CHAPTER 4

CONCEPTUAL FRAMEWORK OF INFORMATION SECURITY AND CORE BANKING
CHAPTER 4

CONCEPTUAL FRAMEWORK OF INFORMATION SECURITY & CORE BANKING

4.1 Introduction:

The growing dependence on information systems is widely accepted among the banks. Information systems can generate many direct and indirect benefits, and as many direct and indirect risks. Electronic information is essential to achieve bank’s objectives. Its reliability, integrity and availability are significant concerns in most audits. The use of computer networks, particularly the Internet, is revolutionizing the way business conducted. While the benefits have been enormous and vast amounts of information are now literally at our fingertips, these interconnections also pose significant risks to computer systems, information, and to the critical operations and infrastructures they support. The infrastructure elements such as telecommunications, power distribution, national defenses, law enforcement, and government and emergency services are subject to these risks. The same factors that benefit operations speed and accessibility if not properly controlled can leave them vulnerable to frauds, damage, and malicious or harmful acts. In addition, natural disasters and inadvertent errors by authorized computer users can have destructive consequences if information resources are inadequately protected. Recent publicized disruptions caused by virus, worm, and denial of service attacks on web sites show the potential for damage.

Computer security is of increasing importance to banks in minimizing the risks of malicious attacks from individuals and groups and to protect the information. These risks include the fraudulent loss or misuse of resources, unauthorized access to release of sensitive customer’s information, disruption of critical operations through viruses or hacker attacks, and modification or destruction of data.

Information and the knowledge based on it have increasingly become recognized as ‘information assets’, which are vital enablers of business operations. Hence, 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 the banks. 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.[1]

The risk that information attacks will threaten with the following developments in information technology:

- Monies are increasingly transferred electronically between and among governmental agencies, commercial enterprises, and individuals.
- Governments are rapidly expanding their use of electronic commerce.
- Customers are increasingly relying on computer systems to manage everyday operations.
- More and more sensitive economic and commercial information is exchanged electronically.
- Computer systems are rapidly increasing in complexity and interconnectivity.
- Easy-to-use hacker tools are readily available, and hacker activities are increasing.

- Paper supporting documents are being reduced or eliminated.

Each of these factors significantly increases the need for ensuring the privacy, security, and availability of urban cooperative banks. Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize risk, and maximize return on investments.

4.2 Information and Information System

'Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected’. Information can be created, stored, destroyed, processed, transmitted, used for proper and improper purpose, corrupted, lost, stolen, printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on corporate video and displayed or published on web.

Whatever forms the information takes, or means by which it is shared or stored, it should always be appropriately protected.

An information system is a collection of people, hardware, software, processes and data for decision-making system to provide information assets, information is necessary to develop solutions to the problems faced by managers of economic agents. Information system is system in which collection, transmission, storage and data processing is done using the elements or components of IT, that means modern computing and communications, specialized software, procedures and techniques in addition specific specialized personnel. Information system can be categorized in four parts:

1. Management Information System (MIS): Management Information system (MIS) provides information needed to manage organizations efficiently and effectively. Management information systems involve three primary resources: people, technology, and information. Management information systems are distinct from other information systems in that they are used to analyze operational activities in the organization.

2. Decision Support System (DSS): Decision support system (DSS) is a computer-based information system that supports business or organizational decision-making activities. DSSs serve the management, operations, and planning levels of
an organization and help to make decisions. DSSs include knowledge-based systems.

3. **Executive Information System (EIS):** EIS are enterprise-wide DSS that help top-level executives analyze, compare, and highlight trends in important variables so that they can monitor performance and identify opportunities and problems. EIS and data warehousing technologies are converging in the marketplace.

4. **Transaction Processing System (TPS):** TPSs collect, store, modify, and retrieve the transactions of an organization. A transaction is an event that generates or modifies data that is eventually stored in an information system. To be considered a transaction processing system the computer must pass the Atomicity, Isolation, Durability and Consistency. The essence of a transaction program is that it manages data that must be left in a consistent state, e.g. if an electronic payment is made, the amount must be both withdrawn from one account and added to the other; it cannot complete only one of those steps.

Information System is “The architecture where an integrated combination of appliances, systems and solutions, software, alarms, and vulnerability scans working together, monitor 24 X 7, Having People, Processes, Technology, Policies and Procedures”

![Figure 4.1: Component of Information System](image)

Today globally all types of businesses (large and small), are using information systems, networks, and Internet technology to conduct their business electronically,
achieving new levels of efficiency and competitiveness. Information systems have both technical and behavioral perspectives.

### 4.3 What is Information Security?

“The quality or state of being secure- to be free from danger”. The protection of information and its critical elements, including systems that use, store, and transmit that information.

Information security (IS) is designed to protect the Confidentiality, Integrity and Availability of data from those with malicious intentions. Confidentiality, Integrity and Availability are sometimes referred to as the CIA Triad of information security. The C.I.A. triangle has been the industry standard for computer security since the development of the mainframe. It is based on the three characteristics of information that give it value for its use in organizations: **Confidentiality, Integrity, and Availability**. The security of these three characteristics of information is as important today. The threats to information confidentiality, integrity, and availability have evolved into a vast collection of events, including accidental or intentional damage, destruction, theft, unintended or unauthorized modification, or other misuses from human or nonhuman threats. This new environment of many constantly evolving threats has prompted the development of a more robust intellectual model that addresses the complexities of the current information security environment.

ISACA defines information security as something that:

“Ensures that within the enterprise, information is protected against disclosure to unauthorized users (Confidentiality), improper modification (Integrity) and non-access when required (Availability)”. 

"
Six major activities involved in Information Security are:

1. Policy development
2. Specification of roles and responsibilities
3. Designing & developing a security control framework
4. Implementing a solution
5. Monitoring
6. Training and Education and Awareness

A successful organization should have the following multiple layers of security in place to protect its operations:

- **Physical security**, to protect physical items, objects, or areas from unauthorized access and misuse.
- **Personal security**, to protect the individual or group of individuals who are authorized to access the organization and its operations.
- **Operations security**, to protect the details of a particular operation or series of activities.
- **Communications security**, to protect communications media, technology, and content.
- **Network security**, to protect networking components, connections, and contents.
- **Information security**, to protect information assets.

### 4.4 History of information security

The history of information security begins with the history of computer security. The need for computer security that is, the need to secure physical locations, hardware, and software from outside threats arise during World War II. Multiple levels of security were implemented to protect these mainframes and secure data integrity. Access to sensitive military locations was controlled through the use of badges, keys, and the facial recognition of authorized personnel by security guards. The growing need to maintain national security eventually led to more complex and more technologically sophisticated computer security safeguards. During these early years, information security was a straightforward process composed predominantly of physical security and simple document classification schemes. The primary threats to security were physical theft of equipment, surveillance against the products of the systems, and damage. One of the first documented security problems that were not physical in nature occurred in the early 1960s, when a systems administrator was working on a MOTD (message of the day) file, and another administrator was editing the password file. A software glitch mixed the two files, and the entire password file was printed on every output file.\(^2\)

#### Stage I: The 1960s

During the Cold War, many more mainframes were brought online to accomplish more complex and sophisticated tasks. It became necessary to find a way to enable these mainframes to communicate with each by means of a less cumbersome process than mailing magnetic tapes between computer centers. In response to this need, the Department of Defense’s Advanced Research Project Agency (DARPA) began examining the feasibility of a redundant, networked communications system to support the military’s exchange of information. Larry Roberts, known as the founder

---

\(^2\) Introduction To Information Security,  
www.arapaho.nsuok.edu/~hutchisd/IS_4853/C6572_01.pdf
of the Internet, developed the project from its inception. This project, called ARPANET, is the origin of today’s Internet.

Stage II: The 1970s and 80s
During the next decade, the ARPANET became popular and more widely used, and the potential for its misuse grew. In December of 1973, Robert M. “Bob” Metcalfe, who is credited with the development of the Ethernet, one of the most popular networking protocols, identified fundamental problems with ARPANET security.

- Individual remote users’ sites did not have sufficient controls and safeguards to protect data from unauthorized remote users.
- The vulnerability of password structure and formats.
- Lack of safety procedures for dial-up connections.
- Nonexistent user identification and authorization to the system.
- Phone numbers were widely distributed and openly publicized on the walls of phone booths, giving hackers easy access to the ARPANET.

Because of the range and frequency of computer security violations and the explosion in the number of hosts and users on the ARPANET, network security was referred to as network insecurity.

Stage III: The 1990s
At the close of the twentieth century, network of computers became more common, as did the need to connect these networks to each other. This gave rise to the Internet, the first global network of networks. This networking resource was made available to the general public in the 1990s, having previously been the domain of government, academia, and dedicated industry professionals. The Internet brought connectivity to virtually all computers that could reach a phone line or an Internet-connected local area network (LAN). After the Internet was commercialized, the technology became pervasive, reaching almost every corner of the globe with an expanding array of uses. Since its inception, the Internet has become an interconnection of millions of networks. However, early Internet deployment treated security as a low priority. For example, many of the problems that plague e-mail on the Internet today are the result of this early lack of security. Early computing approaches relied on security that was built into the physical environment of the data center that housed the computers. As
networked computers became the dominant style of computing, the ability to physically secure a networked computer was lost, and the stored information became more exposed to security threats.

Stage IV: The Present

Today, the Internet brings millions of unsecured computer networks into continuous communication with each other. The security of each computer’s stored information is now contingent on the level of security of every other computer to which it is connected.

![Figure 4.3: History of Information Security](image)

4.5 Need of Information Security

The purpose of information security management is to ensure business continuity and reduce business damage by preventing and minimising the impact of security incidents. An Information Security System enables information to be shared, as ensuring the protection of information and computing assets.

Sources of damage such as computer viruses, computer hacking and denial of service attacks have become more common, more striving and increasingly complicated. The internet exposes organizations to an increased threat if networks will be accessed improperly, data corrupted and viruses introduced. Not all breaches are the result of...
crime; misuse and human errors play a role in damaging business. The virus infections are still the single most prevalent form of abuse. More common and just as destructive as crime, are threats like fire, system crashes, and power cuts. Poor supervision of staffs and lack of proper authorization procedures are the main causes of security incidents.

According to RBI, complaints related to unauthorised fund transfers, fraudulent withdrawals from ATMs using duplicate cards, phishing e-mails aimed at extracting personal information have registered significant increase in recent times.

4.4.1 Threats to information security, Risk to information systems:
The growth of the rapid technology itself is responsible for the rising risks and threats. Attacks can be represented by the relation among the threats, vulnerability and damage. A threat is an object, person, or other entity that represents a constant danger to an asset. A threat can be either "intentional" e.g. an individual cracker or a criminal organization or "accidental" e.g. the possibility of a computer malfunctioning, or the possibility of a natural disaster such as an earthquake, a fire, or a tornado or otherwise a circumstance, capability, action, or event.[3] The Figure 4.4 depicts the potential issues in information security.

Figure 4.4: Potential issues in Information Security, Source: www.google.com

Security vulnerability is a weakness in a product that could allow an attacker to compromise the integrity, availability, or confidentiality of that product. By

examining each threat category in turn, management effectively protects its information through policy, education and training, and technology controls.

4.5.2 Types of threat and cyber crimes

The various sources of threats are listed below:

1. **Humana Error**: Employees are greatest threats to information security. They are closest to the organizational data. Human error includes acts done without malicious intent. This type of error caused by inexperience, improper training, incorrect assumptions. Employee mistakes can easily lead to the following:
   - Exposure/disclosure of confidential data
   - Entry of erroneous data
   - Accidental deletion or modification of data
   - Storage of data in unprotected areas
   - Failure to protect information

2. **Natural and Political Disaster**: Nobody can stop nature from taking its course. Earthquakes, hurricanes, floods, lightning, and fire can cause severe damage to computer systems. Information can be lost, downtime or loss of productivity can occur, and damage to hardware can disrupt other essential services. Few safeguards can be implemented against natural disasters. The best approach is to have disaster recovery plans and contingency plans in place. Other threats such as riots, wars, and terrorist attacks could be included here. Although they are human-caused threats, they are classified as disastrous[^4].

The Table No. 4.1 shows the different category of threats to information security.

<table>
<thead>
<tr>
<th>Types of Threats</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insiders Threats/attacks</td>
<td>An employee or worker with malicious intent to steal sensitive organization’s information, commit fraud or cause damage to systems or information.</td>
</tr>
<tr>
<td>Malware/Software Attacks</td>
<td>Malicious software such as Virus, Worms, Trojan Horse, Macros, Denial-of-service, password Sniffing etc.</td>
</tr>
<tr>
<td>Physical attacks</td>
<td>Hardware or equipment failures, Physical destruction of hardware and equipments, theft or damage.</td>
</tr>
<tr>
<td>Environmental attacks</td>
<td>Natural Disaster like Fire, flood and earthquake.</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>Phishing, Vishing and Cross-site scripting.</td>
</tr>
<tr>
<td>Unauthorized Access</td>
<td>The attempted or successful access of information or systems without permission or rights to do so.</td>
</tr>
<tr>
<td>Email Attacks</td>
<td>Email spoofing, spamming and bombing and Sending malicious codes through email.</td>
</tr>
</tbody>
</table>

Table No. 4.1: Types of information security Threats
1. **Insider threats (Most harmful):** The extensive use of Information technology by banks, the risk of unauthorized access, disclosure and modification of information by insiders or employees of banks is high. Even unintentional errors could have undesirable implications. There is a need to institute robust security processes to mitigate such threats.

