

Control Objectives

Basic Concepts

1. **Effect of Computers on Internal Audit**
 - 1.1 **Changes in the audit and audit evidence:** Data retention and storage, Absence of input documents, Lack of visible audit trail, Lack of visible output, Audit evidence, Legal Issues
 - 1.2 **Change in the type and nature of internal controls:** Personnel, Segregation of duties, Authorization procedures, Record keeping, Access to assets and records, Management supervision and review
 - 1.3 **New causes and sources of error:** System generated transactions, Systematic error
 - 1.4 New Audit Processes
2. **Control Objectives for Information Related Technology (COBIT):** The framework addresses the issue of control from three points or dimensions: Business Objectives, IT Resources, IT Processes
3. **Information Systems Control Techniques:** Accounting Controls, Operational Controls, and Administrative Controls
 - 3.1 **Auditor's Categorization of Controls:** These controls are categorized into four groups: Preventive Controls, Detective Controls, Corrective Controls, and Compensatory Controls
 - 3.2 **Audit Trail Objectives:** Audit trails can be used to support security objectives in three ways: detecting Unauthorized Access, Reconstructing Events, and Personal Accountability
4. **System Development and Acquisition Controls:** It includes the following key elements: Strategic master plan, Project controls, Data processing schedule, System performance measurements, Post implementation review
5. **Controls over system implementation:** Acceptance Testing, Volume Testing, Stress Testing, Security Testing, Clerical procedures checking, Back-up and recovery, Parallel operation
6. **Information Classification:** Top Secret, Highly Confidential, Proprietary, Internal Use only, Public Documents
7. **Data Integrity Controls:** Source data control, Input validation routines, On-line data

entry controls, Data processing and storage controls, Output Controls, Data transmission controls

8. Issues and revelations related with Logical Access

8.1 Technical Exposures: Data Diddling, bombs, Trojan Horse, Worms, Rounding Down, Salami Techniques

8.2 Asynchronous Attacks: Data Leakage, Wire tapping, Piggybacking, Shut down of the Computer/ Denial of Service

8.3 Computer Crime Exposures: Financial Loss, Legal Repercussions, Loss of Credibility or Competitive Edge, Blackmail/Industrial Espionage, Disclosure of Confidential, sensitive or Embarrassing information, spoofing and Sabotage

9. Physical Access Controls

9.1 Locks on doors: Cipher locks, Bolting Door Locks, Electronic Door Locks, and Biometric Door Locks

9.2 Physical Identification Medium: Personal Identification Number (PIN), Plastic Cards, Cryptographic Control, and Identification Badges

9.3 Logging on utilities: Manual logging, and Electronic Logging

9.4 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/s, and Secured Report/ Document Distribution Cart

10. Environmental Controls

10.1 Controls for Environmental Exposures: 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 Ceiling surrounding the computer room, Electrical Surge Protectors, 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 plans

10.2 Audit and Evaluation Techniques for Environmental Controls: Water and smoke detectors, Hand-held Fire Extinguishers, Fire Suppressions Systems, regular Inspection by Fire Department, Fireproof Walls, Floors and Ceiling Surroundings the Computer Room, Electrical Surge Protectors, Power leads from two stations, Fully documented and Tested Business Continuity Plan, Wiring Placed in Electrical Panels and Conduit, documented and tested Emergency Evacuation Plans, and Humidity/Temperature Control

11. Security Concepts and Techniques

11.1 Cryptosystems: A cryptosystem refers to a suite of algorithms needed to implement a particular form of encryption and decryption.

11.2 Data Encryption Standard (DES): The DES is a cipher (a method for encrypting information) selected as an official Federal Information Processing Standard (FIPS) for the United States in 1976, and which has subsequently widespread use internationally.

11.3 Public Key Infrastructure (PKI): The system is based on public key cryptography in which each user has a key pair, a unique electronic value called a Public Key and a mathematically related Private Key. The Public Key is made available to those who need to verify the users' identity.

11.4 Firewalls: A firewall is a collection of components (computers, routers, and software) that mediate access between different security domains. These are of four types: Packet Filter Firewalls, Stateful Inspection Firewalls, Proxy Server Firewalls, and Application Level Firewalls

12. Intrusion Detection: This is the attempt to monitor and possibly prevent attempts to intrude into or otherwise compromise the system and network resources of an organization. It falls into two broad categories: Network based systems, and Host based systems.

13. Hacking: This is an act of penetrating computer systems to gain knowledge about the system and 'how it works'. There are many ways in which a hacker can hack: NetBIOS, ICMP Ping, FTP, RPC statd, HTTP.

14. Virus: A virus is a program (usually destructive) that attaches itself to a legitimate program to penetrate the operating system.

14.1 Anti-Virus Software: There are three types of anti-virus software: Scanners, Active Monitor and Heuristic Scanner, and Integrity Checkers

Question 1

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

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

3.4 Information Systems Control and Audit

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 criteria is as follows:

Top Secret: The information is classified as Top Secret/ confidential that can cause serious damage to the organization if lost or made public. Information is relating to pending mergers or acquisitions; investment strategies; plans or designs etc. is highly sensitive. Many restrictions are imposed on the usage of such information and is protected at the highest level of security possible.

