

CONTROL OBJECTIVES

Question 1

Write short notes on the following:

- (a) *Key elements in System Development and Acquisition Control* (5 Marks) (Nov 2008)
- (b) *Control Objectives for Information related Technology (COBIT)* (5 Marks) (Jun 2009)

or

What is COBIT? Give three vantage points from which the issue of control can be addressed by this framework. (5 Marks) (May 2010)

- (c) *Firewall* (5 Marks) (Jun 2009) and (4 Marks) (May 2011)

Answer

- (a) 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. Methodology also should make it possible for management to trace information inputs from their source to their final disposition or from their final disposition back to the original source (the audit trail).

Software development is an integrated process spanning the entire IT organization. The term “life cycle” can be taken to represent the collection of agreed upon steps to control development, modification and distribution of code. While change and configuration management denote separate entities exerting policy over standards for the production environment, the design of these standards and all efforts between these points can be characterized as the world of software development and code.

The IT Governance Institute (ITGI) has produced clear and aligned frameworks for the representation of software development best practice. The newly numbered control process Acquire and Implement 7 (AI7), Install and accredit solutions and changes of Control Objectives for Information and related Technology (COBIT®)4.1 is the most

widely adopted matrix and measure for all integrated IT and enterprise controls. It aligns with the concepts of the Capability Maturity Model (CMM), IT Infrastructure Library (ITIL), ISO27001 and COSO, COBIT 4.1 advances with increased attention in the areas of SDLC, quality and project risk management.

Install and accredit solutions and changes are the high-level functional area that captures the greatest number of features representing the activities related to SDLC or release management. AI7 as stated in the standards document is given as follows:

New systems need to be made operational once development is complete. This requires proper testing in a dedicated environment with relevant test data, definition of rollout and migration instructions, release planning and actual promotion to production, and a post implementation review. This assures that operational systems are in line with the agreed expectations and outcomes.

AI7 includes inputs and outputs to configuration, project, change, maintenance and acquisition programs. With handoffs based in triggers, performance goals, measurements and business based criteria, documented consensus, and tested results, evidence of their implementation is best suited to automated systems.

(b) 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.

- (c) **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 2

"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.

(5 Marks) (Jun 2009)

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 3

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 Rs. 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 Rs. 2,000 per stock taking period. The time taken for validation causes an additional cost of Rs. 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.*

(10 Marks) (Jun 2009)

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

Table: Manual & Computerized Controls

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.

Question 4

What are the issues that should be considered by a system auditor at post implementation review stage before preparing the audit report?
(5 Marks) (Jun 2009)

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.
- (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 5

Explain the term "Cryptosystems". Briefly discuss Data Encryption Standard. (5 Marks) (Nov 2009)

Answer

Cryptosystems: A cryptosystem refers to a suite of algorithms needed to implement a particular form of encryption and decryption. Typically, it consists of three algorithms viz. 1. Key Generation Algorithm, 2. Encryption Algorithm and 3. Decryption Algorithm. The pair of algorithms of Encryption and Decryption is referred as Cipher or Cypher.

Data Encryption Standard (DES): It is a cipher. It is a mathematical algorithm for encrypting and decrypting 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. 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:

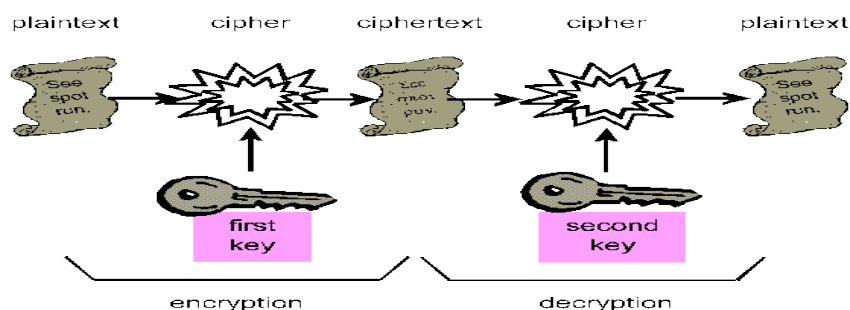


Fig.: Encryption/Decryption Process

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

Question 6

Discuss the three processes of Access Control Mechanism, when a user requests for resources. (5 Marks) (Nov 2009)

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, (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 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 7

Discuss anti-virus software and its types.