2. **Phishing attacks:** Phishing involves an e-mail message being sent out to as many internet e-mail addresses that the hoaxter can obtain. Usually, these e-mails claim to come from a bank. The e-mail requests the recipient to update or to verify their personal and financial information, including date of birth, login information, account details, credit card numbers, PIN numbers etc. The email contains a link that takes you to a spoof website that looks identical or similar to the bank’s website. The hoaxter can then capture personal data like passwords as you type it in. Clicking on a link may also download malware onto your computer which will record your future use of the internet and forward even more information to the fraudster. The fraudsters will then use this information to compromise bank accounts, credit cards etc.

In some cases, pop-up windows can appear in front of a copy of an authentic bank web site. The real web site address is displayed, however, any information you type into the pop-up will go to unauthorized users. In a similar scheme, called “Vishing,” a person calls you and pretends to be a bank representative seeking to verify account information.

3. **Malware:** Short for 'malicious software', this is designed to penetrate a computer system without your consent. The term covers a variety of intrusive software/programmes, including Viruses, Worms, Trojan horses and Spyware. Attacks involving malware are a factor in online financial crime. In fact, it is possible for this type of malicious software to perform the following operations:

   a. **Spyware:** These are programs/files that may already reside on your computer and often arrive as hidden components of free programs. Spyware monitors web usage and in its more extreme forms can include keystroke logging and virtual snooping on all your computer activity.
b. **Trojan horse / Trojan**: It is legitimate software that carries an unwanted application like a virus or spyware - typically used by hackers to gain unauthorized access to computer systems.

c. **Virus**: A computer program designed to replicate by copying itself into other programs stored in a computer. It may be harmless but usually has a negative effect, such as slowing computer down or corrupting its memory and files. Viruses are now mainly spread by email and by file sharing services.

d. **Virus hoax e-mail**: Many e-mail warnings about viruses are hoaxes, designed purely to cause concern and disrupt businesses. Such warnings may be genuine, so don't take them lightly, but always check the story out by visiting an antivirus site before taking any action or forwarding them to friends and colleagues.

e. **Worm**: This is a malicious programme that replicates itself until it fills all of the storage space on a computer drive or network. Worms may use up computer time, space and speed when replicating, with a malicious intent to slow or bring down entire web servers and disrupt Internet use.

f. **Account information theft**: Malware can capture the keystrokes for your login information. Malware can also monitor and capture other data you use to authenticate your identity for example “magic words” you chose.

g. **Fake web site substitution** - Malware can generate web pages that appear to be legitimate but are not. They replace your bank’s legitimate web site with a page that can look identical, except that the web address will vary in some way. Such a “man-in the middle attack” site enables an attacker to intercept user information. The attacker adds additional fields to the copy of the web page opened in your browser. When you submit the information, it is sent to both the bank and the malicious attacker without your knowledge.

h. **Account hijacking**: Malware can hijack your browser and transfer funds without your knowledge. When you attempt to login at a bank’s web site, the software launches a hidden browser window on your computer, logs in to your bank, reads your account balance, and creates a secret fund transfer to the intruder-owned account. In addition to online infections, detections of malicious programs directly on user computers or removable media are also of interest. Removable media devices include USB drives, camera memory cards, mobile phone memory cards, and external hard drives.
4. **Denial of Service (DoS):** Numerous types of attacks make use of the possibility of entering rogue information in input fields.

5. **Pharming:** Pharming attacks involve the installation of malicious code on your computer. However, they can take place without any conscious action on your part. With pharming attacks, you must open an email, or email attachment, to become vulnerable. You then visit a fake website and, without your knowledge, provide information that compromises your financial identity.

In 2015, attacks on online banking systems will be one of the most widespread methods of stealing money from banks and users. The number of crimes committed in this area is rising rapidly all over the world in spite of all the technical measures taken by banks.

Online banking fraud can be performed internally by staff or externally by customers or suppliers. Online banking is the delivery channel to conduct banking activity, for example, transferring funds, paying bills, viewing checking and savings account balances, paying mortgages, and purchasing financial instruments and certificates of deposit. In Internet banking customers access his or her accounts from a browser, software that runs Internet banking programs resident on the bank’s World Wide Web server. Customers can select any online banking services. The traditional branch model of bank is now giving place to an alternative delivery channels with ATM network. Once the branch offices of the banks are interconnected through network or satellite links, there would be no physical identity for any branch. It would a borderless entity permitting anytime, anywhere and anyhow banking. Online Banking has become increasingly popular globally, because it is so easy and convenient for users to manage their bank accounts from any part of the world at any time. Banks have encouraged this trend for years, since online banking also saves lots of resources such as staff training, investment for ATMs and branches, and other operations costs. The Internet enhanced the user experience of banking activities dramatically. However, since the Internet is not originally designed for online banking, Online banking now is facing a wide range of security risks for both the banks and the online banking users such as brute-force attacks, Distributed Denial Service attacks, and social engineering attacks such as phishing, Vishing etc. The banks have to increase
their Online Banking security system constantly, which means that the banks have to keep investing on the security systems all the time.

4.6 Basic principles of information security

For over twenty years, information security has held confidentiality, integrity and availability (known as the CIA Model) 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. [5]

4.6.1 CIA Model

1. 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, and SMS spoofing, and sending malicious code through email or Networks.

2. Integrity: In information security, integrity means that data cannot be modified without authorization. Integrity is despoiled when an employee accidentally or with malicious intent deletes important data files, when he/she is able to modify data, 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.

3. **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 appropriately. 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.

![Figure 4.6: CIA (Confidentiality, Integrity and Availability) Model, Source: ISO 17799](image)

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

5. **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.

6. **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 biometric 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.

7. **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.

8. **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.

### 4.7 Information Security Controls

Security controls are safeguards or countermeasures to avoid, counteract or minimize security risks.

To help to review or design security controls, they can be classified by several criteria, for example according to the time that they act, relative to a security incident:
1. **Before the event, Preventive controls** are intended to prevent an incident from occurring e.g. by locking out unauthorized intruders.

2. **During the event, Detective controls** are intended to identify and characterize an incident in progress e.g. by sounding the intruder alarm and alerting the security guards or police.

3. **After the event, Corrective controls** are intended to limit the extent of any damage caused by the incident e.g. by recovering the organization to normal working status as efficiently as possible.

Security controls can also be categorized according to their nature, for example:

1. Organizational/Management Controls
2. Operational/Procedural Controls
3. Technological Controls

1. **Organizational Controls:**
Organizational controls are procedures and processes that define how people in the organization should perform their duties. [6]

A. Preventative controls

- **Clear defining Roles and Responsibilities:** These must be clearly defined and documented so that management and staff clearly understand who is responsible for ensuring an appropriate level of security which has to be implemented for the important IT assets.

- **Segregation of duties and privileges:** These ensure that people have only enough access to IT systems to effectively perform their job duties.

- **Documented security plans and procedures:** These are developed to explain how controls have been implemented and how they are to be maintained.

- **Security Training and Awareness program:** This is necessary for all members of the organization so that users and members of the IT team understand their responsibilities and how to properly utilize the computing resources while protecting the organization's data.

- Established processes for granting access to contractors, vendors, partners, and customers.
- Sharing some data with one group of external users while sharing a different collection of data with a different group can be challenging. Legal and regulatory requirements often impact the choices.

B. Detection controls
- Performing continuing risk management programs to assess information security risk and control risks to the organization's key assets.
- Executing regular reviews of controls to verify the controls' efficiency.
- Periodic undertaking of system audits to ensure that systems have not been compromised or misconfigured.
- Performing background investigations of employees for employment or being considered for promotions to positions with a significantly higher level of access to the organization's IT assets.
- Establishing a rotation of duties, this is an effective way to uncover reprehensible activities by members of the IT team or users with access to sensitive information.

C. Corrective Controls
- Incident response planning, which provides an organization with the ability to quickly react to and recover from security violations while minimizing their impact and preventing the spread of the incident to other systems.
- Business continuity planning, which enables an organization to recover from catastrophic events that impact a large fraction of the IT infrastructure.

2. Operational Controls:
Operational controls define how people in the organization should handle data, software and hardware. They also include environmental and physical protection as described below. [7]

A. Preventative controls

- Protection of computing facilities by physical means such as guards, electronic badges and locks, biometric locks, and fences.

- Physical protection for end-user systems, including devices such as mobile computer locks and alarms and encryption of files stored on mobile devices.

- Emergency backup power, which can save sensitive electrical systems from harm during power brownouts and blackouts; they can also ensure that applications and operating systems are shut down graceful manner to preserve data and transactions.

- Fire protection systems such as automated fire suppression systems and fire extinguishers, which are essential tools for guarding the organization's key assets.

- Temperature and humidity control systems that extend the life of sensitive electrical equipment and help to protect the data stored on them.

- Media access control and disposal procedures to ensure that only authorized personnel have access to sensitive information and that media used for storing such data is rendered unreadable before disposal.

- Backup systems and provisions for offsite backup storage to facilitate the restoration of lost or corrupted data. In the event of a disastrous incident, backup media stored offsite makes it possible to store critical business data on replacement systems.

B. Detection and recovery controls

- Physical security, which shields the organization from attackers attempting to gain access to its premises; examples include sensors, alarms, cameras, and motion detectors.

- Environmental security, which safeguards the organization from environmental threats such as floods and fires; examples include smoke and fire detectors, alarms, sensors, and flood detectors.
Technological Controls
Technological controls vary considerably in complexity. They include system architecture design, engineering, hardware, software, and firmware. They are all of the technological components used to build an organization's information systems. [8]

A. Preventative controls includes:

- **Authentication**: The process of validating the credentials of a person, computer, process, or device. Authentication requires that the person, process, or device making the request provide a credential that proves it is what or who it says it is. Common forms of credentials are digital signatures, smart cards, biometric data, and a combination of user names and passwords.

- **Authorization**: The process of granting a person, computer process, or device access to certain information, services, or functionality. Authorization is derived from the identity of the person, computer process, or device requesting access, which is verified through authentication.

- **Non-repudiation**: The technique used to ensure that someone performing an action on a computer cannot falsely deny that he or she performed that action. Non-repudiation provides undeniable proof that a user took a specific action such as transferring money, authorizing a purchase, or sending a message.

- **Access control**: The mechanism for limiting access to certain information based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role-based.

- **Protected communications**: These controls use encryption to protect the integrity and confidentiality of information transmitted over networks.

B. Detection and recovery controls include:

- Audit systems: These systems make it possible to monitor and track system behavior that deviates from expected norms. They are a fundamental tool for detecting, understanding, and recovering from security breaches.

- Antivirus programs: Designed to detect and respond to malicious software, such as viruses and worms. Responses may include blocking user access to infected

files, cleaning infected files or systems, or informing the user that an infected program was detected.

- System integrity tools: Make it possible for IT staff to determine whether unauthorized changes have been made to a system. For example, some system integrity tools calculate a checksum for all files present on the system's storage volumes and store the information in a database on a separate computer. Comparisons between a system's current state and its previously-known good configuration can be completed in a reliable and automated fashion with such a tool.

### 4.8 Information Security Standards

Information security plays an important role in protecting the data and assets of an organisation. Over and over again we hear news about security incidents, such as defacement of websites, server hacking and data leakage. Organisations need to be fully aware of the need to devote more resources to the protection of information assets, and information security must become a top concern in both government and business. To address the situation, a number of governments and organisations have set up benchmarks, standards and legal regulations on information security to ensure an adequate level of security is maintained, resources are used in the right way, and the best security practices are adopted.

Banking organization is regulated, and the guidelines or best practices put together as part of those regulations often become standard. The most commonly adopted standards and regulations for information security are listed below:

#### 4.8.1 ISO STANDARD:

ISO (the International Organization for Standardization) and IEC (International Electro technical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the representative organization to deal with particular fields of technical activity.

The ISO/IEC 27000 series is a comprehensive set of controls comprising best practices in information security. It is an internationally recognized information security standard, broad in scope and generic in applicability. It focuses on risk identification, assessment and management. It is aligned with common business goals [9].

- Ensure business continuity
- Minimize business damage
- Maximized return on investments
- It is about information security, not IT security.
- It is much more commonly applied in commercial organizations than in government

Originally created as BS17799, this framework was first submitted in 1995, and revised in 1998, but was not adopted by the International Standards Organization until 1999. Significantly revised in 2005, it was formally converted to two related International Standards Organization/International Electro technical Commission

b. ISO/IEC standards, 27001 & 27002: ISO 17799 covers both security management practices and security controls referred to as Part 1 and Part 2 in the 17799 standard was numerically reversed in the new ISO/IEC numbering, so that Part 1 becomes 27002 and Part 2 becomes 27001.

i. Part 1 - Code of Practice ISO 27002: Provides 133 security controls under 39 security categories organized into 11 major clauses to identify the particular safeguards that are appropriate to their particular business. These security controls correspond to hundreds of more detailed technologies, measures, and elements of practice. The standard stresses the importance of risk management.

ii. Part 2 - IS Management Standard ISO/IEC 27001: It tells how to build an Information Security Management System. It defines a four-step process instructing how to apply ISO/IEC 17799 and how to establish, implement, monitor, and maintain ISMS. It is a formal methodology for

setting up an information security management system. ISO/IEC 27001 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization.

ISO 27002 Information Security clauses/ Security Domains:

1. Security Policy
2. Organizing Information Security
3. Asset Management
4. Human Resources Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. Access Control
8. Information Systems Acquisition, Development and Maintenance
9. Information Security Incident Management
11. Compliance

This standard adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's Information Security Management System (ISMS).

