DISCLAIMER

The Suggested Answers hosted in the website do not constitute the basis for evaluation of the students' answers in the examination. The answers are prepared by the Faculty of the Board of Studies with a view to assist the students in their education. While due care is taken in preparation of the answers, if any errors or omissions are noticed, the same may be brought to the attention of the Director of Studies. The Council of the Institute is not in anyway responsible for the correctness or otherwise of the answers published herein.

PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

Question No. 1 is compulsory.

*Candidates are also required to answer any **five** questions from the remaining **six** questions.*

Question 1

XYZ Company is a retail chain house having many branches located in different places for its operation. Its business processes are cumbersome and tedious as it has multiple sources of procurement and supply destinations.

The CEO of company feels that existing information system does not meet its present requirements. He seeks for high end solution to stream line and integrate its operation processes and information flow to synergize all its major resources. Further he expects that the new system should provide a structured environment in which decisions concerning demand, supply, operational, personnel, finance, logistics etc. are fully supported by accurate and reliable information. The company follows the best practices of System Development Life Cycle (SDLC), which consists of various phases starting from preliminary investigation till post implementation review, controls and security aspects.

The CEO of the company appoints a committee of three persons, one of them is IT expert, second one is security expert and third one is company's auditor to suggest the followings:

(a) List the activities to be performed during the phase of System Requirement Analysis. *(5 Marks)*

(b) What boundary control techniques should be used in user control ? *(5 Marks)*

(c) If committee decides to go for implementing ERP, what general guidelines you would suggest before starting the implementation of ERP package ? *(5 Marks)*

(d) Which aspects should be covered while drafting IS security policy for Business Continuity Planning ? *(5 Marks)*

Answer

(a) The activities to be performed during the phase of System Requirements Analysis are given as follows:

- To identify and consult the stakeholders to determine their expectations and resolve their conflicts;
- To analyze requirements to detect and correct conflicts and determine their priorities;
- To verify that the requirements are complete, consistent, unambiguous, verifiable, modifiable, testable and traceable;
- To gather data or find facts using tools like interviewing, research/document collection, questionnaires, observation;

- To model the activities such as developing models to document Data Flow Diagrams, E-R Diagrams; and
- To document the activities such as interview, questionnaires, reports etc. and development of a system (data) dictionary to document the modeling activities.

The final deliverable of this phase of SDLC is SRS.

(b) The major controls of the boundary system are the access control mechanisms. Access controls are implemented with an access control mechanism and links the authentic users to the authorized resources for which they are permitted to access. The access control mechanism has three steps, identification, authentication and authorization with respect to the access control policy.

Major boundary control techniques are given as follows:

- Cryptography: It deals with programs for transforming data into codes that are meaningless to anyone, who does not possess the authentication to access the respective system resource or file. A cryptographic technique encrypts data (clear text) into cryptograms (cipher text) and its strength depends on the time and cost to decipher the cipher text by a cryptanalyst. The three techniques of cryptography are transposition (permute the order of characters within a set of data), substitution (replace text with a key-text) and product cipher (combination of transposition and substitution).
- Passwords: User identification by an authentication mechanism with personal characteristics like name, birth date, employee code, function, designation or a combination of two or more of these can be used as a password boundary access control. A few best practices followed to avoid failures in this control system are; minimum password length, avoid usage of common dictionary words, periodic change of passwords, encryption of passwords and number of entry attempts.
- Personal Identification Numbers (PIN): PIN is similar to a password assigned to a user by an institution based on the user characteristics and encrypted using a cryptographic algorithm, or the institute generates a random number stored in its database independent to a user identification details, or a customer selected number. Hence, a PIN or a digital signature are exposed to vulnerabilities while issuance or delivery, validation, transmission and storage.
- Identification Cards: Identification cards are used to store information required in an authentication process. These cards used to identify a user, are to be controlled through the application for a card, preparation of the card, issue, use and card return or card termination phases.
- Biometric devices: Biometric identification e.g. thumb and/or finger impression, eye retina etc are also used as boundary control techniques.

(c) If the Committee decides to go for implementing ERP, the general guidelines, which are to be followed before starting the implementation of an ERP package, are given as follows:

- Understanding the corporate needs and culture of the organization and then adapt the implementation technique to match these factors;
- Doing a business process redesign exercise prior to starting the implementation;
- Establishing a good communication network across the organization;
- Providing a strong and effective leadership so that people down the line are well motivated;
- Finding an efficient and capable project manager;
- Creating a balanced team of implementation consultants, who can work together as a team;
- Selecting a good implementation methodology with minimum customization;
- Training end users; and
- Adapting the new system and making the required changes in the working environment to make effective use of the system in future.

