments on adopting the expert's report should form a part of the IS Auditor's Report

(m) Third Party Review of Service Providers

A bank may use a third-party service provider (service organisation) to obtain services of packaged software applications and technology environment, which enables customers to process financial and operational transactions (ATM management, networking and infrastructure development and maintenance, document imaging and indexing, software development and maintenance). RBI has issued "Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks" (*circular no: DBOD.NO.BP.40/21.04.158/ 2006-07 dated November 3, 2006)*, asking banks to adhere to guidelines before outsourcing activities related to financial services.

Services provided by a third party are relevant to the scope of IS Audit. Especially, when those services and controls within them, are a part of the bank's information systems. Though controls at the service organisation are likely to relate to financial reporting, there may be other controls that may also be relevant to the IS Audit (controls over safeguarding of assets or document images).

A service organisation's services are a part of a bank's information system, including related business processes, relevant to IS Audit if these services affect any of the following:

- Segments of Information System that are significant to the bank's IS operations
- Procedures within information system, by which an user entity's transactions are

initiated, recorded, processed, corrected (when necessary), transferred to a general ledger and reported, in financial statements

- The way events and conditions, other than transactions, significant to bank's Information System are captured

IS Auditors will have to obtain an understanding of how a bank uses services of a service organisation in the bank's IS operations, including:

- Nature of services provided by the organisation and significance of those to the bank's information system, including the effect thereof on the bank's internal control
- Nature and materiality of transactions, accounts or financial reporting processes, affected by the service organisation
- Degree of interaction between activities of the organisation and bank
- Nature of relationship between the bank and organisation, including relevant contractual terms for activities undertaken by the organisation

In situations, services provided by the organisation may not appear to be "material" to the bank's IS operations. But, the service nature may be. IS Auditors should determine that an understanding of those controls is necessary in the circumstances. *Information on the nature of services, provided by an organisation, may be available from a variety of sources:*

- User manual
- System overview
- Technical manuals
- Contract or service-level agreement between the bank and organisation
- Reports by service organisation, internal auditors, or regulatory authorities, on service organisation controls
- Reports by an auditor of the organisation (service auditor), including management letters

IS Auditors may use a service auditor to perform procedures such as tests of controls at service organisation, or substantive procedures on the bank's IS operations, served by a service organisation.

5) Reporting and Follow-up

This phase involves reporting audit findings to the CAE and Audit Committee. Before reporting the findings, it is imperative that IS Auditors prepare an audit summary memorandum providing overview of the entire audit processing from planning to audit findings, discuss the findings with auditee and obtain responses. Additionally, reviewing the actions taken by management to mitigate the risks observed in audit findings and appropriately updating the audit summary memorandum is also important. Reporting entails deciding the nature, timing and extent of follow-up activities and planning future audits.

Professional bodies like ISACA, IIA, ICAI have issued guidance in this regard.
Reporting and follow-up entails following activities or steps:
– Drafting audit summary and memorandum
– Discussing findings with management
– Finalising and submitting reports
– Reviewing the Actions taken report
– Undertaking follow-up procedures
– Archiving documents

These are covered in the following sections:

(a) **Audit Summary and Memorandum:** An IS Auditor should perform audits or reviews of control procedures and form a conclusion about, and reporting on, the design and

operating effectiveness of the control procedures based on the identified criteria. The conclusion for an audit is expressed as a positive expression of opinion and provides a high level of assurance. The conclusion for a review is expressed as a statement of negative assurance and provides only a moderate level of assurance.

(b) **Discuss Findings with Management:** Bank's management is responsible for deciding the appropriate action to be taken in response to reported observations and recommendations. IS Auditors are responsible for assessing such management action for appropriateness and the timely resolution of the matters reported as observations and recommendations.

Senior Management may decide to accept the risk of not correcting the reported condition because of cost or other considerations. The Board (or the Audit Committee, if one exists) should be informed of Senior Management's decision on significant observations and recommendations. When Auditors IS believes that an organisation has accepted a level of residual risk that is inappropriate for the organisation, they should discuss the matter with Internal Audit and Senior Management. If the IS Auditors are not in agreement with the decision, regarding residual risk, IS Auditors and Senior Management should report the matter to the Board, or Audit Committee, for resolution.

Events sometimes occur, subsequent to the point in time or period of time of the subject matter being tested, but prior to the date of the IS Auditor's report, that have a material effect on the subject matter and therefore require adjustment or disclosure in the presentation of the subject matter or assertion.

(c) Finalise and Submit Reports

IS Auditors should review and assess the conclusions drawn from the evidence obtained as the basis for forming an opinion on the effectiveness of the control procedures based on the identified criteria.

Major findings identified during an audit should have a definite time line indicated for remedial actions, these should be followed up intensively and compliance should be confirmed.

An IS Auditor's report about the effectiveness of control procedures should cover aspects like:

– Description of the scope of the audit, including:
  – Identification or description of the area of activity
  – Criteria used as a basis for the IS Auditor's conclusion
  – A statement that the maintenance of an effective internal control structure, including control procedures for the area of activity, is the responsibility of management

– A statement that IS Auditors have conducted the engagement to express an opinion on the effectiveness of control

(d) Review Action Taken Report

After reporting of findings and recommendations, IS Auditors should request and evaluate relevant information to conclude whether appropriate action has been taken by management in a timely manner. If management's proposed actions to implement reported recommendations have been discussed with, or provided to, the IS Auditor, these actions should be recorded as a management response in the final report. The nature, timing and extent of the follow-up activities should take into account the significance of the reported finding and the impact if corrective action is not taken. The timing of IS Audit follow-up activities in relation to the original reporting should be a matter of professional judgment dependent on a number of considerations, such as the nature or magnitude of associated risks and costs to the entity.

(e) Follow-up Procedures

Procedures for follow-up activities should be established which includes:
– The recording of a time frame within which management should respond to agreed-upon recommendations
– An evaluation of management's response
– A verification of the response, if thought appropriate
– Follow-up work, if thought appropriate
– A communications procedure that escalates outstanding and unsatisfactory responses/ actions to the appropriate levels of management
– A process for providing reasonable assurance of management's assumption of associated risks, in the event that remedial action is delayed or not proposed to be implemented
– An automated tracking system or database can assist in the carrying out of follow-up activities.

(f) Update Audit Summary Memorandum

An audit summary memorandum should be prepared and addresses the following:
– Conclusion about specific risk
–Changes in the bank, its environment and banking industry that come to the attention after the completion of the audit planning memorandum and that caused to change audit plan
–Conclusion regarding the appropriateness of the going concern assumption and the effect, if any, on financial statements
–The result of subsequent reviews and conclusion regarding the effect of subsequent events on financial statements
–Conclusion reached in evaluation of misstatements, including disclosure deficiencies
–If contradiction or inconsistency with final conclusion regarding a significant matter is observed, there should be proper documentation of addressing the inconsistency
–Conclusion of whether the audit procedures performed and the audit evidence obtained were appropriate and consistent to support the audit conclusion

(g) Archival of Documents

Banks are recommended to have an archiving/ retention policy to archive the audit results. Banks to have an archiving policy that:
– Ensures integrity of the data
– Defines appropriate access rights
– Decides on the appropriate archiving media
– Ensures ease of recovery

6) Quality Review

This section is aimed at emphasising quality of work of IS Auditors, while performing duties as an auditor. Appropriate levels in IS Audit function are recommended to assess audit quality by reviewing documentation, ensuring appropriate supervision of IS Audit members and assessing whether IS Audit members have taken due care while performing their duties. This will bring efficiency, control and improve quality of the IS Audit.

(a) Evidences and Documentation

IS Auditors may perform the following progressive reviews of the evidences and documentation:
– A detailed review of each working paper prepared by a less-experienced member of the IS Audit team, by a more experienced member, who did not participate in the preparation of such working paper
– A primary review of the evidences and documentation by the Manager or IS Audit Head. Where the manager performs a primary review, this does not require that each working paper be reviewed in detail by the manager, as each working paper has already been reviewed in detail by the person who performed the detailed review.
– An overriding review of the working papers by the CAE, as needed

(b) Supervision

IS Audit staff should be supervised to provide reasonable assurance that audit objectives are accomplished and applicable professional auditing standards are met.

(c) Due Care

The standard of “due care” is that level of diligence which a prudent and competent person would exercise under a given set of circumstances. “Due professional care” applies to an individual who professes to exercise a special skill such as IS auditing. Due professional care requires the individual to exercise that skill to a level commonly possessed by auditors with the specialty.

Due professional care applies to the exercise of professional judgment in the conduct of work performed. It implies that the professional approaches matters requiring professional judgment with proper diligence. Despite the exercise of due professional care and professional judgment, situations may arise where an incorrect conclusion may be drawn from a diligent review of the available facts and circumstances. Therefore, the subsequent discovery of incorrect conclusions does not, in and of itself, indicate inadequate professional judgment or lack of diligence on the part of the IS Auditor.

Due professional care should extend to every aspect of the audit, including the evaluation of audit risk, the formulation of audit objectives, the establishment of the audit scope, the selection of audit tests, and the evaluation of test results.

In doing this, IS Auditors should determine or evaluate:

- Type and level of audit resources required to meet audit objectives
- Significance of identified risks and the potential effect of such risks on the audit
- Audit evidence gathered
- Competence, integrity and conclusions of others upon whose work IS Auditors places reliance

Intended recipients of audit reports have an appropriate expectation that IS Auditors have exercised due professional care throughout the course of the audit. IS Auditors should not accept an assignment unless adequate skills, knowledge, and other resources are available to complete the work in a manner expected of a professional. IS Auditors should conduct the audit with diligence while adhering to professional standards. IS Auditors should disclose the circumstances of any non-compliance with professional standards in a manner consistent with the communication of the audit results.

(d) Independent Assurance of the Audit function

With a view to provide assurance to bank’s management and regulators, banks are required to conduct a quality assurance, at least **once in three years**, on the bank's Internal Audit, including IS Audit function, to validate approach and practices adopted by them in the discharge of its responsibilities as laid out in the Audit Policy.

Objectives of performing a quality assessment are:

- Assess efficiency and effectiveness of an Internal Audit for current and future business goals
- Determine value addition from Internal Audit to the business units

Benchmark, identify and recommend, successful practices of Internal Audit

- Assess compliance to standards for professional practice of Internal Audit

Others:

As a matter of prudence, banks should rotate IS Auditors in a specific area on periodic basis,

say atleast once in two years. The same needs to be incorporated in IS Audit policy/charter. Further, in order to avoid conflict of interest an audit firm/consultant who had provided consulting services on a specific area should not audit the area as part of pre or post implementation audit.

ANNEXURE:

Annexure B–*Broad scope of IS Audit*

CHAPTER 6 – CYBER FRAUD

Introduction:

With the advances in information technology, most banks in India have migrated to core banking platforms and have moved transactions to payment cards (debit and credit cards) and to electronic channels like ATMs, Internet Banking and Mobile Banking. Fraudsters have also followed customers into this space. However, the response of most of the banks to frauds in these areas needs further improvement, thereby avoiding putting the entire onus on the customer. There is also a lack of clarity amongst banks on the reporting of these instances as frauds.

A need is therefore felt to have an industry wide framework on fraud governance with particular emphasis on tackling electronic channel based frauds. This note endeavours to bring out the challenges and suggests a framework which can be implemented across banks to effectively tackle the electronic fraud menace. It would be useful to recall the definition of fraud at this stagyuo]\j;'e.

> *'A deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank'.*

This definition has been recommended as per para 9.1 of the Report of the Study Group on Large Value Bank Frauds set up by the Reserve Bank of India in 1997. It follows that like other bank frauds, various IT related frauds need to get captured through the fraud reporting system and banks should take adequate steps to mitigate such risks.

1. Roles/Responsibilities and Organizational structure for fraud risk management:

(a) Indian banks follow the RBI guideline of reporting all frauds above ₹ 1 crore to their respective Audit Committee of the Board. Apart from this, banks are also putting up a detailed annual review of frauds to their Audit Committee of the Board. The Board for Financial Supervision (BFS) of RBI has observed that in terms of higher governance standards, the fraud risk management and fraud investigation must be 'owned' by the bank's CEO, Audit Committee of the Board and the Special Committee of the Board.

(b) Special Committee of the Board for monitoring large value frauds

Banks are required to constitute a special committee for monitoring and follow up of cases of frauds involving amounts of ₹1 crore and above exclusively, while the Audit Committee of the Board (ACB) may continue to monitor all the cases of frauds in general.

Most retail cyber frauds and electronic banking frauds would be of values less than ₹1 crore and hence may not attract the necessary attention of the Special Committee of the Board. Since these frauds are large in number and have the potential to reach large proportions, it is imperative that the Special Committee of the Board be briefed separately on this to keep them aware of the proportions of the fraud, modus operandi and the steps taken by the bank to mitigate them. The Special Committee should specifically monitor and review the progress of the mitigating steps taken by the bank in case of electronic frauds and the efficacy of the same in containing fraud numbers and values at least on **a quarterly basis**.

(c) Separate Department to manage frauds

The activities of fraud prevention, monitoring, investigation, reporting and awareness creation should be owned and carried out by an **independent group in the bank**. The group should be adequately staffed and headed by a senior official of the Bank, not below the rank of General Manager.

(d) Fraud review councils

Fraud review councils should be set up by the above fraud risk management group within various business groups in the bank. The council should comprise of head of the business, head of the fraud risk management department, the head of operations supporting that particular business function and the head of information technology supporting that business function. The councils should meet every quarter to review fraud trends and preventive steps taken by the business group, and report the same to the Special Committee.

