### Basic Concepts

1. **Need for Protection of Information Systems:** Information security failures may result in both financial losses and/or intangible losses such as unauthorized disclosure of competitive or sensitive information. That is why protection of information systems has become a need for organizations.

2. **Information System Security:** Information security refers to the protection of valuable assets against loss, disclosure, or damage. For any organization, the security objective comprises three universally accepted attributes:
   - **Confidentiality:** Prevention of the unauthorized disclosure of information;
   - **Integrity:** Prevention of the unauthorized modification of information; and
   - **Availability:** Prevention of the unauthorized withholding of information.

   The relative priority and significance of Confidentiality, Integrity and Availability (CIA) vary according to the data within the information system and the business context in which it is used.

2.1 **What Information is Sensitive?**

   The common aspect in each organization is the critical information that each organization generates. These are: Strategic Plans, Business Operational data and Financial records etc.

3. **Information Security Policy:** An Information Security policy is the statement of intent by the management about how to protect a company’s information assets. It is a formal statement of the rules, which govern access to people to an organization's technology and information assets, and which they must abide by.


4. **Information Systems Controls:** Control is defined as Policies, procedures, practices and enterprise structure that are designed to provide reasonable assurance that business objectives will be achieved and undesired events are prevented, detected and corrected. Thus, information systems auditing includes reviewing the implemented system or providing consultation and evaluating the reliability of operational effectiveness of controls.
4.1 **Impact of Technology on Internal Controls**: The internal controls within an enterprise in a computerized environment encompass the goal of asset safeguarding, data integrity, system efficiency and effectiveness. These are: Personnel, Segregation of duties, Authorization procedures, Record keeping, Access to assets and records, Management supervision and review, Risks due to concentration of programs and data.

Internal controls comprise of the following five interrelated components: Control Environment, Risk Assessment, Control Activities, Information and Communication, Monitoring.

4.2 **Objective of Controls**: The objective of controls is to reduce or if possible eliminate the causes of exposure to potential loss.

5. **Categories of Controls**

Controls can be classified into following categories as shown in the Fig. below:

(a) Based on the objective of controls, these can be classified as under:

(i) **Preventive Controls**: Preventive controls are those, which are designed to prevent an error, omission or malicious act occurring. An example of a preventive control is the use of passwords to gain access to a financial system.

(ii) **Detective Controls**: These controls are designed to detect errors, omissions or malicious acts that occur and report the occurrence. An example of a detective control would be a use of automatic expenditure profiling where management gets regular reports of spend to date against profiled spend.

(iii) **Corrective Controls**: Corrective controls are designed to reduce the impact or correct an error once it has been detected. Corrective controls may include the use of default dates on invoices where an operator has tried to enter the incorrect date. A
Business Continuity Plan (BCP) is considered to be a corrective control.

(iv) **Compensatory Controls:** Controls are basically designed to reduce the probability of threats, which can exploit the vulnerabilities of an asset and cause a loss to that asset. While designing the appropriate control one thing should be kept in mind—"the cost of the lock should not be more than the cost of the assets it protects."

(b) Another classification of controls is based on the nature of IS resource. These are given as follows:

(i) **Environmental Controls:** These are the controls relating to IT environment such as power, air-conditioning, UPS, smoke detection, fire-extinguishers, dehumidifiers etc. These are related to the external factors in the Information Systems and preventive measures to overcome the conflicts. The controls over environment exposures are: Water Detectors, Hand-Held Fire Extinguishers, Manual Fire Alarms, Smoke Detectors, Fire Suppression Systems, Strategically Locating the Computer Room, Regular Inspection by Fire Department, Fireproof Walls, Floors and Ceilings surrounding the Computer Room, Electrical Surge Protectors, Uninterruptible Power System (UPS)/Generator, Power Leads from Two Substations, Emergency Power-Off Switch, Wiring Placed in Electrical Panels and Conduit, Prohibitions against Eating, Drinking and Smoking within the Information Processing Facility, Fire Resistant Office Materials and Documented and Tested Emergency Evacuation.

(ii) **Physical Access Controls:** These are the controls relating to physical security of tangible IS resources and intangible resources stored on tangible media etc. Such controls include Access control doors, Security guards, door alarms, restricted entry to secure areas, visitor logged access, CCTV monitoring etc. These controls are personnel; hardware and include procedures exercised on access to IT resources by employees/outsiders. The controls relate to establishing appropriate physical security and access control measures for IT facilities, including off-site use of information devices in conformance with the general security policy. These controls are designed to protect the organization from unauthorized access or in other words, to prevent illegal entry. These controls should be designed in such a way that it allows access only to authorized persons. These are as follows:

(a) **Locks on Doors** - Cipher locks (Combination Door Locks), Bolting Door and Electronic Door Locks.

(b) **Physical Identification Medium** - Personal Identification numbers (PIN), Plastic Cards Identification Badges.

(c) **Logging on Facilities** - Manual Logging and Electronic Logging.

(d) **Other means of Controlling Physical Access** - Video Cameras, Security Guards, Controlled Visitor Access, Bonded Personnel, Dead Man Doors, Non-exposure of Sensitive Facilities, Computer Terminal Locks, Controlled Single
Entry Point, Alarm System, Perimeter Fencing, Control of out of hours of employee-employees and Secured Report/Document Distribution Cart.

(iii) **Logical Access Controls:** These are the controls relating to logical access to information resources such as operating systems controls, application software boundary controls, networking controls, access to database objects, encryption controls etc. are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted. Logical access controls are implemented to ensure that access to systems, data and programs is restricted to authorized users so as to safeguard information against unauthorized use, disclosure or modification, damage or loss.

- **Logical Access Paths:** These are Online Terminals, Dial-up Ports and Telecommunication Network etc.

- **Issues and Revelations related to Logical Access:** Compromise or absence of logical access controls in the organizations may result in potential losses due to exposures that may lead to the total shutdown of the computer functions. Intentional or accidental exposures of logical access control encourage technical exposures and computer crimes. These are as follows:
  - **Technical Exposures:** Technical exposures include unauthorized implementation or modification of data and software. Technical exposures include: Data Diddling, Bombs - Time Bomb & Logic Bomb, Trojan Horse, Worms, Rounding, Salami Techniques and Trap Doors.
  - **Computer Crime Exposures:** Crimes are committed by using computers and can damage the reputation, morale and even the existence of an organization. Computer crimes generally result in Loss of customers, embarrassment to management and legal actions against the organizations. These are: Financial Loss, Legal Repercussions, Loss of Credibility or Competitive Edge, Blackmail/Industrial Espionage, Disclosure of Confidential, Sensitive or Embarrassing Information, Sabotage and Spoofing.
  - **Asynchronous Attacks:** They occur in many environments where data can be moved asynchronously across telecommunication lines. Numerous transmissions must wait for the clearance of the line before data can be transmitted. Data that is waiting to be transmitted are liable to unauthorized access called asynchronous attack. There are many forms of asynchronous attacks, some of them are: Data Leakage, Wire-tapping, Piggybacking and Shutting Down of the Computer/Denial of Service.

