

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

Answer **all** questions.

Question 1

ASK International proposes to launch a new subsidiary to provide e-consultancy services for organizations throughout the world, to assist them in system development, strategic planning and e-governance areas. The fundamental guidelines, programmes modules and draft agreements are all preserved and administered in the e-form only.

The company intends to utilize the services of a professional analyst to conduct a preliminary investigation and present a report on smooth implementation of the ideas of the new subsidiary. Based on the report submitted by the analyst, the company decides to proceed further with three specific objectives (i) reduce operational risk, (ii) increase business efficiency and (iii) ensure that information security is being rationally applied. The company has been advised to adopt BS 7799 for achieving the same.

- (a) What are the two primary methods through which the analyst would have collected the data ? (5 marks)
- (b) To achieve their objectives, what are the points BS 7799 has to ensure ? (5 marks)
- (c) Suppose an audit policy is required, how will you lay down the responsibility of audit? (5 marks)
- (d) To retain their e-documents for specified period, what are the conditions laid down by Section 7, Chapter III of Information Technology Act, 2000? (5 marks)

Answer

- (a) Two primary methods through which the analyst would have collected the data are given as follows:
 - (1) **Reviewing internal documents:** The analyst first tries to learn about the organization involved in or affected by the project. For example, to review an inventory system proposal, s/he will try to know 'how the inventory department operates' and 'who are the managers and supervisors'. S/he will examine organization charts and written operating procedures.
 - (2) **Conducting interviews:** Written documents tell the analyst 'how the system should operate' but they may not include enough details to allow a decision to be made about the merits of a system proposal nor do they present users' views about current operations. To learn these details, analysts use interviews. Preliminary investigation interviews involve only management and supervisory personnel.
- (b) BS 7799 should ensure that:
 - (1) Security controls are justified.
 - (2) Policies and procedures are appropriate.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- (3) Security awareness is good amongst staff and managers.
 - (4) All security relevant information processing and supporting activities are auditable and are being audited.
 - (5) Internal audit, incident reporting/management mechanisms are being treated appropriately.
 - (6) Management actively focuses on information security and its effectiveness.
 - (7) Certification can also be used as a part of marketing initiative, providing assurance to business partners and other outsiders.
- (c) The scope of information system auditing should encompass the examination and evaluation of the adequacy and effectiveness of the system of internal control and the quality of performance by the information system. Information System Audit will examine and evaluate the planning, organizing, and directing processes to determine whether reasonable assurance exists that objectives and goals will be achieved. Such evaluations, in the aggregate, provide information to appraise the overall system of internal control.

The audit policy should lay down the responsibilities as follows:

- (1) The policy should lay out the periodicity of reporting and the authority to whom the reporting is to be made.
- (2) A statement of professional proficiency may be included to state the minimum qualification and experience requirements of the auditors.
- (3) All information system auditors will sign a declaration of fidelity and secrecy before commencing the audit work in a form that the inspection department may design.
- (4) The policy may lay out the extent of testing to be done under the various phases of the audit like Planning, Compliance Testing, and Substantive Testing.
- (5) A documented audit program would be developed including the following:
 - ◆ Documentation of the information system auditor's procedures for collecting, analyzing, interpreting, and documenting information during the audit.
 - ◆ Objectives of the audit.
 - ◆ Scope, nature, and degree of testing required for achieving the audit objectives in each phase of the audit.
 - ◆ Identification of technical aspects, risks, processes, and transactions which should be examined.
 - ◆ Procedures for audit will be prepared prior to the commencement of audit work and modified, as appropriate, during the course of the audit.
- (6) The policy should determine when and to whom the audit results would be reported and communicated. It would define the access rights to be given to the auditors.
- (7) The Policy should outline the compliance testing areas.