2. Components of fraud risk management:

(i) Fraud prevention practices

A strong internal control framework is the strongest deterrence for frauds. The fraud risk management department along with the business/operations/support groups, continuously reviews various systems and controls, to remove gaps if any, and to strengthen the internal control framework. The following are some of the fraud prevention practices that are recommended for banks.

(a) Fraud vulnerability assessments

Fraud vulnerability assessments should be undertaken across the bank by the fraud risk management group. Apart from the business and the operations groups, such assessment also cover channels of the bank such as branches, internet, ATM and phone banking, as well as international branches, if any. During the course of a vulnerability assessment, all the processes should be assessed based on their fraud risk. Controls need to be checked and improvements suggested for tightening the same. These should be reviewed in the fraud review councils.

'Mystery Shopping' is an important constituent of vulnerability assessment. Transactions are introduced in 'live' scenarios to test the efficacy of controls. The results of the mystery shopping exercises should be shared with the relevant groups in the fraud review councils and be used for further strengthening of controls.

(b) Review of new products and processes

No new product or process should be introduced or modified in a bank without the approval of control groups like compliance, audit and fraud risk management groups. The product or process needs to be analysed for fraud vulnerabilities and fraud loss limits to be mandated wherever vulnerabilities are noticed.

(c) Fraud loss limits

All residual/open risks in products and processes need to be covered by setting 'fraud-loss' limits. 'Fraud-loss' limits need to be monitored regularly by the fraud risk management group and a review needs to be undertaken with the respective business group when fraud loss amount reaches 90% of the limit set. In case it is difficult to set a fraud- loss limit, a limit on the total number or total value of frauds may be defined. For the purpose of deciding how much a product or a process has used up the limit set, the cumulative value of frauds in that product or process during the financial year needs to be considered.

(d) Root cause analysis

All actual fraud cases above ₹10 lakhs and cases where a unique modus operandi is involved, should be reviewed immediately after such a fraud is detected. The findings should be used to redesign products and processes and remove the gaps so that they do not recur.

(e) Data/information/system security

Most banks have incorporated several security measures for their documents, information, systems and customer deliverables such as cheque books/debit cards. Security measures have also been incorporated during delivery of instruments such as cards/cheque books/internet passwords to customers through couriers. Internet banking systems have security features such as separate transaction passwords, two factor authentication, multi-channel process for registering payees, upper limit on transaction value and SMS alerts to customers. It is also necessary that customer confidential information and other data/information available with banks is secured adequately to ensure that fraudsters do not access it to perpetrate fraudulent transactions. Appropriate steps need to be taken to ensure data/information/system security at the Bank, as indicated earlier in the report. Information security and appropriate access control procedures ensure that only employees who are required to know particular information have access to the same and can put through transactions. Further, a bank's systems need to be adequately secured to ensure that no un-authorised person carries out any system modifications/changes. Appropriate verification procedures should also be incorporated at all channels such as phone banking, ATMs, branches and internet to ensure that only genuine transactions are put through. All the above security measures should be under continuous review for further strengthening. Details in this regard were covered in chapter on information security.

(f) Know Your Customer (KYC) and know your employee/vendor procedures

A strong KYC process is the backbone of any fraud prevention activity. Such a process enables banks to prevent unscrupulous elements from gaining entry into the bank's environment, which gives them an opportunity to carry out their fraudulent intentions. Similarly, appropriate due diligence procedures before recruitment of employees and vendors is essential to prevent known fraudsters or people with fraudulent motives to have access to a bank's channels. Banks have to implement strong procedures to carry out due diligence of potential customers, employees and vendors before they are enrolled.

(g) Physical security

All banks have a dedicated team to take care of the security of the physical infrastructure. This team should conduct regular security audits of various offices to check for deviations/lapses. It is the responsibility of this team to ensure that physical assets and data copied on magnetic/optical media do not go out of the offices of the bank without authorisation.

(h) Creation of fraud awareness amongst staff and customers

Awareness on how to prevent and detect frauds is the basis of fraud management. Banks need to adopt various measures to create awareness amongst staff and customers.

(ii) Fraud detection

a) Detection of fraud

Despite strong prevention controls aimed at fraud deterrence, fraudsters do manage to

perpetrate frauds. In such cases, the earlier the fraud is detected, the better the chance of recovery of the losses and bringing the culprits to book. System triggers that throw up exceptional transactions, opening up channels that take note of customer/employee alerts/disputes, seeding/mystery shopping exercises and encouraging employees/customers/ well- wishers to report suspicious transactions/behaviours are some of the techniques that are used for detection of frauds. The exceptional/suspicious transactions/activities reported through these mechanisms should be investigated in detail.

b) Transaction monitoring

Banks should set up a transaction monitoring unit within the fraud risk management group. The transaction monitoring team should be responsible for monitoring various types of transactions, especially monitoring of potential fraud areas, by means of which, early alarms can be triggered. This unit needs to have the expertise to analyse transactions to detect fraud trends. This unit should work in conjunction with the data warehousing and analytics team within banks for data extraction, filtering, and sanitisation for transaction analysis for determining fraud trends. Banks should put in place automated systems for detection of frauds based on advanced statistical algorithms and fraud detection techniques.

c) Alert generation and redressal mechanisms

Appropriate mechanisms need to be established in banks, to take note of the disputes/exceptions or suspicions highlighted by various stakeholders including transaction monitoring teams in banks and to investigate them thoroughly. Banks should have a well publicised whistle blowing mechanism.

d) Dedicated email ID and phone number for reporting suspected frauds

Banks can have dedicated email IDs and phone numbers for customers to report any fraudulent activity that they may notice. A dedicated team can be created to reply to customer queries and concerns through the above email IDs. Phone banking officers and branch staff should also be trained on response to customers' queries and concerns on frauds.

e) Mystery shopping and reviews

Continuous supervision and control by managers/supervisors on activities is important to detect any abnormal activity. However, considering a bank's size and scope, this needs to be supplemented by mystery shopping to detect system flaws and also to identify unscrupulous employees/vendors. Immediate action needs to be taken on the findings of such reviews.

f) Importance of early detection of frauds

A bank's fraud management function is effective if it is able to minimise frauds and when fraud occurs, is able to detect the fraud so that the loss is minimised.

(iii)Fraud investigation

The examination of a suspected fraud or an exceptional transaction or a customer dispute/alert in a bank shall be undertaken by:

- Fraud risk management group
- Specific committee/team of employees constituted to examine the 'suspected fraud'
- External agencies, if any, as appointed by the bank

a) Fraud Investigation function

It is widely accepted that fraud investigation is a specialised function. Thus, the fraud risk management group should undergo continuous training to enhance its skills and competencies. The first step in an investigation process is gathering the entire transaction details, documents and complete details of the customer/employee or vendor. In order to investigate into suspected cases, the group would adopt various advanced techniques including computer forensics, forensic accounting and tools to analyse large volumes of data.

The investigation team may conduct oral interviews of customers or employees to understand the background and details of the case. In case an interview of the person accused of fraud is required to be undertaken, the investigation group should follow a prescribed procedure and record statements appropriately. The investigation activities need to be carried out discreetly and within a specified time line. The investigating team should take into account all the relationships of the involved parties with the bank while investigating and submitting an investigation report. The investigation report will help the respective business groups take a decision on all the relationships of the customer with the Bank. The investigation report should conclude whether a suspected case is a fraud and thereafter the report would form the basis for further actions such as regulatory reporting.

In case of employee involvement in the fraud, the investigation report may be the basis of staff accountability and HR actions. It may be noted that, during the course of the investigations, banks should adopt only means permitted by law, regulations and code of conduct of the bank and any inconvenience to customers or general public should be avoided. It is also important to note that certain investigations are best carried out by law enforcement authorities and the bank should refer cases to such authorities at the appropriate time, to enable them to carry out their responsibilities efficiently.

In case of need, the investigating team should seek the support of other specialised groups within the bank, such as the audit group to carry out investigations efficiently.

At times, investigation of a fraud wherein money has come into the country to an account in a bank through another bank in the same country needs to be done. The intermediary bank does not investigate or report the case stating that it is merely an intermediary while the recipient bank states that it has no knowledge of the transaction and is merely a recipient of the funds sent by the intermediary bank. In this case, it is clarified that the bank whose customer has received the money should investigate and report the case.

b) Recovery of fraud losses

The concerned group in a bank, in which the fraud has occurred, should make all out efforts to recover the amount lost. They may use specialised groups like legal or collections for this purpose. The investigation team may also be able to recover some amounts during the course of their investigation. The Police may also recover some amount during their investigation. This would be deposited in Court pending final adjudication. The bank should liaise with the Police and keep track of such amounts.

(iv)Reporting of frauds

As per the guidelines on reporting of frauds as indicated in the RBI circular, dated July 1, 2010, fraud reports should be submitted in all cases of fraud of ₹1 lakh and above perpetrated through misrepresentation, breach of trust, manipulation of books of account, fraudulent encashment of instruments like cheques, drafts and bills of exchange, unauthorised handling of securities charged to the bank, misfeasance, embezzlement,

misappropriation of funds, conversion of property, cheating, shortages, irregularities, etc. Banks should also report frauds in the electronic channels and the variants of plastic cards used by a bank and its customers for concluding financial transactions.

a) Frauds in merchant acquiring business

A special mention needs to be made here of frauds done by collusive merchants who use skimmed/stolen cards on the POS terminals given to them by banks and then abscond with the money before the chargeback is received on the transaction. It is imperative that the bank which has provided acquiring services to such merchant, reports the case to RBI.

b) Frauds in ATM acquiring business

Also, it has been observed that in a shared ATM network scenario, when the card of one bank is used to perpetrate a fraud through another bank's ATM, there is a lack of clarity on who should report such a fraud. It is the bank acquiring the transaction that should report the fraud. The acquiring bank should solicit the help of the issuing bank in recovery of the money. The facts of the case would decide as to which bank will bear the loss.

c) Filing of police complaints

Banks should readily share data and documents requested by the police even in cases where the bank in question is not the victim of the fraud but has been a receiver of fraudulent monies into its accounts.

(v) Customer awareness on frauds

a) Creation of customer awareness on frauds

Customer awareness is one of the pillars of fraud prevention. It has been seen that alert customers have enabled prevention of several frauds and in case of frauds which could not be avoided, helped in bringing the culprit to book by raising timely alerts. Banks should thus aim at continuously educating its customers and solicit their participation in various preventive/detective measures. It is the duty of all the groups in banks to create fraud risk awareness amongst their respective customers. The fraud risk management group should share its understanding of frauds with each group, identify areas where customer awareness is lacking and if required, guide the groups on programmes to be run for creation of awareness amongst customers. The groups should ensure that in each of their interaction with customers there is at least one message to make the customer aware of fraud risk.

The following are some of the recommended measures to create awareness amongst customers:

- Publications in leading newspapers
- Detailed 'do's and don'ts' on the web site of the bank
- Messages along with statement of accounts, either physical or online
- Messages printed on bank's stationery such as envelopes, card covers, etc.
- SMS alerts
- Message on phone banking when the customer calls
- As inserts or on the jackets of cheque books
- Posters in branches and ATM centres
- Interstitials on television and radio

It should be ensured that the communication to the customer is simple and aimed at making them aware of fraud risks and seeking their involvement in taking proper

precautions aimed at preventing frauds. Such communication should be reviewed periodically by the fraud risk management group to judge its effectiveness.

(vi) Employee awareness and training

(a) Creation of employee awareness

Employee awareness is crucial to fraud prevention. Training on fraud prevention practices should be provided by the fraud risk management group at various forums. Banks may use the following methods to create employee awareness:

- Class room training programmes at the time of induction or during risk related training sessions
- Publication of newsletters on frauds covering various aspects of frauds and containing important message on fraud prevention from senior functionaries of the Bank
- E-learning module on fraud prevention
- Online games based on fraud risks in specific products or processes
- E-tests on prevention practices and controls
- Detailed 'do's and don'ts' put up on the worksite of the employee
- Safety tips flashed at the time of logging into Core Banking System (CBS), screen savers, etc.
- Emails sent by the respective business heads
- Posters on various safety measures at the work place
- Messages/discussions during daily work huddles

(b) Rewarding employees on fraud prevention

A positive way of creating employee awareness is to reward employees who have gone beyond their call of duty, and prevented frauds. Awards may be given to employees who have done exemplary work in preventing frauds. Details of employees receiving such awards may be published in the fraud newsletters.

CHAPTER 7: BUSINESS CONTINUITY PLANNING

Introduction

The pivotal role that banking sector plays in the economic growth and stability, both at national and individual level, requires continuous and reliable services. Increased contribution of 24x7 electronic banking channels has increased the demand to formulate consolidated Business Continuity Planning (BCP) guidelines covering critical aspects of people, process and technology.

BCP forms a part of an organisation's overall Business Continuity Management (BCM) plan, which is the “preparedness of an organisation”, which includes policies, standards and procedures to ensure continuity, resumption and recovery of critical business processes, at an agreed level and limit the impact of the disaster on people, processes and infrastructure (includes IT); or to minimise the operational, financial, legal, reputational and other material consequences arising from such a disaster.

Effective business continuity management typically incorporates business impact analyses, recovery strategies and business continuity plans, as well as a governance programme covering a testing programme, training and awareness programme, communication and crisis management programme.