(d) The following are the major aspects, which should be covered while drafting IS Security Policy for Business Continuity Planning:

- A Business Continuity Plan (BCP) must be maintained, tested and updated if necessary. All staff must be made aware of it.
- A Business Continuity and Impact Assessment must be conducted annually.
- Suppliers of network services must be contractually obliged to provide a predetermined minimum service level.
- If subsidiaries, divisions, departments, and other organizational units wish to be supported by the management information systems department on a priority basis in the event of an emergency or a disaster, they must implement hardware, software, policies, and related procedures consistent with related standards.
- Computer operations management must establish and use a logical framework for segmenting information resources by recovery priority. This will in turn allow the most critical information resources to be recovered first. All departments must use the same framework when preparing information systems contingency plans.
- In addition, recovery priority of all the applications must also be defined by assessing the criticality of the applications. Further, a classification may also be done for application criticality.
- Management must prepare, periodically update, and regularly test emergency

response plans and disaster recovery plans that will allow all critical computer systems to continue processing and be available in the event of an interruption or degradation of service and also in the event of a major loss, such as a flood, earthquake.

Question 2

(a) What is the goal of a prototype model approach of software development? Enumerate the strength of this model. (6 Marks)

(b) What activities are involved in system conversion ? Explain them briefly. (6 Marks)

(c) How does Executive Information System differs from Traditional Information System?(4 Marks)

Answer

(a) The goal of a prototyping model is to develop a small or pilot version called a prototype of part or all of a system. A prototype is a usable system or system component that is built quickly and at a lesser cost, and with the intention of being modifying or replacing it by a full-scale and fully operational system.

As users work with the prototype, they make suggestions about the ways to improve it. These suggestions are then incorporated into another prototype, which is also used and evaluated and so on. Finally, when a prototype is developed that satisfies all user requirements, either it is refined and turned into the final system or it is scrapped. If it is scrapped, the knowledge gained from building the prototype is used to develop the real system.

Major strengths of Prototyping model are given as follows:

- Prototyping model improves both user participation in system development and communication among project stakeholders.
- This is especially useful for resolving unclear objectives; developing and validating user requirements; experimenting with or comparing various design solutions, or investigating both performance and the human computer interface.
- It has the potential for exploiting knowledge gained in an early iteration as later iterations are developed.
- This helps to easily identify confusing or difficult functions and missing functionality.
- This may generate specifications for a production application.
- This encourages innovation and flexible designs.
- The model provides quick implementation of an incomplete, but functional application.
- Prototyping requires intensive involvement by the system users. Therefore, it typically results in a better definition of these users' needs and requirements than

does the traditional systems development approach.

- A very short time period (e.g., a week) is normally required to develop and start experimenting with a prototype. This short time period allows system users to immediately evaluate proposed system changes.
- Since system users experiment with each version of the prototype through an interactive process, errors are hopefully detected and eliminated early in the developmental process. As a result, the information system ultimately implemented should be more reliable and less costly to develop than when the traditional systems development approach is employed.

(b) Conversion includes all those activities, which must be completed to successfully convert from the previous system to the new information system. These are given as follows:

- Procedure conversion: Operating procedures should be completely documented for the new system that applies to both computer-operations and functional area operations. Before any parallel or conversion activities can start, operating procedures must be clearly spelled out for personnel in the functional areas undergoing changes. Information on input, data files, methods, procedures, output, and internal control must be presented in clear, concise and understandable terms for the average reader. Written operating procedures must be supplemented by oral communication during the training sessions on the system change.
- File conversion: Since large files of information must be converted from one medium to another, this phase should be started long before programming and testing are completed. In order to the conversion to be as accurate as possible, file conversion programs must be thoroughly tested. Adequate control, such as record counts and control totals, should be required output of the conversion program. The existing computer files should be kept for a period of time until sufficient files are accumulated for back up. This is necessary in case the files must be reconstructed from scratch after a "bug" is discovered later in the conversion routine.
- System conversion: After on-line and off-line files have been converted and the reliability of the new system has been confirmed for a functional area, daily processing can be shifted from the existing information system to the new one. All transactions initiated after this time are processed on the new system. Consideration should be given to operating the old system for some more time to permit checking and balancing the total results of both systems.
- Scheduling personnel and equipment: Scheduling data processing operations of a new information system for the first time is a difficult task for the system manager. As users become more familiar with the new system, the job becomes more routine. Schedules should be set up by the system manager in conjunction with departmental managers of operational units serviced by the equipment.
- Alternative plans in case of equipment failure: Alternative processing plans must

be implemented in case of equipment failure. Priorities must be given to those jobs, which are critical to an organization, such as billing, payroll, and inventory. Critical jobs can be performed manually until the equipment is set right.

