PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

Question No. 1 is compulsory.

Attempt any five questions from the remaining six questions.

Question 1

XYZ Industries Ltd., a company engaged in a business of manufacturing and supply of electronic equipments to various companies in India. It intends to implement E-Governance system at all of its departments. A system analyst is engaged to conduct requirement analysis and investigation of the present system. The company's new business models and new methods presume that the information required by the business managers is available all the time; it is accurate and reliable. The company is relying on Information Technology for information and transaction processing. It is also presumed that the company is up and running all the time on 24 x 7 basis. Hence, the company has decided to implement a real time ERP package, which equips the enterprise with necessary capabilities to integrate and synchronise the isolated functions into streamlined business processes in order to gain a competitive edge in the volatile business environment. Also, the company intends to keep all the records in digitized form.

(a) What do you mean by system requirement analysis? What are the activities to be performed during system requirement analysis phase? (5 Marks)

(b) What are the business risks that an organization faces when migrating to real time integrated ERP system? (5 Marks)

(c) What are the points that need to be taken into account for the proper implementation of physical and environmental security in respect of Information System Security? (5 Marks)

(d) What is the provision given in Information Technology (Amended) Act 2008 for the retention of electronic records? (5 Marks)

Answer

(a) System requirements analysis is a phase, which includes a thorough and detailed understanding of the current system, identification of the areas that need modification/s to solve the problem, the determination of user/managerial requirements and to have fair ideas about various system development tools.

The following activities are performed in this phase:

- To identify and consult the stake owners to determine their expectations and resolve their conflicts;
- To analyze requirements to detect and correct conflicts and determine priorities;
- To verify requirements in terms of various parameters like completeness, consistency, unambiguous, verifiable, modifiable, testable and traceable;
- To gather data or find facts using tools like- interviewing, research/document collection, questionnaires, observation;

- To develop models to document Data Flow Diagrams, E-R diagrams; and
- To document activities such as interviews, questionnaires, reports etc. and development of a system dictionary to document the modeling activities.

The document/deliverable of this phase is a detailed system requirements report, which is generally termed as SRS.

(b) Organizations face several business risks when migrating to real-time, integrated ERP systems. These risks are given as follows:

- *Single point of failure:* Since all the organization's data and transaction processing is within one application system, single point failure may be a major risk.
- *Structural changes:* Significant personnel and organizational structure changes associated with reengineering or redesigning business processes may pose a big challenge.
- *Job role changes:* Transition of traditional user's roles to empowered-based roles with much greater access to enterprise information in real time and the point of control shifting from the back-end financial processes to the front-end point of creation are also great risks.
- *Online, real-time:* An online real-time environment requires a continuous business environment capable of utilizing the new capabilities of the ERP application and responding quickly to any problem requiring re-entry of information.
- *Change management:* The level of user acceptance of the system has a significant influence on its success. Users must understand that their actions or inaction have a direct impact upon other users and, therefore, must learn to be more diligent and. efficient in the performance of their day-to-day duties.
- *Distributed computing experience:* Inexperience with implementing and managing distributed computing technology may pose significant challenges.
- *Broad system access:* Increased remote access by users and outsiders and high integration among application functions allow increased access to application and data.
- *Dependency on external assistance:* Organization accustomed to in-house legacy systems may find that they have to rely on external help. Unless such external assistance is properly managed, it could introduce an element of security and resource management risk that may expose the organizations to greater risk.
- *Program interfaces and data conversions:* Extensive interfaces and data conversions from legacy systems and other commercial software are often necessary. The exposure of data integrity, security and capacity requirements for ERP are therefore often much higher.
- *Audit expertise:* Specialist expertise is required to effectively audit and control an ERP environment. The relative complexity of ERP systems has created

specialization such that each specialist may know a small fraction of the entire ERP's functionality in a particular core module.