Highly Confidential: This class of information, is considered critical for the ongoing business operations and can cause serious impediment, if shared around the organization e.g. sensitive customer information of bank's, solicitors and accountants etc., patient's medical records and similar highly sensitive data. It should not be copied or removed without the consent of appropriate authority and must be kept under operational vigilance. Security at this level should be very high.

Proprietary: Information relating to Procedures, operational work routines, project plans, designs and specifications are of propriety in nature. Such information is for proprietary use to authorized personnel only. Security at this level is high.

Internal Use only: This class of information cannot be circulated outside the organization where its loss would inconvenience the organization or management but disclosure is unlikely to result in financial loss or serious damage to credibility. Internal memos, minutes of meetings, internal project reports are examples of such information. Security at this level is controlled but normal.

Public Documents: This Information is published in the public domain; annual reports, press statements etc.; which has been approved for public use. Security at this level is minimal.

Question 2

Briefly explain the formal change management policies, and procedures to have control over system and program changes.

Answer

Formal change management control policies and procedure for system and program changes include the following:

- Periodically review all systems for needed changes.
- Require all requests to be submitted in a standardized format.
- Log and review requests from authorized users for changes and additions to systems.
- Assess the impact of requested changes on system reliability objectives, policies and standards.
- Categorize and rank all changes using established priorities.

- Implement specific procedures to handle urgent matter, such as logging all emergency changes that required deviations from standard procedures and having management review and approve them after the fact. Make sure there is an audit trail for all urgent matters.
- Communication of all changes to management and keep change requestors informed of the status of their requested changes.
- Require IT management to review, monitor, and approve all changes to hardware, software, and personnel responsibilities.
- Assign specific responsibilities to those involved in the change and monitor their work. Make sure that the specific assignments result in an adequate segregation of duties.
- Control system access rights to avoid unauthorized systems and data access.
- Make sure all changes go through the appropriate steps (development, testing, and implementation).
- Test all changes to hardware, infrastructure, and software extensively in a separate, non production environment before placing it into live production mode.
- Make sure there is a plan for backing out of any changes to mission-critical systems in the event that it does not work or does not operate properly.
- Implement a quality assurance function to ensure that all standards and procedures are followed and to assess if change activities achieve their stated objectives. These findings should be communicated to user departments, information systems management, and top management.

Update all documentation and procedures when changes are implemented.

Question 3

Write short notes on the following:

- Key elements in System Development and Acquisition Control
- Firewalls

Answer

- Key elements in System Development and Acquisition Control:** It is important to have a formal, appropriate, and proven methodology to govern the development, acquisition, implementation, and maintenance of information systems and related technologies. Methodology should contain appropriate controls for management review and approval, user involvement, analysis, design, testing, implementation, and conversion.

Key elements in system Development and acquisition controls and given in following table:

Control Category	Threats/Risks	Controls
System development and	System development projects consume	Long-range strategic master plan, data processing schedules, assignment of

3.6 Information Systems Control and Audit

acquisition controls	excessive resources.	each project to manage team, project development plan, project milestones, performance evaluations, system performance measurements.
Change management controls	Systems development projects consume excessive resources, unauthorised systems changes.	Change management control policies and procedures, periodic review of all systems for needed changes, standardized format for changes, log and review change requests, assess impact of changes on system reliability, categorise and rank all, changes, procedures to handle urgent matters, communicate changes to management and users, management approval of changes, assign specific responsibilities while maintaining adequate segregation of duties etc.

- (b) **Firewall:** A firewall is a collection of components (computers, routers, and software) that mediate access between different security domains. All traffic between the security domains must pass through the firewall, regardless of the direction of the flow. Since the firewall serves as an access control point for traffic between security domains, they are ideally situated to inspect and block traffic and coordinate activities with network intrusion detection system (IDSs).

There are four primary firewall types from which to choose: packet filtering, stateful inspection, proxy servers, and application-level firewalls. Any product may have characteristics of one or more firewall types. The selection of firewall type is dependent on many characteristics of the security zone, such as the amount of traffic, the sensitivity of the systems and data, and applications. Additionally, consideration should be given to the ease of firewall administration, degree of firewall monitoring support through automated logging and log analysis, and the capability to provide alerts for abnormal activity.

Typically, firewalls block or allow traffic based on rules configured by the administrator. Rule sets can be static or dynamic. A static rule set is an unchanging statement to be applied to packet header, such as blocking all incoming traffic with certain source addresses. A dynamic rule set often is the result of coordinating a firewall and an IDS. For example, an IDS that alerts on malicious activity may send a message to the firewall to block the incoming IP address. The firewall, after ensuring that the IP is not on a "white list", creates a rule to block the IP. After a specified period of time the rule expires and traffic is once again allowed from that IP.