FINAL (NEW) EXAMINATION : MAY, 2010

- (8) The auditor will carry out substantive testing wherever the auditor observes weakness in internal controls or where risk exposure is high. The auditor may also carry out such tests to gather additional information necessary to form an audit opinion.
- (9) The Audit Policy would define the compulsory audit working papers to be maintained and their formats.
- (d) Section 7, Chapter III of Information Technology Act, 2000/ Information Technology (Amendment) Act, 2008 provides that the documents, records or information which is to be retained for any specified period shall be deemed to have been retained if the same is retained in the electronic form provided the following conditions are satisfied:
- (i) The information therein remains accessible so as to be usable subsequently.
 - (ii) The electronic record is retained in its original format or in a format which accurately represents the information contained.
 - (iii) The details which will facilitate the identification of the origin, destination, dates and time of dispatch or receipt of such electronic record are available therein.

This section does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

Moreover, this section does not apply to any law that provides for the retention of documents, records or information in the form of electronic records.

Question 2

- (a) *What are common threats to the computerized environment other than natural disasters, fire and power failure?* (5 marks)
- (b) *How would you use Data Dictionary as a tool for file security and audit trails?* (5 marks)
- (c) *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)

Answer

- (a) A few common threats to computerized environment other than natural disasters, fire and power failure are:
1. **Communication failure:** Failure of communication lines result in inability to transfer data which primarily travel over communication lines. Where the organization depends on public communication lines e.g. for e-banking, communication failure presents a significant threat that will have a direct impact on operations.
 2. **Disgruntled Employees:** A disgruntled employee presents a threat since, with access to sensitive information of the organization, he may cause intentional harm to the information processing facilities or sabotage operations.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

3. **Errors:** Errors which may result from technical reasons, negligence or otherwise can cause significant integrity issues. A wrong parameter setting at the firewall to “allow” attachments instead of “deny” may result in the entire organization network being compromised with virus attacks.
4. **Malicious Code:** Malicious code such as viruses and worms, which freely access the unprotected networks, may affect organizational and business networks that use these unprotected networks.
5. **Abuse of access privileges by employees:** The security policy of the company authorizes employees based on their job responsibilities to access and execute select functions in critical applications.
6. **Theft or destruction of computing resources:** Since the computing equipment forms the back-bone of information processing, any theft or destruction of the resources can result in compromising the competitive advantage of the organization.
7. **Downtime due to technology failure:** IS facilities may become unavailable due to technical glitches or equipment failure and hence the computing infrastructure may not be available for short or extended periods of time. However, the period for which the facilities are not available may vary in criticality depending on the nature of business and the critical business process that the technology supports.

(b) Data Dictionary

A data dictionary is a computer file that contains descriptive information about the data items in the files of a business information system. Thus, a data dictionary is a computer file about data. Each computer record of a data dictionary contains information about a single data item used in a business information system. Data dictionary contains the information about the identity of the computer programs or individuals permitted to access the data item for the purpose of file maintenance, upkeep or inquiry. It also maintains the identity of the computer programs or individuals, not permitted to access the data items. Because of maintaining above mentioned information, a data dictionary is useful for the security e.g. to prohibit certain employees from gaining access to sensitive payroll data.

Accountants and auditors can also make good use of a data dictionary. For example, a data dictionary can help establish an audit trail because it can identify the input sources of data items, the computer programs that modify particular data items, and the managerial reports on which the data items are output. When an accountant is participating in the design of a new system, a data dictionary can also be used to plan the flow of transaction data through the system.

Finally, a data dictionary can serve as an important aid when investigating or documenting internal control procedures. This is because the details about edit tests, methods of file security, and similar information can be stored in the dictionary.

FINAL (NEW) EXAMINATION : MAY, 2010

(c) 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.