(c) For the proper implementation of Physical and Environmental Security, the following points need to be taken into account:

- Physical security should be maintained and checks must be performed to identify all vulnerable areas within each site.
- The IT infrastructure must be physically protected.
- Access to secure areas must remain limited to authorized staff only.
- Confidential and sensitive information and valuable assets must be securely locked away, when they are not in use.
- Computers must never be left unattended whilst displaying confidential or sensitive information or whilst logged on to the systems.
- Supplies and equipments must be delivered and loaded in an isolated area to prevent any unauthorized access to key facilities.
- Equipment, information or software must not be taken off-site without proper authorization.
- Wherever practical, premises housing computer equipment and data should be located away from, and protected against threats of deliberate or accidental damage such as fire and natural disaster.
- The location of the equipment rooms must be away from, and protected against threats of unauthorized access and deliberate or accidental damage, such as system infiltration and environmental failures.

(d) Retention of Electronic Records: [Section 7] of ITAA 2008

The provision for the retention of electronic records is discussed in Section 7 of ITAA 2008, which is given as follows:

(1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, –

(a) the information contained therein remains accessible so as to be usable for a subsequent reference;

(b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format, which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) The details, which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record.

However,

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

(2) Nothing in this section shall apply to any law that expressly provides for the retention of documents records or information in the form of electronic records, publication of rules, regulation etc. in Electronic Gazette.

Question 2

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

(b) Describe the benefits of performing a technology risk assessment. *(4 Marks)*

(c) Why do you think a separate standard (SAS 70) is useful for auditing a service organization especially with respect to examination of general controls over Information Technology and related processes? *(4 Marks)*

Answer

(a) 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.

(b) Benefits of performing a technology risk assessment are given as follows:

- To have a business driven process to identify, quantify, and manage risks while detailing future suggestions for improvement in technical delivery;
- To have a framework that governs technical choice and delivery processes with cyclic checkpoints during the project lifecycle;
- Interpretation and communication of potential risk impact and where appropriate, risk reduction to a perceived acceptable level; and
- Implementation of strict disciplines for active risk management during the project lifecycle.

The technology risk assessment needs to a mandatory requirement for all projects to ensure that proactive management of risks occurs and that no single point of failure are in advertently built into the overall architecture.

(c) Yes, to our opinion, a separate statement on Auditing Standard (SAS) No. 70 is useful for auditing a service organization especially with respect to examination of general controls. A SAS 70 audit or service auditor's examination is widely recognized, because it represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over Information Technology and related processes.

SAS 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. A SAS 70 examination signifies that a service organization has had its control objectives and control activities examined by an independent accounting and auditing firm. A formal report including the auditor's opinion (Service Auditor's Report) is issued to the service organization at the conclusion of SAS 70 examination.

SAS 70 provides guidance to enable an independent auditor (Service Auditor) to issue an opinion on a service organization's description of controls through a Service Auditor's Report. SAS 70 is not a predetermined set of control objectives or control activities that service organization must achieve.

SAS 70 is generally applicable when an auditor (user auditor) is auditing the financial statements of an entity (user organization) that obtains services from another organization (service organization). Service organizations that provide such services could be application service providers, bank trust departments, claims processing centres, Internet data centres or other data processing service bureaus.

Question 3

(a) As an IS Auditor, discuss the various contents in brief to be included in a standard audit report. (8 Marks)

(b) What are the characteristics of Executive Information System? (4 Marks)

(c) Discuss the various backup options considered by a security administrator when arranging alternate processing facility. (4 Marks)

Answer

(a) An Audit report includes the following sections: title page, table of contents, summary (including recommendations), introduction, findings and appendices.