The approach presented in ISO 27001 encourages its users to emphasize the importance of:

a) Understanding an organization’s information security requirements and the need to establish policy and objectives for information security.

b) Implementing and operating controls to manage an organization's information security risks in the context of the organization’s overall business risks.

c) Monitoring and reviewing the performance and effectiveness of the ISMS.

d) Continual improvement based on objective measurement.
c. **ISO/IEC 15408-1:2009(Evaluation criteria for IT security):**

With the rise of security breaches and the running of technology at its highest gear on the information superhighway, protection of confidential and vital information never has been more crucial. The needs to have some kind of assurance that the products and the systems used provide an adequate security. The Common Criteria (CC) - ISO/IEC 15408 - Evaluation Criteria for Information Technology security represents the outcome of series of efforts to develop criteria for evaluation of IT Security that are broadly useful within the international community. [10]

The Common Criteria document consists of:

i. **Part 1 - Introduction and General Model:** Part 1 defines general concepts and principles of IT security evaluation and presents a general model of evaluation. This part also presents the constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems.

ii. **Part 2 - Security Functional Requirements:** This part establishes a set of security functional components as a standard way of expressing the security requirements for IT products and systems.

---

iii. **Part 3 - Security Assurance Requirements**: This part produces a catalog of establishes set of assurance components that can be used as a standard way of expressing the assurance requirements for IT products and systems. Part 3 presents the seven Evaluation Assurance Levels (EALs), which are predefined packages of assurance components that make up the CC scale for rating confidence in the security of IT products and systems.

d. **ISO/IEC 13335 (Security techniques - Management of information and communications technology security)**:
ISO/IEC 13335 was initially a Technical Report (TR) before becoming a full ISO/IEC standard consists of a series of guidelines for technical security control measures:

1. ISO/IEC 13335-1:2004 documents the concepts and models for information and communications technology security management.
2. ISO/IEC TR 13335-3:1998 documents the techniques for the management of IT security. This is under review and may be superseded by ISO/IEC 27005.
3. ISO/IEC TR 13335-4:2000 covers the selection of safeguards (i.e. technical security controls). This is under review and may be superseded by ISO/IEC 27005.
4. ISO/IEC TR 13335-5:2001 covers management guidance on network security. This is also under review, and may be merged into ISO/IEC 18028-1, and ISO/IEC 27033.

ISO/IEC 17799:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC

17799:2005 contains best practices of control objectives and controls in the following areas of information security management:

1. Information Security policy
2. Organization of information security
3. Asset management
4. Human resources security
5. Physical and environmental security
6. Communications and operations management
7. Access control
8. Information systems acquisition, development and maintenance
9. Information security incident management
10. Business continuity management
11. Compliance.

The control objectives and controls in ISO/IEC 17799:2005 are intended to be implemented to meet the requirements identified by a risk assessment. ISO/IEC 17799:2005 is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities [12].

### 4.8.2 Payment card industry data security standard

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed by a number of major credit card companies (including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International) as members of the PCI Standards Council to enhance payment account data security. The standard consists of 12 core requirements, which include security management, policies, procedures, network architecture, software design and other critical measures. These requirements are organised into the following areas [13]:

---


1. Build and maintain a secure network
2. Protect cardholder data
3. Maintain a vulnerability management program
4. Implement strong access control measures
5. Regularly monitor and test networks
6. Maintain an information security policy

4.8.3 COBIT (Control Objectives for Information and Related Technology)

Control Objectives for Information and Related Technology (COBIT) is a framework created and published by Information Systems Audit and Control Association (ISACA) for information technology (IT) management and IT governance. It is a supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks.

The process focus of COBIT 4.1 is illustrated by a process model as shown in Figure 4.8 that subdivides IT into four domains (Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate) and 34 processes in line with the responsibility areas of plan, build, run and monitor. It is positioned at a high level and has been aligned and harmonized with other, more detailed IT standards and good practices such as COSO, ITIL, and ISO27000. COBIT acts as an integrator of these different guidance materials, summarizing key objectives under one umbrella framework that link the good practice models with governance and business requirements[14].

4.8.4 Information Technology Infrastructure Library (ITIL)

ITIL is a set of best practices standards for Information Technology (IT) service management. The United Kingdom's Central Computer and Telecommunications Agency (CCTA) created ITIL in response to the growing dependence on Information Technology to meet business needs and goals.

ITIL provides businesses with a customizable framework of best practices to achieve quality service and overcome difficulties associated with the growth of IT systems. The ITIL emerged as the world's most widely accepted approach to the management and delivery of IT Services because of its scalability.

The core processes of ITIL are IT planning, Service delivery such as Availability Management, Capacity Management, IT Service Continuity Planning, Financial Management, and Service Level Management and support for IT Services such as
Incident Management, Problem Management, Change Management, Release Management, Configuration Management.[15]

4.9 Information Security Domains
ISO/IEC 27002:2005 is an international standard, refers to a code of practice for information security management, and is intended as a common basis and practical guideline for developing organizational security standards and effective management practices. This standard contains guidelines and best practices recommendations for these 11 security domains [16]. Implementing an Information Security Management System involves with 3 key aspects of an organization; physical aspect, management aspect and technical aspect. An ISMS contains 11 Domains as ISO/IEC 27002:2005 is an international standard, refers to a code of practice for information security management, and is intended as a common basis and practical guideline for developing organizational security standards and effective management practices. This standard contains guidelines and best practices recommendations for these 11 security domains [17]:

2.9.1 Information Security policy
2.9.2 Organization of information security
2.9.3 Asset management
2.9.4 Human resources security
2.9.5 Physical and environmental security
2.9.6 Communications and operations management
2.9.7 Access control
2.9.8 Information systems acquisition, Development and maintenance
2.9.9 Information security incident management
2.9.10 Business continuity management
2.9.11 Regulatory Compliance

Among these 11 security domains, a total of 39 control objectives and hundreds of best-practice information security control measures are recommended for organizations to satisfy the control objectives and protect information assets against threats to confidentiality, integrity and availability.\[18\].

![ISO/IEC 27001 Information Security Domains](image)

**Figure 4.9:** ISO/IEC 27001 Information Security Domains

### 4.9.1 Information Security Policy

In order to protect information, businesses need to implement rules and controls around the protection of information and the systems that store and process this information. This is commonly achieved through the implementation of information security policies, standards, guidelines and procedures.

#### A. Information Security Policies Framework

- **Security Policies:** A policy is typically a document that outlines specific requirements or rules that must be met. "Policies" are management instructions indicating a course of action, a guiding principle or appropriate procedures, which

is useful, practical, or advantageous. An information security policy consists of high level statements relating to the protection of information across the business and should be produced by senior management. The policy outlines security roles and responsibilities, defines the scope of information to be protected, and provides a high level description of the controls that must be in place to protect information. In addition, it should make references to the standards and guidelines that support it. From a legal and compliance perspective, an information security policy is often viewed as a commitment from senior management to protect information. A documented policy is frequently a requirement to satisfy regulations or laws, such as those relating to privacy and finance. It should be viewed as a business mandate and must be driven from the top (i.e. senior management) downwards in order to be effective. Businesses may have a single encompassing policy, or several specific policies that target different areas.

- **Standards**: Standards consist of specific low level mandatory controls that help enforce and support the information security policy. Standards help to ensure security consistency across the business and usually contain security controls relating to the implementation of specific technology, hardware or software.

- **Guidelines**: Guidelines consist of recommended, non-mandatory controls that help support standards or serve as a reference when no applicable standard is in place. Guidelines should be viewed as best practices that are not usually requirements, but are strongly recommended. They could consist of additional recommended controls that support a standard, or help to fill in the gaps where no specific standard applies. For example, a standard may require passwords to be 8 characters or more and a supporting guideline may state that it is best practice to also ensure the password expires after 30 days.

- **Procedures**: Procedures consist of step by step instructions to assist staff in implementing the various policies, standards and guidelines.
B. Need for Information Security Policy and Guidelines

The business operations in the banking and the financial sector are becoming increasingly dependent on computerized information systems. It has now become impossible to separate technology from the business of the banks. On account of the phenomenal growth in the use of IT and IT based applications by the banks in its day-to-day operations, the need for putting in place the security controls for all the information systems has grown tremendously. The information systems security has, therefore, assumed great importance for the commercial success of the banks, as the survival of the banks depends on the speed, accuracy and reliability of the flow of information within the banks vis-à-vis its customers.

The security controls are required to minimize the vulnerability to unauthorized use of the information and the information systems. However, such controls may have to be consistent with the degree of exposure of such systems and the information and the impact of loss to the banks on account of unauthorized access and misuse, including accidental misuse, of such systems and information. The unauthorized including accidental misuse of the information may result in financial loss, competitive disadvantage, damaged reputation, improper disclosure, law suits and non-compliance with the regulatory provisions etc. Structured, well-defined and documented security policies, standards and guidelines set the foundation for good information systems security.
No threat becomes obsolete. Further, new threats surface from time to time. The banking and the financial sector is now poised to countenance various developments such as Internet banking, e-money, e-cheque, e-commerce etc., which have been made possible by the revolutionary researches and discoveries in Information Technology and its applications and the future promises to remain challenging. Constant developments of far reaching implications dictate constant vigilance and necessitate sound information systems security infrastructure. The information security policy is the foundation for secure infrastructure \[19\]. The information security policy serve as a guide and a reference point to numerous security tasks in an organization. Without security policies, no enforcement of security configurations or standards can be made.

C. Implementation of Information Security Policy and Procedures

At the corporate level, the Chief Information Security Officer (CISO) would be responsible for Information Systems Security. He will be assisted by a team of officers comprising both technical and banking officers to be responsible for the information systems security policies implementation in each of the offices/locations of the banks.

Information Systems Security Department in the banks will address various issues such as the development of the information security policy, updating of the information security guidelines on an on-going basis, provision of consultancy and information security requirements, maintenance of centralized security functions etc. Further, the system administration responsibilities should, among others, relate to the implementation of the security controls, compliance with the information security guidelines, management of day-to-day security functions etc. The information security department would be responsible for \[20\]:

- Identification of individuals to be responsible for the protection of information assets at each office/location of the banks.
- Classification of information assets and specifications of the appropriate levels of security for each class of information assets.


• Implementation of an awareness/education programme to ensure security of information and information systems in the banks.

• Reporting of information systems security incidents and provision for their resolution.

• Preparation of written (comprehensively documented) plans and procedures for business continuity following disasters.

• Laying down precisely the responsibilities to ensure compliance with and to assess soundness and comprehensiveness of the information security policies on a continuous basis.

• Reviewing, updating and upgradation of the information security policies in the light of new threats and technology on a continuous basis.

• Preparation of the audit records, where necessary and the monitoring of the audit trails for the detection of uncharacteristic behavior of individuals and activities.

4.9.2 Organization of Information Security

A governance structure is essential for organizing information security within and across the organization. Governance maintains balance between the value of information security, the management of security-related risks, and increased requirements for control over information. The value, risk, and control constitute the core of an effective information security governance structure. The information security governance is the responsibility of senior management and executive staff.[21]

A. Roles & Responsibilities and organization framework

• 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. 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.

- **Information Security Team/Group**: 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 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 and forensic assessment etc.

- **Information Security Committee**: It includes business heads from different units and is responsible for enforcing organization wide policies and procedures. 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.

- **Chief Information Security Officer (CISO)**: A sufficiently senior level official of the rank of GM/DGM/AGM needs to be designated as the Chief Information Security Officer (CISO) responsible for articulating and enforcing the policies that a bank uses to protect its information assets. The CISO needs to report directly to the head of the risk management function and should not have a direct reporting
relationship with the CIO. The Figure 4.11 shows the organization structure for information security.

![Diagram](image-url)

**Figure 4.11: Organization Structure for Information Security, Source:** [www.google.com](http://www.google.com)

B. Major responsibilities of the Information Security Committee

- Developing and facilitating the implementation of information security policies, standards and procedures for the banks. (applications, data, infrastructure and people related)
- Monitoring security logs of applications, operating systems, databases and networks, etc.
- Business Continuity and Disaster Recovery Planning and Monitoring.
- Facilitating investigations in IT frauds and improvement method.
- 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 banks.
- Reviewing the status of information security training and awareness programmes.
- Assessing new developments or issues relating to information security.
4.9.3 Asset management

Asset management is required to identify and manage information and information technology assets associated with information systems or services ("assets") to provide control and accountability, support strategic planning, enhance critical incident response, system planning, protection, maintenance and recovery.

The responsibility included in the assets management are development and maintenance of policies, standards, processes, systems and measurements that enable the organization to manage the IT asset portfolio with respect to risks, cost, controls, IT governance, compliance and business performance objectives as established by the business.

The asset protection refers to a process where organization identifies inventory assets, agree upon ownership and the classification of information, and document the process of safeguarding each asset to protect against loss or theft. The inventories of assets can assist to ensure effective asset protection, identification of missing assets, and may satisfy other business purposes, such as safety or other asset management requirements.

An organization must ensure the necessary policies, standards, guidelines, processes, and procedures in place to be in compliance with laws, regulations, statutes, and state policies with respect to asset inventory, identification, classification, use, and disposition requirements. This effort may involve establishing cooperative relationships with management in other functional units across the organization (e.g. business areas, human resources and labour relations, business services, procurement, IT services, and legal).

The policies are basic foundations, however, organizations must also ensure that all information created and used by its employees and contractors are properly classified. The classification categorizes information, whether that information is contained on paper or in electronic format, in terms of its sensitivity to loss, disclosure, and availability. The classification is required to implement the appropriate security controls. The data classification is the responsibility of the data owner, or their
designee, and requires the initial classification, as well as periodic reviews to ensure the appropriate level of security controls are in place. There are many types of assets that require protection, including but not limited to:[22]

- **Information**: Databases and files, contracts and agreements, system documentation, training material, business continuity plans, specialized contact lists, audit trails, and operation or support procedures.
- **Software assets**: Application and system software, development tools, and utilities.
- **Physical assets**: Computer equipment, communications equipment, uninterruptible power supplies, removable media, Closed Circuit Television (CCTV), and identification badges.
- **Services**: Computing and communications services and general utilities, such as telephone, internet access, heating, lighting, power and air conditioning.