(5 Marks) (Nov 2009)

Answer

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

Types: The three types of anti-virus software are: Scanners, Active Monitor and Heuristic Scanner, Integrity Checkers.

Scanners: This looks for a sequence of bits called virus signatures that are characteristic of virus codes. They check memory, disk boot sectors, and 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 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 8

The management of ABC Ltd. wants to design a detective control mechanism for achieving security policy objective in a computerized environment. As an auditor explain, how audit trails can be used to support security objectives.
(10 marks) (May 2010)

Answer**Audit Trail**

Audit trail are logs that can be designed to record activity at the system, application, and user level. It provides an important detective control to help and accomplish security objectives. Many operating systems allow management to select the level of auditing to be provided by the system. This determines which events will be recorded in the log.

Audit trails can be used to support security objectives in three ways:

- Detecting unauthorized access to the system,
- Facilitating the reconstruction of events, and
- Promoting personal accountability.

These are discussed below one by one:

- **Detecting unauthorized access to the system:** Detecting unauthorized access can occur in real time or after the fact. The primary objective of real-time detection is to protect the system from outsiders who are attempting to breach system controls. A real-time audit trail can also

be used to report on changes in system performance that may indicate infestation by a virus or worm. Depending upon how much activity is being logged and reviewed, real-time detection can impose a significant overhead on the operating system, which can degrade operational performance. After-the-fact detection logs can be stored electronically and reviewed periodically or as needed. When properly designed, they can be used to determine if unauthorized access was accomplished, or attempted and failed.

- **Reconstructing Events:** Audit analysis can be used to reconstruct the steps that led to events such as system failures, security violations by individuals, or application processing errors. Knowledge of the conditions that existed at the time of a system failure can be used to assign responsibility and to avoid similar situations in the future. Audit trail analysis also plays an important role in accounting control. For example, by maintaining a record of all changes to account balances, the audit trail can be used to reconstruct accounting data files that were corrupted by a system failure.
- **Personal Accountability:** Audit trails can be used to monitor user activity at the lowest level of detail. This capability is a preventive control that can be used to influence behavior. Individuals are less likely to violate an organization's security policy if they know that their actions are recorded in an audit log.

Audit trail are used to measure the potential damage and financial loss associated with application errors, abuse of authority, unauthorized access by outside intruders. Audit logs also provide valuable evidence or accessing both the adequacies of controls in place and the need for additional controls.

Question 9

Explain the role of IS auditor in evaluating logical access controls. (5 Marks) (May 2010)

Answer

The role of an IS auditor in evaluating logical access controls is briefly discussed below:

- S/he reviews the relevant documents pertaining to logical facilities, risk assessment and evaluation techniques and understands the security risks facing the information processing system.
- The potential access paths into the system is evaluated by the auditor and documented to assess their sufficiency.
- Deficiencies and redundancies are identified and evaluated.
- By supplying appropriate audit techniques, s/he verifies test controls over access paths to determine its effective functioning.
- S/he evaluates the access control mechanism, analyzes the test results and other auditing evidences and verifies whether the control objective has been achieved.
- The auditor also compares security policies and practices of other organizations with the policies of their organizations and assesses its adequacy.

Question 10

“Once the information is classified on various levels, the organization has to decide about the implementation of different data integrity controls.” Do you agree? If yes, explain about data integrity and its policies.
(8 Marks) (Nov 2010)

Answer

Yes, we agree with the statement given in the question.

Data integrity is a reflection of the accuracy, correctness, validity and currency of the data. The primary objective in ensuring integrity is to protect the data against erroneous input from authorized users.

Data Integrity Policies:

These policies are given as follows:

- **Virus Signature updating** – Virus signatures must be updated immediately when they are made available from the vendor.
- **Software testing:** All software must be tested in a suitable test environment before installation on production systems.
- **Division of Environments** – The division of environment into Development, Test and Production is required for critical systems.
- **Version Zero Software** – Version Zero Software (1.0, 2.0 and so on) must be avoided whenever possible to avoid undiscovered bugs.
- **Off-site Backup Storage** – Backups older than one month must be sent offsite for permanent storage.
- **Quarter-End and year-End Backups** – These 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 outrage.