These are discussed below:

- Cover and Title Page: Audit reports should use a standard cover page, with a window showing the title "Information System Audit" or “Data Audit”, the department's name and the report's date of issue. These items are repeated at the bottom of each page. The title page may also indicate the names of the audit team members.
- Table of contents: The table lists the sections and subsections with page numbers including summary and recommendations, introduction, findings and appendices.
- Summary/Executive Summary: The summary gives a quick overview of the salient features at the time of the audit in light of the main issues covered by the report. It should not exceed three pages, including recommendations.
- Introduction: It should include the following elements:
  - Context: This subsection briefly describes conditions in the audit entity during the period under review, for instance, the entity's role, size and organization with regard to information system management, significant pressures on information system management during the period under review, events that need to be noted, organizational changes, IT disruptions, changes in roles and programs, results of internal audits or follow-up to our previous audits, if applicable.
  - Purpose: This subsection is a short description of what functions and special programs were audited and the client's authorities.
  - Scope: The scope lists the period under review, the issues covered in each function and program, the locations visited and the on-site dates.
  - Methodology: This section briefly describes sampling, data collection techniques and the basis for auditor's options. It also identifies any

weakness/es in the methodology to allow the client and auditee to make informed decisions as a result of the report.

- Findings: Findings constitute the main part of an audit report. They result from the examination of each audit issue in the context of established objectives and client's expectations. If the auditor is using any standard grading, the arrived value should also be stated.
- Opinion: If the audit assignment requires the auditor to express an audit opinion, the auditor shall do so in consonance to the requirement.
- Appendices: Appendices can be used when they are essential for understanding the report. They usually include comprehensive statistics, quotes from publications, documents, and references.

(b) Major characteristics of an Executive Information System (EIS) are given as follows:

- EIS is a computer-based-information system that serves the information need of top executives.
- EIS enables users to extract summary data and model complex problems without the need to learn query languages, statistical formulae or high computing skills.
- EIS provides rapid access for timely information and direct access to the management reports.
- EIS is capable of accessing internal and external data both.
- EIS provides extensive online analysis tools like trend analysis, market conditions etc.
- EIS can easily be given a DSS support for decision making.

(c) Security administrators should consider the following backup options while arranging alternate processing facility:

- Cold site: If an organization can tolerate some down time, cold site backup might be appropriate. A cold site has all the facilities needed to install a mainframe system, raised floors, air conditioning, power, communication lines, and so on. An organization can establish its own cold site facility or enter into an agreement with another organization to provide a cold site facility.
- Hot site: If fast recovery is critical, an organization might need hot site backup. All hardware and operations facilities will be available at the host site. In some cases, software, data and supplies might also be stored there. A hot site is expensive to maintain. They are usually shared with other organizations that have hot site needs.
- Warm site: It provides an intermediate level of backup. It has all cold site facilities in addition with hardware that might be difficult to obtain or install. For example, a warm site might contain selected peripheral equipment plus a small mainframe with sufficient power to handle critical applications in the short run.

- Reciprocal agreement: Two or more organizations might agree to provide backup facilities to each other in the event of one suffering a disaster. This backup option is relatively cheap, but each participant must maintain sufficient capacity to operate another's critical system.

Question 4

(a) *Explain the common threats to the computerized environment of an organization.* *(8 Marks)*

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

(c) What are the tasks for which the company should be ready for post implementation period of an ERP System? *(4 Marks)*

Answer

(a) The common threats to the computerized environment of an organization are given as follows:

(i) Power failure: Power failure can cause disruption of entire computing equipments since computing equipments depend on power supply.

(ii) 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 present a significant threat that will have a direct impact on operations.

(iii) 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.

(iv) 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.

(v) Malicious code: Malicious codes such as viruses and worms which freely access the unprotected networks may affect organizational and business networks that use these unprotected networks.

(vi) 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.

(vii) Natural disasters: Natural disasters such as earthquakes, lighting, floods, tornado, tsunami, etc. can adversely affect the functioning of the Information System operations due to damage to Information System facilities.

(viii) Theft or destruction of computing resources: Since the computing equipments form the back-bone of information processing, any theft or destruction of the resource can result in compromising the competitive advantage of the organization.

(ix) Downtime due to technology failure: Information System 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.

(x) Fire, etc: Fire due to electric short circuit or due to riots, war or such other reasons can cause irreversible damage to the IS infrastructure.

(b) 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.