All information assets shall be managed at organization level. The ownership of the information assets shall reside with the organization and individuals shall be assigned and made responsible and accountable for the information assets. Specific individuals shall be assigned with the ownership / custodianship / operational usage and support rights of the information assets.

A. **Information Asset Management Responsibilities**[23]

a. **Legal Owner**: The top management shall be legal owner of information asset. No individual can claim intellectual property rights of an information asset, unless and otherwise specifically agreed and approved by the management in contractual agreement. The responsibilities of the asset owner are as follows:


- Updating of information asset inventory register.
- Identifying the classification level of information asset.
- Defining and implementing appropriate safeguards to ensure the confidentiality, integrity, and availability of the information asset.
- Assessing and monitoring safeguards to ensure their compliance and report situations of non-compliance.
- Authorizing access to those who have a business need for the information, and ensuring access is removed from those who have no longer a business need for the information.

b. Delegated Ownership: The CEO shall have authority to represent the organization for the protection and security of the information asset as ownership of information assets. The CEO shall approve the information management / security policy. The CEO may delegate full / partial ownership along with the defined responsibilities to any officer / contractor / third party with operational rights and responsibilities.

c. Director Information Management: The Director, information management ensures that the information resources of organization are managed as a corporate asset and assists in establishing the strategic direction of information management for the organization. They provide support and leadership to officers and other directors responsible for managing information resources on a day-to-day basis.

d. Chief Information Officer: The CIO ensures that strategic planning processes are undertaken so that information requirements and supporting systems and infrastructure are aligned to legislative requirements and strategic goals. The CIO ensures that information security policies and governance practices are established to ensure the quality and integrity of the organization’s information resources and supporting IT systems. They oversee the development of tools, systems and information technology infrastructure to maximize the access and use of an organization’s information resources.

e. Information Security Officer: The information security officer is responsible for developing and implementing information security policy designed to protect information and any supporting information systems from any unauthorized access, use, disclosure, corruption or destruction. The responsibilities of information security officer are as follows:
developing policies, procedures and standards to ensure the security, confidentiality and privacy of information that is consistent with organizational information security policy.

- Monitor and report on any information intrusion incidents and activate strategies to prevent further incidents.
- Work with information custodians to ensure that information assets have been assigned appropriate security classifications.
- Maintenance and upkeep of the asset as defined by the asset owner.
- System restart and recovery
- Implementing any changes as per the change management procedure.
- Backup of the information.
- Updating of information asset inventory register.
- Defining and implementing appropriate safeguards to ensure the confidentiality, integrity, and availability of the information asset.
- Assessing and monitoring safeguards to ensure their compliance and report situations of non-compliance.
- Authorizing access to those who have a business need for the information.
- Ensuring access is removed from those who have no longer a business need for the information.

f. Data Operators / End Users: Employees, third parties, contractors authorized by the owner / custodian to access information and use the safeguards established by the owner / custodian. Being granted access to information does not imply or confer authority to grant other users access to that information. The users are bound by the acceptable usage policy of the organization.

B. Asset Management – Responsibility for assets

An inventory of all important assets associated with information systems must be documented and maintained.[24]

---

a. Identification of assets
b. Documenting and maintaining asset inventories
c. Loss, theft or misappropriation of assets

a. **Identification of assets**: The information owners and information custodians must identify assets under their control including:

- Software
- Hardware
- Services including computer and communications services, and general utilities
- Information assets required to be inventoried in the personal information directory required under the freedom of information and protection of privacy act.
- All other information assets including database and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements, archived information.

b. **Documenting and maintaining asset inventories**: Information owners and information custodians must document, maintain and verify asset inventories on a regular basis, depending on the criticality and value of the assets and validate the measures taken to protect the assets as part of an enterprise risk management strategy. Information owners and information custodians must document, maintain and verify the personal information directory including the personal information of a bank and privacy impact assessment sections.

The following information should be recorded to facilitate the system planning and asset recovery in the case of interruption, corruption, loss or destruction:

- Type of asset
- Ownership
- Format
- Location
- Back-up information and location
- License information
- Sensitivity and safeguards requirements
- Criticality for service delivery and maintaining business functions
- Consequences of losses

Information owners and information custodians are accountable for asset identification and inventory maintenance.

c. **Loss, theft or misappropriation of assets:** The loss, theft or misappropriation of assets must be reported immediately using the general incident or loss report. Where the loss, theft or misappropriation involves information the information incident management process must be followed.

### 4.9.4 Human Resources Security

Human resource or personal security refers to those practices, technologies, and services to ensure the employees and contractors authorized to access or maintain systems have the appropriate levels of access needed to perform their duties. Because of their internal access levels, authorized users create a potential threat to systems and data. Additionally, reducing the amount of users with system administrator privileges reduces the risk of accidental damage or loss of information and systems.

A key component to assure that legitimate users understand their role and responsibilities for information security is through an ongoing awareness program. An effective program ensures employees and contractors know about information security and privacy relative to their job responsibilities.

A successful security awareness program should target various groups such as employees and contractors, IT staff, or managers and end users with information pertinent to their respective roles. Most of the users would be interested in awareness material addressing Internet use, email, and handling confidential information. The technical support personnel would be more focused on access control, antivirus, and patch management administration. The executives would be more interested in the benefits of enabling business through information security, risk management and business continuity.

**Best Practices for Human Resource Security**
- Inform all users about organization information security policies and procedures.
- Segregation of duties by assigning tasks to different personnel, preventing one person from having total control of the security measures.
- Remove physical and logical access as soon as an employee or contractor leaves, retires, or is terminated.
- Create forms and instructions to ensure return of state property and notification to appropriate internal staff for transfers and terminations.
- Provide specific requirements regarding use and access for non-state entities including vendors and contractors and document in agreements in order to comply with all state policy and law regarding use of information resources and data.
- Implement formal disciplinary processes for employees who have committed a security breach.
- Promote information security awareness and training program using techniques such as posters, email messages, formal instruction, newsletters, and security awareness days.
- Ensure all users sign confidential and acceptable use agreement.
- Train all users to quickly identify threats, and how to respond to security incidents.
- Review and update training content regularly to reflect changes to the organization environment.

4.9.5 Physical and Environmental Security

Physical and Environmental security refers to those practices, technologies and services used to address the threats, vulnerabilities, and counter measures utilized to protect information assets and the premises in which they reside. These safeguards take into account:

- The physical facilities housing the information resources
- The general operating location and environmental factors
- Any additional facilities that support the operation of the information systems (e.g. server room/closet, data centers)

Physical security is primarily concerned with restricting physical access by unauthorized people (commonly interpreted as intruders) to controlled facilities, although there are other considerations and situations in which physical security
measures are valuable (for example limiting access within a facility and/or to specific assets, and environmental controls to reduce physical incidents such as fires and floods).

Security can never be perfect or complete. In other words, security can reduce but cannot entirely eliminate risks. Physical access controls to protect facilities are generally intended to:

- **Environmental design**: Prevent potential intruders e.g. warning signs and perimeter markings. Delay, frustrate and ideally prevent intrusion attempts e.g. strong walls, door locks and safes.
- **Access Control**: Distinguish authorized from unauthorized people e.g. using swipe card/key cards/access badges, biometric authentication etc.
- **Intrusion Detection and Prevention**: Detect intrusions and monitor/record intruders e.g. intruder alarms, monitor sensors and glass break detector.
- **Personal Authentication**: The last layer is video monitoring systems. Security cameras can be a deterrent. E.g. CCTV, Surveillance camera. Although the closed-circuit television (CCTV) is common, it is quickly becoming outdated as more video systems lose the closed circuit for signal transmission and are instead transmitting on IP camera networks.
- **Human response**: Trigger appropriate incident responses e.g. by security guards and police.

![Figure 4.12: Physical and Environmental Security system](http://en.wikipedia.org/wiki)
New developments in information and communications technology, as well as new demands on security managers, have widened the scope of physical security apparatus.

Fire alarm systems are increasingly becoming based on Internet Protocol, thus leading to them being accessible via local and wide area networks within organisations. The emergency notification is now a new standard in many industries, as well as physical security information management (PSIM). A PSIM application integrates all physical security systems in a facility and provides a single and comprehensive means of managing all of these resources. It consequently saves on time and cost in the effectual management of physical security. Best Practices for implementing physical and environmental security are listed below [25]:

- Locate system components used to deliver mission critical, confidential, or sensitive programs in a strategically placed location with limited access, and ensure it is an environmentally controlled area. The placement might include an access that is restricted, windowless, temperature controlled area, with special floors, fire protection, Heating, Ventilation, Air Conditioning and Cooling (HVAC), UPS, and walls extending through the ceilings.
- Control access to mission critical and non-mission critical computer hardware, wiring, displays and network by the principle of least privilege (e.g. assigned the fewest privileges consistent with their assigned duties and functions).
- Document system configurations (such as hardware, wiring, displays, and network) and treat it as sensitive information. Any changes should be governed by a formal change management process.
- Ensure physical access security for back-up systems, tapes, and storage media meet or exceed physical access security of the primary facilities and related access controls.
- Monitor and audit access to facilities, computer hardware, wiring, displays, and networks (e.g. badges, cameras, access logs, sign-in sheets, etc.).
- Establish additional controls (such as CCTV or cameras) and special access authorizations for restricted areas (such as network area, server rooms, data center, ...

computer rooms, or any area processing financial implements, such as cash or checks).

- Include contractual language for physical security services (e.g. security guards) by requiring full security clearances for all physical security personnel. The clearances should be completed prior to the security guards reporting to the facility.
- Ensure that security guards check credentials of those entering facilities.
- Establish physical security policies, standards, and guidelines and communicate them to all personnel, including employees, contractors, vendors, and volunteers.
- Establish processes to ensure physical security logs are reviewed and retained according to established policy.

**Figure 4.13: Physical and Environmental Security control Systems**

### 4.9.6 Communications and operations management

System communications protection refers to the key elements used to assure data and systems are available, and exhibit the confidentiality and integrity expected by owners and users to conduct their business. The key elements of system and communications protection are backup protection, denial of service protection, boundary protection, use of validated cryptography (encryption), public access protection and protection from malicious code. Although the elements are described in terms of the technologies needed and/or used for system and communication protection it is really
the processes that administer and monitor the technologies that assure the required level of security.

Operations management refers to implementing appropriate controls and protections on hardware, software, and resources, maintaining appropriate auditing and monitoring, and evaluating system threats and vulnerabilities.

Proper operations management safeguards all of the organization’s computing resources from loss or compromise, including main storage, storage media (e.g. tape, disk, and optical devices), communications software and hardware, processing equipments, standalone computers, and printers. Best Practices for implementing communication and operation management are listed as below: [26]

- Establish procedures to implement an agreed backup policy and strategy, including the extent (e.g. full or differential/incremental), frequency, offsite storage, testing, physical and environmental protection, restoration, and encryption.
- Implement cryptographic or encryption solutions when the confidentiality or sensitivity of information must be maintained while a message is in transit between computing devices and when confidential or sensitive information is stored in a file or database.
- Deploy and regularly update appropriate anti-virus, anti-spyware and file extension blocking solutions at the gateway entry points and on the desktop and server systems to prevent these systems from being compromised.
- Ensure a firewall or other boundary protection mechanism is in place and has the ability to evaluate source and destination network addresses and determine the validity of the service requested.
- Deploy appropriate Intrusion Detection System and Intrusion Prevention System (IDS/IPS) solutions at the correct network locations and monitor to detect attack so an effective detection.
- Implement an appropriate change management process to ensure changes to systems are controlled.

Follows separation of duties by assigning tasks to different personnel, preventing one person from having total control of the security measures.

- Secure certain internal data and systems from other data and systems on the networks.
- Do not place confidential or sensitive data on any application servers, database servers, or infrastructure components that require direct Internet access in the Demilitarized Zone (DMZ). The components that meet these criteria must be placed behind the DMZ where they are not accessible from the Internet and can only interact with DMZ components through a second and more restrictive firewall.

- Establish appropriate procedures to protect documents, computer media, information/data, and system documentation from unauthorized disclosure, modification, removal, and destruction, including suitable measures to properly dispose of media when it is no longer needed.

- Establish procedures and standards to protect information and physical media containing information in transit, including using replica machines, exchange agreements between the organization’s and external parties, transportation of physical media, and monitoring (e.g. audit logging, monitoring system use).

- Implement appropriate levels of security monitoring including intrusion detection, penetration testing, and violation analysis.

- Perform reviews of audit trails on a regular basis to alert an organization’s to inappropriate practices.

- Ensure preventive or detection controls are in place to decrease or identify the threat of unintentional errors or unauthorized users accessing the system and modifying the data.

- Implement appropriate retention policies as dictated by the organization’s policies, standards, legal and business rules.

- Implement appropriate documentation such as security policies and procedures, business contingency plans, disaster recovery plans, and incident response plans, including a plan for cyber attacks, such as a denial of service attack.
4.9.7 Access control

In order to maintain information confidentiality, integrity, and availability, it is important to control access to information. Access control prevents unauthorized users from retrieving, using, or altering information. They are determined by an organization's risks, threats, and vulnerabilities. Banks have many types of resources. They need to ensure that only the intended people can access and need to make sure that these intended users have only the level of access required to accomplish their tasks. These resources can be physical (a facility, sensitive room, or expensive equipment), informational (intellectual property, confidential data), or personnel (employees and contractors). Access control is more than simply requiring usernames and passwords when users want to access resources. It can be much more. There are multiple methods, techniques, technologies, and models that can be implemented. There are different ways to administer control access and there are a variety of attacks that are launched against many of these access control mechanisms.[27]

Access controls are categorized in three ways:

1. **Preventive**: Preventive controls try to stop harmful events from occurring
2. **Detective**: Detective controls identify if a harmful event has occurred
3. **Corrective**: Corrective controls are used after a harmful event to restore the system.