- **Logical Access Control across the System:** The purpose of logical access controls is to restrict access to information assets/resources. They are expected to provide access to information resources on a need to know and need to do...
basis using principle of least privileges. These are: User access management, User responsibilities, Network access control, Operating system access control, Application and monitoring system access control and Mobile computing related controls.

(c) Classification based on “Audit Functions” – Managerial Controls and Application Controls

(i) Managerial Controls: These are the controls over the managerial functions that must be performed to ensure the development, implementation, operation and maintenance of information systems in a planned and controlled manner in an organization.

- **Top Management**: Top management must ensure that information systems function is well managed. It is responsible primarily for long – run policy decisions on how Information Systems will be used in the organization.
- **Information Systems Management**: IS management has overall responsibility for the planning and control of all information system activities. It also provides advice to top management in relation to long-run policy decision making and translates long-run policies into short-run goals and objectives.
- **Systems Development Management**: Systems Development Management is responsible for the design, implementation, and maintenance of application systems.
- **Programming Management**: It is responsible for programming new system; maintain old systems and provides general systems support software.
- **Data Administration**: Data administration is responsible for addressing planning and control issues in relation to use of an organization’s data.
- **Quality Assurance Management**: It is responsible for ensuring information systems development; implementation, operation, and maintenance conform to established quality standards.
- **Security Administration**: It is responsible for access controls and physical security over the information systems function.
- **Operations Management**: It is responsible for planning and control of the day-to-day operations of information systems.

(ii) Application Controls: Application system controls are undertaken to accomplish reliable information processing cycles that perform the processes across the enterprise. Applications represent the interface between the user and the business functions. Application Control Techniques include the programmatic routines within the application program code. The objective of application controls is to ensure that data remains complete, accurate and valid during its input, update and storage. These
Protection of Information Systems

are – Boundary Controls, Input Controls, Communication Controls, Processing Controls, Database Controls and Output Controls.

- **Boundary Controls**: Major controls of the boundary system are the access control mechanisms. Access control mechanism links authentic users to authorized resources that they are permitted to access. Major Boundary Control techniques are Cryptography, Passwords, Personal Identification Numbers (PIN), Identification Cards and Biometric Devices.

- **Input Controls**: These controls are responsible for ensuring the accuracy and completeness of data and instruction input into an application system.

- **Communication Controls**: These controls discuss exposures in the communication subsystem, controls over physical components, communication line errors, flows, and links, topological controls, channel access controls, controls over subversive attacks, internetworking controls, communication architecture controls, audit trail controls, and existence controls.

- **Processing Controls**: Data processing controls perform validation checks to identify errors during processing of data. They are required to ensure both the completeness and the accuracy of data being processed.

- **Database Controls**: Protecting the integrity of a database when application software acts as an interface to interact between the user and the database, are called update controls and report controls. Major update controls are: Sequence Check between Transaction and Master Files, Ensure All Records on Files are processed, Process multiple transactions for a single record in the correct order and maintain a suspense account.

- **Output Controls**: These controls ensure that the data delivered to users will be presented, formatted and delivered in a consistent and secure manner. Output can be in any form, it can either be a printed data report or a database file in a removable media such as a CD-ROM or it can be a Word document on the computer’s hard disk.

  Major Report controls are: Standing Data, Print-Run-to Run control Totals, Print Suspense Account Entries and Existence/Recovery Controls.

6. **General Controls**: Information Technology General Controls (ITGC) are the basic policies and procedures that ensure that an organization’s information systems are properly safeguarded, that application programs and data are secure, and that computerized operations can be recovered in case of unexpected interruptions.

7. **Financial Controls**: These controls are generally defined as the procedures exercised by the system user personnel over source, or transactions origination, documents before system input. These areas exercise control over transactions processing using reports generated by
the computer applications to reflect un-posted items, non-monetary changes, item counts and amounts of transactions for settlement of transactions processed and reconciliation of the applications (subsystem) to general ledger.

8. **Controls over Data Integrity and Security:** The primary objective of data integrity control techniques is to prevent, detect, and correct errors in transactions as they flow through various stages of a specific data processing program. There are six categories of integrity controls: Source data control, Input validation routines, On-line data entry controls, Data processing and storage controls, Output controls and Data Transmission controls.

**Data Integrity Policies:** Major data integrity policies are: Virus-Signature Updating, Software Testing, Division of Environments etc.

9 **Cyber Frauds:** Cyber Fraud shall mean fraud committed by use of technology. Cyber fraud refers to any type of deliberate deception for unfair or unlawful gain that occurs online. The most common form is online credit card theft. Based on the functionality, these are of two types:

- **Pure Cyber Frauds:** Frauds, which exist only in cyber world. They are borne out of use of technology. For example: Website hacking.
- **Cyber Enabled Frauds:** Frauds, which can be committed in physical world also but with use of technology; the size, scale and location of frauds changes. For example: Withdrawal of money from bank account by stealing PIN numbers.

9.1 **Cyber Attacks:** Major cyber-attacks are: Phishing, Network Scanning, Virus/Malicious Code, Spam, Website Compromise/Malware Propagation and others like Cracking, Eavesdropping, E-mail Forgery, E-mail Threats and Scavenging.

9.2 **Impact of Cyber Frauds on Enterprises:** The impact of cyber frauds on enterprises can be viewed under the following dimensions: Financial Loss, Legal Repercussions, Loss of credibility or Competitive Edge, Disclosure of Confidential, Sensitive or Embarrassing Information and Sabotage.

9.3 **Techniques to Commit Cyber Frauds:** These are: Hacking, Cracking, Data Diddling, Data Leakage, Denial of Service (DoS) Attack, Internet Terrorism, Logic Time Bombs, Masquerading or Impersonation, Password Cracking, Piggybacking, Round Down, Scavenging or Dumpster Diving, Social Engineering Techniques, Super Zapping and Trap Door.

In spite of having various controls as well as countermeasures in place, cyber frauds are happening and increasing on a continuous basis. To overcome these frauds, there is an urgent need to conduct research in the related areas and come up with more appropriate security mechanisms, which can make information systems more secure.
Question 1

Discuss various types of Information Security policies and their hierarchy.

Answer

Various types of information security policies are as follows:

- **Information Security Policy** – This policy provides a definition of Information Security, its overall objective and the importance that applies to all users.

- **User Security Policy** – This policy sets out the responsibilities and requirements for all IT system users. It provides security terms of reference for Users, Line Managers and System Owners.

- **Acceptable Usage Policy** – This sets out the policy for acceptable use of email, Internet services and other IT resources.

- **Organizational Information Security Policy** – This policy sets out the Group policy for the security of its information assets and the Information Technology (IT) systems processing this information. Though it is positioned at the bottom of the hierarchy, it is the main IT security policy document.

- **Network & System Security Policy** – This policy sets out detailed policy for system and network security and applies to IT department users.

- **Information Classification Policy** – This policy sets out the policy for the classification of information.

- **Conditions of Connection** – This policy sets out the Group policy for connecting to the network. It applies to all organizations connecting to the Group, and relates to the conditions that apply to different suppliers’ systems.

The hierarchy of Information Security Policies
Question 2

What is meant by Information Security Policy? What are the key components of a good security policy?