(c) Having evolved the processes while the configuration, construction and implementation are in progress, the organization needs to ready itself for the post-implementation period. Some of the tasks that are to be performed are to:

- develop the new job descriptions and organization structure to suit the post ERP Scenario;
- determine the skill gap between existing jobs and envisioned jobs;
- assess training requirements, and create and implement a training plan;
- develop and amend HR, financial and operational policies to suit the future ERP environment; and

- develop a plan for workforce logistics adjustment.

Question 5

(a) An organization is audited for effective implementation of ISO 27001 – Information Security Management Standard. What are the factors verified under

(i) establishing management framework?

(ii) Implementation?

(iii) documentation? *(8 Marks)*

(b) Enumerate the characteristics of a Computer Based Information System. (4 Marks)

(c) Describe the duties of certifying authorities under Section 30 of Information Technology (Amended) Act 2008. (4 Marks)

Answer

(a) ISO 27001-Information Security Management Standard: The requirements of information security system as described by the standard are stated below. An organization must take a clear view on these issues before trying to implement an Information Security Management Systems (ISMS).

General: Organization shall establish and maintain documented ISMS addressing assets to be protected, organizations approach to risk management, control objectives and controls, and degree of assurance required.

Establishing Management Framework: This would include the following:

- Defining information security policy;
- Defining scope of ISMS including functional, asset, technical, and locational boundaries;
- Making appropriate risk assessment;
- Identifying areas of risk to be managed and degree of assurance required;
- Selecting appropriate controls;
- Preparing Statement of Applicability,

Implementation: Effectiveness of procedures to implement controls to be verified while reviewing security policy and technical compliance.

Documentation: The documentation shall consist of evidence of actions undertaken under establishment of the following:

- Management control;
- Management framework summary, security policy, control objective, and implemented controls given in the Statement of Applicability;
- Procedure adopted to implement control under Implementation clause;

- ISMS management procedure;
- Document Control: The issues focused under this clause would be:
  - § Ready availability,
  - § Periodic review,
  - § Maintain version control,
  - § Withdrawal when obsolete, and
  - § Preservation for legal purpose.
- Records: The issues involved in record maintenance are as follows:
  - § Maintain evidence compliance to the standard,
  - § Procedure for identifying, maintaining, retaining, and disposing of such evidence,
  - § Records to be legible, identifiable and traceable to activety involved, and
  - § Storage to augment retrieval, and protection against damage.

(b) Major characteristics of a Computer Based Information System are as follows:

1. All systems work for predetermined objectives and the system is designed and developed, accordingly.
2. In general, a system has a number of interrelated and interdependent subsystems or components. No subsystem can function in isolation; it depends on other subsystems for its inputs.
3. If one subsystem or component of a system fails, in most of the cases, the whole system does not work. However, it depends on 'how the subsystems are interrelated'.
4. The way a subsystem works with another subsystem is called interaction. Different subsystems interact with each other to achieve the goal of the system.
5 The work done by individual subsystem is integrated to achieve the central goal of the system. The goal of the individual subsystem is of lower priority than the goal of the entire system.

(c) Duties of Certifying Authorities-Section 30 of ITAA 2008

This section provides that every Certifying Authority shall follow certain procedures with respect of Digital Signatures as given below.

Every Certifying authority shall-

a. make use of hardware, software and procedures that are secure from intrusion and misuse;

b. provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;

c. adhere to security procedures to ensure that the secrecy and privacy of the Electronic Signature are assured (Amended vide ITAA 2008) .

(ca) be the repository of all Electronic Signature Certificates issued under this Act (Inserted vide ITAA 2008)

(cb) publish information regarding its practices, Electronic Signature Certificates and current status of such certificates; and (Inserted vide ITAA 2008)

d. Observe such other standards as may be specified by regulations.

Question 6

(a) Discus in brief the various functional areas to be studied by a system analyst for a detailed investigation of the present system. (8 Marks)

(b) As an IS Auditor, explain the types of information collected for auditing by using System Control Audit Review File (SCARF) technique. (4 Marks)

(c) What are the audit tools and techniques used by an IS Auditor to ensure that disaster recovery plan is in order? Briefly explain them. (4 Marks)

Answer

(a) Detailed investigation of the present system involves collecting, organizing and evaluating facts about the system and the environment in which it operates. Survey of existing methods, procedures, data flow, outputs, files, input and internal controls should be done intensively to fully understand the present system and its related problems.