The primary steps in the access control process are shown in Figure 4.14:

![Access Control Process](image)

**Figure 4.14: Access Control Process**

There are four important components of access control identification, authentication, authorization and accounting.

1. **Identification** is the assignment of unique user IDs and password.

2. **Authentication** is the process of proving a user's identity before accessing the system or information. The three different mechanism to authenticate users are based upon:
   
   a. Something a user knows (e.g. PIN, password, phrase, pass code)
   
   b. Something a user has (e.g. smart card, ATM card, token)
   
   c. Something a user is (e.g. retina scan, fingerprint, voice scan)

   If one mechanism providing one of these characteristics is used, it is referred to as one-factor. If two mechanisms are being used then it is called as two-factor authentication. An authentication process that requires all three is referred to as three-factor authentication. For the authentication process to be considered strong authentication it must be at least two-factor.

3. **Authorization** is a process of assigning authenticated subjects access and the right to carry out specific operations depending upon their preconfigured access rights and permissions outlined in access criteria. An access criterion is developed by the administrator or security officer to support and carry out the organization’s security policy.

4. **Accounting** is the final step in the access control process. Limiting user access to the minimum necessary can be challenging. Therefore audit controls should be implemented for holding users accountable for their actions.

The Figure 4.15 shows different types of access control mechanisms.
Figure 4.15: Access Control Mechanisms

4.9.8 Information systems acquisition, development and maintenance:
The process of designing, developing and maintaining business systems needs to include considerations for security from the beginning.

A. Software Development And Acquisition:
Financial institutions obtain software through self development, contracted development, the purchase of pre-written code, or variations of those development and acquisition approaches. The security issues associated with the approaches involve the security controls built into the code and the trustworthiness of the code that is placed into the financial institution’s environment. The security features of the code can be assessed regardless of the means of development or acquisition. The trustworthiness of the code, however, is ascertained differently depending on the availability of information necessary to perform an assessment. Test data consisting of institution data or customer’s data frequently used in development tests or certifications. Appropriate risk mitigation techniques should be employed to protect data from unauthorized disclosure.
Financial institutions should develop security control requirements for new systems, system revisions, or new system acquisitions. Management should define the security control requirements based on their risk assessment process evaluating the value of the information at risk and the potential impact of unauthorized access or damage. Based on the risks posed by the system, management may use a defined methodology for determining security requirements, such as ISO27001 [28].

![Diagram: Information security System Development Life Cycle (SDLC)]

Development environments should be appropriately secured as a part of the overall institution environment. Monitoring of the development environment can assist in assuring that the implemented controls are functioning properly. The information security controls in application software, application development should incorporate appropriate security controls, audit trails, and activity logs. Application security controls should also include validation controls for data entry and data processing. Data entry validation controls include access controls over entry and changes to data, error checks, review of suspicious or unusual data, and dual entry or additional review and authorization for highly sensitive transactions or data. Data processing controls include batch control totals, hash totals of data for comparison after processing, identification of any changes made to data outside the application (e.g. data altering utilities), and job control checks to ensure programs run in correct sequence.

http://www.isaca.org/information_security.pdf
Some applications will require the integration of additional authentication and encryption controls to ensure integrity and confidentiality of the data. Trustworthiness software can contain erroneous or intentional code that introduces covert channels, back-doors, and other security risks into systems and applications. These hidden access points can provide unauthorized access to systems or data, unauthorized communications capabilities, and unauthorized abilities to change the software. The additional controls can exist at various levels, including the network, host, and application layers. Assessment of both self developed and purchased software should consider the development process, the source code, and the history and reputation of the developers or vendors.

B. Development Process
The development process provides important indicators of code reliability. Specific features include:

- Establishment of security requirements, considering the current and expected threat, network, and host environments.
- Use of secure coding standards.
- Tests and reviews for compliance with security requirements.
- Background checks on employees and code development and testing processes.
- Signed nondisclosure agreements to protect the financial institution’s rights to source code and customer’s data as appropriate.
- Restrictions on developer write access to production source code and systems, and monitoring developer access to development systems.
- Physical security over developer work areas, including restrictions on media taken to and from the work area.

C. Systems Maintenance
Financial institutions that introduce reliable systems into their environment should ensure that the systems retain reliability over time. The essential control elements are the development of appropriately hardened systems, usage of standard builds, the appropriate updating of builds and deployed systems through patch
management, and the controlled introduction of changes into the institution’s environment.

Financial institutions use commercial off-the-shelf software for operating systems and applications. For example, a default installation of a server operating system may install mail, web, and file-sharing services on a system whose only function is a DNS. Unnecessary software and services represent a potential security weakness. Their presence increases the potential number of discovered and undiscovered vulnerabilities present in the system. Additionally, system administrators may not install patches or monitor the unused software and services to the same degree as operational software and services. The protection against risks begins when the systems are constructed and software installed through a process that is referred to as hardening a system. When deploying off-the-shelf software, management should harden the resulting system. The hardening includes the following actions:

- Determining the purpose of the system and minimum software and hardware requirements.
- Documenting the minimum hardware, software, and services to be included on the system.
- Installing the minimum hardware, software, and services necessary to meet the requirements using a documented installation procedure.
- Installing necessary patches.
- Installing the most secure and up-to-date versions of applications.
- Configuring privilege and access controls by first denying all, then granting back the minimum necessary to each user.
- Configuring security settings as appropriate, enabling allowed activity, and disallowing other activity.
- Enabling logging
- Creating cryptographic hashes of key files.
- Archiving the configuration and checksums in secure storage prior to system deployment.
- Testing the system to ensure a secure configuration.
Using secure replication procedures for additional, identically configured systems, making configuration changes on a case-by-case basis.

- Changing all default passwords.
- Testing the resulting systems.

D. Testing The Resulting Systems
After deployment, systems may need updating with current security patches. Additionally, the systems should be periodically audited to ensure that the software present on the systems is authorized and properly configured.

E. Audits and Monitoring
To maintain operational assurance, organizations use two basic methods as system audits and monitoring. These terms are used loosely within the computer security community and often overlap. A system audit is a one-time or periodic event to evaluate security. Monitoring refers to an ongoing activity that examines either the system or the users. In general, the more "real-time" an activity is, the more it falls into the category of monitoring.[29]

4.9.9 Information Security Incident Management
Definition:

Wikipedia defines information security Incident Management as

“Information Security Incident Management involves the monitoring and detection of security events on a computer or computer network, and the execution of proper responses to those events.”

ISACA:

“Information Security Incident Management is the operational part of risk management. It is the activities that take place as a result of unanticipated attacks, losses, theft, accidents, or any other unexpected adverse events that occur as a result of the failure or lack of controls.”

Effective management and response to information security incidents is critical to maintaining secure operations within the organization. Organization minimum must:

- Ensure that information security incident management procedures are established to ensure appropriate responses in the event of information security incidents, breaches or system failures.
- Ensure all information security incidents are reported and escalate (where applicable) through appropriate management channels and/or authorities.
- Establish and maintain an information security incident and response register and record all incidents.
- Ensure that information security incidents caused by employees are investigated and where it is found that accidental information security violation or breach has occurred that formal disciplinary processes are applied.

4.9.10 Business continuity management

Business continuity management is the business process that sets the objectives, scope and requirements for IT service continuity management. Business Continuity Management (BCM) is responsible for managing risks that could seriously impact the business. BCM ensures that the business can operate to a minimum agreed level by reducing the risk to an acceptable level and planning to restore business processes (source: ITIL).

Business continuity planning (BCP) involves the processes and procedures for the development, testing and maintenance of plans that enable an organisation to continue operating during and after a disaster. Business continuity plans are typically designed to handle incidents affecting all the organization's business critical processes and activities from failure of a single server all the way through to complete loss of a major facility. BCP is a response to an enterprise level risk assessment.

ISACA defines “BCM is an ongoing management and governance process supported by senior management and resourced to ensure that the necessary steps are taken to identify the impact of potential losses, manage risk, develop resiliency, maintain practical recovery strategies and plans and ensure continuity of products or services through exercising, preparation, testing, training, maintenance and assurance”.
A systematic procedure is necessary to design the business continuity management process. The business continuity management process consists of the following phases:\(^\text{[30]}\):

1. **Initiate BCM**
2. **Contingency planning**
3. **Implementation of the contingency planning concept**
4. **Business continuity response**
5. **Tests and Training**
6. **Maintenance and continuous improvement of the BCM process**

Before business continuity management can be established in an organization, the general conditions must be determined. A policy for business continuity management must be created, and the policy must be initiated, developed, and released by the management. In addition, the organizational prerequisites for business continuity management must be met. To do this, the roles and responsibilities must be specified, and an adequate budget must be provided for it by the organization’s management. The successful integration of the subject of business continuity management into the existing organization culture is decisive for the success of the business continuity management process. The employees must be integrated into the process and must be prepared for their roles through awareness and training programs to accomplish this.

**4.9.11 Regulatory Compliance**

With increasing regulatory norms being enforced for organization to ensure the confidentiality, integrity and availability of important information assets, information security compliance or regulatory compliance has become one of the most important controls in information security. The regulatory compliance issues should concern the board, not just the IT department, and include issues of data governance, the data protection act, operational risk, information security and best practices.

Some organizations still receive little management support or funding for a sound information security policy program. Within the last several years, however, numerous federal, state and international regulations have been passed that require the protection of information. Many of the organizations are now enhancing their information security policies in response to legal and regulatory requirements.

- Compliance and Best Practice

In some cases, these regulations are very specific about the requirements for written security and privacy policies. In other cases, a regulation simply requires safeguards that are appropriate for the size and type of organization. In these cases, enforcement agencies and auditors must defer to accepted best practices or frameworks for guidance, all of which require written policies. Examples of these are the **Generally Accepted Information Security Principles (GAISP)**, **Control Objectives for Information Technology (COBIT)** and **ISO/IEC 17799, ISO 27001, ITIL (Information Technology Infrastructure Library)** are all potentially part of a best-practice approach to regulatory and corporate governance compliance. The challenge for many organisations is to establish a coordinated, integrated framework that draws on all of these standards. The Joint Framework, combining COBIT and ITIL is a good starting place [31]. ISO27001, the international standard for an information security system, also sets out a best practices approach. This standard links to all the IT-related regulations and provides completely independent structured guidance for a risk-based approach for securing the confidentiality, availability and integrity of information. It also provides the general control environment within which the specific controls of an internal control structure can most effectively operate.

[31] http://www.itgovernance.co.uk
<table>
<thead>
<tr>
<th>Regulation/ Framework</th>
<th>Industry/ Organization</th>
<th>Policy Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC 17799</td>
<td>Security Framework</td>
<td>A written policy document should be available to all employees responsible for information security.</td>
</tr>
<tr>
<td>GAISP - Generally</td>
<td>Security Framework</td>
<td>Management shall ensure that policy and supporting standards, baselines, procedures, and guidelines are developed and maintained to address all aspects of information security.</td>
</tr>
<tr>
<td>GAISP - Generally</td>
<td>Information Security</td>
<td>The ISO / IEC 27000 family is a series of information security standards developed and published by the International Standards Organisation (ISO) and the International Electrotechnical Commission (IEC). These standards provide a globally recognised framework for best practice information security management.</td>
</tr>
</tbody>
</table>

**Table No. 4.2: Regulatory Requirements for Information Security Policies**

Source: http://www.informationshield.com/securitypolicyregulatoryrequirements.html

**4.10 Information Security Framework**

The ISMS standards specify a framework for organisations to manage information security aspects of their business, and if necessary to demonstrate to other parties (e.g. business partners, auditors, customers and suppliers) their ability to manage information security. It specifies a risk-based security management system that is designed to ensure that organisations select and operate adequate and proportionate
(i.e. cost effective) security controls to protect information assets. It uses the ‘plan-do-check-act (improve)’ model. The Figure 4.17 shows the ISO 27001 ISMS framework steps for successfully implementation of information security management system. This framework consists of major 12 steps as listed below:

1. Obtain management support
2. Define ISMS scope
3. Inventory of information assets
4. Perform risk assessment
5. Prepare risk assessment report
6. Prepare Statement of Applicability (SOA)
7. Plan-Do-Check-Act (PDCA) model
8. ISMS Implementation Programme
9. Information Security Management System (ISMS)
10. Compliance Review and Corrective Actions
11. Pre-Certification Assessment
12. Certification Audit
Figure 4.17: ISO 27001 ISMS Framework
Source: http://www.iso27001security.com/html/iso27k_toolkit.html
The ISO 27001 ISMS steps are listed below [32]

1. **Obtain management support**

Management plays an important role in the success of ISMS. Management must make a commitment to the establishment, implementation, operation, monitoring, review, maintenance, and improvement of the ISMS. Commitment must include activities such as ensuring that the proper resources are available to work on the ISMS and that all employees affected by the ISMS have the proper training, awareness, and competency. Management should actively support information security by giving clear direction (e.g. policies), demonstrating the organization’s commitment, plus explicitly assigning information security responsibilities to suitable people. Management should approve the information security policy, allocate resources, assign security roles and co-ordinate and review the implementation of security across the organization. Management support makes information security more effective throughout the organization, not least by aligning it with business and strategic objectives.

2. **Defining ISMS scope**

Management should define the scope of the ISMS in terms of the nature of the business, the organization, its location, information assets and technologies. Any exclusion from the ISMS scope should be justified and documented. Areas outside the ISMS are inherently less trustworthy, hence additional security controls may be needed for any business processes passing information across the boundary. Descoping usually reduces the business benefits of the ISMS. If commonplace controls are deemed not applicable, this should be justified and documented in the Statement of Applicability (SOA). The certification auditors will check the documentation.