Firewalls are subject to failure. When firewalls fail, they typically should fail closed, blocking all traffic, rather than failing open and allowing all traffic to pass. Firewalls

provide some additional services such as network address translation, dynamic host configuration protocols and virtual private network gateways.

Question 4

"While reviewing a client's control system, an information system auditor will identify three components of internal control." State and briefly explain these three components.

Answer

The basic purpose of information system controls in an organization is to ensure that the business objectives are achieved and undesired risk events are prevented or detected and corrected. This is achieved by designing an effective information control framework, which comprises of policies, procedures, practices, and organization structure to give reasonable assurances that the business objectives will be achieved.

While reviewing a client's control systems, the auditor will be able to identify three components of internal controls. Each component is aimed at achieving different objectives as stated below:

- (i) Accounting Controls: These controls are extended to safeguard the client's assets and ensure reliability of financial records.
- (ii) Operational Controls: These deals with the day to day operations, functions and activities to ensure that the operational activities are contributing to business objectives.
- (iii) Administrative Control: These are concerned with ensuring efficiency and compliance with management policies, including the operational controls.

Question 5

A company is engaged in the stores taking data activities. Whenever, input data error occurs, the entire stock data is to be reprocessed at a cost of ₹ 50,000. The management has decided to introduce a data validation step that would reduce errors from 12% to 0.5% at a cost of ₹ 2,000 per stock taking period. The time taken for validation causes an additional cost of ₹ 200. (i) Evaluate the percentage of cost-benefit effectiveness of the decision taken by the management and (ii) suggest preventive control measures to avoid errors for improvement.

Answer

- (i) The percentage of cost benefit effectiveness based on the information is calculated in the following table:

S. No.	Particulars	Without validation Procedure	With Validation Procedure
1.	Cost of reprocessing the stock data	₹ 50,000	₹ 50,000
2.	Risk of data errors	12%	0.5%
3.	Expected processing cost	₹ 6,000	₹ 250
4.	Cost of validation procedure	Nil	₹ 2,000

3.8 Information Systems Control and Audit

5.	Cost of delay due to validation	Nil	₹ 200
6.	Total cost involved	₹ 56,000	₹ 52,450
7.	Net expected benefit in %		₹ 3,550 6.3%

Hence there is 6.3% cost benefit effectiveness of the decision taken by the management.

(ii) Preventive Control Measures

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. The broad characteristics of preventive controls are:

- (i) A clear-cut understanding about the vulnerabilities of the asset.
- (ii) Understanding probable threats.
- (iii) Provision of necessary controls for probable threats from materializing.

Any control 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.

Some of the major preventive controls to avoid errors are as follows:

- Employ qualified personnel
- Segregation of duty
- Access controls
- Vaccination against disease
- Maintain proper documentation
- Prescribing appropriate books for a course
- Training and retraining of personnel
- Authorization of transactions
- Validation, edit checks in the application programs
- Firewalls
- Anti-virus software
- Passwords

The above list in no way is exhaustive, but is a mix of manual and computerized preventive controls. The following table enumerates the kind of manual controls and computerized controls applied to a similar scenario.

Scenario	Manual Control	Computerized Control
Restrict unauthorized entry into the premises	Build a gate and post a security guard.	Use access control software, smart card, biometrics, etc.
Restricted unauthorized entry into the software applications	Keep the computer in a secured location and allow only authorized person to use the applications.	Use access control, viz. User ID, password, smart card, etc.

Table-2: Manual & Computerized Controls

Question 6

What are the issues that should be considered by a system auditor at post implementation review stage before preparing the audit report?

Answer

An auditor will consider following issues at PIR (Post Implementation Review) stage before preparing the audit report:

- (i) Interview business users in each functional area covered by the system, and assess their satisfaction with, and overall use of, the system.
- (ii) Interview security, operations and maintenance staff and, within the context of their particular responsibilities, assess their reactions to the system.
- (iii) Based on the User Requirements Specification, determine whether the system's requirements have been met. Identify the reasons(s) why any requirements are not to be provided, are yet to be delivered, or which do not work properly.
- (iv) Confirm that the previous system has been de-commissioned or establish the reasons(s) why it remains in use.
- (v) Review system problem reports and change proposals to establish the number and nature (routine, significant, major) of problems, and changes being made to remedy them. The volume of system change activity can provide an indicator of the quality of systems development.
- (vi) Confirm that adequate internal controls have been built into the system, that these are adequately documented, and that they are being operated correctly. Review the number and nature of internal control rejections to determine whether there are any underlying system design weaknesses.
- (vii) Confirm that an adequate Service Level Agreement has been drawn up and implemented. Identify and report on any area where service delivery either falls below the level specified, or is inadequate in terms of what was specified.

3.10 Information Systems Control and Audit

- (viii) Confirm that the system is being backed up in accordance with user requirements, and that it has been successfully restored from backup media.
- (ix) Review the Business Case and determine whether:
 - anticipate benefits have / are been achieved;
 - any unplanned benefits have been identified;
 - costs are in line with those estimated;
 - benefits and costs are falling with the anticipated time-frame.
- (x) Review trends in transaction throughput and growth in storage use to identify that the anticipated growth of the system is in line with the forecast.