1. Roles, Responsibilities and Organisational structure

Board of Directors and Senior Management

A bank’s Board has the ultimate responsibility and oversight over BCP activity of a bank. The Board approves the Business Continuity Policy of a bank. Senior Management is responsible for overseeing the BCP process which includes*:*

- Determining how the institution will manage and control identified risks
- Allocating knowledgeable personnel and sufficient financial resources to implement the BCP
- Prioritizing critical business functions
- Designating a BCP committee who will be responsible for the Business Continuity Management
- The top management should annually review the adequacy of the institution's business recovery, contingency plans and the test results and put up the same to the Board.
- The top management should consider evaluating the adequacy of contingency planning and their periodic testing by service providers whenever critical operations are outsourced.
- Ensuring that the BCP is independently reviewed and approved at least annually;
- Ensuring employees are trained and aware of their roles in the implementation of the BCP
- Ensuring the BCP is regularly tested on an enterprise-wide basis
- Reviewing the BCP testing programme and test results on a regular basis and
- Ensuring the BCP is continually updated to reflect the current operating environment

1.1 BCP Head or Business Continuity Coordinator

A senior official needs to be designated as the Head of BCP activity or function.

His or her responsibilities include:

- Developing of an enterprise-wide BCP and prioritisation of business objectives and critical operations that are essential for recovery
- Business continuity planning to include the recovery, resumption, and maintenance of all aspects of the business, not just recovery of the technology components;
- Considering the integration of the institution's role in financial markets;
- Regularly updating business continuity plans based on changes in business processes, audit recommendations, and lessons learned from testing
- Following a cyclical, process-oriented approach that includes a business impact analysis (BIA), a risk assessment, management and monitoring and testing
- Considering all factors and deciding upon declaring a "crisis"

1.2 BCP Committee or Crisis Management Team

Since electronic banking has functions spread across more than one department, it is necessary that each department understands its role in the plan. It is also important that each gives its support to maintain it. In case of a disaster, each has to be prepared for a recovery process, aimed at protection of critical functions. To this end, it would be helpful if a set up like the BCP Committee, charged with the implementation of BCP, in an eventuality and all departments expected to fulfill their respective roles in a coordinated manner.

Hence, a committee consisting of senior officials from departments like HR, IT, Legal, Business and Information Security needs to be instituted with the following broad mandate:

- To exercise, maintain and to invoke business continuity plan, as needed
- Communicate, train and promote awareness
- Ensure that the Business Continuity Plan (BCP) fits with other plans and requirement of concerned authorities
- Budgetary issues
- Ensure training and awareness on BCP to concerned teams and employees
- Co-ordinating the activities of other recovery, continuity, response teams and handling key decision-making
- They determine the activation of the BCP
- Other functions entail handling legal matters evolving from the disaster, and handling public relations and media inquiries

1.3 BCP Teams

There needs to be adequate teams for various aspects of BCP at central office, as well as individual controlling offices or at a branch level, as required. Among the teams that can be considered based on need, are the incident response team, emergency action and operations team, team from particular business functions, damage assessment team, IT teams for hardware, software, network support, supplies team, team for organizing logistics, relocation team, administrative support team, coordination team. Illustrative guidelines for committees *or teams for BCP are provided in Annex C.*

2. Critical Components of Business Continuity Management Framework

The BCP requirements enunciated in this document should be considered. The onus lies on the Board and Senior Management for generating detailed components of BCP in the light of an individual bank's activities, systems and processes.

2.1 BCP Methodology

Banks should consider looking at BCP methodologies and standards–BS 25999 by BSI– which follows the "Plan-Do-Check-Act Principle".

BCP methodology should include:

Phase 1: Business Impact Analysis

- Identification of critical businesses, owned and shared resources with supporting functions to come up with the Business Impact Analysis (BIA)
- Formulating Recovery Time Objectives (RTO), based on BIA. It may also be periodically fine-tuned by benchmarking against industry best practices
- Critical and tough assumptions in terms of disaster, so that the framework would be exhaustive enough to address most stressful situations
- Identification of the Recovery Point Objective (RPO), for data loss for each of the critical systems and strategy to deal with such data loss
- Alternate procedures during the time systems are not available and estimating resource requirements

Phase 2: Risk Assessment

- Structured risk assessment based on comprehensive business impact analysis. This assessment considers all business processes and is not limited to the information processing facilities.
- Risk management by implementing appropriate strategy/ architecture to attain the bank's agreed RTOs and RPOs.

v) Impact on restoring critical business functions, including customer-facing systems and payment and settlement systems such as cash disbursements, ATMs, internet banking, or call centres

- Dependency and risk involved in use of external resources and support

Phase 3: Determining Choices and Business Continuity Strategy

- BCP should evolve beyond the information technology realm and must also cover people, processes and infrastructure
- The methodology should prove for the safety and well-being of people in the branch / outside location at the time of the disaster.
- Define response actions based on identified classes of disaster.
- To arrive at the selected process resumption plan, one must consider the risk acceptance for the bank, industry and applicable regulations

Phase 4: Developing and Implementing BCP

- Action plans, i.e.: defined response actions specific to the bank's processes , practical manuals(do and don'ts, specific paragraph's customised to individual business units) and testing procedures
- Establishing management succession and emergency powers
- Compatibility and co-ordination of contingency plans at both the bank and its service providers
- The recovery procedure should not compromise on the control environment at the recovery location
- Having specific contingency plans for each outsourcing arrangement based on the degree of materiality of the outsourced activity to the bank's business
- Periodic updating to absorb changes in the institution or its service providers. Examples of situations that might necessitate updating the plans include acquisition of new equipment, upgradation of the operational systems and changes in:
    a) Personnel
    b) Addresses or telephone numbers
    c) Business strategy
    d) Location, facilities and resources
    e) Legislation
    f) Contractors, suppliers and key customers
    g) Processes–new or withdrawn ones
    h) Risk (operational and financial)

2.3 Key Factors to be considered for BCP Design

Following factors should be considered while designing the BCP:

- Probability of unplanned events, including natural or man-made disasters, earthquakes, fire, hurricanes or bio-chemical disaster
- Security threats
- Increasing infrastructure and application interdependencies
- Regulatory and compliance requirements, which are growing increasingly complex
- Failure of key third party arrangements
- Globalisation and the challenges of operating in multiple countries.

1.4 BCP Considerations

(a) Banks must consider implementing a BCP process to reduce the impact of disruption, caused by disasters and security failures to an acceptable level through a combination of preventive and recovery measures.
(b) BCP should include measures to identify and reduce probability of risk to limit the consequences of damaging incidents and enable the timely resumption of essential operations. BCP should amongst others, consider reputation, operational, financial, regulatory risks.
(c) The failure of critical systems or the interruption of vital business processes could prevent timely recovery of operations. Therefore, financial institution management must fully understand the vulnerabilities associated with interrelationships between various systems, departments, and business processes. These vulnerabilities should be incorporated into the BIA, which analyses the correlation between system components and the services they provide.
(d) Various tools can be used to analyse these critical interdependencies, such as a work flow analysis, an organisational chart, a network topology, and inventory records. A work flow analysis can be performed by observing daily operations and

interviewing employees to determine what resources and services are shared among various departments. This analysis, in conjunction with the other tools, will allow management to understand various processing priorities, documentation requirements, and the interrelationships between various systems. The following issues when determining critical interdependencies within the organisation:

i. Key personnel;
ii. Vital records;
iii. Shared equipment, hardware, software, data files, and workspace;
iv. Production processes;
v. Customer services;
vi. Network connectivity; and
vii. Management information systems.

(e) Key Considerations while Formulating A BCP:

- Ensuring prompt and accurate processing of securities transactions, including, but not limited to, order taking, order entry, execution, comparison, allocation, clearance and settlement of securities transactions, the maintenance of customer accounts, access to customer accounts and the delivery of funds and securities.
- Honouring of all customer payouts (i.e. obligation)
- Providing priority to intra-day deal payment
- Providing customers prompt access to their funds and securities – measures should be undertaken to make customer funds and securities available to customers in the event of a significant business disruption.
- Continuing compliance with regulatory reporting requirements etc.

(f) A single framework of BCP should be maintained to ensure that all plans are consistent, and to identify priorities and dependencies for testing and maintenance.

A BCP framework should consider the following:

- Conditions for activating plans, which describe a process to be followed (how to assess the situation, who is to be involved, etc.) before each plan is activated
- Emergency procedures, which describe the actions to be taken following an incident which jeopardises business operations and/ or human life. This should include arrangements for public relations management and for effective liaison with appropriate public authorities e.g. police, fire service, health-care services and local government
- Identification of the processing resources and locations, available to replace those supporting critical activities; fall back procedures which describe the actions to be taken to move essential business activities or support services to alternative temporary locations and to bring business processes back into operation in the required time-scales
- Identification of information to be backed up and the location for storage, as well as the requirement for the information to be saved for back-up purpose on a stated schedule and compliance therewith
- Resumption procedures, which describe the actions to be taken to return to normal business operations
- A maintenance schedule which specifies how and when the plan will be tested and the process for maintaining the plan
- Awareness and education activities, which are designed to create understanding of critical banking operations and functions, business continuity processes and ensure

that the processes continue to be effective

- The responsibilities of the individuals, describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.

(g) Pandemic Planning

Pandemics are defined as epidemics, or outbreaks in humans, of infectious diseases that have the ability to spread rapidly over large areas, possibly worldwide. Adverse economic effects of a pandemic could be significant, both nationally and internationally. Due to their crucial financial and economic role, financial institutions should have plans in place that describe how they will manage through a pandemic event.

Pandemic planning presents unique challenges to financial institution management. Unlike natural disasters, technical disasters, malicious acts, or terrorist events, the impact of a pandemic is much more difficult to determine because of the anticipated difference in scale and duration. Further, while traditional disasters and disruptions normally have limited time durations, pandemics generally occur in multiple waves, each lasting two to three months. Consequently, no individual or organisation is safe from the adverse effects that might result from a pandemic event.

One of the most significant challenges likely from a severe pandemic event will be staffing shortages due to absenteeism. These differences and challenges highlight the need for all financial institutions, no matter their size, to plan for a pandemic event when developing their BCP.

It is important for institutions to actively keep abreast of international and national developments and health advisories issued in this regard.

Accordingly, a bank's BCP needs to provide for the following:

1. A preventive programme to reduce the likelihood that a bank's operations will be significantly affected by a pandemic event, including: monitoring of potential outbreaks, educating employees, communicating and coordinating with critical service providers and suppliers, in addition to providing appropriate hygiene training and tools to employees.

2. A documented strategy that provides for scaling the institution's pandemic efforts so they are consistent with the effects of a particular stage of a pandemic outbreak, such as first cases of humans contracting the disease overseas or in India and first cases within the organisation itself. The strategy will also need to outline plans that state how to recover from a pandemic wave and proper preparations for any following wave(s).

3. A comprehensive framework of facilities, systems, or procedures that provide the organisation the capability to continue its critical operations in the event that large numbers of the institution's staff are unavailable for prolonged periods. Such procedures could include social distancing to minimise staff contact, telecommuting, redirecting customers from branch to electronic banking services, or conducting operations from alternative sites.

4. The framework should consider the impact of customer reactions and the potential demand for, and increased reliance on, online banking, telephone banking, ATMs, and call support services. In addition, consideration should be given to possible actions by public health and other government authorities that may affect critical business functions of a financial institution.

5. A testing programme to ensure that the institution's pandemic planning practices and capabilities are effective and will allow critical operations to continue.

6. An oversight programme to ensure ongoing review and updates to the pandemic plan so that policies, standards, and procedures include up-to-date, relevant information provided by governmental sources or by the institution's monitoring programme.

7. Banks may also consider insurance to transfer risk to a third party, however taking due care regarding certainty of payments in the event of disruptions.

3. Testing A BCP

– *Banks must regularly test BCP to ensure that they are up to date and effective:* Testing of BCP should include all aspects and constituents of a bank i.e. people, processes and resources (including technology). BCP, after full or partial testing may fail. Reasons are incorrect assumptions, oversights or changes in equipment or personnel. BCP tests should ensure that all members of the recovery team and other relevant staff are aware of the plans. The test schedule for BCPs should indicate how and when each component of a plan is to be tested. It is recommended to test the individual components of the plans(s) frequently, typically at a minimum of once a year. A variety of techniques should be used in order to provide assurance that the plan(s) will operate in real life.

– *Banks should involve their Internal Auditors (including IS Auditors) to audit the effectiveness of BCP:* And its periodic testing as part of their Internal Audit work and their findings/ recommendations in this regard should be incorporated in their report to the Board of Directors.

– *Banks should consider having a BCP drill planned along with the critical third parties:* In order to provide services and support to continue with pre-identified minimal required processes.

– *Banks should also periodically moving their operations:* Including people, processes and resources (IT and non-IT) to the planned fall-over or DR site in order to test the BCP effectiveness and also gauge the recovery time needed to bring operations to normal functioning.

– *Banks should consider performing the above test without movement of bank personnel to the DR site*. This will help in testing the readiness of alternative staff at the DR site.

– *Banks should consider having unplanned BCP drill:* Wherein only a restricted set of people and certain identified personnel may be aware of the drill and not the floor or business personnel. In such cases banks should have a "Lookout Team" deployed at the location to study and assimilate the responses and needs of different teams. Based on the outcome of this study, banks should revise their BCP Plan to suit the ground requirements.