3. **Inventory of Assets**

An inventory of all important information assets should be developed and maintained, recording details such as:

- Type of asset

---

4. Risk Assessment
Risk assessments should identify, quantify, and prioritize information security risks against defined criteria for risk acceptance and objectives relevant to the organization. The results should guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks. Assessing risks and selecting controls need to be performed repeatedly across different parts of the organization and information systems, and to respond to changes. The process should systematically estimate the magnitude of risks (risk analysis) and compare risks against risk criteria to determine their significance (risk evaluation). The information security risk assessment should have a clearly defined scope and complement risk assessments in other aspects of the business, where appropriate.

5. Prepare Statement of Applicability (SOA)
The Statement of Applicability (SOA) is a key ISMS document listing the organization’s information security control objectives and controls. The SOA is derived from the results of the risk assessment, where:

- Risk treatments selection
- All relevant legal and regulatory requirements have to be identified
- Understood contractual obligations
- Conduct a review of the organization’s own business needs and requirements

6. Plan-Do-Check-Act (PDCA) model
The "Plan-Do-Check-Act" (PDCA) model applies at different levels throughout the ISMS.
The ISMS takes as input the information security requirements and expectations and through the PDCA cycle produces managed information security outcomes that satisfy those requirements and expectations.

1. **Plan (Establish the ISMS):** Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization’s overall policies and objectives.

2. **Do (Implement and Operate the ISMS):** Implement and operate the ISMS policy, controls, processes and procedures.

3. **Checks (Monitors and Review the ISMS):** Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.

4. **Act (Maintain and Improve the ISMS):** Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

7. **ISMS Implementation Programme**

Implement the Risk Treatment Plan in order to achieve the identified control objectives, which includes consideration of funding and allocation of roles and responsibilities. Implement controls selected during establishing the ISMS to meet the control objectives.

Define how to measure the effectiveness of controls to allow managers and staff to determine how well controls achieve planned control objectives. Implement security training and awareness programmes.

8. **Information Security Management System (ISMS)**

It is important to be able to demonstrate the relationship from the selected controls back to the risk assessment and risk treatment process, and subsequently back to the ISMS policy and objectives. ISMS documentation should include:

a. Documented statements of the ISMS policy and objectives

b. The scope of the ISMS
c. Procedures and other controls in support of the ISMS  
d. A description of the risk assessment methodology  
e. A risk assessment report and Risk Treatment Plan (RTP)  
f. Procedures for effective planning, operation and control of the information security processes, describing how to measure the effectiveness of controls  
g. Various records specifically required by the standards  
h. The Statement of Applicability (SOA).  

9. Compliance Review and Corrective Actions  
Management must review the organization’s ISMS at least once a year to ensure its continuing suitability, adequacy and effectiveness. They must assess opportunities for improvement and the need for changes to the ISMS, including the information security policy and information security objectives. The results of these reviews must be clearly documented and maintained. Reviews are part of the ‘Check’ phase of the PDCA cycle, any corrective actions arising must be managed accordingly.  

10. Pre-Certification Assessment  
Prior to certification, the organization should carry out a comprehensive review of the ISMS and SOA. The organization need to demonstrate compliance with both the full PDCA cycle, the requirement for continual improvement. Certification auditors seek evidence (in the form of records of processes such as risk assessments, management reviews, incident reports, corrective actions etc.) that the ISMS is operating and continually improving. The ISMS therefore needs a while to settle down, operate normally and generate the records after it has been implemented.  

11. Certification Audit  
Certification involves the organization’s ISMS being assessed for compliance with ISO27001. The certification body needs to gain assurance that the organization’s information security risk assessment properly reflects its business activities for the full scope of the ISMS. The assessors check that the organization has properly analysed and treated its information security risks and continues managing its information security risks systematically. A certificate of compliance from an accredited certification body has credibility with other organizations. The
organization must continually improve the effectiveness of the ISMS through the use of:

- The information security policy
- Information security objectives
- Audit results
- Analysis of monitored events
- Corrective and preventive actions
- Management review

4.11 Introduction to CORE Banking

The world is changing rapidly and technology is considered to be the key driver for these changes around us. Many activities are handled electronically due to the acceptance of information technology at home as well as at workplaces. The Indian customers are moving towards the internet banking. The ATM and the Net transactions are conventionally adopted. But the customer is clear on one thing that he wants net-banking to be simple and secure. CORE is a generic term for the delivery of banking services and products through the electronic channels such as the telephone, the internet, the mobile phone etc. The concept and scope of CORE banking is still evolving. It facilitates an effective payment and accounting system thereby enhancing the speed of delivery of banking services significantly. Several initiatives have been taken by the Government of India as well as the RBI (Reserve Bank of India) to facilitate the development of CORE banking in India. The government of India enacted the IT Act, 2000, which provides legal recognition to electronic transactions and other means of electronic commerce. The RBI has been preparing to upgrade itself as regulator and supervisor of the technologically dominated financial system. It issued guidelines on the risks and controls in computer and telecommunication systems to all the banks of India, advising them to evaluate the risks inherent in the systems and put in place adequate control mechanisms to address these risks.

Banking business has evolved over a period and grown exponentially encompassing an entire range of products and transactions under a wide umbrella. All such activities undertaken by the bank is called core banking. "Centralized Online Real-time environment". This basically means that the entire bank's branches access applications
from centralized data centres. This means that the deposits made are reflected immediately on the bank's servers and the customer can withdraw the deposited money from any of the bank's branches throughout the world. These applications now also have the capability to address the needs of corporate customers, providing a comprehensive banking solution.

The CORE banking policy has been approved by the board of directors. The policy fits into the banks overall Information Technology and information security policy and ensures confidentiality, integrity and accountability of information and information processing security system.

- **What is CORE Banking?**

CORE (Centralised Online Real-time Environment) banking enables anytime anywhere banking. The bank customers can operate their accounts from anywhere 24X7. The customers are no more the customer of a branch. He becomes the bank’s customer. Thus CBS is a step towards enhancing customer convenience through anywhere and anytime banking. This is achieves through the centralised processing of transactions. All the transaction is processed at central site called as data centre where all the data relating to core branches resides.

![Figure 4.18: CORE Banking, Source: www.google.com](image)

Thus the core banking in simple terms is a highly efficient “customer accounting” and transaction processing engine for high volumes of back office transactions. The
The purpose of a core banking system is thus to give banks the ability to process large transaction volumes in a fast and efficient way.

Core banking also handles transactions such as interest and fee calculation, pre-processing for statement printing, end-of-day processing, and consolidation of daily individual transactions as “accounting entries” which are posted into the bank’s general ledger system according to its chart of accounts structure for the daily trial balance sheet preparation. The CBS process is advantageous both to the customers and the banks.

4.12 History of CORE Banking

The IT revolution had a great impact in the Indian banking system. The use of computers had led to introduction of online banking in India. The use of the modern innovation and computerisation of the banking sector of India has increased many folds after the economic liberalisation of 1991 as the country's banking sector has been exposed to the world's market. The Indian banks were finding it difficult to compete with the international banks in terms of the customer services without the use of the information technology and computers.[33]

- In 1984 formed the committee on mechanisation in the Banking Industry (1984) whose chairman was Dr. C. R. Rangarajan, Deputy Governor, Reserve Bank of India. The major recommendations of this committee were introducing MICR (Magnetic Ink Character Recogniser) technology in all the banks in the metropolis in India. This provided use of standardized cheque forms and encoders.

- In 1988, the RBI set up the committee on computerisation in banks (1988) headed by Dr. C. R. Rangarajan which emphasized that settlement operation must be computerized in the clearing houses of RBI in Bhubaneshwar, Guwahati, Jaipur, Patna and Thiruvananthapuram. It further stated that there should be National Clearing of inter-city cheques at Kolkata, Mumbai, Delhi, Chennai and MICR should be made operational. It also focused on computerisation of branches and increasing connectivity among branches through computers. It also suggested modalities for implementing online banking. The committee submitted its reports in 1989 and computerisation began from 1993 with the settlement between IBA and bank employees' association.

[33] http://en.wikipedia.org/wiki/Banking_in_India
In 1994, committee on Technology Issues relating to payment systems, Cheque clearing and securities settlement in the Banking Industry (1994) was set up under chairman Shri. W. S. Saraf. It emphasized Electronic Funds Transfer (EFT) system, with the BANKNET communications network as its carrier. It also said that MICR clearing should be set up in all branches of all banks with more than 100 branches.


4.13 Need for CORE Banking

In order to meet the requirements and needs of the IT modernization as per direction given by Reserve Bank of India core banking solution (CBS) is be implemented across India covering all the urban cooperative banks.

Core Banking Solution (CBS) is networking of all the bank’s branches which enables customers to operate their accounts and avail account related services from anywhere at any times on CBS network, regardless of where he maintains his account. The customer is no more the customer of a branch; he becomes the customer of the bank.

Thus CBS is a step towards enhancing customer convenience through “Anywhere and Anytime Banking”

4.13.1 Benefits of core banking solution

- **Increase operational efficiency - Reduce cost of operations:** CBS provide anytime and anywhere banking. Core banking provides various alternative delivery service channels, which reduce cost and time required to complete the transactions. The centralized process of CBS also increases the efficiency by reducing the duplication and redundancy of work on branch level and Head Office (HO).

- **Improve customer service and satisfaction:** Core banking provides various alternative delivery service channels (ATM, Internet, Phone, SMS and Mobile Banking) on 24 X 7 basis, which allows to increase quality of the service provided to the customers and allow customer to operate their account from anywhere at any time. Customer gets full attention and service satisfaction at the branches as the branches are freed from all back office functions, clearing
functions and almost all accounting functions. Customer can receive SMS alerts on his mobile or e-mail alerts through net for transaction taking place in his account. This gives him comfort and security.

- **Timely effective Decision Making**: CBS provide timely and accurate information for management decision making. Better MIS and reporting to external agencies such as Govt., RBI etc. All the transactions of the banks directly impact the General Ledger and Profit and Loss Account. This provides a real time total depiction about the financial position and situation of the banks.

- **Integrate with electronic payment systems**: Integration with electronic payment systems allow banks to participate in an inter-operable electronic payment network run by the National Payments Corporation of India. This help in fast and safe transfer of funds through National Electronic Fund Transfer (NEFT) and Real Time Gross Settlement (RTGS).

- **Customer Relationship Management**: In order to enhance the effectiveness of the various channels such as branch banking, mobile banking, internet banking, and banks may consider the use of a comprehensive customer relationship management (CRM) solution which enables the user to access the entire customer details and provides a 360 degree view across channels and products and enhances service quality. This enables customer interactions across various touch points (such as a call or email) to be captured on a centralized single system. Banks need to transit from transaction orientation to customer orientation.

- **Standardized and Automated business process**: Banks can deliver needed business service more faster by introducing modular business services comprised of common data, business rules and processes that can be configured quickly to get new products and services to market with less risk and cost. Back office performance can be improved by monitoring operations of system performance.

- **Strong audit and internal controls and Compliance**: The integrated process consisting of the internal control system and the internal audit system which involve monitoring, independent evaluation and timely reporting to management levels systematically in order to ensure that all the bank’s activities are performed in accordance with current policies and standard, methods, instructions.
4.13.2 Challenges in front CORE banking Solution

The security and availability of IT systems, networks and data is critical importance in terms of ensuring business continuity. Security breaches mostly fall into three categories:

1. Serious criminal intent (fraud, theft of commercially sensitive or financial information)
2. Hackers attack, Phishing attacks (defacement of web sites or ‘denial of service’ - causing web sites to crash)
3. Flaws in systems design and/or set up leading to security breaches

All of these threats have potentially serious financial, legal and reputational implications. Many banks are finding that their systems are being probed for weaknesses hundreds of times a day but damage/losses arising from security breaches have so far tended to be minor. However some banks could develop more sensitive burglar alarms, so that they are better aware of the nature and frequency of unsuccessful attempts to break into their system. The most sensitive computer systems, such as those used for high value payments or those storing highly confidential information, be likely to be the most carefully secured. Complex encryption software is used to protect account information. However, there are no perfect systems. Accounts are prone to hacking attacks, phishing, malware and illegal activities.

4.14 Technology Development in Indian Banking Sector: [34]

Developments in the field of Information Technology (IT) strongly support the growth and inclusiveness of the banking sector, thereby facilitating inclusive economic growth. IT not only enhances the competitive efficiency of the banking sector by strengthening back-end administrative processes but it also improves the front-end operations and helps in bringing down the transaction costs for the customers. It has the potential of furthering financial inclusion by making small ticket retail transactions cheaper, easier and faster for the banking sector as well as for the

small customers. The Reserve Bank has, thus, been actively involved in harnessing technology for the development of the Indian banking sector over the years.

Information Technology has basically been used under two different avenues in banking. One is communication and connectivity and other is business process reengineering. Information technology enables sophisticated product development, better market infrastructure, implementation of reliable techniques for control of risks and helps the financial intermediaries to reach geographically distant and diversified markets. In view of this, technology has changed the contours of three major functions performed by banks i.e. access to liquidity, transformation of assets and monitoring of risks. Further, Information technology and the communication networking systems have a crucial bearing on the efficiency of money, capital and foreign exchange markets.

The software packages for banking applications in India had their beginnings in the middle of 80s, when the banks started computerizing the branches in a limited manner. The early 90s saw the plummeting hardware prices and advent of cheap and inexpensive but high-powered PCs and servers and banks went in for what was called Total Branch Automation (TBA) Packages. The middle and late 90s witnessed the tornado of financial reforms, deregulation, globalization etc. coupled with rapid revolution in communication technologies and evolution of novel concept of 'convergence' of computer and communication technologies, like Internet, mobile / cell phones etc.