Question 7

Explain the term "Cryptosystems". Briefly discuss Data Encryption Standard.

Answer

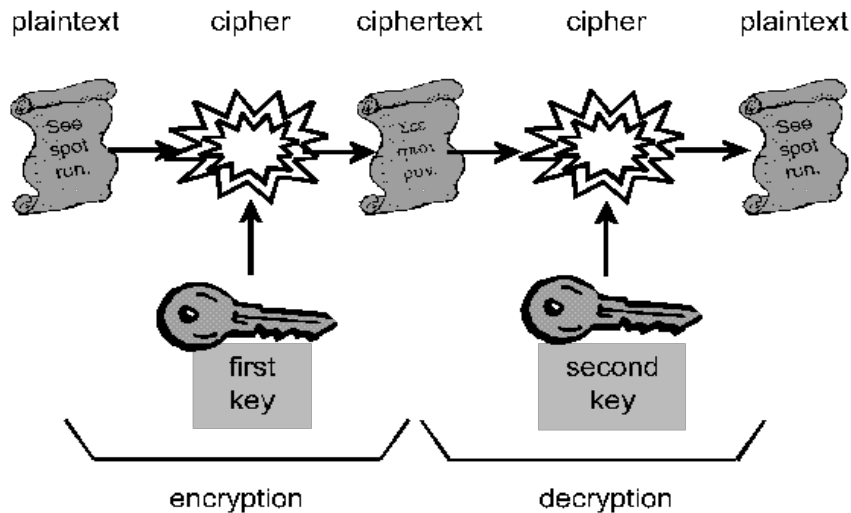
Cryptosystems: A cryptosystem refers to a suite of algorithms needed to implement a particular form of encryption and decryption. Typically, it consists of following three algorithms:

- Key Generation Algorithm,
- Encryption Algorithm and
- Decryption Algorithm.

The pair of algorithms of Encryption and Decryption is referred as Cipher or Cipher.

Data Encryption Standard (DES): It is a cipher. It is a mathematical algorithm for encrypting and decrypting binary coded information. Encrypting of data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. Encryption and Decryption operations are done by using a binary number called a key. A key consists of 64(bits) binary digits. Among these 64 bits, 56 bits are used for encryption/decryption and remaining 8 bits are used for error detection. Authorized users of the encrypted data must have the unique key that was used to encipher the data in order to decrypt it. Selection of a different key causes the cipher that is produced for any given set of inputs to be different. The cryptographic security of the data depends on the security provided for the key used to encipher and decipher the data. A standard algorithm based on a secure key thus provides a basis for exchanging encrypted computer data by issuing the key used to encipher it to those authorized to have the data.

The encryption and decryption processes are depicted in the following diagram:



Some documentation distinguishes DES from its algorithms. It refers algorithms as *DEA* (*Data Encryption Algorithm*).

Question 8

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

Answer

Access control mechanism processes the user request for resources in three steps. They are:

- Identification
- Authentication
- Authorization

The access control mechanisms operate in the following sequence:

1. The users have to identify themselves, thereby indicating their intent to request the usage of system resources,
2. The users must authenticate themselves and the mechanism must authenticate itself, and
3. The users request for specific resources, their need for those resources and their areas of usage of these resources.

The mechanism accesses

- (a) previously stored information about users,

3.12 Information Systems Control and Audit

- (b) the resources they can access, and
- (c) the action privileges they have with respect to these resources.

The mechanism verifies this information against the user entries and it then permits or denies the request.

Identification and Authentication: Users identify themselves to the access control mechanism by providing information such as a name, account number, badge, plastic card, finger print, voice print or a signature. To validate the user, his entry is matched with the entry in the authentication file. The authentication process then proceeds on the basis of information contained in the entry, the user having to indicate prior knowledge of the information.

Authorization: There are two approaches to implementing the authorization module in an access control mechanism:

- *Ticket oriented:* In this approach the access control mechanism assigns the 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
- *List oriented:* In this 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.

Question 9

Discuss anti-virus software and its types.

Answer

Anti-virus Software: It is a program that is used to detect viruses, and prevent their further propagation and harm.

Three types of anti-virus software are briefly discussed below:

Scanners: Scanners for a sequence of bits called virus signatures that are characteristic of virus codes. They check memory, disk boot sectors, executables and systems files to find matching bit patterns. As new viruses emerge frequently, it is necessary to frequently update the scanners with the data on virus code patterns for the scanners to be reasonably effective.

Active Monitor and Heuristic Scanner: This looks for critical interrupt calls and critical operating systems functions such as OS calls and BIOS calls, which resemble virus action.

Integrity Checkers: These can detect any unauthorized changes to files on the system. These can detect any unauthorized changes to the files on the system. The software performs a "take stock" of all files resident on the system and computes a binary check data called the Cyclic Redundancy Check (CRC). When a program is called for execution, the software computes the CRC again and checks with the parameter stored on the disk.