Answer

An Information Security Policy may be defined as a formal statement of the rules, which give access to people to an organization's technology and information assets, and which they must abide. In its basic form, an information security policy is a document that describes an organization's information security controls and activities. The policy does not specify technologies or specific solutions; it defines a specific set of intentions and conditions that help protect a company's information assets and its ability to conduct business. An Information Security Policy is the essential foundation for an effective and comprehensive information security program. It is the primary way in which management's information security concerns are translated into specific measurable and testable goals and objectives. It provides guidance to the people, who build, install, and maintain information systems.

A good security policy should clearly state the following:

- Purpose and Scope of the Document and the intended audience;
- The Security Infrastructure;
- Security policy document maintenance and compliance requirements;
- Incident response mechanism and incident reporting;
- Security organization Structure;
- Inventory and Classification of assets;
- Description of technologies and computing structure;
- Physical and Environmental Security;
- Identity Management and access control;
- IT Operations management;
- IT Communications;
- System Development and Maintenance Controls;
- Business Continuity Planning;
- Legal Compliance; and
- Monitoring and Auditing Requirements.

Question 3

The Information Security Policy of an organization has been defined and documented as given below:
“Our organization is committed to ensure Information Security through established goals and principles. Responsibilities for implementing every aspect of specific applicable proprietary and general principles, standards and compliance requirements have been defined. This is reviewed at least once a year for continued suitability regarding cost and technological changes.”

Discuss Information Security Policy and identify the salient components that have not been covered in the above policy.

Answer

A Policy is a plan or course of action, designed to influence and determine decisions, actions and other matters. The security policy is a set of laws, rules, and practices that regulates how assets including sensitive information are managed, protected, and distributed within the user organization.

An Information Security Policy addresses many issues such as disclosure, integrity and availability concerns, who may access what information and in what manner, basis on which access decision is made, maximized sharing versus least privilege, separation of duties, who controls, who owns the information, and authority issues.

Issues to address: This policy does not need to be extremely extensive, but clearly state senior management's commitment to information security, be under change and version control and be signed by an appropriate senior manager. The policy should at least address the following issues:

- a definition of information security,
- reasons why information security is important to the organization, and its goals and principles,
- a brief explanation of the security policies, principles, standards and compliance requirements,
- definition of all relevant information security responsibilities, and
- reference to supporting documentation.

The auditor should ensure that the policy is readily accessible to all employees and that all employees are aware of its existence and understand its contents. The policy may be a stand-alone statement or part of more extensive documentation (e.g. a security policy manual) that defines how the information security policy is implemented in the organization. In general, most if not all employees covered by the ISMS scope will have some responsibilities for information security, and auditors should review any declarations to the contrary with care. The auditor should also ensure that the policy has an owner who is responsible for its maintenance and that it is updated responding to any changes affecting the basis of the original risk assessment.

In the stated scenario of the question, the Information System Management System (ISMS) Policy of the given organization does not address the following issues:

- Definition of information security,
3.11 Information Systems Control and Audit

- Reasons why information security is important to the organization,
- A brief explanation of the security policies, principles, standards and compliance, and
- Reference to supporting documents.

**Question 4**

*What do you mean by Preventive Controls? Explain with the help of examples. Also, discuss their broad characteristics in brief.*

**Answer**

**Preventive Controls:** Preventive controls are those inputs, which are designed to prevent an error, omission or malicious act occurring. An example of a preventive control is the use of passwords to gain access to a financial system. These can be implemented in both manual and computerized environment for the same purpose. Only, the implementation methodology may differ from one environment to the other. Examples of preventive controls are given as follows:

- Employ qualified personnel,
- Segregation of duties,
- Access control,
- Vaccination against diseases,
- Documentation,
- Prescribing appropriate books for a course,
- Training and retraining of staff,
- Authorization of transaction,
- Validation, edit checks in the application,
- Firewalls,
- Anti-virus software (sometimes this acts like a corrective control also), etc., and
- Passwords.

The above list contains both manual and computerized, preventive controls. The broad characteristics of preventive controls are given as follows:

- A clear-cut understanding about the vulnerabilities of the asset;
- Understanding probable threats; and
- Provision of necessary controls to prevent probable threats from materializing.

**Question 5**

*What do you mean by Corrective Controls? Explain with the help of examples. Also, discuss their broad characteristics in brief.*
Answer

**Corrective Controls**: Corrective controls are designed to reduce the impact or correct an error once it has been detected. Corrective controls may include the use of default dates on invoices where an operator has tried to enter the incorrect date. A Business Continuity Plan (BCP) is a corrective control. Examples of Corrective Controls are given as follows:

- Contingency planning,
- Rerun procedures,
- Change input value to an application system, and
- Investigate budget variance and report violations.

The main characteristics of the corrective controls are given as follows:

- Minimizing the impact of the threat;
- Identifying the cause of the problem;
- Providing remedy to the problems discovered by detective controls;
- Getting feedback from preventive and detective controls;
- Correcting error arising from a problem; and
- Modifying processing systems to minimize future occurrences of incidents.

**Question 6**

*What do you understand by Financial Controls? Explain major financial control techniques in brief.*

**Answer**

**Financial Controls**: These controls are generally defined as the procedures exercised by the system user personnel over source, or transactions origination, documents before system input. These areas exercise control over transactions processing using reports generated by the computer applications to reflect un-posted items, non-monetary changes, item counts and amounts of transactions for settlement of transactions processed and reconciliation of the applications (subsystem) to general ledger.

Major financial control techniques are given as follows:

- **Authorization**: This entails obtaining the authority to perform some act typically accessing such assets as accounting or application entries.
- **Budgets**: These are estimates of the amount of time or money expected to be spent during a particular period, project, or event. The budget alone is not an effective control. Budgets must be compared with the actual performance, including isolating differences and researching them for a cause and possible resolution.
3.13 Information Systems Control and Audit

- **Cancellation of documents**: This marks a document in such a way to prevent its reuse. This is a typical control over invoices marking them with a “paid” or “processed” stamp or punching a hole in the document.

- **Documentation**: This includes written or typed explanations of actions taken on specific transactions; it also refers to written or typed instructions, which explain the performance of tasks.

- **Dual control**: This entails having two people simultaneously access an asset. For example, the depositories of banks’ 24-hour teller machines should be accessed and emptied with two people present, many people confuse dual control with dual access, but these are distinct and different. Dual access divides the access function between two people: once access is achieved, only one person handles the asset. With teller-machines, for example, two tellers would open the depository vault door together, but only one would retrieve the deposit envelopes.

- **Input/output verification**: This entails comparing the information provided by a computer system with the input documents. This is an expensive control that tends to be over-recommended by auditors.

- **Safekeeping**: This entails physically securing assets, such as computer disks, under lock and key, in a desk drawer, file cabinet storeroom, or vault.

- **Sequentially numbered documents**: These are working documents with preprinted sequential numbers, which enables the detection of missing documents.

