ambitious baba .com
INDIA'S LARGEST TEST PREP PLATFORM

Module-C Unit-7

JAIIB PAPER-2

Principles and Practices of Banking (PPB)

JAIIB PPB Module C Unit 7- Security Considerations and Mitigation Measures in Banks

Risk Concern Areas

The Customer Demands have triggered a fierce competition among banks and financial companies for the application of information technology in their operations to help them offer innovative products and services at reduced costs. This also helps those entering new geographical areas.

- **Data and software:** Data is critical resource, necessary for an organisation's continuing operations. Incorrect data can have serious implications in decision making, as well. The increasing availability and use of expert system and the potential impact erroneous data can result in playing havoc with an organisation's business.
- **Infrastructure:** Banks have to invest heavily for implementing technology-based tools and solutions. In addition to software and data, same hardware components are required for operations of the computer and communication systems.
- **Peopleware:** Peopleware refers to the group of persons directly or indirectly involved in managing and running the computerized systems.

Different types of Threats

The threats to computerized system manifests in the form of business interruptions as under:

- Errors and omissions in data and software
- Unauthorised disclosure of confidential information
- Computer abuse and mis-utilisation of banks assets
- Computer/cyber frauds

Accidental Damages

Computers and communications systems have found their applications to be quite extensive in banking and other financial organisations. However, at the same time, these systems are vulnerable to damages caused accidentally, both due human failures and natural calamities.

- Environmental Hazards
- Human Error and Omissions
- Unreliable systems

Malicious Damages

Risk of malicious damages to computerized systems can be from disgruntled employees who wish to disrupt the services or from individuals with malafide intentions, using the technology for perpetrating fraud for financial gains.

- Interruptions in Services
- Frauds

Control Mechanism

Implementation of effective control mechanism is required management of risks associated with the use of IT tools.

Physical Control

Internal Control

- Accounting Control
- Administrative Control

Operational Control

- Audit Trails (i)Accounting Audit Trail (ii) Operations Audit Trail
- Checksum
- Data Encryption

Computer Audit

- Banks can achieve effective, secure and reliable computer systems only through the use of appropriate control techniques discussed above. The control techniques selected, varies from bank to bank, reflecting the particular risks within each bank and the costs of related security and control procedures.
- A regular programme of independent tests of security and control procedures by auditors help in in identifying lapses before the banking operations land into serious risk. The generic organizational function aimed at evaluation of the asset safeguarding, data integrity, system effectiveness, and system efficiency in computerized systems is termed as “Computer Audit”.

Information System Audit (IS Audit)

An information system (IS) audit or information technology(IT) audit is an examination of the controls within an entity's Information technology infrastructure. These reviews may be performed in conjunction with a financial statement audit, internal audit, or other form of attestation engagement. It is the process of collecting and evaluating evidence of an organization's information systems, practices, and operations. Obtained evidence evaluation can ensure whether the organization's information systems

safeguard assets, maintains data integrity, and are operating effectively and efficiently to achieve the organization's goals or objectives.

Information Systems Audit Methodology

- **PHASE 1:** Audit Planning
- **PHASE 2 –** Risk Assessment and Business Process Analysis
- **PHASE 3** – Performance of Audit Work
- **PHASE 4**: Reporting

Benefit of IS Audit

- It would identify the risks of exposure to an existing computerized environment. On Identification of the risks, remedial measure can be taken to protect the interests of an organisation.
- It would deter people/employees/ users from indulging in corruption/ manipulation of data, frauds etc. An undesired activity will be detected through implementation of IS audit.

Information System Security (IS Security)

Information systems security, also known as INFOSEC, is a broad subject within the field of information technology (IT) that focuses on protecting computers, networks, and their users. Almost all modern companies, as well as many families and individuals, have justified concerns about digital risks to their well-being.

Need for IS Security

- To Comply with law of the land and regulator's guidelines.
- To comply with business policy.
- To comply with business partner's requirements.

IS Security in Banking

Banks must meet their customers requirement for security aspects in special way on many levels, whether it is with their saving, taking advantage of over-the counter services at a branch office, withdrawing money from the teller machines, making deposits via the cash recycling system, online banking etc.

Threats to IS Security

- E-mail Viruses
- Phishing Attacks
- Hackers Attack
- Vishing
- Smishing

Modus Operandi Of Online Frauds and Cyber Security Awareness

Cyber Fraud

- The goal of cybercriminals is to steal user credentials and introduce fraudulent transactions into back office systems. Criminals hide their tracks and destroy any proof they may have left behind after sending fraudulent funds.
- Doing so, they erase or alter records and disrupt computer systems to thwart investigators. This puts the back office at risk and undermines the very business controls that are supposed to keep fraud at bay.

Modus Operandi of a Cyber-Attack

The modus operandi of Cyber fraud comprises the following steps.

- Reconnaissance and Compromise
- Obtain credentials
- Send fraudulent messages
- Hide/cover up evidence

Modus Operandi of Cyberattacks

The common modus Operandi followed by cyber attackers are;

- ATM card skimming
- Phishing/Vishing/Smishing Payment Fraud
- Lottery Fraud/Fake Prize Fraud
- Frauds due to using Unknown/Unverified Mobile Apps
- Account takeover Fraud
- Online Marketplaces Fraud
- Card fraud
- Sim Swapping

Evaluation Requirements

The IT resources continuously undergo changes in the form of development of new applications, acquisition of new hardware, turnover of trained employees etc.

- Computer Hardware

- Computer Software
- Data
- Communication channels
- Disaster Recovery Management
- System Development Process

Legal Framework for Electronic Transactions

At present, many legal provisions recognize the paper-based records and documents that should bear signature. Since, electronic commerce eliminates the need for paper-based transactions. Therefore to facilitate e-commerce, there was a need for enactment/amendment of necessary Law.

Indian Parliament enacted a comprehensive information Technology Bill, which received the Present's assent on 9 June 2000.

Consequent upon the recognition given to the electronic records, electronic documents and electronic signatures, incidental amendments have also been made in the following Acts:

- The Indian Penal Code, 1860
- The Indian Evidence Act, 1872
- The Banker's Bank Evidence Act, 1891
- The Reserve Bank of India Act, 1934

The Act purports to include the work "electronic record" along with the word "record"/"document" appearing generally in various sections of these act.

The amendment to Indian Penal Code, 1860, also states that for the purpose of the Section 466 (dealing with forgery of records) a "register" shall include any list, data or record of any entires maintained in the electronic form as defined in the IT Act 2000.

Bankers Books Evidence Act, 1891 redefines banker's books as ledgers, daybooks, cash books and account Books used in the ordinary business of the Bank.

The RBI act, 1934 has been amended by the IT act, 2000, empowering the central board to make regulations for fund transfers through electronic means between the banks or between the banks and other financial institutions.

Read One time Gopalakrishana Committee Report Click Here

- **Join Telegram Group**

- **For Mock test and Video Course Visit**: **test.ambitiousbaba.com**
- Join Free Classes: **JAIIBCAIIB BABA**
- Download APP For Study Material: Click Here
- Download More PDF

Click here to get Free Study Materials Just by Fill this form