Question 10

Discuss Audit and Evaluation techniques for Physical access.

Answer

Audit and Evaluation Techniques for Physical Access: Information Systems Processing Facility (IPF) is used to gain an overall understanding and perception of the installation being reviewed. This expedition provides the opportunity to being reviewing the physical access restriction. Information processing facility (Computer room, programmers area, tape library, printer stations and management offices) and any off-site storage facilities should also be included in this tour. Much of the testing of physical safeguards can be achieved by visually observation of the safeguards tested previously. Documents to assist with this effort include emergency evacuation procedures, inspection tags, fire suppression system test results and key lock logs. Testing should extend beyond the information processing. The facility/computer room should include the following related facilities:

- Computer storage rooms (this includes equipment, paper and supply rooms
- Location of all communication equipment identified on the network diagram.
- Location of all operator consoles.
- Off-site backup storage facility.
- Printer rooms.
- Tape library.
- UPS/generator.

To do thorough testing, we have to look above the ceiling panels and below the raised floor in the computer operations centre. Keen observation is done on smoke and water detectors, and special emphasis is given to general cleanliness and walls that extend all the way to the real ceiling. The following paths of physical entry should be evaluated for proper security.

- All entrance points.
- Glass windows and walls
- Movable walls and modular cubicles.
- Above suspended ceilings and beneath raised floors.
- Ventilation systems.

These security points must be properly governed to avoid illegal entry.

Question 11

Describe various types of firewalls in brief.

Answer

Firewalls: A firewall is a collection of components (computers, routers, and software) that mediate access between different security domains. All traffic between the security domains

must pass through the firewall, regardless of the direction of the flow. Since the firewall serves as an access control point for traffic between security domains, they are ideally situated to inspect and block traffic and coordinate activities with network intrusion detection systems (IDSs).

The four primary firewall types are given as follows:

- (i) **Packet Filter Firewalls:** Packet filter firewalls evaluate the headers of each incoming and outgoing packet to ensure it has a valid internal address, originates from a permitted external address, connects to an authorized protocol or service, and contains valid basic header instructions. If the packet does not match the pre-defined policy for allowed traffic, then the firewall drops the packet. Packet filters generally do not analyze the packet contents beyond the header information. Many routers contain access control lists (ACLs) that allow for packet-filtering capabilities.
- (ii) **Stateful Inspection Firewalls:** Stateful inspection firewalls are packet filters that monitor the state of the TCP connection. Each TCP session starts with an initial “handshake” communicated through TCP flags in the header information. When a connection is established the firewall adds the connection information to a table. The firewall can then compare future packets to the connection or state table. This essentially verifies that inbound traffic is in response to requests initiated from inside the firewall.
- (iii) **Proxy Server Firewalls:** Proxy servers act as an intermediary between internal and external IP addresses and block direct access to the internal network. Essentially, they rewrite packet headers to substitute the IP of the proxy server for the IP of the internal machine and forward packets to and from the internal and external machines. Due to that limited capability, proxy servers are commonly employed behind other firewall devices. The primary firewall receives all traffic, determines which application is being targeted, and hands off the traffic to the appropriate proxy server. Common proxy servers are the domain name server (DNS), Web server (HTTP), and mail (SMTP) server. Proxy servers frequently cache requests and responses, providing potential performance benefits.

Additionally, proxy servers provide another layer of access control by segregating the flow of Internet traffic to support additional authentication and logging capability, as well as content filtering. Web and e-mail proxy servers, for example, are capable of filtering for potential malicious code and application-specific commands (see “Malicious Code”). They may implement anti-virus and anti-spam filtering, disallow connections to potentially malicious servers, and disallow the downloading of files in accordance with the institution's security policy.

- (iv) **Application-Level Firewalls:** Application-level firewalls perform application-level screening, typically including the filtering capabilities of packet filter firewalls with additional validation of the packet content based on the application. Application-level firewalls capture and compare packets to state information in the connection tables.

Unlike a packet filter firewall, an application-level firewall continues to examine each packet after the initial connection is established for specific application or services such as telnet, FTP, HTTP, SMTP, etc. The application-level firewall can provide additional screening of the packet payload for commands, protocols, packet length, authorization, content, or invalid headers. Application level firewalls provide the strongest level of security, but are slower and require greater expertise to administer properly.

Question 12

What is data privacy? Explain the major techniques to address privacy protection for IT systems.

Answer

Data Privacy: This refers to the evolving relationship between technology and the legal right to, or public expectation of privacy in the collection and sharing of data. Privacy problems exist wherever uniquely identifiable data relating to a person or persons are collected and stored, in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues. The most common sources of data that are affected by data privacy issues are:

- Health information
- Criminal justice
- Financial information
- Genetic information
- Location information

Protecting data privacy in information systems : Increasingly, as heterogeneous information systems with different privacy rules are interconnected, technical control and logging mechanisms (policy appliances) will be required to reconcile, enforce and monitor privacy policy rules (and laws) as information is shared across systems and to ensure accountability for information use. There are several technologies to address privacy protection in enterprise IT systems. These falls into two categories: communication and enforcement.