Question 11

What do you understand from the term 'database'? How is it implemented in three different levels?
(4 Marks) (Nov 2010)

Answer**Database:**

Database can be defined as a 'Super-file' which consolidates data records formerly stored in many data files. The data in a database is organized in such a way that access to the data is improved and redundancy is reduced.

Implementation of Databases: Three levels at which database can be implemented, are as under:

- (i) *Physical Level:* It involves the implementation of the database on the hard disk. The management of storage and access is controlled by operating system.
- (ii) *Logical Level:* It is designed by professional programs, which have complete knowledge of DBMS. The storage is logically divided into various tables having techniques for defining relationships with indexes.
- (iii) *External Level:* The logical level defines schema, which is divided into smaller units known as sub-schemas and given to the managers, each sub-schema containing all relevant data needed by one manager.

Question 12

System maintenance is an important phase during the implementation of the system. If so, what are the three categories in which maintenance can be undertaken? As an IS auditor of the organization, how will you evaluate the effectiveness and efficiency of the system maintenance process?
(8 Marks) (Nov 2010)

Answer

Three categories of system maintenance are as follows:

- (i) **Corrective maintenance:** Emergency program fixes and routine debugging-logical errors.
- (ii) **Adaptive maintenance:** Accommodation of change in the user environment.
- (iii) **Perfective maintenance:** User enhancements, improved documentation and recording for improving processing efficiency.

Auditor's Role in System Maintenance:

The effectiveness and efficiency of the system maintenance process is evaluated with the following metrics:

- The ratio of actual maintenance cost per application/operation versus the average of all applications / processes;
- Average time to deliver change requests;
- The number of change requests for the system application that were related to bugs, critical errors and new functional specifications;
- The number of production problems per application and per respective maintenance changes;
- The instances of divergence from standard procedures such as undocumented applications, unapproved and testing reductions;

- The quantity of modules returned to development due to errors discovered in acceptance testing; and
- Time elapsed to analyze and fix problems.

Question 13

Discuss the policies and controls that any financial institution needs to consider when utilizing public key infrastructure.
(8 Marks) (May 2011)

Answer

When utilizing PKI, financial institutions need to consider the following policies and controls:

- Defining within the certificate issuance policy, the methods of initial verification that are appropriate for different types of certificate applicants and the controls for issuing digital certificates and key pairs;
- Selecting an appropriate certificate validity period to minimize transactional and reputation risk exposure- expiration provides an opportunity to evaluate the continuing adequacy of key lengths and encryption algorithms, which can be changed as needed before issuing a new certificate;
- Ensuring that the digital certificate is valid by such means as checking a certificate revocation list before accepting transactions accompanied by a certificate;
- Defining the circumstances for authorizing a certificate's revocation, such as the compromise of a user's private key or the closing of user accounts;
- Updating the database of revoked certificates frequently, ideally in real-time mode;
- Employing stringent measures to protect the root key including limited physical access to Certifying Authority (CA) facilities, tamper-resistant security modules, dual control over private keys and the process of signing certificates, as well as the storage of original and backup keys on computer that do not connect with outside networks;
- Requiring regular independent audits to ensure controls are in place, public and private key lengths remain appropriate, cryptographic modules conform to industry standards, and procedures are followed to safeguard the CA system;
- Recording in a secure audit log all significant events performed by the CA system, including the use of the root key, where each entry is time/date stamped and signed;
- Regularly reviewing exception reports and system activity by the CA's employees to detect malfunctions and unauthorized activities; and
- Ensuring the institution's certificates and authentication systems comply with widely accepted PKI standards to retain the flexibility to participate in ventures that require the acceptance of the financial institution's certificates by other CAs.

Question 14

Describe the role of an IS auditor in the evaluation of physical access control. (4 Marks) (May 2011)

Answer

Role of an IS auditor in evaluation of Physical Access Controls is described below:

- (i) **Risk assessment:** The auditor must satisfy him/herself that the risk assessment procedure adequately covers periodic and timely assessment of all assets, physical access threats, vulnerabilities of safeguards and exposure 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;
 - Examination of physical access logs and reports. Review of physical access procedures including user registration and authorization etc.; and Observation of safeguards and physical access procedures.