3.1 Testing Techniques

The below are few of the illustrative techniques that can be used for BCP testing purposes:

- **Table-top testing** for scenarios (discussing business recovery arrangements using example interruptions)
- **Simulations** (particularly for training people in their post-incident or crisis

management roles)

- **Technical recovery testing** (ensuring information systems can be restored effectively)
- **Testing recovery at an alternate site** (running business processes in parallel with recovery operations away from the main site)
- **Tests of supplier facilities and services** (ensuring externally provided services and products will meet the contracted commitment)
- **Complete rehearsals** (testing that the organisation, personnel, equipment, facilities and processes can cope with interruptions)

a) Simulation testing: It is when participants choose a specific scenario and simulate an on-location BCP situation. It involves testing of all resources: people, IT and others, who are required to enable the business continuity for a chosen scenario. The focus is on demonstration of capability, including knowledge, team interaction and decision-making capabilities. It can also specify role playing with simulated response at alternate locations/facilities to act out critical steps, recognise difficulties, and resolve problems.

b) Component testing: This is to validate the functioning of an individual part or a sub-process of a process, in the event of BCP invocation. It focuses on concentrating on in-depth testing of the part or sub-process to identify and prepare for any risk that may hamper its smooth running. For example, testing of ATM switch.

Each organisation must define frequency, schedule and clusters of Business Areas, selected for test after a through Risk and Business Impact Analysis has been done.

The bank can consider broad guidelines provided below for determining the testing frequency based on critical of a process:

Impact on processes	**Table-top testing**	**Call tree**	**Simulation testing**	**Component testing**	**Complete Rehearsals**
High	Quarterly	Quarterly	Quarterly	Quarterly	Annually
Medium	Quarterly	Half-yearly	Half-yearly	Annually	Annually
Low	Half-yearly	Annually	NA	NA	NA

4. Maintenance and Re-assessment of Plans

(a) BCPs should be maintained by annual reviews and updates to ensure their continued effectiveness. Procedures should be included within the organisation's change management programme to ensure that business continuity matters are appropriately addressed. Responsibility should be assigned for regular reviews of each business continuity plan. The identification of changes in business arrangements/processes, not yet reflected in the business continuity plans, should be followed by an appropriate update of the plan on a periodic basis, say quarterly. This would require a process of conveying any changes to the institution's business, structure, systems, software, hardware, personnel, or facilities to the BCP coordinator/team. If significant

changes have occurred in the business environment, or if audit findings warrant changes to the BCP or test programme, the business continuity policy guidelines and programme requirements should be updated accordingly.

(b) Changes should follow the bank's formal change management process in place for its policy or procedure documents. This formal change control process should ensure that the updated plans are distributed and reinforced by regular reviews of the complete plan.

(c) A copy of the BCP, approved by the Board, should be forwarded for perusal to the RBI on an annual basis. In addition, the bank should also submit:

– An annual statement at the end of each financial year describing the critical systems, their Rots and the bank's strategy to achieve them, and

– A quarterly statement, reporting major failures during the period for critical systems, customer segment or services impacted due to the failures and steps taken to avoid such failures in future.

5. Procedural aspects of BCP

(a) An effective BCP should take into account the potential of wide area disasters, which impact an entire region, and for resulting loss or inaccessibility of staff. It should also consider and address inter dependencies, both market-based and geographic, among financial system participants as well as infrastructure service providers.

(b) Further, banks should also consider the need to put in place necessary backup sites for their critical payment systems which interact with the systems at the Data centres of the Reserve Bank.

(c) Banks may also consider running some critical processes and business operations from primary and the secondary sites, wherein each would provide back-up to the other.

(d) Namely prioritising process and alternative location for personnel in the following categories:

- Dealers and traders
- Operations (e.g. teller, loan desk, cash desk etc.)
- Treasury department staff
- Sales staff
- IT staff
- Corporate functions (HR, Admin) staff
- Comprehensive testing would help banks to further fine-tune BCP/DR processes to ensure their robustness and also enable smooth switch-over to the DR site, as per the priority and scale of processes identified for each process.

(e) All critical processes should be documented to reduce dependency on personnel for scenarios where the staff is not able to reach the designated office premises.

(f) Backup/standby personnel should be identified for all critical roles. A call matrix should be developed to better co-ordinate future emergency calls involving individual financial authorities, financial sector trade associations, and other banks and stakeholders. In addition the organisation should have calling tree with branches

across specific region/business processes. Based on the nature of the emergency a particular branch/the entire calling tree should be activated.

(g) The relevant portion of the BCP adopted should also be disseminated to all concerned, including the customers, so that the awareness would enable them to react positively and in consonance with the BCP. This would help maintain the customer's faith on the banking institution, and the possibility of a bank-run would be exponentially minimised. The part of the plan kept in the public domain should normally be confined to information relating to the general readiness of the banks in this regard without any detailed specifics, to protect the banks from becoming vulnerable to security threats

(h) Banks should consider formulating a clear 'Communication Strategy' with the help of media management personnel to control the content and form of news being percolated to their customers in times of panic.

(i) Banks should consider having a detailed BCP plan for encountering natural calamity/ disaster situation. A formal exception policy should be documented which will guide the affected areas Personnel to act independently till connection to the outside world is resumed.

(j) The above mentioned guideline should have exceptions documented for critical process which will ensure continuation of critical process without the regular operational formalities.

(k) After appropriate approvals or permissions are obtained internally and from RBI, banks should consider having a guideline ready on relaxing certain rules/ requirements for customers affected by the calamity.

(l) Like:

- Extending loan/interest payment timeliness
- Issuance of fresh loan with minimal required documents
- Waving off late payment fees and penalties in certain cases
- Allowing more than normal cash withdrawal from ATM's

(m) Banks can consider expediting cheque clearing for customers by directing all cheques to a different region than the one affected by the calamity. In case of severe calamity banks should consider restricting existing loans to facilitate rebuilding efforts by the Govt. for the calamity areas. The banks may also be consider ensuring quick processing of loan applications, preferably within 48 hours of receipt of such applications. It should consider dispatching credit bill, agreement notes, etc. due to customer by having an arrangement to print the same at an alternative location and should consider accepting late payments for credit card dues for customers in the calamity affected area.

(n) Banks may also endeavor for resumption of banking services by setting up satellite offices, extension counters or mobile banking facilities.

6. Infrastructure Aspects of BCP

– Banks should consider paying special attention to availability of basic amenities such as electricity, water and first-aid box in all offices. (e.g. evaluate the need of electricity backup not just for its systems but also for its people and running the infrastructure like central air-conditioning.)

– Banks should consider assigning ownership for each area. Emergency procedures, manual fallback plans and resumption plans should be within the responsibility of the owners of the appropriate business resources or processes involved.

– In-house telecommunications systems and wireless transmitters on buildings should have backup power. Redundant systems, such as analogue line phones and satellite phones (where appropriate), and other simple measures, such as ensuring the availability of extra batteries for mobile phones, may prove essential to maintaining communications in a wide-scale infrastructure failure.

– Possible fallback arrangements should be considered and alternative services should be carried out in co-ordination with the service providers, contractors, suppliers under written agreement or contract, setting out roles and responsibilities of each party, for meeting emergencies. Also, imposition of penalties, including legal action, may be initiated by an organisation against service providers or contractors or suppliers, in the event of noncompliance or non-co-operation.

– When new requirements are identified, established emergency procedures: e.g. evacuation plans or any existing fallback arrangements, should be amended as appropriate.

– Banks may consider having backup resources (erg. stationery required for cheque printing, special printers, stamps) at a secondary operational location.

– The plans may also suitably be aligned with those of the local government authorities

– Banks should consider not storing critical papers, files, servers in the ground floors where there is possibility of floods or water logging. However, banks should also consider avoiding top floors in taller building to reduce impact due to probable fire.

– Fire-proof and water-proof storage areas must be considered for critical documents.

– Banks should consider having alternative means of power source (like procurement of more diesel/ emergency battery backup etc.) for extended period of power cuts.

– Banks should consider having an emergency helpline number or nationalised IVR message to resolve queries of customers and ensure that panic situation is avoided. For this an alternative backup area call centre should be identified to take over part load of the calamity affected area. Designated person/ team must be responsible for enabling line diversion. A similar service can also be considered for the benefit of employee related communication.

7. Human Aspects of BCP

People are a vital component of any organisation. They should therefore be an integral part of a BCP. Generally, plans are often too focused on the technical issues, therefore, it is suggested that a separate section relating to people should be incorporated, including details on staff welfare, counseling, relocation considerations, etc. BCP awareness programmer should also be implemented which serve to strengthen staff involvement in BCP. This can be done through induction programme newsletters, staff training exercises, etc.

Banks must consider training more than one individual staff for specific critical jobs (ire. in the absence on one employee the work must not be stalled or delayed). They must consider cross-training employees for critical functions and document-operating procedures. Banks

should consider possibility of enabling work-from--home capabilities and resources for employees performing critical functions.

Role of HR in the BCP context

a) Crisis Management Team: As a core member of the CMT, HR provides guidance to team on people-related issues, including evacuation, welfare, whether to invoke the HR incident line, alternative travel arrangements and what to communicate to staff.

b) HR Incident Line: Operated from within the centralised HR function, the incident helpline is invoked in those instances, where there are possible casualties or missing staff, as a result of an incident. Invoked by the CMT, the line is manned by qualified HR officers trained in how to deal with distressed callers. The staff may be provided with an emergency card, which includes the incident line number. Information on the hotline is updated on a regular basis. The facility enables line managers to keep the central crisis team up to speed on the whereabouts and well-being of staff. Ongoing welfare and support for staff is also provided via an employee assistance provider.

c) Exceptional Travel arrangements: Transportation plans should be considered in the event of the need to relocate. Key staff needs to be identified including details of where they are located, and vehicles are on standby to transport them if required.

8. Technology Aspects of BCP

The are many applications and services in banking system that are highly mission critical in nature and therefore requires high availability, and fault tolerance to be considered while designing and implementing the solution. This aspect is to be taken into account especially while designing the data centre solution and the corporate network solution.

Data Recovery Strategies

Prior to selecting a data recovery (DR) strategy, a DR planner should refer to their organisation's BCP, which should indicate key metrics of recovery point objective and recovery time objective for business processes:

Recovery Point Objective (RPO)–The acceptable latency of data that will be recovered

Recovery Time Objective (RTO)–The acceptable amount of time to restore the function

Recovery Point Objective must ensure that the Maximum Tolerable Data Loss for each activity is not exceeded. The **Recovery Time Objective** must ensure that the Maximum Tolerable Period of Disruption (MTPD), for each activity, is not exceeded. The metrics specified for the business processes must then be mapped to the underlying IT systems and infrastructure that support those processes. Once, RTO and RPO metrics have been mapped to the IT infrastructure, the DR planner can determine the most suitable recovery strategy for each system. An important note here, however, is that the business ultimately sets the IT budget. Therefore, RTO and RPO metrics need to fit with the available budget and the critical of the business process/function.

A List of Common Strategies for Data Protection:

- Backups made to tape and sent off-site at regular intervals (preferably daily)
- Backups made to disk on-site and automatically copied to off-site disk, or made directly to off-site disk
- Replication of data to an off-site location, which overcomes the need to restore the data (only the systems then need to be restored or synced). This generally makes

use of storage area network (SAN) technology

- High availability systems that keep both data and system replicated, off-site, enabling continuous access to systems and data

In many cases, an organisation may elect to use an outsourced disaster recovery provider to provide a stand-by site and systems rather than using their own remote facilities. In addition to preparing for the need to recover systems, organisations must also implement precautionary measures with an objective of preventing a disaster in the first place. *These may include some of the following:*

- Local mirrors of systems or data. Use of disk protection technology such as RAID
- Surge protectors—to minimise the effect of power surges on delicate electronic equipment
- Uninterrupted power supply (UPS) or backup generator to keep systems going in the event of a power failure
- Fire preventions—alarms, fire extinguishers
- Anti-virus software and security measures

A disaster recovery plan is a part of the BCP. It dictates every facet of the recovery process, including:

- What events denote possible disasters;
- What people in the organisation have the authority to declare a disaster and thereby put the plan into effect;
- The sequence of events necessary to prepare the backup site once a disaster has been declared;
- The roles and responsibilities of all key personnel with respect to carrying out the plan;
- An inventory of the necessary hardware and software required to restore production;
- A schedule listing the personnel that will be staffing the backup site, including a rotation schedule to support ongoing operations without burning out the disaster team members.

A disaster recovery plan must be a living document; as the data centre changes, the plan must be updated to reflect those changes.

It is to be noted that the technology issues are a derivative of the Business Continuity plan and Management.

For example, BCP and Management will lead to the Business Impact Analysis, which will lead to the Performance Impact Analysis (PIA). That will depend on the Technology Performance of the total IT Solution Architecture.

To amplify business impact analysis is to identify the critical operations and services, key internal and external dependencies and appropriate resilience levels. It also analysis the risks and quantify the impact of those risks from the point of view of the business disruptions. For example, in order to provide state of the art customer services both at the branch level and the delivery channels we need to take into account the services levels that are committed.

If an ATM transaction has to take place in 10 seconds and cash withdrawal or deposit has to take place in 60 seconds at the counter, then based on the load one can compute the number of customers who can be serviced in a day. The above example is to understand the fact that the business latency introduced by the system is a combination of technology, process and people. Therefore, the technical latency is a derivative of the committed business latency and the technology solution architecture has to deliver the same under varying loads.