The following areas should be studied in depth by a System Analyst for a detailed investigation of the present system:

(i) Review historical aspects: A brief history of the organization is a logical starting point for an analysis of the present system. The historical facts should identify the major turning points and milestones that have influenced its growth. A review of annual reports and organization chart can identify the growth of management levels as well as the development of various functional areas and departments. The system analyst should investigate what system changes have occurred in the past including operations that have been successful or unsuccessful with computer equipments and techniques.

(ii) Analyze inputs: A detailed analysis of present inputs is important since they are basic to the manipulation of data. Source documents are used to capture the originating data for any type of system. The system analyst should be aware of the various sources from where the data are initially captured, keeping in view the fact that outputs for one area may serve as an input for another area. The system analyst must understand the nature of each form, what is contained in it, who prepared it, from where the form is initiated, where it is completed, the distribution of the form and other similar considerations. If the analyst investigates these questions thoroughly, he will be able to determine how these inputs fit into the framework of the present system.

(iii) Review data files maintained: The analyst should investigate the data files maintained by each department, noting their number and size, where they are located, who uses them and the number of times per given time interval these are used. Information on common data files and their size will be an important factor, which will influence the new information system. This information may be contained in the systems and procedures manuals. The system analyst should also review all on-line and off-line files which are maintained in the organization as it will reveal information about data that are not contained in any outputs. The related cost of retrieving and processing the data is another important factor that should be considered by the systems analyst.

(iv) Review methods, procedures and data communications: Methods and procedures transform input data into useful output. A method is defined as a way of doing something; a procedure is a series of logical steps by which a job is accomplished. A procedure review is an intensive survey of the methods by which each job is accomplished, the equipment utilized and the actual location of the operations. Its basic objective is to eliminate unnecessary tasks or to perceive improvement opportunities in the present information system. The system analyst must review the types of data communication equipments including data interface, data links, modems, dial up and leased lines and multiplexers, The system analyst must also understand how the data-communications network is used in the present system so as to identify the need to revamp the network when the new system is installed.

(v) Analyze outputs: The outputs or reports should be scrutinized carefully by the system analysts in order to determine how well they will meet the organization's needs. The analysts must understand what information is needed and why, who needs it and when and where it is needed. Additional questions concerning the sequence of the data, how often the form reporting is used, how long it is kept on file, etc. must be investigated.

(vi) Review internal controls: A detailed investigation of the present information system is not complete until internal control is reviewed. Locating the control points helps the analyst to visualize the essential parts and framework of a system. An examination of the present system of internal controls may indicate weaknesses that should be removed in the new system. The adoption of advanced methods, procedures and equipments might allow much greater control over the data.

(vii) Model the existing physical system and logical system: As the logic of inputs, methods, procedures, data files, data communications, reports, internal controls and other important items are reviewed and analyzed in a top down manner; the process must be properly documented. The flow charting and diagramming of present information not only organizes the facts, but also helps disclose gaps and duplication in the data gathered. It allows a thorough comprehension of the numerous details and related problems in the present operation.

(viii) Undertake overall analysis of the present system: The final phase of the detailed investigation includes the analysis of the present work volume; the current personnel requirements; the present benefits and costs and each of these must be investigated thoroughly.

(b) An IS Auditor might use SCARF to collect the following types of information:

- Application system errors: SCARF audit routines provide an independent check on the quality of system processing, whether there are any design and programming errors as well as errors that could creep into the system when it is modified and maintained.
- Policy and procedural variances: Organizations have to adhere to the policies, procedures and standards of the organization and the industry to which they belong. SCARF audit routines can be used to check when variations from these policies, procedures and standards have occurred.
- System exception: SCARF can be used to monitor different types of application system exceptions.
- Statistical sample: Some embedded audit routines might be statistical sampling routines, SCARF provides a convenient way of collecting all the sample information together on one file and use analytical review tools thereon.
- Snapshots and extended records: Snapshots and extended records can be written into the SCARF file and printed when required.
- Profiling data: Auditor can use embedded audit routines to collect data to build profiles of system users. Deviations from these profiles indicate that there may be some errors or irregularities.
- Performance measurement: Auditors can use embedded routines to collect data that is useful for measuring or improving the performance of an application system.