- **Supervisory review**: This refers to review of specific work by a supervisor but this control requires a sign-off on the documents by the supervisor, to provide evidence that the supervisor at least handled them. This is an extremely difficult control to test after the fact because the auditor cannot judge the quality of the review unless he or she witnesses it, and, even then, the auditor cannot attest to what the supervisor did when the auditor was not watching.

**Question 7**

*What do you understand by Boundary Controls? Explain major Boundary Control techniques in brief.*

**Answer**

**Boundary Controls**: The major controls of the boundary system are the access control mechanisms. Access control mechanism links authentic users to resources, they are permitted to access. The access control mechanism has three steps of identification, authentication and authorization with respect to the access control policy.

Major Boundary Control techniques are given as follows:

- **Cryptography**: It deals with programs for transforming data into cipher text that are meaningless to anyone, who does not possess the authentication to access the respective system resource or file. A cryptographic technique encrypts data (clear text) into
cryptograms (cipher text) and its strength depends on the time and cost to decipher the cipher text by a cryptanalyst. Three techniques of cryptography are transposition (permute the order of characters within a set of data), substitution (replace text with a key-text) and product cipher (combination of transposition and substitution).

- **Passwords**: User identification by an authentication mechanism normally with strong password may be a good boundary access control. A few best practices followed to avoid failures in this control system are; minimum password length, avoid usage of common dictionary words, periodic change of passwords, hashing of passwords and number of unsuccessful entry attempts.

- **Personal Identification Numbers (PIN)**: PIN is like a password. It is assigned to a user by an institution using a random number stored in its database and sent independently to a user after identification. It can also be a customer selected number. Hence, a PIN may be exposed to vulnerabilities while issuance or delivery, validation, transmission and storage.

- **Identification Cards**: Identification cards are used to store information required in an authentication process. These cards are to be controlled through the application for a card, preparation of the card, issue, use and card return or card termination phases.

- **Biometric Devices**: Biometric identification e.g. thumb and/or finger impression, eye retina etc. are also used as boundary control techniques.

**Question 8**

Briefly explain major Update and Report Controls regarding Database Controls in brief.

**Answer**

Major Update Controls are given as follows:

- **Sequence Check between Transaction and Master Files**: Synchronization and the correct sequence of processing between the master file and transaction file is critical to maintain the integrity of updating, insertion or deletion of records in the master file with respect to the transaction records. If errors in this stage are overlooked, it leads to corruption of critical data. For example, transaction on a new inventory item should be processed only after the creating the inventory master record for the item.

- **Ensure All Records on Files are processed**: During processing, ensure that all the transactions till the end of the file marker are processed and similarly when processing master records, all records till end to master file marker are processed.

- **Process multiple transactions for a single record in the correct order**: Multiple transactions can occur based on a single master record (e.g. dispatch of a product to different distribution centers). Here, the order in which transactions are processed against the product master record must be done based on a sorted transaction codes e.g. chronological order.
3.15 Information Systems Control and Audit

- **Maintain a suspense account:** When mapping between the master record to transaction record results in a mismatch due to failure in the corresponding record entry in the master record; then these transactions are maintained in a suspense account. If the suspense account has a non-zero balance, it reflects the errors to be corrected.

Major Report Controls are given as follows:

- **Standing Data:** Application programs use many internal tables to perform various functions like gross pay calculation, billing calculation based on a price table, bank interest calculation etc. Maintaining integrity of the pay rate table, price table and interest table is critical within an organization. Any changes or errors in these tables would have an adverse effect on the organizations basic functions. Periodic monitoring of these internal tables by means of manual check or by calculating a control total is mandatory.

- **Print Run-to-Run Control Totals:** Run-to-Run control totals help in identifying errors or irregularities like record dropped erroneously from a transaction file, wrong sequence of updating or the application software processing errors.

- **Print Suspense Account Entries:** Like the update controls, the suspense account entries are to be periodically monitored with the respective error file and action taken on time.

- **Existence/Recovery Controls:** The back-up and recovery strategies together encompass the controls required to restore failure in a database. Backup strategies are implemented using prior version and logs of transactions or changes to the database. Recovery strategies involve roll-forward (current state database from a previous version) or the roll-back (previous state database from the current version) methods.

**Question 9**

*What do you understand by classification of Information? Explain different classifications of Information.*

*Or*

*As a member of IS Steering Committee, how do you classify the information for better integrity and security?*

**Answer**

Information classification does not follow any predefined rules. It is a conscious decision to assign a certain sensitivity level to information that is being created, amended, updated, stored, or transmitted. The sensitivity level depends upon the nature of business in an organization and the market influence.

The classification of information further determines the level of control and security requirements. Classification of information is essential to understand and differentiate between the value of an asset and its sensitivity and confidentiality. When data is stored, whether received, created or amended, it should always be classified into an appropriate sensitivity level to ensure adequate security.
For many organizations, a very simple classification criterion is given as follows:

- **Top Secret**: Highly sensitive internal information (e.g., pending mergers or acquisitions; investment strategies; plans or designs) that could seriously damage the organization if such information were lost or made public. Information classified as Top Secret information has very restricted distribution and must be protected at all times. Security at this level should be the highest possible.

- **Highly Confidential**: Information that, if made public or even shared around the organization, could seriously impede the organization’s operations and is considered critical to its ongoing operations. Information would include accounting information, business plans, sensitive customer information of banks, solicitors and accountants, patient’s medical records and similar highly sensitive data. Such information should not be copied or removed from the organization’s operational control without specific authority. Security at this level should be very high.

- **Proprietary**: Information of a proprietary nature; procedures, operational work routines, project plans, designs and specifications that define the way in which the organization operates. Such information is normally for proprietary use to authorized personnel only. Security at this level should be high.

- **Internal Use only**: Information not approved for general circulation outside the organization where its loss would inconvenience the organization or management but where disclosure is unlikely to result in financial loss or serious damage to credibility. Examples would include, internal memos, minutes of meetings, internal project reports. Security at this level should be controlled but normal.

- **Public Documents**: Information in the public domain; annual reports, press statements etc.; which has been approved for public use. Security at this level should be minimal.

**Question 10**

*What are the major data integrity policies followed by an organization?*

**Answer**

Major Data Integrity Policies are given as under:

- **Virus-Signature Updating**: Virus signatures must be updated automatically when they are made available from the vendor through enabling of automatic updates.

- **Software Testing**: All software must be tested in a suitable test environment before installation on production systems.

- **Division of Environments**: The division of environments into Development, Test, and Production is required for critical systems.

- **Offsite Backup Storage**: Backups must be sent offsite for permanent storage.
Quarter-End and Year-End Backups: Quarter-end and year-end backups must be done separately from the normal schedule for accounting purposes.

Disaster Recovery: A comprehensive disaster-recovery plan must be used to ensure continuity of the corporate business in the event of an outage.

Question 11
Write short notes on the following:

(i) **Time Bomb**

These are the programs that lie idle until some date or time triggers it. Once triggered, the bomb sabotages the system by destroying programs, data or both.

(ii) **Logic Bomb**

These are the programs that lie idle until some specified circumstances trigger it. Once triggered, the bomb sabotages the system by destroying programs, data or both.