Technology Solution Architecture to address specific BCM requirements are:

- Performance
- Availability
- Security and Access Control
- Conformance to standards to ensure Interoperability

Performance of the technology solution architecture for operations needs to be quantified. It should be possible to measure, as and when required, the quantified parameters. (For example, if the latency for a complex transaction initiated at the branch has to be completed in four seconds under peak load, it should be possible to have adequate measuring environments to ensure that performance degradations have not taken place due to increasing loads.)

Solution architecture has to be designed with high-availability, and no single point of failure. It is inevitable that a complex solution architecture with point products from different sources procured and implemented at different points in time will have some outage once in a while and the important issue is that with clearly defined SLAs, mean time to restore, it should be possible to identify the fault and correct the same without any degradation in performance.

Accordingly, with respect to the performance and availability aspects the following architectures have to be designed and configured to provide high levels of up time round the clock to ensure uninterrupted functioning.

Summation of the required processes:

–**Data centre solution architecture**

–DR solution architecture

–Near site solution architecture

–Enterprise network and security architecture

– Branch or delivery channel architecture

– *Based on the above observation, banks are required to do the following:* Take up the performance and availability audit of the solutions deployed to ensure that the architecture is designed and implemented with no single point of failure.

– Audit the deployed architecture for all the mission critical applications and services and resolve the concerns that arise in a time bound manner.

– Periodically investigate the outages that are experienced from time to time, which are mini disasters that result in non availability of services for a short span of time, systems not responding when transactions are initiated at the branch level, delivery channels not functioning for a brief period of time to ensure that the customer service is not affected.

– Ensure availability of appropriate technology solutions to measure and monitor the functioning of products. And, have competent and capable technical people within the system to resolve issues expeditiously.

The issues detailed above have to be borne in mind while finalising the data centre architecture and the corporate network architecture which are expected to have redundancy built in the solution with no single point of failure.

With reference to the network architecture it is recommended that the Banks built in redundancies as under:

- Link level redundancy
- Path level redundancy
- Route level redundancy
- Equipment level redundancy
- Service provider level redundancy

Issues in choosing a backup site and implementing a DC or DR solution:

Backup site: Is a location where an organisation can easily relocate following a disaster, such as fire, flood, terrorist threat or other disruptive event. This is an integral part of the disaster recovery plan and wider business continuity planning of an organisation. A backup site can be another location operated by the organisation, or contracted via a company that specialises in disaster recovery services. In some cases, an organisation will have an agreement with a second organisation to operate a joint backup site.

There are three main types of backup sites:

- *cold sites*
- *warm sites*
- *hot sites*

Differences between them are determined by costs and effort required to implement each. Another term used to describe a backup site is a work area recovery site.

1. Cold Sites: A cold site is the most inexpensive type of backup site for an organisation to operate. It does not include backed up copies of data and information from the original location of the organisation, nor does it include hardware already set up. The lack of hardware contributes to the minimal start up costs of the cold site, but requires additional time following the disaster to have the operation running at a capacity close to that prior to the disaster.

2. Hot Sites*:* A hot site is a duplicate of the original site of the organisation, with full computer systems as well as near-complete backups of user data. Real-time synchronisation between the two sites may be used to mirror the data environment of the original site, using wide area network links and specialised software. Following a disruption to the original site, the hot site exists so that the organisation can relocate with minimal losses to normal operations. Ideally, a hot site will be up and running within a matter of hours or even less. Personnel may still have to be moved to the hot site so it is possible that the hot site may be operational from a data processing perspective before staff has relocated. The capacity of the hot site may or may not match the capacity of the original site depending on the organisation's requirements. This type of backup site is the most expensive to

operate. Hot sites are popular with organisations that operate real time processes such as financial institutions, government agencies and ecommerce providers

3. Warm Sites: A warm site is, quite logically, a compromise between hot and cold. These sites will have hardware and connectivity already established, though on a smaller scale than the original production site or even a hot site. Warm sites will have backups on hand, but they may not be complete and may be between several days and a week old. An example would be backup tapes sent to the warm site by courier.

8.1 The following issues arise in choosing a back up site and implementing a DC/DR solution*:*

1. Solution architectures of DC and DR are not identical for all the applications and services. Critical applications and services, namely the retail, corporate, trade finance and government business solutions as well as the delivery channels are having the same DR configurations whereas surround or interfacing applications do not have the DR support. Banks will have to conduct periodical review with reference to the above aspect and upgrade the DR solutions from time to time and ensure that all the critical applications and services have a perfect replica in terms of performance and availability.

2. The configurations of servers, network devices and other products at the DC and DR have to be identical at all times. This includes the patches that are applied at the DC periodically and the changes made to the software from time to time by customization and parameterization to account for the regulatory requirements, system changes etc .

3. Periodic checks with reference to ensuring data and transaction integrity between DC and DR are mandatory. It could be done over the week end or as a part of the EoD / BoD process.

4. Solutions have to have a defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) parameter. These two parameters have a very clear bearing on the technology aspects as well as the process defined for cut over to the DR and the competency levels required moving over in the specified time frame.

5. Values chosen for the RTO and RPO is more to follow the industry practice and not derived from first principles. Therefore, the DR drills that are conducted periodically have to ensure that the above parameters are strictly complied with.

6. Technology operations processes which support business operations (such as EOD/ BOD) need to formally included into the IT Continuity Plan.

7. Banks may also consider Recovery Time Objective and Recovery Point Objectives (RTO/ RPO) for services being offered and not just a specific application. For example--for internet portal and not retail banking. This is done to avoid any inconsistency in business users understanding.

6. DR drills currently conducted periodically come under the category of planned shutdown. Banks have to evolve a suitable methodology to conduct the drills which are closer to the real disaster scenario so that the confidence levels of the technical team taking up this exercise is built to address the requirement in the event of a real disaster.

7. It is also recommended that the support infrastructure at the DC and DR, namely the electrical systems, air-conditioning environment and other support systems have no single point of failure and do have a building management and monitoring system to constantly and continuously monitor the resources. If it is specified that the solution has a high availability of 99.95 measured on a monthly basis and a mean time to restore of 2 hrs in the event of any failure, it has to include the support system also.

8. Data replication mechanism followed between DC and DR is the asynchronous replication mechanism and implemented across the industry either using database replication techniques or the storage based replication techniques. They do have relative merits and demerits. The RTO and RPO discussed earlier, along with the replication mechanism used and the data transfer required to be accomplished during the peak load will decide the bandwidth required between the DC and the DR. The RPO is directly related to the latency permissible for the transaction data from the DC to update the database at the DR. Therefore, the process implemented for the data replication requirement has to conform to the above and with no compromise to data and transaction integrity.

9. Given the need for drastically minimizing the data loss during exigencies and enable quick recovery and continuity of critical business operations, banks may need to consider near site DR architecture. Major banks with significant customer delivery channel usage and significant participation in financial markets/payment and settlement systems may need to have a plan of action for creating a near site DR architecture over the medium term (say, within three years).

8.2 Issues/Challenges in DC/DR implementation by the Banks

(a) Despite considerable advances in equipment and telecommunications design and recovery services, IT disaster recovery is becoming challenging. Continuity and recovery aspects are impacting IT strategy and cost implications are challenging IT budgets.

(b) The time window for recovery is shrinking in face of the demand for 24 / 365 operations. Some studies claim that around 30 percent of high-availability applications have to be recovered in less than three hours. A further 45 percent within 24 hours, before losses become unsustainable; others claim that 60 percent of Enterprise Resource Planning (ERP) Systems have to be restored in under 24 hours. This means that traditional off-site backup and restore methods are often no longer adequate. It simply takes too long to recover incremental and full image backups of various inter-related applications (backed up at different times), synchronise them and re-create the position as at disaster. Continuous operation–data mirroring to off-site locations and standby computing and telecommunications–may be the only solution.

(c) A risk assessment and business impact analysis should establish the justification for continuity for specific IT and telecommunication services and applications.

(d) Achieving robust security (security assurance) is not a onetime activity. It cannot be obtained just by purchasing and installing suitable software and hardware. It is a continuous process that requires regular assessment of the security health of the organisation and proactive steps to detect and fix any vulnerability. Every bank should have in place quick and reliable access to expertise for tracking suspicious behavior, monitoring users and performing forensics. Adequate reporting to the authorities concerned – such as the RBI/ IDRBT/CERT-In and other institutions should be an automatic sub process whenever such events occur.

Important steps that need to be institutionalised are the following:

a) Rigorous self-assessment of security measures by banks and comprehensive security audit by external agencies, as detailed under the “Chapter on Information Security” earlier.

b) Random Security Preparedness. It is proposed that a sufficiently large ``question bank'' related to security health of the organization be prepared and given to RBI's inspection teams who go for inspection of banks. A random subset of these queries could then be given to a bank’s IT team for which answers need to be

provided in near real time. Sample checks related to user accounts could be the number of new accounts, terminated accounts, most active accounts. There could also be demonstrations of data recovery from archives.

(e) **Telecommunications issues may also arise: I**t is important to ensure that relevant links are in place and that communications capability is compatible. The adequacy of voice and data capacity needs to be checked. Telephony needs to be switched from the disaster site to the standby site. A financial institution's BCP should consider addressing diversity guidelines for its telecommunications capabilities. This is particularly important for the financial services sector that provides critical payment, clearing, and settlement processes; however, diversity guidelines should be considered by all financial institutions and should be commensurate with the institution's size, complexity, and overall risk profile. Diversity guidelines may include arrangements with multiple telecommunications providers. However, diverse routing may be difficult to achieve since primary telecommunications carriers may have an agreement with the same sub-carriers to provide local access service, and these sub-carriers may also have a contract with the same local access service providers. Financial institutions do not have any control over the number of circuit segments that will be needed, and they typically do not have a business relationship with any of the sub-carriers. Consequently, it is important for financial institutions to understand the relationship between their primary telecommunications carrier and these various sub-carriers and how this complex network connects to their primary and back-up facilities. To determine whether telecommunications providers use the same sub-carrier or local access service provider, banks may consider performing an end-to-end trace of all critical or sensitive circuits to search for single points of failure such as a common switch, router, PBX, or central telephone office.

(f) ***Banks may consider the following telecommunications diversity components to enhance BCP:***

(i) Alternative media, such as secure wireless systems

(ii) Internet protocol networking equipment that provides easily configurable re-routing and traffic load balancing capabilities

(iii) Local services to more than one telecommunications carrier's central office, or diverse physical paths to independent central offices

(iv) Multiple, geographically diverse cables and separate points of entry

(v) Frame relay circuits that do not require network interconnections, which often causes delays due to concentration points between frame relay providers

(vi) Separate power sources for equipment with generator or uninterrupted power supply back-up

(vii) Separate connections to back-up locations

(viii) Regular use of multiple facilities in which traffic is continually split between the connections; and

(ix) Separate suppliers for hardware and software infrastructure needs.

(g) **Banks need to monitor their service relationship with telecommunications providers:** In order to manage the inherent risks more effectively. In coordination with vendors, management should ensure that risk management strategies include

the following, at a minimum:

– Establish service level agreements that address contingency measures and change management for services provided;

– Ensure that primary and back-up telecommunications paths do not share a single point of failure

– Establish processes to periodically inventory and validate telecommunications circuits and routing paths through comprehensive testing.

(h) **Some vendors offer a drop-ship service as an alternative to occupying the standby site.** That is, in the event of equipment failure, for instance, they will drop off a replacement rather than insist the client occupy the standby site, with all the inconvenience that may involve. But it is essential that a site survey is undertaken to ensure they can be parked on the required site. Most commercial standby sites offering IT and work area recovery facilities do not guarantee a service: the contract merely provides access to the equipment. Although most reputable vendors will negotiate a Service Level Agreement that specifies the quality of the service, it is rarely offered.

It is important to ensure that a bank's service will not suffer from unacceptable downtime or response. The vendor may have skilled staff available – but this is rarely guaranteed and they come at a cost. In terms of cost, there may be additional fees to pay for testing, on invocation of a disaster, and for occupation in a disaster. The vendor charging structure also needs to be carefully considered.

(i) **Outsourcing Risks:** In theory a commercial hot or warm standby site is available 24 / 365. It has staff skilled in assisting recovery. Its equipment is constantly kept up to date, while older equipment remains supported. It is always available for use and offers testing periods once or twice a year. The practice may be different. These days, organizations have a wide range of equipment from different vendors and different models from the same vendor. Not every commercial standby site is able to support the entire range of equipment that a bank may have. Instead, vendors form alliances with others – but this may mean that a bank's recovery effort is split between more than one standby site. The standby site may not have identical IT equipment: instead of the use of an identical piece of equipment, it will offer a partition on a compatible large computer or server. Operating systems and security packages may not be the same version as the client usually uses. These aspects may cause setbacks when attempting recovery of IT systems and applications – and weak change control at the recovery site could cause a disaster on return to the normal site.

It is the responsibility of the IT manager/bank to ensure effective recovery by those vendors, who apply the highest standards, supporting this by a stringent contract, clearly defining service specifications and technical requirements, and service-level agreements**.**

CHAPTER 8- CUSTOMER EDUCATION

Introduction:

With the advent of electronic banking, the neighbourhood bank has set up a branch on the desktop of the customer. The customer's experience of banking is therefore no longer fully under the control of the bank. In the age of the self-service model of banking, the customer also has to be equipped to do safe banking through self help. It is often said that the best defence against frauds is an aware customer. With fraudsters constantly creating more diverse and complex fraudulent ruses using advanced technology and social engineering techniques to access their victims' accounts, spreading awareness among consumers becomes imperative.