(i) Policy Communication

- P3P - The Platform for Privacy Preferences. P3P is a standard for communicating privacy practices and comparing them to the preferences of individuals.

(ii) Policy Enforcement

- XACML - The extensible Access Control Markup Language together with its Privacy Profile is a standard for expressing privacy policies in a machine-readable language which a software system can use to enforce the policy in enterprise IT systems.

3.16 Information Systems Control and Audit

- EPAL - The Enterprise Privacy Authorization Language is very similar to XACML, but is not yet a standard.
- WS-Privacy - "Web Service Privacy" will be a specification for communicating privacy policy in web services. For example, it may specify how privacy policy information can be embedded in the SOAP envelope of a web service message.

Question 13

Describe any three ways in which a hacker can hack the system.

Answer

The three ways in which a hacker can hack, are given as follows:

- **NetBIOS:** NetBIOS hackers are the worst kind, since they don't require you to have any hidden backdoor program running on your computer. This kind of hack exploits a bug in Windows 9x. NetBIOS is meant to be used on local area networks, so machines on that network can share information. Unfortunately, the bug is that NetBIOS can also be used across the Internet - so a hacker can access your machine remotely.
- **ICMP 'Ping' (Internet Control Message Protocol):** ICMP is one of the main protocols that make the Internet work. It stands for Internet Control Message Protocol. 'Ping' is one of the commands that can be sent to a computer using ICMP. Ordinarily, a computer would respond to this ping, telling the sender that the computer does exist. This is all pings are meant to do. Pings may seem harmless enough, but a large number of pings can make a Denial-of-Service attack, which overloads a computer. Also, hackers can use pings to see if a computer exists and does not have a firewall (firewalls can block pings). If a computer responds to a ping, then the hacker could launch a more serious form of attack against a computer.
- **FTP (File Transfer Protocol) :**FTP is a standard Internet protocol, standing for File Transfer Protocol. It can be used for file downloads from some websites. If you have a web page of your own, you may use FTP to upload it from your home computer to the web server. However, FTP can also be used by some hackers. FTP normally requires some form of authentication for access to private files, or for writing to files. FTP backdoor programs, such as: Doly Trojan, Fore, and Blade Runner. Simply we can turn the computer into an FTP server, without any authentication.

Question 14

Explain the role of IS Auditor with respect to quality control of systems.

Answer

IS Auditor's Role: In case, the auditor intends to carry out detailed reviews of, for example, logical design, it will probably be necessary either to employ expert assistance, or to undertake training in the particular technical skills required.

The following are the general questions that the IS Auditor needs to consider for quality control:

- (a) does system design follow a defined and acceptable standard?
- (b) are completed designs discussed and agreed with the users?
- (c) does the project's quality assurance procedures ensure that project documentation is reviewed against the organization's technical standards and policies, and the user requirements specification.
- (d) do quality reviews follow a defined and acceptable standard?
- (e) are quality reviews carried out under the direction of a technically competent person who is managerially independent from the design team;
- (f) are auditors/security staff invited to comment on the internal control aspects of system designs and development specifications?
- (g) are statistics of defects uncovered during quality reviews and other forms of quality control maintained and analyzed for trends? Is the outcome of trend analysis fed back into the project to improve the quality of other deliverables?
- (h) are defects uncovered during quality reviews always corrected?
- (i) does the production of development specifications also include the production of relevant acceptance criteria?
- (j) has a configuration manager been appointed? Has the configuration management role been adequately defined?
- (k) are all configuration items (hardware, software, documentation) that have passed quality review been placed under configuration management and version control?
- (l) has sufficient IT been provided to assist with the configuration management task?
- (m) are effective procedures in place for recording, analyzing and reporting failures uncovered during testing?
- (n) are effective change management procedures are in place to control changes to configuration items?
- (o) has a Training Plan been developed and quality reviewed? Has sufficient time and resources been allocated to its delivery?
- (p) has a system installation plan been developed and quality reviewed?
- (q) has an acceptance testing plan been drawn up? Is it to an acceptable standard? Does it cover all aspects of the user requirements specification?
- (r) does the acceptance test plan clearly allocate roles and responsibilities for undertaking and reviewing the results of acceptance testing?
- (s) has the acceptance test plan been discussed with, and signed off by the prospective system owner?

3.18 Information Systems Control and Audit

- (t) is the system development environment regularly backed up with copies of backed up configuration item held securely at a remote location?
- (u) has the development environment been recovered from backup media?
- (v) are contingency plans commensurate with the critically of the project.
- (w) do regular project board meetings take place to review project progress against budget and deadline?
- (x) is the Business Case regularly updated to ensure that the project remains viable?