(iii) **Trojan Horse**

These are malicious programs that are hidden under any authorized program. Typically, a Trojan horse is an illicit coding contained in a legitimate program, and causes an illegitimate action. The concept of Trojan is like bombs but a computer clock or circumstances do not necessarily activate it. A Trojan may:

- Change or steal the password or
- Modify records in protected files or
- Allow illicit users to use the systems.

Trojan Horses hide in a host and generally do not damage the host program. Trojans cannot copy themselves to other software in the same or other systems. The Trojans may get activated only if the illicit program is called explicitly. It can be transferred to other system only if an unsuspecting user copies the Trojan program.

Christmas Card is a well-known example of Trojan. It was detected on internal E-mail of IBM system. On typing the word 'Christmas', it will draw the Christmas tree as expected, but in addition, it will send copies of similar output to all other users connected to the network. Because of this message on other terminals, other users cannot save their half-finished work.

(iv) **Worms**

A worm does not require a host program like a Trojan to replicate itself. Thus, a Worm program copies itself to another machine on the network. Since worms are stand-alone programs, they can be detected easily in comparison to Trojans and computer viruses.
Examples of worms are Existential Worm, Alarm clock Worm etc. The Alarm Clock worm places wake-up calls on a list of users. It passes through the network to an outgoing terminal while the sole purpose of existential worm is to remain alive. Existential worm does not cause damage to the system, but only copies itself to several places in a computer network.

(v) The impact of Technology on Internal Controls is as follows:

- **Competent and Trustworthy Personnel**: Personnel should have proper skill and knowledge to discharge their duties. Substantial power is often vested in the persons responsible for the computer-based information systems developed, implemented, operated, and maintained within organizations.

- **Segregation of Duties**: In a computerized system, the auditor should be concerned with the segregation of duties within the IT department. As a basic control, segregation of duties prevents or detects errors or irregularities. Within an IT environment, the staff in the IT department of an enterprise will have a detailed knowledge of the interrelationship between the source of data, how it is processed and distribution and use of output.

- **Authorization Procedures**: In computer systems, authorization procedures often are embedded within a computer program. For example: In some on-line transaction systems, written evidence of individual data entry authorization, e.g. a supervisor’s signature, may be replaced by computerized authorization controls such as automated controls written into the computer programs (e.g. programmed credit limit approvals).

- **Adequate Documents and Records**: In computer systems, documents might not be used to support the initiation, execution, and recording of some transactions. Thus, no visible audit or management trail would be available to trace the transactions in a computerized system. However, if the controls over the protection and storage of documents, transaction details, and audit trails etc. are placed properly, it will not be a problem for auditor.

- **Physical Control over Assets and Records**: Physical control over access and records is critical in both manual systems and computer systems. Computerized financial systems have not changed the need to protect the data. A client’s financial data and computer programs can all be maintained at a single site – namely the site where the computer is located. This concentration of information systems assets and records also increases the losses that can arise from computer abuse or a disaster. The nature and types of control available have changed to address these new risks.

- **Adequate Management Supervision**: In computer system, data communication facilities can be used to enable employees to be closer to the customers they service. Thus, supervision of employees might have to be carried out remotely. The Management’s supervision and review helps to deter and detect both errors and fraud.
3.19 Information Systems Control and Audit

- **Independent Checks on Performance:** If the program code in a computer system is authorized, accurate, and complete, the system will always follow the designated procedures in the absence of some other type of failure like hardware or systems software failure.

- **Comparing Recorded Accountability with Assets:** Data and the assets that the data purports to represent should periodically be compared to determine whether incompleteness or inaccuracies in the data exist or whether shortages or excesses in the assets have occurred. In a computer system, however, software is used to prepare this data. Again, internal controls must be implemented to ensure the veracity of program code, because traditional separation of duties no longer applies to the data being prepared for comparison purposes.

- **Delegation of Authority and Responsibility:** A clear line of authority and responsibility is an essential control in both manual and computer systems. In a computer system, delegating authority and responsibility in an unambiguous way might be difficult because some resources are shared among multiple users. Further, more users are developing, modifying, operating, and maintaining their own application systems instead of having this work performed by IS professionals.

**Question 12**

*What do you understand by Asynchronous Attacks? Explain various forms of Asynchronous Attacks in brief.*

**Answer**

Asynchronous Attacks: They occur in many environments where data can be moved asynchronously across telecommunication lines. Numerous transmissions must wait for the clearance of the line before data being transmitted. Data that is waiting to be transmitted are liable to unauthorized access called asynchronous attack. These attacks are hard to detect because they are usually very small pin like insertions.

There are many forms of asynchronous attacks; some of them are given as follows:

(i) **Data Leakage:** Data is a critical resource for an organization to function effectively. Data leakage involves leaking information out of the computer by means of dumping files to paper or stealing computer reports and tape.
(ii) **Wire-tapping:** This involves spying on information being transmitted over telecommunication network.

(iii) **Piggybacking:** This is the act of following an authorized person through a secured door or electronically attaching to an authorized telecommunication link that intercepts and alters transmissions. This involves intercepting communication between the operating system and the user and modifying them or substituting new messages.

(iv) **Shutting Down of the Computer/Denial of Service:** This is initiated through terminals or microcomputers that are directly or indirectly connected to the computer. Individuals, who know the high-level systems log on-ID initiate shutting down process. The security measure will function effectively if there are appropriate access controls over the logging on through a telecommunication network. Some systems have been proved to be vulnerable to shutting themselves down to prevent harm when they are overloaded. Hackers use this technique to shut down computer systems over the Internet.
3.21 Information Systems Control and Audit

Question 13

*Explain some of the key ways to control remote and distributed data processing applications in brief.*

**Answer**

Remote and distributed data processing applications can be controlled in many ways. Some of these are given as follows:

- Remote access to computer and data files through the network should be implemented.
- Having a terminal lock can assure physical security to some extent.
- Applications that can be remotely accessed via modems and other devices should be controlled appropriately.
- Terminal and computer operations at remote locations should be monitored carefully and frequently for violations.
- To prevent unauthorized users from accessing the system, there should be proper control mechanisms over system documentation and manuals.
- Data transmission over remote locations should be controlled. The location which sends data should attach needed control information that helps the receiving location to verify the genuineness and integrity.
- When replicated copies of files exist at multiple locations it must be ensured that all identical copies contain the same information and checks are also implemented to ensure that duplicate data does not exist.

Question 14

*Discuss the three processes of Access Control Mechanism, when a user requests for resources.*

**Answer**

An Access Control Mechanism is associated with identified, authorized users the resources they can access and action privileges. The mechanism processes the users request for Real Time Memory and Virtual Memory resources in three steps:

- **Identification:** First and foremost, the users have to identify themselves.
- **Authentication:** Secondly, the users must authenticate themselves and the mechanism must authenticate itself. The mechanism accesses previously stored information about users, the resources they can access, and the action privileges they have with respect to these resources; it then permits or denies the request. Users may provide four factor of authentication information as described in Table below:

<table>
<thead>
<tr>
<th>Classes of Authentication</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remembered information</td>
<td>Name, Account number, passwords</td>
</tr>
<tr>
<td>Objects Possessed by the user</td>
<td>Badge, plastic card, key</td>
</tr>
</tbody>
</table>
Protection of Information Systems

<table>
<thead>
<tr>
<th>Personal characteristics</th>
<th>Finger print, voice print, signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dialog</td>
<td>Through/around computer</td>
</tr>
</tbody>
</table>

- **Authorization**: Third, the users request for specific resources, their need for those resources and their areas of usage of these resources. There are two approaches to implementing the authorization module in an access control mechanism:
  - a “ticket oriented approach”, and
  - a “list oriented approach”.