Some banks regularly run campaigns to raise consumer awareness on a variety of fraud related issues. However, to generate a standard understanding of the evolving fraud scenarios, a combined effort could proliferate the information to a larger customer base. It is also important to educate the other stakeholders, including bank employees, who can then act as resource persons for customer queries, law enforcement personnel for more understanding response to customer complaints and media for dissemination of accurate and timely information.

Scope:

- Illustrate how to plan, organise and implement a fraud awareness raising initiative
- Provide a framework to evaluate the effectiveness of an awareness program
- Offer a communication framework
- Highlight potential risks associated with awareness initiatives in an effort to avoid such issues in future programs
- Contribute to the development of a safe and secure culture by encouraging users to act responsibly and operate more securely

1) Roles and Responsibility - Board of Directors/Senior Management:

There needs to be commitment from the Board of Directors/Senior Management towards the process of consumer education initiatives by providing adequate resources, evaluating the effectiveness of the process and fine-tuning and improving customer education measures on an ongoing process.

2) Organisational structure

Working group

To get desired support for the programme, it is important to identify and involve key stakeholders in decision-making, planning, implementation and evaluation.

- Establish a clear goal for the endpoint, in consultation with key stakeholders.
- Clearly define roles, responsibilities and accountabilities.
- Communicate in an open, honest, clear and timely manner.

- Allow for flexibility in approaches to suit different stakeholder needs.
- Support with training and development to ensure a change in behaviour and culture.
- Learn from previous and ongoing experiences and celebrate achievements.

3) Communication Strategy

1. Defining 'Awareness'

Security awareness is the understanding and knowledge of the threats to the sensitive personal information of the customer and the protection measures to be adopted. It is the basic component of the education strategy of an organisation which tries to change the attitude, behaviour and practice of its target audience (e.g. customers, general public, employees etc.). Awareness activities need to be done an ongoing basis, using a variety of delivery methods and are less formal and shorter than formal training processes.

The purpose of awareness presentations is simply to focus attention on security. Such presentations are intended to allow individuals to recognise security concerns and respond accordingly. In awareness activities, the learner is only the recipient of information.

2. Suggested approach for awareness programmes

The three main stages in the development of an awareness programme are:

a. Planning and design **:** Awareness programmes can be successful only if users feel the content is in their interest and is relevant to their banking needs. In the planning stage, the needs of the target audience should be identified, a plan developed, organizational buy-in and appropriate budgets obtained and priorities established. The work plan should clearly mention the main activities with the required resources, timelines and milestones. This plan must be reviewed periodically as the programme progresses.

b.Execution and management :This process focuses on the activities to implement the awareness program. A suitable vendor should be engaged for content creation and publication.

c.Evaluation and course correction :Continuous improvement cannot occur without knowing how the existing programme is working. A well-calibrated feedback strategy must be designed and implemented.

The component processes under the above sections can be listed as under:

Plan, assess and design	Execute and manage	Evaluate and adjust
Establish a working group	Nominate team members	Establish baseline for evaluation
Define goals and objectives	Review work plan	Gather data

Define target group	Launch and implement the activities	Collect feedback on communications
Identify human and material resources required	Document learning	Assess effectiveness through number of events
Evaluate potential solutions		Review program objectives
Select desired solutions and procedures		Make necessary changes in the plan
Identify programme benefits and obtain budgetary sanctions		
Prepare work plan and checklists		
Define communications concept		
Define indicators to measure the progress		
Establish baseline for evaluation		
Document learning		

3. Target audience

Since awareness programmes should be customized for a specific audience, it is important to identify and segment the target users for the programs.

The target groups for these programs would be:

- Bank customers
- Bank employees and consultants
- Law Enforcement Agencies – Police, Judiciary and Consumer Forums
- Fraud risk professionals
- Media personnel
- Channel partners and suppliers
- General public of varying age and technical knowledge – children, youth, adults, senior citizens and silver surfers

4. Stake holder support

Building consensus amongst decision makers and stakeholders for financial and administrative support is an important step in the programme. In this respect, both fixed and variable costs need to be identified. These will include personnel, operational costs, awareness material, advertisements and promotions and maintenance of website.

The common objectives of the awareness programme will be to:

- Provide a focal point and a driving force for a range of awareness, training and educational activities
- Provide general and specific information about fraud risk trends, types or controls to people who need to know
- Help consumers identify areas vulnerable to fraud attempts and make them aware of their responsibilities in relation to fraud prevention
- Motivate individuals to adopt recommended guidelines or practices
- Create a stronger culture of security with better understanding and commitment
- Help minimise the number and extent of incidents, thus reducing costs directly (fraud losses) and indirectly (for eg., reduced need to investigate)

5. Concept of communication

Communication is crucial for the success of any awareness programme. The key elements of effective communication are:

- Ability to reach out to a broad audience which can contribute to the multiplier effect to maximize the reach of the message
- Not to be alarming or overly negative about a situation. If issues or risks need to be detailed, it is often easier for the audience to understand in the context of real world experiences
- Deliver the right message content to the right audience using the most effective communication channels
- The message should state the risks and threats facing the users, why it is relevant to them, what to do and not to do, and finally how to be protected. The message should be compelling and clearly state why security is important. Users who understand why certain types of behaviour are risky are most likely to take ownership of the issue and change their behaviour.

6. Communication content

The messages through these communications would carry information related to various frauds in general with specific focus on electronic frauds through fake websites, phishing, vishing, skimming and emails.

7. Communication collaterals

Awareness building collaterals can be created in the form of:

- Leaflets and brochures
- Educational material in account opening kits
- Safety tips in cheque books, PIN, account statements and envelopes
- Receipts dispensed by ATMs

- DVDs with animated case studies and videos
- Screensavers
- Electronic newsletters
- Short Messaging Service (SMS) texts
- Recorded messages played during waiting period of phone banking calls

The collaterals should be created in regional languages wherever required.

8. Communication channels

Since the target groups obtain information from a variety of sources, more than one communication channel could be used to engage them successfully. These could be:

- Advertising campaigns though print and TV media
- Talk shows on television/radio
- Customer meets and interactive sessions with specialists
- Common website developed with content from all stakeholders
- Online training modules and demos hosted on this site
- Groups, games and profiles on social media
- Advertisements on online shopping sites
- Bill boards
- Posters in prominent locations such as petrol pumps and popular restaurants
- Interactive guidance in the form of helplines
- ATM screens , Emails and SMS texts
- Distance learning programmes and demos

The message delivered, the channels used and the sender of the message should be influential and credible, otherwise the target group may be less inclined to listen.

An effective way to deliver the message would be the use of multipliers that can help communicate to a broad range of audience. Few examples of such bodies could be:

- Community centres
- Schools and colleges
- Computer and book stores
- Libraries
- NGOs
- Clubs
- Adult education centres

9. Research and analysis

In addition to the above, a research group should be formed to continually update the team with the latest trends and evolving modus operandi. The team would maintain a repository of material such as:

- Case studies
- Sample mails
- Sample of fraudulent documents
- Data collected from victims or targets of frauds
- International practices and developments

10. Evaluation

Evaluation of the effects of various campaigns for specific target groups can be measured through qualitative (e.g. focus groups, interviews) and/or quantitative (e.g. questionnaires, omnibus surveys) research. Evaluation against metrics, performance objectives, etc. should also be conducted to check the campaign's effectiveness, and to establish lessons learned to improve future initiatives.

Other issues relating to bank customer education:

Apart from regular education efforts, when new operating features or functions, particularly those relating to security, integrity and authentication, are being introduced, banks should ensure that customers have sufficient instruction and information to be able to properly utilize them. Continual education and timely information provided to customers will help them to understand security requirements and take appropriate steps in reporting security problems.

CHAPTER 9: LEGAL ISSUES

Introduction

Basel Committee on Banking Supervision, in its "Consultative Document on Operational Risk", defines "operational risk" as the risk of direct, or indirect, loss resulting from inadequate or failed internal processes, people and systems, or from external events. This definition includes legal risk[1].

The Information Technology Act, 2000 (IT Act, 2000) was enacted to handle certain issues relating to Information Technology. The IT Amendment Act, 2008 has made further modifications to address more issues such as cyber crimes. It is critical that impact of cyber laws is taken into consideration by banks to obviate any risk arising there from.

A. Guidance for Banks

Roles and Responsibilities and Organizational Structure

Board: The Risk Management Committee at the Board-level needs to put in place, the processes to ensure that legal risks arising from cyber laws are identified and addressed. It also needs to ensure that the concerned functions are adequately staffed and that the human resources are trained to carry out the relevant tasks in this regard

Operational Risk Group: This group needs to incorporate legal risks as part of operational risk framework and take steps to mitigate the risks involved in consultation with its legal functions within the bank.

Legal Department: The legal function within the bank needs to advise the business groups on the legal issues arising out of use of Information Technology with respect to the legal risk identified and referred to it by the Operational Risk Group.

Computer related offences and Penalty/Punishment

The IT Act, 2000 as amended, exposes the banks to both civil[2] and criminal[3] liability. The civil liability could consist of exposure to pay damages by way of compensation upto ₹ 5 crore under the amended Information Technology Act before the Adjudicating Officer and beyond ₹ five crore in a court of competent jurisdiction. There could also be exposure to criminal liability to the top management of the banks given the provisions of Chapter XI of the amended IT Act[4] and the exposure to criminal liability could consist of imprisonment for a term which could extend from three years to life imprisonment as also fine. Further, various computer related offences are enumerated in the aforesaid provisions.

Critical aspects

(a) Legal risk and operational risk are same. Most risks are sought to be covered by documentation, particularly where the law is silent. The Basel-II accord

1 http://www.bis.org/publ/bcbsca07.pdf

2 Sections 43-45

3 Sections 65-74

4 Section 85

covers “legal risk” under “operational risk.” Documentation forms an important part of the banking and financial sector. For many, documentation is a panacea to the legal risks that may arise in banking activities. But then, it has also been realized and widely acknowledged that loopholes do exist in documentation.

(b) Legal risks need to be incorporated as part of operational risks and the position need to be periodically communicated to the top management and Board/Risk Management Committee of the Board.

(c) As the law on data protection and privacy, in the Indian context are in an evolving stage, banks have to keep in view the specific provisions of IT Act, 2000 (as amended in 2008), various judicial and quasi judicial pronouncements and related developments in the Cyber laws in India as part of legal risk mitigation measures. Banks are also required to keep abreast of latest developments in the IT Act, 2000 and the rules, regulations, notifications and orders issued there under pertaining to bank transactions and emerging legal standards on digital signature, electronic signature, data protection, cheque truncation, electronic fund transfer etc. as part of overall operational risk management process.

Annexures

ANNEX –A

An Illustrative Information Security Check List

- ***Security Policy - Governance, Implementation & Review***

Whether there exists a well-documented Information security policy	Yes/ No
When was the policy last approved by the Board of directors/ Management	mm/dd/yy
What is the review frequency of the policy	Quarterly/ Half-yearly/ Yearly
When was the last review conducted	mm/dd/yy
What was the last review purpose	a. Periodic
	b. Incident driven
	c. Infrastructure changes
Whether the policy addresses legal and regulatory requirements	Yes/ No
Who is the security policy owner for maintenance and review	a. Board of directors
	b. Security Committee
	c. CISO
Whether IS committee is constituted comprising of representatives from all verticals	Yes/ No
What is the meeting frequency of the IS committee	quarterly/ half-yearly/yearly
Whether the role and responsibilities of IS committee is clearly defined	Yes/ No
Whether the role and responsibilities of CISO is clearly defined	Yes/ No
Whether the policy is communicated to relevant users	Yes/ No
What is the medium of communication	a. Email

	b. Intranet
	c. In-house Periodic trainings
	d. Induction training for new recruits
	e. Undertaking
Whether supporting procedures/ sub-policies have been developed for organizational security	Yes/ No
Who reviews the supporting procedures/ sub-policies	a. CISO
	b. IS Committee
Whether security policy is in line with global best practices guidelines like ISO 27001 (and other frameworks like COBIT etc) and/or as per requirements of RBI circular	Yes/ No
Whether every procedure/ sub-policy has a designated owner	Yes/ No
Whether the policy takes into consideration the long-term business strategy of the organisation	Yes/ No
Whether the organisation has considered IS security for budgetary allocation	Yes/ No
Whether independent audit is conducted to ensure adherence to security policy	Yes/ No
Frequency of internal audit	Quarterly/ Half-yearly/ Yearly
Frequency of external audit	Quarterly/ Half-yearly/ Yearly/ Bi-annually

- **Asset classification and control - *Accountability of assets***

Whether the organization has distinguished its information assets	Yes/ No
Whether an inventory database is maintained for all information assets	Yes/ No
Whether there is a designated owner for each distinguished asset	Yes/ No
How is the inventory database maintained	Centrally/ Locally
Whether a separate asset inventory exists for datacentre and DR site	Yes/ No
Whether there is a designated owner for the datacentre asset inventory	Yes/ No

Whether a process exist for updation of asset inventory	Yes/ No
Whether each information asset is labeled	Yes/ No
Whether information classification guidelines exist and are enforced	Yes/ No
Whether the classification level of information asset is reviewed periodically	Yes/ No
Who is responsible for deciding the asset classification level	a. IS Committee
	b. CISO
	c. Asset owner
Whether classification level for each asset is recorded in inventory database.	Yes/ No