In India, banks as well as other financial entities entered the world of information technology and with Indian Financial Net (INFINET). INFINET, a wide area satellite based network (WAN) using VSAT (Very Small Aperture Terminals) technology, was jointly set up by the Reserve Bank and Institute for Development and Research in Banking Technology (IDRBT) in June 1999. The Indian Financial Network (INFINET) which initially comprised only the public sector banks was opened up for participation by other categories of members.

The first set of applications that could benefit greatly from the use of technological advances in the computer and communications area relate to the payment systems
which form the lifeline of any banking activity. The process of reforms in payment and settlement systems has gained momentum with the implementation of projects such as NDS (Negotiated Dealing System), CFMS (Centralized Funds Management System) for better funds management by banks and SFMS (Structured Financial Messaging Solution) for secure message transfer. This would result in funds transfers and funds-related message transfer to be routed electronically across banks using the medium of the INFINET. Negotiated dealing system (NDS), which has become operational since February 2002 and RTGS (Real Time Gross Settlement system) scheduled towards the end of 2003 are other major developments in the area.

Internet has significantly influenced delivery channels of the banks. Internet has emerged as an important medium for delivery of banking products and services. The detailed guidelines of RBI for Internet Banking have prepared the necessary ground for growth of Internet banking in India. The Information Technology Act, 2000 has given legal recognition to creation, transmission and retention of an electronic (or magnetic) data to be treated as valid proof in a court of law, except in those areas, which continue to be governed by the provisions of the Negotiable Instruments Act, 1881.

As stated in RBI's Annual Monetary and Credit Policy 2002-2003: "To reap the full benefits of such electronic message transfers, it is necessary that banks confer sufficient attention on the computerization and networking of the branches situated at commercially important centers on a time-bound basis. Intra-city and intra-bank networking would facilitate in addressing the "last mile" problem which would in turn result in quick and efficient funds transfers across the country".

A major technological development in banking sector is the adoption of the Core Banking Solutions (CBS). CBS is networking of branches, which enables customers to operate their accounts and avail of banking services from any branch of the bank on CBS network, regardless of where the customer maintains his/her account. The customer is no more the customer of a branch as he becomes the bank’s customer. Thus, CBS is a step towards enhancing, customer convenience through, anywhere, anytime banking. It is important to leverage on to this technological advancement to
look at areas beyond CBS that can help in not just delivering quality and efficient services to customers but also generating and managing information effectively.

4.14.1 Recent Technology Development in banking Sector \[35][36][37]

1. Development of National Payment Systems: The payment system could be broadly divided in two segments:
   a. Paper-based Payments: Use of paper-based instruments (like cheques, drafts etc.) account for nearly 60 percent of the volume of total non-cash transactions in the country. In value terms, the share is presently around 11 percent. Reserve bank of India had introduced Magnetic Ink Character Recognition (MICR) technology for speeding up and bringing in efficiency in processing of cheques. The recent developments in paper-based instruments include launch of Speed Clearing (for local clearance of outstation cheques drawn on core-banking enabled branches of banks) and introduction of cheque truncation system (to restrict physical movement of cheques and enable use of images for payment processing).

   b. Electronic Payments: The overall thrust is to reduce the use of paper for transactions and move towards electronic mode. Following are various electronic payment services available in the country:
      - Electronic Clearing Service (ECS)/National ECS (NECS): ECS is an electronic mode of payment / receipt for transactions that are repetitive and periodic in nature. ECS is used by institutions for making bulk payment of amounts towards distribution of dividend, interest, salary and pension etc. or for bulk collection of amounts towards telephone / electricity / water

\[35\] http://www.banknetindia.com/special/itb1.htm
\[36\] Dr. T. Sreelatha, CH. Chandra Sekhar, Role of Technology in Indian Banking Sector, International Journal of Management & Business studies, Vol 2, ISSUE 4 Dec 2012.ISSN: 2230-9519 (Online)
\[37\] Prof. M.C. Sharma, Abhinav Sharma, Role of Information Technology in Indian Banking Sector, International Journal in Multidisciplinary and Academic Research (SSIJMAR), Vol. 2, No. 1, ISSN 2278 –5973
• dues, tax collections, loan installment repayments, periodic investments in mutual funds and insurance premium etc. Basically ECS facilitates bulk transfer of monies from one bank’s account too many banks accounts or vice versa.

• National Electronic Funds Transfer (NEFT): NEFT is a payment system facilitating one-to-one funds transfer. Under this, individuals, firms and corporate can electronically transfer funds from any bank branch to any individual, firm or corporate having an account with any other bank branch in the country participating in the scheme. Thus, this is an interbank fund transfer system.

• Real Time Gross Settlement (RTGS) System: This Real Time Gross Settlement is a continuous (real-time) settlement of funds transfer individually on an order by order basis. ‘Real Time’ means the processing of instructions at the time they are received rather than at some later time. ‘Gross Settlement’ means the settlement of funds transfer instruction occurs individually (on an instruction by instruction basis). Considering that the funds settlement takes place in the books of the Reserve Bank of India, the payments are final and irrevocable.

• Pre-paid Payment Systems: Pre-paid instruments are payment instruments that facilitate purchase of goods and services against the value stored on these instruments. The pre-paid payment instruments can be issued in the form of smart cards, magnetic stripe cards, internet accounts, internet wallets, mobile accounts, mobile wallets and paper vouchers etc.

• Point of Sale (POS) Terminals / Online Transactions: There are over five lakhs POS terminals in the country, which enable customers to make payments for purchases of goods and services by means of credit/debit cards. To facilitate customer convenience the banks have also permitted cash withdrawal using debit cards issued by the banks at POS terminals.

2. Automatic Teller Machine (ATM): Automatic Teller Machine is the most popular devise in India, which enables the customers to withdraw their money 24 hours a day, 7 days a week. It is a device that allows customers who have an Automatic Teller Machine (ATM) card to perform routine banking transactions
without interacting with a human teller. In addition to cash withdrawal, Automatic Teller Machines (ATMs) can be used for payment of utility bills, funds transfer between accounts, deposit of cheques and cash into accounts, balance enquiry etc.

3. **Cash Dispensers:** Cash withdrawal is the basic service rendered by the bank branches. The cash payment is made by the cashier or teller of the cash dispenses is an alternate to time saving. The operations by this machine are cheaper than manual operations and this machine is cheaper and faster than that of ATM. The customers are provided with a plastic card, which is magnetically coated. After completing the formalities, the machine allows the transactions for required amount.

4. **Chip Card:** The customers of the banks are provided with a special type of credit card which bears customer’s name, code etc. The credit amount of the customer account is written on the card with magnetic methods. The computer can read these magnetic spots. When the customer uses this card, the credit amount written on the card starts decreasing. After use of number of times, at one stage, the balance becomes nil on the card. At that moment, the card is of no use. The customers have to deposit cash in their account for reuse of the card. Again the credit amount is written on the card by magnetic means.

5. **Phone Banking:** Customers can now dial up the bank’s designed telephone number and he by dialing his ID number will be able to get connectivity to bank’s designated computer. The software provided in the machine interactive with the computer asking him to dial the code number of service required by him and suitably answers him. By using Automatic voice recorder (AVR) for simple queries and transactions and manned phone terminals for complicated queries and transactions, the customer can actually do entire non-cash relating banking on telephone anywhere, anytime.

6. **Tele-banking:** Tele banking is another innovation, which provided the facility of 24 hour banking to the customer. Tele-banking is based on the voice processing facility available on bank’s computers. The caller usually a customer calls the
bank anytime and can enquire balance of his account or other transaction history. In this system, the computers at bank are connected to a telephone link with the help of a modem. The voice processing facility provided in the software. This software identifies the voice of caller and provides him suitable reply. Some banks also use telephonic answering machine but this is limited to some brief functions. This is only telephone answering system and now Tele-banking. Tele banking is becoming popular.

7. **Internet Banking:** Internet banking enables customers to do banking transactions through the bank’s website on the Internet. It is a system of accessing accounts and general information on bank products and services through a computer while sitting in his/her office or home. This is also called as virtual banking. It is more or less bringing the bank to your computer. In traditional banking one has to approach the branch in person, to withdraw cash or deposit a cheque or request a statement of accounts etc. but internet banking has changed the way of banking. One can operate all these type of transactions on his computer through website of the bank. All such transactions are encrypted using sophisticated multi-layered security architecture, including firewalls and filters. One can be rest assured that one’s transactions are secure and confidential.

8. **Mobile Banking:** Mobile banking facility is an extension of internet banking. The bank in association with the cellular service providers offers this service. For this service, mobile phone should either be SMS or WAP enabled. These facilities are available even to those customers with only credit card accounts with the bank.

9. **Any where Banking:** With expansion of technology, it is now possible to obtain financial details from the bank from remote locations. Basic transaction can be effected from faraway places. Automated Teller Machines are playing an important role in providing remote services to the customers. Withdrawals from other stations have been possible due to inter-station connectivity of ATM’s. The Rangarajan committee had also suggested the installation of ATM at non-branch locations, airports, hotels, railway stations. Remote Banking is being further extended to the customer’s office and home.
10. **Voice Mail:** Talking of answering systems, there are several banks mainly foreign banks now offering very advanced touch tone telephone answering service which route the customer call directly to the department concerned and allow the customer to leave a message for the concerned desk or department, if the person is not available.

### 4.15 Technological requirement for core banking solution (CBS)

In core banking solution all the server are centrally located called as the central data centre. All the branches are connected to the data centre through a leased line or any other network connectivity with security and redundancy built in. The Figure 4.19 depicts the technology and connectivity details in the implementation of CBS. [38]

![Data Centre Network Diagram](image)

*Figure 4.19: Data Centre Network Diagram*

Source: Core Banking Solution: Evaluation Of Security and Controls

Most of the servers like application server and database server are placed behind the firewall and protected from unauthorised access. In order to manage load and also to build redundancy, multiple server performing the same function are clustered. All the

servers are not in same local area network (LAN). They are segregated using the concept of virtual local area network (VLAN) which has its own built in security.

**Technology Requirements**

CORE banking environment consist of

- Central Database Server that store the data of the bank.
- Application architecture /Central Application Server that run the CORE banking solution (CBS) centrally accessed by branches.
- Necessary infrastructure to provide for internet banking and Automated Teller Machine (ATMs).
- Authentication techniques
- Information Security system

### 4.15.1 Application Architecture Requirements

A computer-based application may be built as a huge software, or may be structured to run on a client–server environment, or even have three or multi-tiered architecture. A computer application typically separates its three main tasks: interactions with the user, processing of transactions as per the business rules, and the storage of business data. The three tasks can be viewed as three layers, which may run on the same system (possibly a large, proprietary computer system), or may be separated on to multiple computers (across the Internet), leading to three-tier or multi-tier architecture. These layers can be briefly described as follows [39]:

- **Presentation Layer**: This layer is responsible for managing the front-end devices, which include browsers on personal computers, Personal Digital Assistants (PDAs), mobile phones, Internet kiosks, Web TV etc. The presentation layer takes care of user interface related issues like display details, color, layout, image etc. It also has important responsibilities in user authentication and session management activity.

- **Application layer**: It contains the business logic (for processing of data and transactions) and necessary interfaces to the data layer. It processes requests from the presentation layer, connects to the data layer, receives and processes the information and passes results back to the presentation layer. It is responsible for

ensuring that all the business rules are incorporated in the software. The issues of scalability, reliability and performance of the services to a great extent depend upon the application layer architecture.

- **Data Layer**: The data layer uses a database package to store, retrieve and update application data. The database may be maintained on one or multiple servers. A database package also supports back-up and recovery of data, as well as logging of all transactions.

- **System & Network logging**: Operating systems, database packages and even business applications produce a ‘log’ of various tasks performed by them. Most operating systems keep a log of all user actions. Log files are the primary record of suspicious behavior. Log files alert the administrator to carry out further investigation in case of suspicious activity and help in determining the extent of intrusion. Log files can also provide evidence in case of legal proceedings. The administrator has to select types of information to be logged, the mechanisms for logging, locations for logging, and locations where the log files are stored. The information required to be logged should include login/logout information, location and time of failed attempts, changes in status, status of any resource, changes in system status such as shutdowns, initializations and restart, file accesses, change to file access control lists, mail logs, modem logs, network access logs, web server logs, etc. The log files must be protected and archived regularly and securely.

### 4.15.2 Computer Networking and Internet[^40]

The purpose of computer networking is sharing of computing resources and data across the whole organization and the outside world. Computer Networks can be primarily divided into two categories based on speed of data transfers and geographical reach. A Local area network (LAN) connects many servers and workstations within a small geographical area, such as a floor or a building. Some of the common LAN technologies are 10MB Ethernet, 100 MB Ethernet, 1GB Ethernet, Fiber Distributed Data Interface (FDDI) and Asynchronous Transfer Mode (ATM).

[^40]: Report on Internet Banking (Part 1 of 2)
The data transfer rates here are very high. They commonly use broadcast mode of data transfer. The Wide Area Network (WAN), on the other hand, is designed to carry data over great distances and is generally point-to-point. Connectivity in WAN set-up is provided by using dial-up modems on the Public Switched Telephone Network (PSTN) or leased lines, VSAT networks, an Integrated Services Digital Network (ISDN) or T1 lines, Frame Relay/X.25 (Permanent Virtual Circuits), Synchronous Optical Network (SONET), or by using Virtual Private Networks (VPN) which are software-defined dedicated and customized services used to carry traffic over the Internet. The different topologies, technologies and data communication protocols have different implications on safety and security of services.

To standardize on communications between systems, the International Organization of Standards developed the OSI model (the Open System Interconnection Reference Model) in 1977. The OSI breaks up the communication process into 7 layers and describe the functions and interfaces of each layer. The important services provided by some of the layers are mentioned below. It is necessary to have a good understanding of these layers for developing applications and for deploying firewalls.