Considering the authorization function in terms of a matrix where rows represent the users and columns represent the resources and the element represents the users privilege on the resources, we can see the distinction between these two approaches.

- **In a ticket-oriented approach** to authorization, the access control mechanism assigns users, a ticket for each resource they are permitted to access. Ticket oriented approach operates via a row in the matrix. Each row along with the user resources holds the action privileges specific to that user.

- **In a list-oriented approach**, the mechanism associates with each resource a list of users who can access the resource and the action privileges that each user has with respect to the resource. This mechanism operates via a column in the matrix.

**Question 15**

Discuss Locks on Doors with respect to physical access controls in brief.

**Answer**

**Locks on Doors**: Different types of locks on doors for physical security are discussed below:

- **Cipher locks (Combination Door Locks)** – The cipher lock consists of a pushbutton panel that is mounted near the door outside of a secured area. There are ten numbered buttons on the panel. To enter, a person presses a four-digit number, and the door will unlock for a predetermined period of time, usually ten to thirty seconds. Cipher locks are used in low security situations or when a large number of entrances and exits must be usable all the time.

- **Bolting Door Locks** – A special metal key is used to gain entry when the lock is a bolting door lock. To avoid illegal entry the keys should be not be duplicated.

- **Electronic Door Locks** – A magnetic or embedded chip-based plastics card key or token may be entered a reader to gain access in these systems. The reader device reads the special code that is internally stored within the card activates the door locking mechanism.

**Question 16**

Discuss major dimensions under which the impact of cyber frauds on enterprises can be viewed.
3.23 Information Systems Control and Audit

What are the repercussions of cyber frauds on an enterprise?

Answer

The impact of cyber frauds on enterprises can be viewed under the following dimensions:

- **Financial Loss:** Cyber frauds lead to actual cash loss to target company/organization. For example, wrongful withdrawal of money from bank accounts.

- **Legal Repercussions:** Entities hit by cyber frauds are caught in legal liabilities to their customers. Section 43A of the Information Technology Act, 2000, fixes liability for companies/organizations having secured data of customers. These entities need to ensure that such data is well protected. In case a fraudster breaks into such database, it adds to the liability of entities.

- **Loss of credibility or Competitive Edge:** News that an organization’s database has been hit by fraudsters, leads to loss of competitive advantage. This also leads to loss of credibility. There have been instances where share prices of such companies went down, when the news of such attach percolated to the market.

- **Disclosure of Confidential, Sensitive or Embarrassing Information:** Cyber-attack may expose critical information in public domain. For example, instances of individuals leaking information about government’s secret programs.

- **Sabotage:** The above situation may lead to misuse of such information by enemy country.

**Question 17**

Discuss major techniques to commit cyber frauds in brief.

Or

In spite of having various controls as well as counter measures in place, cyber frauds are happening and increasing on a continuous basis. Discuss any six types of Cyber Frauds.

**Answer**

Following are the major techniques to commit cyber frauds:

- **Hacking:** It refers to unauthorized access and use of computer systems, usually by means of personal computer and a telecommunication network. Normally, hackers do not intend to cause any damage.

- **Cracking:** Crackers are hackers with malicious intentions, which means, intent to cause harm. Now across the world hacking is a general term, with two nomenclatures namely: Ethical and Un-ethical hacking. Un-ethical hacking is classified as Cracking.

- **Data Diddling:** Changing data before, during, or after it is entered into the system in order to delete, alter, or add key system data is referred as data diddling.
• **Data Leakage**: It refers to the unauthorized copying of company data such as computer files.

• **Denial of Service (DoS) Attack**: It refers to an action or series of actions that prevents access to a system by its intended/authorized users; causes the delay of its time-critical operations; or prevents any part of the system from functioning.

• **Internet Terrorism**: It refers to using the Internet to disrupt electronic commerce and to destroy company and individual communications.

• **Logic Time Bombs**: These are programs that lie idle until some specified circumstances or a time triggers it. Once triggered, the bomb sabotages the system by destroying programs, data or both.

• **Masquerading or Impersonation**: In this case, perpetrator gains access to the system by pretending to be an authorized user.

• **Password Cracking**: Intruder penetrates a system’s defense, steals the file containing valid passwords, decrypts them and then uses them to gain access to system resources such as programs, files and data.

• **Piggybacking**: It refers to the tapping into a telecommunication line and latching on to a legitimate user before s/he logs into the system.

• **Round Down**: Computer rounds down all interest calculations to 2 decimal places. Remaining fraction is placed in account controlled by perpetrator.

• **Scavenging or Dumpster Diving**: It refers to the gaining access to confidential information by searching discarded corporate records.

• **Social Engineering Techniques**: In this case, perpetrator tricks an employee into giving out the information needed to get into the system.

• **Super Zapping**: It refers to the unauthorized use of special system programs to bypass regular system controls and perform illegal acts.

• **Trap Door**: In this technique, perpetrator enters into the system using a back door that bypasses normal system controls and perpetrates fraud.

**Question 18**

Discuss any three Internetworking devices.

**Answer**

<table>
<thead>
<tr>
<th>Device</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge</td>
<td>A bridge connects similar local area networks (e.g. one token ring network to another token ring network).</td>
</tr>
<tr>
<td>Router</td>
<td>A router performs all the functions of a bridge. In addition, it can connect heterogeneous local area networks (e.g. a bus network to a token ring network) and</td>
</tr>
</tbody>
</table>
direct network traffic over the fastest channel between two nodes that reside in different sub-networks (e.g. by examining traffic patterns within a network and between different networks to determine channel availability.)

### Gateway

Gateways are the most complex of the three network connection devices. Their primary function is to perform protocol conversion to allow different types of communication architectures to communicate with one another. The gateway maps the functions performed in an application on one computer to the functions performed by a different application with similar functions on another computer.

---

**Question 19**

*You are selected by UVW Limited to review and strengthen Software Access Control mechanism for their Company. Prepare a report on the need of boundary controls enlisting major boundary control techniques to be implemented by them.*

**Answer**

The company UVW Limited intends to review and strengthen its Software Access Control mechanism. To achieve this objective, the Boundary controls can be put in place that will establish interface between the user of the system and the system itself. The major controls of the boundary system are the access control mechanisms that links the authentic users to the authorized resources, they are permitted to access and thus are the line of control for intruders to gain access to UVW Company’s asset. The access control mechanism has three steps of Identification, Authentication and Authorization with respect to the access control policy implemented. The user can provide three factors of input information for the authentication process and gain access to his required resources.