- **Human resource security**

How do you communicate individual security roles and responsibilities to employee end users	a. Employment contract
	b. Induction trainings
	c. Periodic IS awareness trainings
Is there a training calendar for IS awareness trainings	Yes/ No
Number of IS awareness trainings conducted in a year	_____
Number of induction trainings conducted in a year	_____
Whether a background verification check is part of the recruitment process of the organisation	Yes/ No
How the background verification check is conducted	a. In-house
	b Outsourced
Whether employment contract covers non-disclosure/ confidentiality clause	Yes/ No
Whether written acknowledgement w.r.t understanding and acceptance of employment contract is obtained	Yes/ No
Whether employment contract covers appropriate controls to address post employment responsibilities	Yes/ No

- **Third Party Security/ Vendor Management**

How do you communicate individual security roles and responsibilities to third party users	a. Third party contract
	b. Periodic IS awareness trainings
	c. Both
Whether a background verification check is a mandatory requirement in third party contracts	Yes/ No
What process there is to ensure background verification check is performed	a. SLA review
	b Third party audit
Whether third party contract mentions adherence to security policy and procedures of the organization	Yes/ No
Whether third party contract covers non-disclosure/ confidentiality clause	Yes/ No
Whether written acknowledgement w.r.t understanding and acceptance of third party contract is obtained	Yes/ No
Do you conduct due diligence for third parties/ vendor before outsourcing	Yes/ No
Do you conduct onsite security audit of third party/ vendor before outsourcing	Yes/ No
Have you identified the risks associated with third party contractors working on-site	Yes/ No
Do you conduct periodic reviews of all accesses provided to third parties/ vendor	Yes/ No
What is the frequency of such reviews	Monthly/ Quarterly/ Yearly
Whether the CISO reviews all security controls w.r.t third party contracts	Yes/ No

- **Physical and Environmental Security**

What physical border security facility has been implemented to protect the Information processing facilities	a. Electronic access control (access cards)
	b. Biometric system
	c. Security guards

	d. Perimeter walls
	e. All of the above
What entry controls are in place to allow only authorised personnel into various areas within the organisation	a. Electronic access control (access cards)
	b. Biometric system
	c. Manned reception
	d. All of the above
Whether access to information processing facilities is limited to approved personnel only	Yes/ No
Whether the physical access control procedures differentiate employees, vendors, equipment & facility maintenance staff	Yes/ No
Whether potential threats to information processing facilities like fire, flood, earthquake, theft are taken into consideration in the risk assessment exercise	Yes/ No
Whether separate security controls are in place for third party/ vendor personnel working in secure areas	Yes/ No
Whether goods delivery area and secure area are isolated from each other to avoid any unauthorized access	Yes/ No
Whether appropriate controls are deployed to minimize the risk from heat, smoke, adverse environmental conditions, explosives, dust, chemical effects, electrical supply interfaces, electromagnetic radiation, vibrations, water leakages, rodents etc.	Yes/ No
What is the frequency of conducting fire drill and training	Quaterly/ Half-yearly/ Yearly
Whether evacuation plan with clear responsibilities is in place in case of a disaster	Yes/ No
Whether there is a policy dealing with eating, drinking and smoking in proximity to information processing services	Yes/ No
Whether appropriate signages are displayed with reference to above	Yes/ No
Whether the power and telecommunications cable carrying data or supporting information services are protected from interception or damage	Yes/ No

Whether information processing facility is equipped with all of the following: multiple feed power supply; UPS, generator backups	Yes/ No
Whether the equipment is maintained/ upgraded as per the supplier's recommended service intervals and specifications	Yes/ No
Who carries out the maintenance/ upgradation of critical information processing systems and facilities	a. Third party support personnel
	b. Equipment manufacturer
	c. In-house personnel
Whether logs are maintained with all suspected or actual faults and all preventive and corrective measures	Yes/ No
Who reviews the above logs	a. CISO
	b. Datacentre Head
	c. IT Head
Whether appropriate controls are implemented while sending equipment off premises	Yes/ No
Whether the equipment insurance requirements are satisfied	Yes/ No
Whether secure disposal policy is in place for sensitive information	Yes/ No
How many workstations and servers exist	_____
Whether the organisation maintains a network diagram that includes IP addresses, room numbers/ location and asset owners/ responsible parties	Yes/ No
Whether clear desk and clear screen policies exist	Yes/ No
Whether screen saver time out is implemented	Yes/ No

- **Information Security Incident Management**

Is there a well-documented Incident Management process to handle security incidents	Yes/ No

Whether end users are aware of incident management process	Yes/ No
Whether the process clearly spells out responsibilities, steps for orderly response to a security incident	Yes/ No
Whether the procedure separately addresses different types of incidents like denial of service attacks, breach of confidentiality etc., and ways to handle them	Yes/ No
What kind of monitoring system/ forensic investigation capability is in place so that proactive action is taken to avoid security incidents and malfunctions	a. Audit trail
	b. Log Correlation
	c. Intrusion Prevention/ Detection System
	d. Any other system, please specify
Whether appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunication operators are maintained to ensure that appropriate action can be quickly taken and specialist advice obtained, in the event of a security incident (Eg. CERT-IN, IDRBT, IBA etc.)	Yes/ No
Whether an escalation reporting procedure exists to report security incidents, security weakness, software malfunctions, threats to systems and processes through appropriate management channels as quickly as possible	Yes/ No
Has the security escalation matrix been defined and documented	Yes/ No
Whether CISO periodically reviews the security incidents	Yes/ No
What is the frequency of such reviews	Monthly/ Quarterly
Whether such incidents are brought to the notice of the Security Steering Committee	Yes/ No
What kind of mechanism is in place to analyse the type of damage and quantify the volume and cost of malfunctions and incidents. Please specify	_____
Number of security incidents in the last six months	_____

Whether there is a formal disciplinary process in place for employees who have violated organisational security policies and procedures	Yes/ No
Do you have contacts with the cybercrime cell/ investigation agencies	Yes/ No

- **Communications and Operations Management**

Whether operating procedures have been documented for critical processes like Back-up, Capacity planning, Equipment maintenance, Application monitoring, Network monitoring, Server monitoring, Security monitoring etc.	Yes/ No
Whether a documented change request procedure exist for all of the above critical processes	Yes/ No
Whether process owner reviews and endorses every change request	Yes/ No
Whether business approval is required for every change request	Yes/ No
Whether audit logs are maintained for any change made to the production programs	Yes/ No
Whether segregation of duties is clearly spelt out for the above critical processes	Yes/ No
Whether the development and testing facilities are isolated from operational facilities	Yes/ No
Whether any of the Information processing facility is managed by third party/ vendor	Yes/ No
Whether the risks associated with such outsourced management are addressed by deploying appropriate controls	Yes/ No
Whether necessary approval is obtained from business owners for such engagement	Yes/ No
Whether the performance is monitored and projections for upgrade requirements are made to ensure that adequate processing power and storage are available. Example: Monitoring Hard disk space, RAM, CPU on critical servers	Yes/ No
Whether suitable User Acceptance tests (UAT) are carried out prior to acceptance of new information systems, upgrades and new versions	Yes/ No
Which of these controls exist against malicious software usage	a. Desktop firewall

	b. Endpoint security solutions
	c. Active Directory group policies
	d. Anti-virus software
	e. All of the above
Have you subscribed to warning bulletins/ alerts with regards to malicious software usage	Yes/ No
Whether Anti-virus software is installed on end user desktops, internet gateway and mail gateway	Yes/ No
Total number of desktops in the organisation	_____
Total number of dekstops updated with today's Anti-virus Definition	_____
How many regional servers are there for Anti-virus updates in the organisation	_____
Whether a dedicated Virus Helpdesk is established	Yes/ No
Is there a defined procedure to connect vendor/consultant/support personnel laptops to the organization network	Yes/ No
Who reviews daily Anti-virus coverage reports	_____
Whether comprehensive Back-up schedule of essential business applications is in place	Yes/ No
Whether comprehensive Back-up schedule is also implemented at DR Site	Yes/ No
Whether the backup media along with the procedure to restore the backup are stored securely	Yes/ No
Whether the backup media are stored at off-site location	Yes/ No
Whether dedicated media liabrary is created for backup media	Yes/ No
Whether the backup copies of critical applications/databases are available on SAN Storage	Yes/ No
Whether the backup media are regularly tested for restoration within the time frame allotted in the operational procedure for recovery	Yes/ No
When was the restoration last tested	mm/dd/yy

Whether daily operations log sheet is maintained for Database housekeeping tasks	Yes/ No
Who reviews the operations log sheets for Database housekeeping tasks	_____
Whether operations logs sheets are randomly compared with system generated operator logs	Yes/ No
Whether a defined fault logging mechanism is in place for Database related issues	Yes/ No
Which technique is used to grant network access to the user	a. AD Authentication
	b. Single Sign-on
	c. Identity Management
	d. Workgroup Environment
Which Network Monitoring tool is used by the organisation	_____
Whether Network/System Administration task is isolated (Network Isolation) from End User Network Segments	Yes/ No
Whether central authentication tools like TACACS/RADIUS are used for Network Device Authentication	Yes/ No
Whether all routers (Branch/WAN) have ACLs	Yes/ No
Who reviews the ACLs periodically	_____
Whether clear guidelines exist for remote management of critical equipment (Servers/Routers etc.)	Yes/ No
Whether VPN is used for remote management/administration of critical equipment	Yes/ No
Which type of VPN is being used	_____
Whether VPN Access Authorization process is established	Yes/ No
Whether Media handling guidelines are established	Yes/ No
Whether secure disposal process for media is in place	Yes/ No
Whether the media is transported in a secured manner	Yes/ No
Whether disposal of sensitive items are logged where necessary in order to maintain an audit trail	Yes/ No

Whether System Documentation is stored in a secure manner and protected from unauthorised access	Yes/ No
Whether a list of individuals having access to System Documentation is maintained	Yes/ No
Whether all exchanges of information, for business purposes, are governed by formal agreements	Yes/ No
Whether such agreements adequately address Security issues	Yes/ No
Whether e-commerce transactions are SSL enabled	Yes/ No
Whether multi-factor authentication mechanism is in place for e-commerce environment	Yes/ No
Which of the following additional factors is used for authentication	a. Hardware Token
	b. OTP
	c. MobiToken
	d. IVR Callback
Whether controls are in place to guard e-commerce systems against phishing attacks	Yes/ No
Whether e-commerce systems are under periodic VA/PT cycles	Yes/ No
Whether standard defensive techniques like IPS, Malware Scanning etc. are deployed for e-commerce systems	Yes/ No
Whether the use of the organisation's electronic mail system is governed by acceptable use policy or guidelines	Yes/ No
Whether all e-mails are archived centrally	Yes/ No
Whether gateway level anti-virus, anti-spam protection is enforced for E-mail system	Yes/ No
Whether data leakage prevention system is implemented to maintain confidentiality of the information	Yes/ No
Whether the e-mail traffic is encrypted	Yes/ No
Whether use of all electronic office systems is governed by acceptable use policy	Yes/ No
Whether there is any formal authorisation process in place for the information to be made publicly available	Yes/ No

Whether there are any policies, procedures or controls in place to protect the exchange of information through the use of voice, facsimile and video communication facilities	Yes/ No
Whether continuous education/ awareness is imparted to employees w.r.t Information Security best practices while exchanging the information over phone/fax/video etc.	Yes/ No

- **Access Control**

Whether business requirements are documented for access control	Yes/ No
Whether there is any formal user registration and de-registration procedure for granting access to multi-user information systems and services	Yes/ No
Whether privileges are allocated on need-to-use basis and after formal authorisation process	Yes/ No
Whether there exists a process to review user access rights at regular intervals. Eg. Special privilege review every 3 months, normal privileges every 6 months	Yes/ No
Frequency of user access review	Quarterly/ Half-yearly/ Yearly
Whether clear password policy is in place and communicated to all users	Yes/ No
Whether the users and contractors are made aware of the security requirements and procedures for protecting unattended equipment	Yes/ No
Whether networks and network services access policy is in place for the organization	Yes/ No
Which of these authentication mechanisms is used for challenging external connections	a. Cryptography based technique
	b. Hardware Tokens
	c. Software Tokens
	d. Challenge Response protocol
	e. Any other
Whether all external connections have proper Management and Security approvals	Yes/ No

Whether accesses to diagnostic ports are securely controlled and have Security approvals	Yes/ No
Whether Perimeter and Internal Firewalls are distinctly installed in the organization	Yes/ No
Whether ftp is allowed across the organization	Yes/ No
Whether NIDS/NIPS controls are deployed in the organization	Yes/ No
Whether access to information systems is attainable only via a secure log-on process	Yes/ No
Whether unique identifier is provided to every user such as operators, system administrators and all other staff including technical	Yes/ No
Whether there exists a password management system that enforces various password controls such as: individual password for accountability, enforce password changes, store passwords in encrypted form, not display passwords on screen etc.	Yes/ No
Whether Inactive terminal in public areas are configured to clear the screen or shut down automatically after a defined period of inactivity	Yes/ No
Whether sensitive systems are provided with isolated computing environment such as running on a dedicated computer, share resources only with trusted application systems, etc.	Yes/ No
Whether there exist any restrictions on connection time for high-risk applications	Yes/ No
Whether procedures are set up for monitoring the use of information processing facility	Yes/ No
Whether the results of the monitoring activities are reviewed regularly	Yes/ No
Whether audit logs recording exceptions and other security relevant events are enabled	Yes/ No
What is the retention period for audit logs	_____
Whether NTP is implemented and clock for all servers/ devices is in sync with NTP	Yes/ No
Whether a formal policy is in place to address the risks of working with computing facilities such as notebooks, palmtops etc. especially in unprotected environments	Yes/ No