Question 15

Write short notes on the following:

- (i) *Locks on Doors with respect to physical access control*
- (ii) *Data encryption standard*
- (iii) *Hacking*

Answer

- (i) **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 sequence, 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 exists must be usable all the time. More sophisticated and expensive cipher locks can be computer coded with a person's handprint. A matching handprint unlocks the door.

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 not be duplicated.

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

Biometric Door Locks: These locks are extremely secure where an individual's unique body features, such as voice, retina, fingerprint or signature, activate these locks. This system is used in instances when extremely sensitive facilities must be protected, such as in the military.

- (ii) **Data Encryption Standard (DES):** It is a Cipher (a method for encrypting information) selected as an official Federal Information Processing Standard (FIPS) for the United

States in 1976, and which has subsequently enjoyed widespread use internationally. It is a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key. A key consists of 64 binary digits ('0's or '1's) of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits which are not used by the algorithm are used for error detection. The 8 error detecting bits are set to make the parity of each 8 bits byte of the key odd, i.e. there is an odd number of "1" in each 8-bits byte.

- (iii) **Hacking:** It is an act of penetrating computer systems to gain knowledge about the system and how it works. Technically, a hacker is someone who is enthusiastic about computer programming and all things relating to the technical workings of a computer.

Crackers are people who try to gain unauthorized access to computers. This is normally done through the use of a "backdoor" program installed on the machine. A lot of crackers also try to gain access to resources through the use of password cracking software, which tries billions of passwords to find the correct one for accessing a computer.

There are many ways in which a hacker can hack. These are:

- .. Net BIOS
- .. ICMP Ping
- .. FTP
- .. RPC. Statd
- .. HTTP.

Question 16

Discuss the role of IS auditor with respect to

- (a) *Physical access controls*
- (b) *Environmental controls.*

Answer

- (a) **Role of IS Auditor in Physical Access Controls:** Auditing Physical Access requires the auditor to review the physical access risk and controls to form an opinion on the effectiveness of the physical access controls. This involves the following:

- (i) **Risk Assessment:** The auditor must satisfy himself that the risk assessment procedure adequately covers periodic and timely assessment of all assets, physical access threats, vulnerabilities of safeguards and exposures there from.

- (ii) **Controls Assessment:** The auditor based on the risk profile evaluates whether the physical access controls are in place and adequate to protect the IS assets against the risks.
- (iii) **Planning for review of physical access controls:** It requires examination of relevant documentation such as the security policy and procedures, premises plans, building plans, inventory list and cabling diagrams.
- (iv) **Testing of Controls:** The auditor should review physical access controls to satisfy for their effectiveness. This involves:
 - .. Tour of organizational facilities including outsourced and offsite facilities.
 - .. Physical inventory of computing equipment and supporting infrastructure.
 - .. Interviewing personnel can also provide information on the awareness and knowledge of procedures.
 - .. Observation of safeguards and physical access procedures. This would also include inspection of:
 - (i) Core computing facilities.
 - (ii) Computer storage rooms.
 - (iii) Communication closets.
 - (iv) Backup and off site facilities.
 - (v) Printer rooms.
 - (vi) Disposal yards and bins.
 - (vii) Inventory of supplies and consumables.
 - .. Review of physical access procedures including user registration and authorization, authorization for special access, logging, review, supervision etc. Employee termination procedures should provide withdrawal of rights such as retrieval of physical devices like smart cards, access tokens, deactivation of access rights and its appropriate communication to relevant constituents in the organization.
 - .. Examination of physical access logs and reports. This includes examination of incident reporting logs and problem resolution reports.
- (b) **Role of Auditor in Environment Controls:** The attack on the World Trade Centre in 2001 has created a worldwide alert bringing focus on business continuity planning and environmental controls. Audit of environment controls should form a critical part of every IS audit plan. The IS auditor should satisfy not only the effectiveness of various technical controls but that the overall controls assure safeguarding the business against environmental risks. Some of the critical audit considerations that an IS auditor should take into account while conducting his audit are given below:

Audit Planning and Assessment: As part of risk assessment:

- .. The risk profile should include the different kinds of environmental risks that the organization is exposed to. These should comprise both natural and man-made threats. The profile should be periodically reviewed to ensure updation with newer risk that may arise.
- .. The controls assessment must ascertain that controls safeguard the organization against all acceptable risks including probable ones and are in place.
- .. The security policy of the organization should be reviewed to access policies and procedures that safeguard the organization against environmental risks.
- .. Building plans and wiring plans need to be reviewed to determine the appropriateness of location of IPF, review of surroundings, power and cable wiring etc.
- .. The IS Auditor should interview relevant personnel to satisfy himself about employees' awareness of environmental threats and controls, role of the interviewee in environmental control procedures such as prohibited activities in IPF, incident handling, and evacuation procedures to determine if adequate incident reporting procedures exist.
- .. Administrative procedures such as preventive maintenance plans and their implementation, incident reporting and handling procedures, inspection and testing plan and procedures need to be reviewed.