Major Boundary Control techniques are as follows:

- **Cryptography:** It deals with programs for transforming data into cipher text that are meaningless to anyone, who does not possess the authentication to access the respective system resource or file. Techniques of cryptography are Transposition, Substitution and Product Cipher.

- **Passwords:** User identification by an authentication mechanism with personal characteristics like name, birth date, employee code, function, designation or a combination of two or more of these can be used as a password boundary access control.

- **Personal Identification Numbers (PIN):** PIN, like a password assigned to a user by an institution, is a random number stored in its database independent to a user identification details, or a customer selected number.

- **Identification Cards:** Identification cards are used to store information required in an authentication process. These cards are to be controlled through the application for a card, preparation of the card, issue, use and card return or card termination phases.
• **Biometric Devices:** Biometric identification e.g. thumbs and/or finger impression, eye retina etc. are also used as boundary control techniques.

**Question 20**

*Mr. 'X' has opened a new departmental store and all the activities are computerized. He uses Personal Computers (PCs) for carrying out the business activities. As an IS auditor, list the risks related to the use of PCs in the business of Mr. 'X' and suggest any two security measures to be exercised to overcome them.*

**Answer**

Risks related to the use of PCs in the business are as follows:

- Personal computers are small and easy to connect and disconnect, they are likely to be shifted from one location to another or even taken outside the organization for theft of information.
- Pen drives can be very conveniently transported from one place to another, as a result of which data theft may occur. Even hard disks can be ported easily these days.
- PC is basically a single user oriented machine and hence, does not provide inherent data safeguards. Problems can be caused by computer viruses and pirated software, namely, data corruption, slow operations and system break down etc.
- Segregation of duty is not possible, owing to limited number of staff.
- Due to vast number of installations, the staff mobility is higher and hence becomes a source of leakage of information.
- The operating staff may not be adequately trained.
- Weak access control: Most of the log-on procedures become active at the booting of the computer from the hard drive.

The Security Measures that could be exercised to overcome these aforementioned risks are given as follows:

- Physically locking the system;
- Proper logging of equipment shifting must be done;
- Centralized purchase of hardware and software;
- Standards set for developing, testing and documenting;
- Uses of antimalware software; and
- The use of personal computer and their peripheral must have controls.
- Use of disc locks that prevent unauthorized access to floppy disk or pen drive of a computer.
Question 21

As an IS auditor, what are the output controls required to be reviewed with respect to application controls?

Answer

As an IS Auditor, various Output Controls required to be reviewed with respect to Application Controls are as follows:

- **Storage and logging of sensitive, critical forms**: Pre-printed stationery should be stored securely to prevent unauthorized destruction or removal and usage. Only authorized persons should be allowed access to stationery supplies such as security forms, negotiable instruments, etc.

- **Logging of output program executions**: When programs used for output of data are executed, these should be logged and monitored; otherwise on confidentiality/ integrity of the data may be compromised.

- **Spooling/queuing**: “Spool” is an acronym for “Simultaneous Peripherals Operations Online”. This is a process used to ensure that the user is able to continue working, while the print operation is getting completed.

- **Controls over printing**: Outputs should be made on the correct printer and it should be ensured that unauthorized disclosure of information printed does not take place. Users must be trained to select the correct printer and access restrictions may be placed on the workstations that can be used for printing.

- **Report distribution and collection controls**: Distribution of reports should be made in a secure way to prevent unauthorized disclosure of data. A log should be maintained for reports that were generated and to whom these were distributed. Uncollected reports should be stored securely.

- **Retention controls**: Retention controls consider the duration for which outputs should be retained before being destroyed. Consideration should be given to the type of medium on which the output is stored. Retention control requires that a date should be determined for each output item produced.

Question 22

Software Applications require interface between user and the business functions. Discuss User Controls describing various types of controls to be exercised to achieve system effectiveness and efficiency.

Answer

**User Controls**: Application system represents the interface between the user and the business functions. From the users’ perspective, it is the applications that drive the business logic and thus User Controls are required. The user controls that are to be exercised for system effectiveness and efficiency are as follows:
• **Boundary Controls:** These establish interface between the user of the system and the system itself. The system must ensure that it has an authentic user. Further users are allowed using resources in restricted ways.

• **Input Controls:** Responsible for ensuring the accuracy and completeness of data and instruction input into an application system. Input Controls are validation and error detection of data input into the system.

• **Processing Controls:** These controls are responsible for computing, sorting, classifying and summarizing data. These maintain the chronology of events from the time data is received from input or communication systems to the time data is stored into the database or output as results.

• **Communication Controls:** These controls are responsible for controls over physical components, communication line errors, flows, and links, topological controls, channel access controls, controls over subversive attacks, internetworking controls, communication architecture controls, audit trail controls, and existence controls.

• **Output Controls:** These controls provide functions that determine the data content available to users, data format, timeliness of data and how data is prepared and routed to users.

• **Database Controls:** These are responsible to provide functions to define, create, modify, delete and read data in an information system. These maintain procedural data-set of rules to perform operations on the data to help a manager to take decisions.

**Question 23**

_Do you consider Corrective Controls are a part of Internal Controls? Describe the characteristics of Corrective Controls._

**Answer**

Yes, we consider Corrective Controls to be a part of Internal Controls. Corrective controls are designed to reduce the impact or correct an error once it has been detected. Contingency planning, Backup procedure, Rerun procedures, and Investigate budget variance and report violations are some of the examples of corrective controls. The main characteristics of the corrective controls are as follows:

• Minimizing the impact of the threat;
• Identifying the cause of the problem;
• Providing remedy to the problems discovered by detective controls;
• Getting feedback from preventive and detective controls;
• Correcting error arising from a problem; and
• Modifying the processing systems to minimize future occurrences of the incidents.
Question 24

Operating System not only provides the platform for an application to use various Information System resources but is also the last barrier to be conquered for unlimited access to all the resources. Explain the statement by describing any six operating system access controls to protect IT resources from unauthorized access.

Answer

Operating system not only provides the platform for an application to use various Information System resources but is also the last barrier to be conquered for unlimited access to all the resources. Hence, protecting operating system access is extremely crucial. Some of the common operating system access controls to protect IS resources from unauthorized access are as follows:

- **Automated terminal identification**: This will help to ensure that a session could only be initiated from a location or computer terminal.
- **Terminal log-on procedures**: The log-on procedure does not provide unnecessary help or information, which could be misused by an intruder.
- **User identification and authentication**: The users must be identified and authenticated in a foolproof manner. Depending on risk assessment, more stringent methods like Biometric Authentication or Cryptographic means like Digital Certificates should be employed.
- **Password management system**: An operating system could enforce selection of good passwords. Internal storage of password should use one-way hashing algorithms and the password file should not be accessible to users.
- **Use of system utilities**: System utilities are the programs that help to manage critical functions of the operating system e.g. addition or deletion of users. Obviously, this utility should not be accessible to a general user. Use and access to these utilities should be strictly controlled and logged.
- **Duress alarm to safeguard users**: If users are forced to execute some instruction under threat, the system should provide a means to alert the authorities.
- **Terminal time out**: Log out the user if the terminal is inactive for a defined period. This will prevent misuse in absence of the legitimate user.
- **Limitation of connection time**: Define the available time slot. Do not allow any transaction beyond this time. For example, no computer access after 8.00 p.m. and before 8.00 a.m.—or on a Saturday or Sunday.