Whether there is any policy, procedure and/ or standard to control teleworking activities	Yes/ No
Whether suitable protection of teleworking site is in place against threats such as theft of equipment, unauthorised disclosure of information etc.	Yes/ No

- **Systems acquisition, development and maintenance**

Whether security requirements and controls are incorporated as part of business requirement statement for new systems	Yes/ No
Whether risk assessments are conducted before commencement of system development	Yes/ No
Whether data input to application system is validated to ensure that it is correct and appropriate	Yes/ No
Whether areas of risks are identified in the processing cycle and validation checks included	Yes/ No
Whether appropriate controls are identified based on nature of application and business impact in case of data corruption to mitigate risks during internal processing	Yes/ No
Whether Message authentication mechanism is in place, if necessary	Yes/ No
Whether the data output of application system is validated to ensure that the processing of stored information is correct	Yes/ No
Whether there is a policy in use of cryptographic controls for protection of information is in place	Yes/ No
Whether a risk assessment was carried out to identify the level of protection the information should be given	Yes/ No
Whether encryption techniques are used to protect the data.	Yes/ No
Whether assessments are conducted to analyze the sensitivity of the data and the level of protection needed	Yes/ No
Whether Digital signatures are used to protect the authenticity and integrity of electronic documents	Yes/ No
Whether non-repudiation services are used to resolve disputes	Yes/ No
Whether there is a management system in place to support the organization's use of cryptographic techniques like Secret	Yes/ No

key technique and Public key technique	
Whether the Key management system is based on agreed set of standards and secure methods	Yes/ No
Whether there are any controls in place for the implementation of software on operational systems	Yes/ No
Whether system test data is protected and controlled	Yes/ No
Whether strict controls are in place over access to program source libraries so as to reduce the potential for corruption of computer programs	Yes/ No
Whether there are strict control procedures in place over implementation of changes to the information system so as to minimize the corruption of information system	Yes/ No
Whether there are any restrictions in place to limit changes to software packages	Yes/ No
Whether there are controls in place to ensure that the covert channels and Trojan codes are not introduced into new or upgraded system	Yes/ No
Whether there is any process in place to ensure application system is reviewed and tested after operating system changes like installation of service packs, patches etc.	Yes/ No

- **Compliance**

Whether relevant regulatory and contractual requirements are documented for each information system	Yes/ No
Whether responsibilities of individuals concerned to meet these requirements are well defined and communicated	Yes/ No
Whether there exist procedures to ensure compliance with legal restrictions on use of material like intellectual property rights, trademarks, copy rights etc.	Yes/ No
Whether important records of the organisation is protected from loss destruction	Yes/ No
Whether there is a management structure and control in place to protect data and privacy of personal information	Yes/ No
Whether at the log-on security banner or a warning message is presented on the computer screen indicating that the	Yes/ No

system being entered is private and that unauthorised access is not permitted	
Whether the process involved in collecting the evidence is in accordance with legal best practices	Yes/ No
Whether all areas within the organisation are considered for regular review to ensure compliance with security policy, standards and procedures	Yes/ No
Whether information systems are regularly checked for compliance with security implementation standards	Yes/ No
Whether the technical compliance check is carried out by, or under the supervision of, competent, authorised persons	Yes/ No
Whether all computers, systems and network devices like routers and switches within your organization regularly tested for exploitable vulnerabilities and illegally copied software	Yes/ No
Whether audit requirements and activities involving checks on operational systems are planned and agreed upon to minimise the risk of disruptions to business process	Yes/ No
Whether access to system audit tools such as software or data files are protected to prevent misuse	Yes/ No
Whether there is a designated compliance officer for the organisation	Yes/ No

ANNEX–B

IS Audit Scope

Indicative scope of IS Audit is given below:

The indicative scope of IS Audit is given below:

- Alignment of IT strategy with Business strategy
- IT Governance related processes
- Long term IT strategy and Short term IT plans
- Information security governance, effectiveness of implementation of security policies and processes
- IT Architecture
  - Acquisation and Implementation of Packaged software
    - Requirement Identification and Analysis
    - Product and Vendor selection criteria
    - Vendor selection process
    - Contracts
    - Implementation
    - Post Implementation Issues
  - Development of software- In-house and Out-sourced
    - Audit framework for software developed in house, if any
    - Software Audit process
      - Audit at Program level
      - Audit at Application level
      - Audit at Organizational level
    - Audit framework for software outsourcing
  - Operating Systems Controls
    - Adherence to licensing requirements
    - Version maintenance and application of patches
    - Network Security
    - User Account Management
    - Logical Access Controls
    - System Administration
    - Maintenance of sensitive user accounts
  - Application Systems and Controls
    - Logical Access Controls
    - Input Controls
    - Processing Controls
    - Output Controls
    - Interface Controls
    - Authorization Controls
    - Data Integrity/ File Continuity controls
    - Review of logs and audit trails
  - Database Controls
    - Physical access and protection

        - Referential Integrity and accuracy
        - Administration and Housekeeping
    - Network Management audit
        - Process
        - Risk acceptance (deviation)
        - Authentication
        - Passwords
        - Personal Identification Numbers ('PINS')
        - Dynamic password
        - Public key Infrastructure ('PKI')
        - Biometrics authentication
        - Access Control
        - Cyptography
        - Network Information Security
        - E-mail and Voicemail rules and requirements
        - Information security administration
        - Microcomputer/ PC security
        - Audit trails
        - Violation logging management
        - Information storage and retrieval
        - Penetration testing
- Physical and environmental security
- Maintenance
    - Change Request Management
        - Software developed in-house
    - Version Control
    - Software procured from outside vendors
    - Software trouble-shooting
        - Helpdesk
    - File/ Data reorganization
    - Backup and recovery
        - Software
        - Data
        - Purging of data
    - Hardware maintenance
    - Training
- Internet Banking
    - Information systems security framework
    - Web server
    - Logs of activity
    - De-militarized zone and firewall
    - Security reviews of all servers used for Internet Banking
    - Database and Systems Administration
    - Operational activities
    - Application Control reviews for internet banking application
    - Application security
- Privacy and Data Protection

- Controls established for data coversion process
- Information classification based on criticality and sensitivity to business operations
- Fraud prevention and Security standards
- Isolation and confidentiality in maintaining of Bank's customer information, documents, records by banks
- Procedures for identification of owners
- Procedures of erasing, shredding of documents and media containing sensitive information after the period of usage.
- Media control within the premises

- Business Continuity Management
  - Top Management guidance and support on BCP
  - The BCP methodology covering the following:
    - Identification of critical business
    - Owned and shared resources with supporting function
    - Risk assessment on the basis of Business Impact Analysis ('BIA')
    - Formulation of Recovery Time Objective ('RTO') and Identification of Recovery Point Objective('RPO')
    - Minimising immediate damage and losses
    - Restoring of critical business functions, including customer-facing systems and payment settlement systems
    - Establishing management succession and emergency powers
  - Addressing of HR issues and training aspects
  - Providing for the safety and wellbeing of people at branch or location at the time of disaster
  - Assurance from Service providers of critical operations for having BCP in place with testing performed on periodic basis.
  - Independent Audit and review of the BCP and test result
  - Participation in drills conducted by RBI for Banks using RTGS/ NDS/ CFMS services
  - Maintaining of robust framework for documenting, maintaining and testing business continuity and recovery plans by Banks and service providers
- Asset Management
  - Records of assets mapped to owners
  - For PCI covered data, the following should be implemented:
    - Proper usage policies for use of critical employee facing technologies
    - Maintenance of Inventory logs for media
  - Restriction of access to assets through acceptable useage policies, explicit management approval, authentication use of technology, access control list covering list of employees and devices, labeling of devices, list of approved company products, automatic session disconnection of remote devices after prolong inactivity
  - Review of duties of employees having access to asset on regular basis.
- Human Resources
  - Recruitment policy and procedures for staff
  - Formal organization chart and defined job description prepared and reviewed regularly
  - Proper segregation of duties maintained and reviewed regularly
  - Prevention of unauthorized access of Former employees
  - Close supervision of staff in sensitive position

  - People on notice period moved in non-sensitive role
  - Dismissed staff to be removed from premises on immediate effect
- IT Financial Control
  - Comprehensive outsourcing policy
  - Coverage of confidentiality clause and clear assignment of liability for loss resulting from information security laspe in the vendor contract
  - Periodic review of financial and operational condition of service provider with emphasis to performance standards, confidentiality and security, business continuity preparedness
  - Contract clauses for vendor to allow RBI or personnel authorized by RBI access relevant information/ records within reasonable frame of time.
- IT Operations
  - Application Security covering access control
  - Business Relationship Management
    - Customer Education and awareness for adoptation of security measures
    - Mechanism for informing banks for deceptive domains, suspecious emails
    - Trademarking and monitoring of domain names to help prevent entity for registering in deceptively similar names
    - Use of SSL and updated certification in website
    - Informing client of various attacks like phishing
  - Capacity Management
  - Service Continuity and availability management
    - Consistency in handling and storing of information in accordance to its classification
    - Securing of confidential data with proper storage
    - Media disposal
    - Infrastructure for backup and recovery
    - Regular backups for essential business information and software
    - Continuation of voice mail and telephone services as part of business contingency and disaster recovery plans
    - Adequate insurance maintained to cover the cost of replacement of IT resources in event of disaster
    - Avoidance of single point failure through contingency planning
  - Service Level Management
- Project Management
  - Information System Acquisition, Development and Maintenance
    - Sponsorship of senior management for development projects
    - New system or changes to current systems should be adequately specified, programmed, tested, documented prior to transfer in the live environment
    - Scrambling of sensitive data prior to use for testing purpose
  - Release Management
    - Access to computer environment and data based on job roles and responsibilities
    - Proper segregation of duties to be maintained while granting access in the following enviornment
      - Live
      - Test
      - Development

    - Segregration of development, test and operating environments for software
- Record Management
  - Record processes and controls
    - Policies for media handling, disposal and transit
    - Periodic review of Authorization levels and distribution lists
    - Procedures of handling, storage and disposal of information and media
    - Storage of media backups
    - Protection of records from loss, destruction and falsification in accordance to statutory, regulatory, contractual and business requirement
- Technology Licensing
  - Periodic review of software licenses
  - Legal and regulatory requirement of Importing or exporting of software
- IT outsourcing related controls
- Detailed audit delivery channels and related processes like ATM, internet banking, mobile banking, phone banking, card based processes
- Data centre operations and processes
  Review relating to requirements of card networks (for example, PIN security review)

ANNEX C

Illustrative guidance for *committees or teams for BCP*

BCP people or Group	**HR**
Topic	Ideas
1.Roles, responsibilities and authorities	Communication to staff and onsite contractors Fatalities handling or counselling Resourcing Maintain staff and contractors database
2.Necessary competencies	Documentation planning Change management HR CIPD (Chartered Institute of Personnel and Development) certification Health and safety
3. Approach to training needs analysis	Counselling Training scenarios Desktop exercises Find out if managers know responsibilities for embedding BCP in community
4. Appropriate training	Table top Scenario walkthroughs Full exercises
5.Ways of measuring necessary competence	Audits Practical exercise Live invocation
6. Suitable records of education, training, skills, experience and qualifications	Past exercise reports

BCP people or group:	**BCP Teams**
Topic	Ideas
1. Roles, responsibilities and authorities	Set out in plan Assigned to position
2. Necessary competencies	Knowledge of business Understanding impact Ability to analyse information Leadership
3. Approach to training needs analysis	Interview Previous experience Skills required Scenario-"what would you do if" impact analysis
4. Appropriate training	Sharing knowledge: • Senior staff • Junior staff • External Exercise
5. Ways of measuring necessary competence	Assess practical Review capability following event
6. Suitable records of education, training, skills, experience and qualifications	Past exercise records

BCP people or group:	**Spokesperson (Communications)**
Topic	Ideas
1. Roles, responsibilities and authorities	CEO- Spokesperson PR and marketing Designated senior official Internal and external communications

2. Necessary competencies	Media training Write coherent briefs Be up-to-date with mission statement, value statement and general company policies Consistency with message
3. Approach to training needs analysis	Identify gaps in knowledge and liaise with appropriate departments, whose message will be included(e.g. Health and Safety)
4. Appropriate training	Exercises
5. Ways of measuring necessary competence	Review Notes
6. Suitable records of education, training, skills, experience and qualifications	Past exercise reports

BCP people or group:	**BCP Committee**
Topic	Ideas
1. Roles, responsibilities and authorities	Authorities to exercise, maintain and to invoke plan(if specified) Communication, training and promoting awareness Fits with other plans/ authorities Budget Ensure others are trained
2. Necessary competencies	Understanding of business and business continuity framework Proficiency and expertise in own function Trained Ability to communicate
3. Approach to training needs analysis	Corporate approach/strategy for BCP How is BCP implemented Include deputies Capability to exercise skills

4. Appropriate training	Same as the topic Approach to training needs analysis
5. Ways of measuring necessary competence	Through exercising Predefine success criteria and review Measure plan and people Range of exercise types • Desktop • Simulation
6. Suitable records of education, training, skills, experience and qualifications	Records of training participation • Memberships • Formal qualifications • Personal development plans