Audit of Technical Controls: Audit of environmental controls requires the IS Auditor to conduct physical inspections and observe practices. S/he must verify:

- .. The IPF and the construction with regard to the type of materials used for construction.
- .. The presence of water and smoke detectors, power supply arrangements to such devices, and testing logs.
- .. The location of fire extinguishers, fire fighting equipment and refilling date of fire extinguishers.
- .. Emergency procedures, evacuation plans and making of fire exists. If necessary, the IS Auditor may also use a mock drill to test the preparedness with respect to disaster.
- .. Documents for compliance with legal and regulatory requirements with regard to fire safety equipment, external inspection certificate and shortcomings pointed out by other inspectors / auditors.
- .. Power sources and conduct tests to assure the quality of power, effectiveness of the power conditioning equipment and generators. Also the power supply interruptions must be checked to test the effectiveness of the back-up power.

3.22 Information Systems Control and Audit

- .. Environmental control equipment such as air-conditioning, dehumidifiers, heaters, ionizers etc.
- .. Compliant logs and maintenance logs to assess if MTBF and MTTR are within acceptable levels.
- .. Activities in the IPF. Identify undesired activities such as smoking, consumption of eatables etc.

Question 17

Write short notes on the Control Objectives for Information related Technology (COBIT).

Answer

Control Objectives for Information Related Technology (COBIT): The Information Systems Audit and Control Foundation (ISACF) developed the Control Objectives for Information and Related Technology (COBIT). COBIT is a trademark of generally applicable information systems security and control practices for IT controls. The framework allows:

- (i) management to benchmark the security and control, practices of IT environments;
- (ii) users of IT services to be assured that adequate security and control exist, and
- (iii) auditors to substantiate their opinions on internal control and to advice on IT security and control matters.

The framework addresses the issue of control from three vantage points, or dimensions:

- (1) Business Objectives. To satisfy business objectives, information must conform to certain criteria the COBIT refers to as business requirements for information. The criteria are divided into seven distinct yet overlapping categories that map into the COSO objectives: effectiveness (relevant, pertinent, and timely), efficiency, confidentiality, integrity, availability, compliance with legal requirements and reliability.
- (2) IT resources, while include people, application systems, technology, facilities, and data.
- (3) IT processes, which are broken into four domains: planning and organization, acquisition and implementation, delivery and support, and monitoring.

COBIT, which consolidates standards from 36 different sources into a single framework, is having a big impact on the information systems profession. It is helping managers to learn how to balance risk and control investment in an information system environment. It provides users with greater assurance that the security and IT controls provided by internal and third parties are adequate. It guides auditors as they substantiate their opinions and as they provide advice to management on internal controls.

Exercise

Question 1

An auditor while evaluating the reliability of a control implemented in a transaction process, had to estimate the reliability per transaction. A test was undertaken and the result indicated that the control was unreliable. The reliability of the process was 0.15 when the control was in place and was 0.09 when the control was absent. The management had estimated the cost of reprocessing the errors as Rs.1000 per transaction procedure. Evaluate the net benefit of the control procedure if the cost of implementation of the control is Rs.10, 000.

Question 2

Identify and briefly discuss the necessary data integrity control techniques for the following processes in a payroll system:

- (a) *Addition/deletion/updating of employee data by the HR department,*
- (b) *Payroll processing and storage, and*
- (c) *Pay slip generation and consolidated pay report department-wise.*

Question 3

The Techno organization is implementing an off-site storage for its critical data. As an internal auditor, what are your recommendations for identifying the physical and environmental exposure and suggest controls for the same.

Question 4

In today's pervasive, internet banking systems with a centralized database environment monitoring of unauthorized intrusion into the banking network is a critical task. Prepare a report on the control methods by which the network can be protected.

Question 5

Do a comparative analysis on the different types of firewalls that mediate the access between different domains.

Question 6

ABC University currently provides the ability to register for classes via an enterprise software system within its intranet. However, the university is in the process of modifying its student registration system to allow registrations via the web.

Based on the given case, answer the following:

- (a) *As an IS Auditor, suggest the change controls to be implemented to monitor the change.*
- (b) *Role of an IS auditor in evaluating the logical access controls implemented in the new system.*

3.24 Information Systems Control and Audit

(c) As an IS Auditor, list the issues that need to be considered for quality control.

Question 7

The post implementation audit follow-up is an important step in the information systems audit process. What are the major control considerations that are to be addressed by the auditor in this step?

Question 8

Briefly state the need to install a 'Fire Suppression System' in an information processing facility and the various installation techniques.

Question 9

Discuss the various environmental control techniques that can be implemented to prevent the unauthorized access for critical IT infrastructures like server room, storage network devices, and switch/router installations.

Question 10

"A financial institute needs to authenticate its electronic credentials by ensuring its PKI policies and controls". Comment on the statement.

Question 11

The validity of the output generated from application software ultimately depends on the user, who is responsible for data submission and correction of errors. Briefly discuss the various user controls and error correction techniques to be followed.

Question 12

As a member of the system implementation and quality control team, prepare a quality control review checklist from an IS Auditor's perspective.