Question 25

Explain any four advantages of electronic door locks over bolting and combinational locks as a part of Physical Access Controls.
Protection of Information Systems

Answer

The following are the advantages of electronic door locks over bolting and combinational locks:

- Through the special internal code that is stored internally within the card; cards can be made to identify the correct individual.
- Individuals access needs can be restricted through the special internal code and sensor devices. Restrictions can be assigned to doors or to hours of the day.
- Degree of duplication is reduced.
- Card entry can be easily deactivated in the event an employee is terminated or a card is lost or stolen. If unauthorized entry is attempted silent or audible alarms can be automatically activated.
- An administrative process, which may deal with issuing, accounting for and retrieving the card keys, are also, parts of security. The card key becomes an important item to retrieve when an employee leaves the firm.

Question 26

‘Crimes are committed by using computers and can damage the reputation, morale and even the existence of an organization.’ What are the problems do you think that any organization can face with the result of computer crimes?

Answer

(a) ‘Crimes are committed by using computers and can damage the reputation, morale and even the existence of an organization.’ Crimes are committed by using computers and can damage the reputation, morale and even the existence of an organization. Computer crimes generally result in loss of customers, embarrassment to management and legal actions against the organizations. These are given as follows:

- **Financial Loss**: Financial losses may be direct like loss of electronic funds or indirect like expenditure towards repair of damaged electronic components.

- **Legal Repercussions**: An organization must adhere to many laws while developing security policies and procedures. These laws protect both the perpetrator and organization from trial. The organizations will be exposed to lawsuits from investors and insurers if there have no proper security measures.

- **Loss of Credibility or Competitive Edge**: To maintain competitive edge, many companies, especially service firms such as banks and investment firms, needs credibility and public trust. This credibility will be shattered resulting in loss of business and prestige if security violation occurs.

- **Blackmail/Industrial Espionage**: By knowing the confidential information, the perpetrator can obtain money from the organization by threatening and exploiting the security violation.
• **Disclosure of Confidential, Sensitive or Embarrassing Information:** These events can spoil the reputation of the organization. Legal or regulatory actions against the company may be also a result of disclosure.

• **Sabotage:** People, who may not be interested in financial gain but who want to spoil the credibility of the company or to will involve in such activities. They do it because of their dislike towards the organization or for their intemperance.

• **Spoofing:** A spoofing attack involves forging one’s source address. One machine is used to impersonate the other in spoofing technique. A penetrator makes the user think that s/he is interacting with the operating system. For example, a penetrator duplicates the login procedure, captures the user’s password, attempts for a system crash and makes the user login again.

**Question 27**

*What are the main characteristics of Detective Controls which are designed to detect errors, omissions or malicious acts that occur?*

**Answer**

The main characteristics of Detective controls which are designed to detect errors, omissions or malicious acts that occur are as follows:

• **Clear understanding of lawful activities so that anything which deviates from these is reported as unlawful, malicious, etc.;**

• **An established mechanism to refer the reported unlawful activities to the appropriate person or group;**

• **Interaction with the preventive control to prevent such acts from occurring; and**

• **Surprise checks by supervisor.**

**Question 28**

*Discuss File Interrogation as one of the three levels of Input Validation Controls.*

**Answer**

Input Validation Controls are intended to detect errors in the transaction data before the data are processed. **File Interrogation is one of the three levels of input validation controls.**

• **Version Usage:** Proper version of a file should be used for processing the data correctly. In this regard, it should be ensured that only the most current file be processed.

• **Internal and External Labeling:** Labeling of storage media is important to ensure that the proper files are loaded for process. Where there is a manual process for loading
files, external labeling is important to ensure that the correct file is being processed. Where there is an automated tape loader system, internal labeling is more important.

- **Data File Security**: Unauthorized access to data file should be prevented, to ensure its confidentiality, integrity and availability. These controls ensure that the correct file is used for processing.

- **Before and after Image and Logging**: The application may provide for reporting of before and after images of transactions. These images combined with the logging of events enable re-construction of the data file back to its last state of integrity, after which the application can ensure that the incremental transactions/events are rolled back or forward.

- **File Updating and Maintenance Authorization**: Sufficient controls should exist for file updating and maintenance to ensure that stored data are protected. The access restrictions may either be part of the application program or of the overall system access restrictions.

- **Parity Check**: When programs or data are transmitted, additional controls are needed. Transmission errors are controlled primarily by detecting errors or correcting codes.

**Question 29**

What should an IS Auditor evaluate while reviewing the adequacy of Data Security Controls?

**Answer**

An Information Systems (IS) Auditor is responsible to evaluate the following while reviewing the adequacy of Data Security Controls:

- Who is responsible for the accuracy of the data?
- Who is permitted to update data?
- Who is permitted to read and use the data?
- Who is responsible for determining who can read and update the data?
- Who controls the security of the data?
- If the IS system is outsourced, what security controls and protection mechanism does the vendor have in place to secure and protect data?
- Contractually, what penalties or remedies are in place to protect the tangible and intangible values of the information?
- The disclosure of sensitive information is a serious concern to the organization and is mandatory on the auditor's list of priorities.
Question 30
What are Asynchronous Attacks? Explain Subversive threats to an Information System.

Answer

Asynchronous Attacks: They occur in many environments where data can be moved asynchronously across telecommunication lines. Numerous transmissions must wait for the clearance of the line before data being transmitted. Data that is waiting to be transmitted are liable to unauthorized access called Asynchronous Attack. These attacks are hard to detect because they are usually very small pin like insertions.

Subversive Threats: An intruder attempts to violate the integrity of some components in the sub-system. Subversive attacks can provide intruders with important information about messages being transmitted and the intruder can manipulate these messages in many ways. An intruder attempts to violate the integrity of some components in the sub-system by:

- **Invasive tap:** By installing it on communication lines, s/he may read and modify data.
- **Inductive tap:** It monitors electromagnetic transmissions and allows the data to be read only.

**Exercise**

1. Discuss major General Controls within an enterprise in brief.
2. What do you mean by Detective Controls? Explain with the help of examples. Also, describe their main characteristics in brief.
3. Discuss Application Controls and their categories in brief.
4. ‘There are various general guidelines, regarding ‘Segregation of Duties’, which may be followed in addition with the concepts like, ‘maker should not be the checker’. Explain those guidelines.
5. What is ‘Data Integrity’? Explain six categories of Integrity Controls in brief.
6. Explain some of the key logical access controls in detail with the help of suitable examples.
7. Describe major controls over environmental exposures.
8. What is Cyber Fraud? Differentiate between pure cyber frauds and cyber enabled frauds.
9. Explain major cyber-attacks reported by various agencies in recent years.
10. Discuss Managerial Controls and their categories in brief.
11. Write short notes on the following:
   (i) Need for protection of Information Systems  
   (ii) Compensatory Controls
   (iii) BCP Controls  
   (iv) Cyber Frauds
   (v) Topological Controls  
   (vi) Backup Controls