- **Application Layer**: Network Management, File Transfer Protocol, Information validation, Application-level access security checking.
- **Session Layer**: Establishing, managing and terminating connections (sessions) between applications.
- **Transport Layer**: Reliable transparent transfer of data between end points, end to end recovery and flow control.
- **Network Layer**: Routing, switching, traffic monitoring and congestion control, control of network connections, logical channels and data flow.
- **Data Link Layer**: Reliable transfer of data across physical link and control of flow of data from one machine to another.

**Protocols**: The data transmission protocol suite used for the Internet is known as the Transmission Control Protocol/Internet Protocol (TCP/IP). The Internet is primarily a network of networks. The networks in a particular geographical area are connected into a large regional network. The regional networks are connected via a high speed 'back bone'. The data sent from one region to another is first transmitted to a Network Access Point (NAP) and are then routed over the backbone. Each computer connected
to the Internet is given a unique IP address (such as 142.16.111.84) and a hierarchical domain name (such as cse.iitb.ernet.in). The Internet can be accessed using various application-level protocols such as FTP (File Transfer Protocol), Telnet (Remote Terminal Control Protocol), Simple Mail Transport Protocol (SMTP), Hypertext Transfer Protocol (HTTP). These protocols run on top of TCP/IP. The most innovative part of the Internet is the World Wide Web (WWW). The web uses hyperlinks, which allow users to move from any place on the web to any other place. The web consists of web pages, which are multimedia pages composed of text, graphics, sound and video. The web pages are made using Hypertext Markup Language (HTML). The web works on a client-server model in which the client software, known as the browser, runs on the local machine and the server software called the web server runs on a possibly remote machine. Some of the popular browsers are Microsoft Internet Explorer and Netscape Navigator.

With the popularity of web, organizations find it beneficial to provide access to their services through the Internet to its employees and the public. In a typical situation component of the application runs (as an ‘applet’) within the browser on user’s workstation. The applet connects to the application (directly using TCP/IP or through web server using HTTP protocols) on the organization’s application and database servers. These servers may be on different computer systems. The web based applications provide flexible access from anywhere using the browsers that support graphics and multimedia. The solutions are also scalable and easy to extend.

4.15.3 Authentication Techniques

Authentication is a process to verify the claimed identity. There are various techniques available for authentication. Password is the most extensively used method. Most of the financial institutions use password along with PIN (Personal Identification Number) for authentication. Technologies such as tokens, smart cards and biometrics can be used to strengthen the security structure by requiring the user to possess something physical.[41]

[41] Report on Internet Banking (Part 1 of 2)
Token technology relies on a separate physical device, which is retained by an individual, to verify the user’s identity. The token resembles a small hand-held card or calculator and is used to generate passwords. The device is usually synchronized with security software in the host computer such as an internal clock or an identical time based mathematical algorithm. Tokens are well suited for one-time password generation and access control. A separate PIN is typically required to activate the token.

- **Smart cards** look like credit cards or other traditional magnetic stripe cards, but contain an embedded computer chip. The chip includes a processor, operating system, and both Read Only Memory (ROM) and Random Access Memory (RAM). They can be used to generate one-time passwords when prompted by a host computer, or to carry cryptographic keys. A smart card reader is required for their use.

- **Biometrics** involves identification and verification of an individual based on some physical characteristic, such as fingerprint analysis, hand geometry or retina scanning. This technology is advancing rapidly and offers an alternative means to authenticate a user.

### 4.15.4 Security Systems /Firewalls

The connection between internal networks and the outside world must be watched and monitored carefully. Firewalls do this job. Otherwise, there is a risk of exposing the internal network and systems, often leaving them vulnerable and compromising the integrity and privacy of data. Firewalls are a component or set of components that restrict access between a protected network and the outside world (i.e. the Internet). They control traffic between outside and inside a network, providing a single entry point where access control and auditing can be imposed. All firewalls examine the pieces or packets of data flowing into and out of a network and determine whether a particular person should be given access inside the network. As a result, unauthorized computers outside the firewall are prevented from directly accessing the computers inside the internal network. Broadly, there are three types of firewalls i.e. Packet filtering firewall, Proxy servers and stateful inspection firewall. The Figure 4.20
shows a typical firewall organization consisting of ‘militarized zone’ that separates the protected network from the internet.

![Firewall Diagram](image)

**Figure 4.20: Firewall**

- **Packet filtering routers**: Packet filtering routers are the simplest form of firewalls. They are connected between the host computer of an internal network and the Internet gateway as shown in Figure 4.21. The bastion host directs message accepted by the router to the appropriate application servers in the protected network. Their function is to route data of a network and to allow only certain types of data into the network by checking the type of data and its source and destination address. If the router determines that the data is sourced from an Internet address which is not on its acceptable or trusted sources list, the connection would be simply refused. The advantage of this type of firewall is that it is simple and cheaper to implement and also fast and transparent to the users. The disadvantage is that if the security of the router were compromised, computers on the internal network would be open to external network for attacks. Also, the filtering rules can be difficult to configure and a poorly configured firewall could result in security loopholes by unintentionally allowing access to an internal network.
b. **Proxy servers**: Proxy server controls incoming and outgoing traffic for a network by executing specific proxy program for each requested connection. If any computer outside the internal network wants to access some application running on a computer inside the internal network, then it would actually communicate with the proxy server, and proxy server in turn pass the request to the internal computer and get the response which will be given to the recipient (outside user). That is, there is no direct connection between the internal network and Internet. This approach allows a high level of control and in-depth monitoring using logging and auditing tools. However, since it doubles the amount of processing, this approach may lead to some degradation in performance.

4.15.5 Servers at the Data Centre[^42]

i. **Application Server**: Application server is a program that handles all application operations between users and an organization's backend business applications or databases. An application server is used for complex transaction-based applications. To support high-end needs, an application server has to have built-

in redundancy, monitor for high-availability, high-performance distributed application services and support for complex database access.

In CORE banking solution an application server hosts the core banking application. It is robust and powerful system that performs all CORE banking application. In the branches only the client version of application that merely collect data from the user and perform basic validation is installed. The application server receives data from all the client machines installed at the branches and performs necessary operation and updates the central database. Any patches or updation to core banking application is done at the application server after testing the same in testing environment. Application server is placed in the trusted zone in separate Virtual Local Area Network (VLAN).

ii. **Database Server:** The Database server of the bank contains the entire data of the bank. Database server is accessed by the application server for processing. Apart from that the Automated Teller Machine (ATM) server and Internet Banking Application Server (IBAS) access the database server through their own channel of middleware and firewall. All customer transactions performed from the branches or internet or ATM or mobile at this central database. Database server is placed in the trusted zone in separate Virtual Local Area Network (VLAN).

iii. **Antivirus Server:** In core banking setup, there is centralized antivirus server. The advantage of setting up an antivirus server is:

   - The antivirus program updated with the latest virus signature is pushed to all the system in the bank’s network from a central location.
   - It facilitates better administration as the antivirus software is updated in the central location and becomes available to all the system in the bank’s network.
   - Antivirus server is located in trusted zone of separate VLAN.

iv. **Automated Teller Machine (ATM) Server:** ATM server contains the details of all ATM account holder. Also ATM server temporarily holds data that is
converted by the middleware as requested by ATM switch. When the central database is not accessible a file containing account balance, referred to as Positive Balance File (PBF) of the ATM customer is sent to ATM switch. During this period, the ATM transactions are based on the balance available in its server. Once the database server is restored, these transactions are updated in the central database. ATM server is located in trusted zone of separate VLAN.

v. **Web server:** The web server host the bank’s website. There is web host attached to the web server. The web host has an operating system and runs the services from the web server. It accepts the web page requests from the customer and processes the same. The web host generates a dynamic web page for each user while processing his service. It facilitates secured (encrypted) connection when configured properly for confidential data transfer. Web server is placed inside the de-militarized zone in a separate VLAN that contains the proxy server, mail server, Internet Banking Application Server (IBAS) and Internet Banking Database Server (IBDS).

vi. **Internet Banking Application Server (IBAS):** The internet banking application is hosted in Internet Banking Application Server (IBAS). All internet banking service requests are received by IBAS from the web server. The IBAS works with the support of Internet Banking Database Server (IBDS), middleware and central database server to process the internet banking services requests. The IBAS placed inside the de-militarized zone in a separate VLAN that contains the proxy server, mail server, web server, Internet Banking Database Server (IBDS).

vii. **Internet Banking Database Server (IBDS):** IBDS stores the user name and password of all internet banking customers. It also contains the home branches details of each internet banking customer. Whenever an internet customer attempts to login to the bank’s website, the IBAS authenticate the customer with the login details stored in IBDS. Also IBDS temporarily stores the data requested by the customer while performing an internet banking transaction. The IBDS retrieves this data of the customer based on the request from IBAS. The
IBDS access the central database server through a middleware and firewall to retrieves the required customer details.

4.15.6 Middleware:
Middleware is software that formats the data to make it compatible with different application. Thus middleware is required when more than one application with different data requirements processes a common database middleware is placed in the trusted zone in separate VLAN.

4.15.7 Proxy Server:
A proxy server also known as “Application level gateway” is a computer that acts as a gateway between a local network and a larger-scale network such as the Internet.
Proxy servers provide increased performance and security. A proxy server works by intercepting connections between sender and receiver. All incoming data enters through one port and is forwarded to the rest of the network via another port. By blocking direct access between two networks, proxy servers make it much more difficult for hackers to get internal addresses and details of a private network.

![Proxy Server Diagram](http://en.wikipedia.org/wiki/Proxy_server)

**Figure 4.22: Proxy Server**

A proxy server has a variety of possible function such as [43]
- To keep machines behind it unidentified mainly for security.

To speed up access to resources (using caching). Web proxies are commonly used to cache web pages from a web server.

To prevent downloading the same content multiple times and save bandwidth.

To log or audit usage e.g. to provide organization employees internet usage reporting.

To scan transmitted content for malware before delivery.

To scan outbound content e.g. for data loss prevention.

To bypass website restrictions at work.

Access enhancement or restriction

- To apply access policy to network services or content e.g. to block undesired sites.
- To access sites prohibited or filtered by ISP or organization.
- To bypass security controls.

4.15.8 Domain Controller

It is primarily used for authentication. Access to set of server is controlled by domain controller.

4.16 Safety Concerns in IT enable environment:

The substantially larger proportion of technology related frauds by number is only expected as there has been a remarkable shift in the service delivery model with greater technology integration in the financial services sector. Banks are increasingly pushing their customers to adopt newer service delivery platforms like mobile, internet and social media for enhanced efficiency and cost-cutting. But while banks customers have become tech-savvy and started using online banking services and products, evidence suggests that even fraudsters are devising newer ways of perpetrating frauds by exploiting the loopholes in technology systems and processes. There have been several instances of low value frauds wherein the fraudsters have employed hostile software programs or malware attacks, phishing, Vishing (voicemail), SMSishing (text messages), Whaling (targeted phishing on high networth
individuals) techniques apart from stealing confidential data to perpetrate frauds\textsuperscript{[44]}. Bank group-wise detail of the number of technology related fraud cases with the amount involved therein over the last 4 years is shown in the Table No. 4.3

\textsuperscript{[44]} Dr. K. C. Chakrabarty, Deputy Governor, Reserve Bank of India “Frauds in the Banking Sector: Causes, Concerns and Cures”, National Conference on Financial Fraud organized by ASSOCHAM, New Delhi, July 2013
The majority of the new private sector banks and the foreign banks in the number of technology related frauds are intuitive as they lead the technology enabled service delivery in the Indian banking sector. From the Table no 4.3, it has been observe that the incidence of cyber frauds is extremely high but the actual amount involved is generally very low. However while the amounts involved may be small from banks perspective, these are significant from the viewpoint of individuals, who are victims of such frauds. The banks must realize that the community that uses online banking services is a very powerful group capable of launching attacks using the social media. It is therefore in banks own interest to ensure that they are constantly on the guard and up to the challenge of providing a secure environment for customers to conduct banking transactions. For this purpose, the banks would need to constantly monitor the fraudulent activities and regularly review and update the existing security features to prevent easy manipulation by hackers, skimmers, phishers, etc. With cyber attack becoming more frequent, RBI has advised banks in February 2013 to introduce certain minimum checks and balances like introduction of two factor authentication in case of ‘card not present’ transactions, converting all strip based cards to chip based cards for better security, issuing debit and credit cards only for domestic usage unless sought specifically by the customer, putting threshold limit on international usage of

Table No. 4.3: Frauds in the Banking Sector: Causes, Concerns and Cures,  
As on 29 Jul 2013, Source: www.rbi.org
debit or credit cards, constant review of the pattern of card transactions in coordination with customers, sending SMS alerts in respect of card transactions etc. to minimize the impact of such attacks on banks as well as customers.

The electronic modes of payment like NEFT and RTGS have gained traction due to their almost real time impact and also comparatively lower cost. These transactions are generally undertaken remotely, through internet banking, by using specific ID and password provided to the users. Though, it is the responsibility of the user to ensure that his unique ID and password are properly secured and do not get misused due to his carelessness, the banks, on their part, should also ensure that these payment channels are safe and secure. Towards this end, RBI has advised banks to introduce preventive measures such as putting a cap on the value or number of beneficiaries, introducing system of issuing alert on inclusion of additional beneficiary, velocity checks on number of transactions effected per day or per beneficiary, considering introduction of digital signature for large value payments, capturing internet protocol check as an additional validation check for any transaction etc. Banks need to improve the peripheral and system security in ATM locations and at the same time educate their customers about using their payment cards with due caution [45].

[45] Dr. K. C. Chakrabarty, Deputy Governor, Reserve Bank of India “Frauds in the Banking Sector: Causes, Concerns and Cures”, National Conference on Financial Fraud organized by ASSOCHAM, New Delhi, July 2013