1. **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.
2. **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.
3. **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 3

- (a) *How will you get over the impediments for the successful implementation of ERP? Mention any five.* (10 marks)

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- (b) *A company has decided to outsource a third party site for its alternate back-up and recovery process. What are the issues to be considered by the security administrator while drafting the contract?* (5 marks)
- (c) *Explain the role of IS auditor in evaluating logical access controls.* (5 marks)

Answer

(a) Implementation of ERP

ERP implementation is a special event, which integrates different business functions, different personalities, procedures, ideologies and philosophies together, brings worthwhile and beneficial changes throughout the organization. It involves considerable amount of time, effort, and valuable resources. One can get over the impediments for successful implementation of ERP in the following manner:

- ◆ The success of an implementation mainly depends on how closely the implementation consultants, users and vendors work together to achieve the overall objectives of the organization. The consultants should understand the needs of the users, understanding the business realities and design the business solutions keeping in mind all these factors. It is the users who will be driving the implementation and therefore their active involvement at all stages of implementation is vital for the overall success of implementation.
 - ◆ During the course of implementation, the standard packages may undergo changes which may be a simple one or a major functionality' change. Implementing such change is known as customization. It is always better to satisfy user requirements and overall objectives within the available framework of the existing package because any change in any functional module will have an adverse impact on the functioning of the other modules of the package.
 - ◆ The roles and responsibilities of an employee to be clearly identified, understood and configured in the system. The employees will have to accept new processes and procedures laid down in the ERP system. At the same time, these process and procedures have to be simple and user friendly.
 - ◆ The ability of the ERP package to manage and support dynamically changing business processes is critical requirement for the organization and therefore the package should be expandable and adaptable to meet these changes.
 - ◆ An ERP package after implementation is expected to improve the flow of information and formalize and standardize all the business processes and workflow that exist in an enterprise. It is worthwhile to remember that ERP is an enabling tool, which makes one to do his/her work better, naturally needs additional efforts. A well managed and implemented ERP can give 200% return on investment.
- (b) If a third party site is to be used for backup and recovery purposes, security administrators must ensure that a contract is written to cover the following issues :
- ◆ How soon the site will be made available subsequent to a disaster,

FINAL (NEW) EXAMINATION : MAY, 2010

- ◆ The number of organizations that will be allowed to use the site concurrently in the event of a disaster,
- ◆ The priority to be given to concurrent users of the site in the event of a common disaster,
- ◆ The period during which the site can be used,
- ◆ The conditions under which the site can be used,
- ◆ The facilities and services the site provider agrees to make available, and
- ◆ What controls will be in place and working at the off-site facility.

The above are the main issues that should be covered while drafting a contract. These issues are often poorly specified in reciprocal agreements. Moreover, they can be difficult to enforce under a reciprocal agreement because of the informal nature of the agreement.

(c) 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 4

- (a) *Describe some of the advantages of continuous audit techniques.* (5 marks)
- (b) *Define the following terms related to Information Technology Act, 2000:* (5 marks)
- (i) *Computer contaminant*
 - (ii) *Cyber cafe*
 - (iii) *Electronic form*
 - (iv) *Traffic data*
 - (v) *Asymmetric crypto system.*
- (c) *Give some important advantages of Information System in business* (5 marks)

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- (d) *What is COBIT? Give three vantage points from which the issue of control can be addressed by this framework.* (5 marks)

Answer

- (a) Some of the advantages of continuous audit techniques are given as follows:
- (i) *Timely, comprehensive and detailed auditing* – Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analysed rather than examining the inputs and the outputs only.
 - (ii) *Surprise test capability* – As evidences are collected from the system itself by using continuous audit techniques, auditors can gather evidence without the systems staff and application system users being aware that evidence is being collected at that particular moment. This brings in the surprise test advantages.
 - (iii) *Information to system staff on meeting of objectives* - Continuous audit techniques provides information to systems staff regarding the test vehicle to be used in evaluating whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency.
 - (iv) *Training for new users* – Using the Integrated Test Facilities (ITFs) new users can submit data to the application system, and obtain feedback on any mistakes they make via the system's error reports.
- (b) (i) **Computer Contaminant:** It refers to any set of computer instructions that are designed:
- ◆ to modify, destroy, record, transmit data or program residing within a computer, computer system or computer network; or
 - ◆ by any means to disrupt the normal operation of the computer, computer system, or computer network.
- (ii) **Cyber Cafe:** It refers to any facility from where access to the Internet is offered by any person in the ordinary course of business to the members of the public.
- (iii) **Electronic Form:** It refers to any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device.
- (iv) **Traffic Data:** It refers to any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, data size, duration or type of underlying service or any other information.
- (v) **Asymmetric crypto system:** It refers to a system of secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.
- (c) Some of the important advantages of information system in business are discussed as under:

FINAL (NEW) EXAMINATION : MAY, 2010

- (i) Information system will help managers in effective decision making to achieve the organizational goal.
 - (ii) Based on well designed information system, an organization will gain edge in the competitive environment.
 - (iii) Information systems help in taking right decision at the right time.
 - (iv) Innovative ideas for solving critical problems may come out from good information system.
 - (v) Knowledge gathered through information system may be utilized by managers in unusual situations.
 - (vi) If information system is viewed as a process, it can be integrated to formulate a strategy of action or operation.
- (d) COBIT or Control Objectives for Information and Related Technology is a framework of generally applicable information systems, security and control practices for IT Control. The framework allows:
- management to benchmark the security and control practices of IT environments,
 - users of IT services to be assured that adequate security and control exist, and
 - auditors to substantiate their opinions on internal control and to advise on IT security and control matters.

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

1. **Business objectives:** To satisfy business objectives, information must conform to certain criteria that COBIT refers to as business requirements for information. The criteria are divided into seven distinct yet overlapping categories that map into the COSO objectives namely, effectiveness (relevant, pertinent, and timely), efficiency, confidentiality, integrity, availability, compliance with legal requirements, and reliability.
2. **IT resources** which 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 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.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

Question 5

- (a) *What are the two primary questions to consider when evaluating the risk inherent in a business function in the context of the risk assessment methodologies? Give the purposes of risk evaluation.* (5 marks)
- (b) *If you are the CEO of a company, what factors would be considered before undertaking implementation of an ERP system?* (5 marks)
- (c) *Briefly describe any three of the characteristics of the types of information used in Executive Decision making.* (5 marks)
- (d) *Discuss the benefits and limitations of unit testing.* (5 marks)

Answer

- (a) The two primary questions to consider when evaluating the risk inherent in a business function are given below:
- (i) What is the probability that things can go wrong? (Probability). This view will have to be taken strictly on the technical point of view and has to focus on the available measures that can prevent such happening.
- (ii) What is the cost if 'what can go wrong' does go wrong? (Exposure)

Purposes of Risk Evaluation

The purpose of risk evaluation is to:

- identify the probabilities of failures and threats,
- calculate the exposure i.e. the damage or loss to assets, and
- make control recommendations keeping the cost benefit analysis in mind.

- (b) Various factors which should be considered before undertaking the implementation of an ERP system are:
- (i) **Integrate financial information:** As the CEO tries to understand the company's overall performance; he may find many different versions of the truth. Finance has its own set of revenue numbers, sales has another version, and the different business units may each have their own version of how much they contributed to revenue. ERP creates a single version of the truth that cannot be questioned because everyone is using the same system.
- (ii) **Integrate customer order information:** ERP systems can become the place where the customer order lives from the time a customer service representative receives it until the loading dock ships the merchandise and finance department sends an invoice. By having this information in one software system, rather than scattered among many different systems that can't communicate with one another, companies can keep track of orders more easily, and coordinate manufacturing, inventory and shipping among many different locations simultaneously.