(c) The audit tools and techniques used by an IS Auditor to ensure that disaster recovery plan is in order, are given as follows:

(i) Automated Tools: Automated tools make it possible to review large computer systems for a variety of flaws in a short time period. They can be used to find threats and vulnerabilities such as weak access controls, weak passwords, lack of integrity of the system software, etc.

(ii) Internal Control Auditing: This includes inquiry, observation and testing. The process can detect illegal acts, errors, irregularities or lack of compliance of laws and regulations.

(iii) Disaster and Security Checklists: A checklist can be used against which the system can be audited. The checklist should be based upon disaster recovery policies and practices, which form the baseline. Checklists can also be used to verify changes to the system from contingency point of view.

(iv) Penetration Testing: Penetration testing can be used to locate vulnerabilities.

Question 7

Write Short notes on any four of the following:

(a) Business applications of Expert systems for Management Support systems.

(b) Firewalls.

(c) Delphi technique for risk evaluation.

(d) Capability Maturity Model.

(e) Authentication of electronic records in Information Technology (Amended) Act 2008.

(4 x 4=16 Marks)

Answer

(a) Business applications of Expert Systems for Management Support Systems are given as follows:

(i) Accounting and Finance: It provides tax advice and assistance, helping with credit authorization decisions, selecting forecasting models, providing investment advice.

(ii) Marketing: It provides establishing sales quotas, responding to customer inquiries, referring problems to telemarketing centers, assisting with marketing timing decisions, determining discount policies.

(iii) Manufacturing: It helps in determining whether a process is running correctly, analyzing quality and providing corrective measures, maintaining facilities, scheduling job-shop tasks, selecting transportation routes, assisting with product design and faculty layouts.

(iv) Personnel: It is useful in assessing applicant qualifications, giving employees assisting at filling out forms.

(v) General Business: It helps in assisting with project proposals, recommending acquisition strategies, educating trainees, evaluating performance.

(b) 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 co-ordinate activities with network Intrusion Detection Systems (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 characterization of one or more firewall types. The selection of firewall type is dependent on many types of 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 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.

(c) Delphi Technique for Risk Evaluation

The Delphi Technique was first used by the Rand Corporation for obtaining a consensus opinion. Here, a panel of experts is appointed. Each expert gives his/her opinion in a written and independent manner. They enlist the estimate of the cost, benefits and the reasons why a particular system should be chosen, the risks and the exposures of the system. These estimates are then compiled together. The estimates within a pre-decided acceptable range are taken. The process may be repeated four times for revising the estimates falling beyond the range. Then a curve is drawn taking all the estimates as points on the graph. The median is drawn and this is the consensus opinion.

(d) Capability Maturity Model (CMM)

The CMM presents sets of recommended practices in a number of key process areas that have been shown to enhance software process capability. The CMM is based on knowledge acquired from software process assessments and extensive feedback from both industry and government.

The capability maturity model for software provides software organizations with guidance on how to gain control of their processes for developing and maintaining software and how to evolve toward a culture of software engineering and management excellence. The CMM was designed to guide software organizations in selecting process improvement strategies by determining current process maturity and identifying the few issues most critical to software quality and process improvement. By focusing on a limited set of activities and working aggressively to achieve them, an organization can steadily improve its organization-wide software process to enable continuous and lasting gains in software process capability.

(e) Authentication of Electronic Records: [Section 3] of ITAA 2008

Section 3 of ITAA 2008 provides the conditions subject to which an electronic record may be authenticated by means of affixing digital signature, which is given below:

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his Digital Signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation -

For the purposes of this subsection, "Hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller set known as "Hash Result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.