FINAL (NEW) EXAMINATION : MAY, 2010

- (iii) **Standardize and speed up manufacturing processes:** Manufacturing companies -especially those with an appetite for mergers and acquisitions—often find that multiple business units across the company make the same transaction/ recording/ report using different methods and computer systems. ERP systems come with standard methods for automating some of the steps of the manufacturing process. Standardizing those processes and using a single, integrated computer system can save time, increase productivity and reduce headcount.
 - (iv) **Reduce inventory:** ERP helps the manufacturing process flow more smoothly, and it improves visibility of the order fulfillment process inside the company. It can lead to reduced inventories of the materials used to make products (work-in-progress inventory), and it can help users to better plan deliveries to customers, thereby reducing the finished good inventory at the warehouses and shipping docks. To really improve the flow of the supply chain, one needs supply chain software, but ERP helps too.
 - (v) **Standardize HR information:** Especially in companies with multiple business units, HR may not have a unified, simple method for tracking employees' time and communicating with them about benefits and services. ERP can fix that problem.
- (c) The characteristics of the types of information used in Executive Decision Making are:
- (1) **Lack of structure:** Many of the decisions made by executives are relatively unstructured. For instance, what general direction should the company take? Or what type of advertising campaign will best promote the new product line? These types of decisions are not as clear-cut as deciding how to debug a computer program or how to deal with an overdue account balance. Also, it is not always obvious which data are required or how to weigh available data for reaching at a decision. For example, how does an executive assess the future direction of the economy if the six sources on which that person typically depends for information, each forecasts something different? Even the portfolio of decisions that need to be made by the executive is an open issue. Should time be spent, for instance, considering new businesses to enter- or should the company concentrate on looking for new markets for existing products?
 - (2) **High degree of uncertainty:** Executives work in a decision space that is often characterized by a lack of precedent. For example, when the Arab oil embargo hit in the mid-1970s, no such previous event could be referenced for advice. Executives also work in a decision space where results are not scientifically predictable from actions. If prices are lowered, for instance, product demand will not automatically increase.
 - (3) **Future Orientation:** Strategic-planning decisions are made in order to shape future events. As conditions change, organizations must change also. It is the executive's responsibility to make sure that the organization keeps pointed toward the future. Some key questions about the future include: "How will future technologies affect what the company is currently doing? What will the competition (or the government) do next? What products will consumers demand five years from now? Where will the economy move next, and how might that affect consumer buying patterns?" As

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

one can see, the answers to all of these questions about the future external environment are vital.

- (4) **Informal source:** Executives, more than other types of managers, rely heavily on informal sources for key information. For example, lunch with a colleague in another firm might reveal some important competitor strategies. Informal sources such as television might also feature news of momentous concern to the executive – news that he or she would probably never encounter in the company's database or in scheduled computer reports. Besides business meals and the media, some other important information sources of information are meetings, tours around the company's facilities to chat with employees, brainstorming with a trusted colleague or two, and social events.
- (5) **Low level of detail:** Most important executive decisions are made by observing broad trends. This requires the executive to be more aware of the large overview than the tiny items. Even so, many executives insist that the answers to some questions can only be found by mucking through details.

(d) Unit Testing

In computer programming, unit testing is a method of testing the correctness of a particular module of source code. The idea is to write test cases for every non-trivial function or method in the module so that each test case is separate from the others if possible. This type of testing is mostly done by the developers.

Benefits of Unit Testing : The goal of unit testing is to isolate each part of the program and show that the individual parts are correct. It provides a written contract that the piece must satisfy. The benefits of Unit testing are:

- **Encourages change:** Unit testing allows the programmer to re-factor code at a later date, and make sure that the module still works correctly (regression testing). This provides the benefit of encouraging programmers to make changes to the code since it is easy for the programmer to check if the piece is still working properly.
- **Simplifies Integration:** Unit testing helps eliminate uncertainty in the pieces themselves and can be used in a bottom-up testing style approach. By testing the parts of a program first and then testing the sum of its parts will make integration testing easier.
- **Documents the code:** Unit testing provides a sort of "living document" for the class being tested. Clients wishing to learn to use the class, can look at the unit tests to determine how to use the class to fit their needs.

Limitations: The limitations of Unit testing are:

- Unit testing will not catch every error in the program.
- It only tests the functionality of the units themselves.
- It will not catch integration errors, performance problems and any other system-wide issues.
- Unit testing is only effective if it is used in conjunction with other software testing activities.