(c) Executive Information Systems differs from Traditional Information Systems in many ways. The following table presents the difference on various related dimensions:

Dimensions of Difference	Executive Information System	Traditional Information System
Level of management	For top or near top executives	For lower staff
Nature of Information Access	Specific issues/problems and aggregate reports	Status reporting
Nature of information provided	Online tools and analysis	Offline status reporting.
Information Sources	More external, less internal	Internal
Drill down facility to go through details at	Available	Not available
Information format	Text with graphics	Tabular
Nature of interface	User-friendly	Computer-operator

Question 3

(a) What is scope of output control of an application system ? Suggest various types of output controls which are enforced for confidentiality, integrity and consistency of output.

(6 Marks)

(b) What is an Expert System? List the properties which an application should posses to qualify for Expert System development. *(6 Marks)*

(c) What do you mean by 'Packet Filter Firewall'? Explain the major weaknesses associated with it. *(4 Marks)*

Answer

(a) The scope of Output controls of an application system is given as follows:

To provide functions that determine the data content available to users, data format, timeliness of data and how data is prepared and routed to users.

Various types of output controls, which are enforced for confidentiality, integrity and consistency of output, are given as follows:

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

- *Logging of output program executions:* When programs used for output of data are executed, it should be logged and monitored. In the absence of control over such output program executions, confidentiality of data could be compromised.
- *Spooling/Queuing:* This is a process used to ensure that the user is able to continue working, even before the print operation is completed. When a file is to be printed, the operating system stores the data stream to be sent to the printer in a temporary file on the hard disk. This file is them "spooled" to the printer as soon as the printer is ready to accept the data. This intermediate storage of output could lead to unauthorized disclosure and/or modification. A queue is the list of documents waiting to be printed on a particular printer. This queue should not be subject to unauthorized modifications.
- *Controls over printing:* It should be ensured that unauthorized disclosure of information printed is prevented. Users must be trained to select the correct printer and access restrictions may be placed on the workstations that can be used for printing.
- *Report distribution and collection controls:* Distribution of reports should be made in a secure way to ensure unauthorized disclosure of data. A log should be maintained as to what reports were generated and to whom it was distributed. Where users have to collect reports; the user should be responsible for timely collection of the report especially if it is printed in a public area. A log should be maintained as to what reports where printed and which of them where collected. Uncollected reports should be stored securely.
- *Retention controls:* Retention controls consider the duration for which outputs should be retained before being destroyed. Consideration should be given to the type of medium on which the output is stored. Retention control requires that a date should be determined for each output item produced.
- *Existence/Recovery Controls:* These are needed to recover output in the event that it is lost or destroyed. If the output is written to a spool of files or report files and has been kept, then recovering and new generation is easy and straight-forward.

(b) Expert System: An Expert System is highly developed Decision Support System (DSS) that utilizes the knowledge generally possessed by an expert to solve a problem. Expert Systems are software systems that imitate the reasoning processes of human experts and provide decision makers with the type of advice they would normally receive from such expert systems. For instance, an expert system in the area of investment portfolio management might ask its user a number of specific questions relating to investments for a particular client like – how much can be invested. Does the client have any preferences regarding specific types of securities?

Major properties that an application should possess to qualify for Expert System development are given as follows:

- Availability: One or more experts are capable of communicating 'how they go about solving the problems to which the Expert System will be applied'.
- Complexity: Solution of the problems for which the Expert Systems will be used is a complex task that requires logical inference processing, which would not be easily handled by conventional information processing.
- Domain: The domain, or subject area, of the problem is relatively small and limited to a relatively well-defined problem area.
- Expertise: Solutions to the problem require the efforts of experts. That is, only a few possess the knowledge, techniques, and intuition needed.
- Structure: The solution process must be able to cope with ill-structured, uncertain, missing, and conflicting data, and a dynamic problem-solving situation.

(c) Packet Filter Firewalls: Packet filter firewalls evaluate the headers of each incoming and outgoing packet to ensure that it has a valid internal address, originates from a permitted external address, connects to an authorized protocol or service, and contains valid basic header instructions. If the packet does not match the pre-defined policy for allowed traffic, then the firewall drops the packet.

Major weaknesses associated with packet filtering firewalls are given as follows:

- The system is unable to prevent attacks that exploit application-specific vulnerabilities and functions because the packet filter does not examine packet contents.
- Logging functionality is limited to the same information used to make access control decisions.
- Most of the packet filtering firewalls do not support advanced user authentication schemes.
- These firewalls are generally vulnerable to attacks and exploitation that take advantage of vulnerabilities in network protocols.
- These firewalls are easy to misconfigure, which allows traffic to pass that should be blocked.

Question 4

(a) What do you mean by 'System Control Audit Review File' (SCARF)? What types of information can be collected by Auditor using SCARF? (6 Marks)

(b) What is Business Impact Analysis ? Enumerate the tasks which are to be undertaken in this analysis. (6 Marks)

(c) *Describe the procedure to apply for a licence to issue electronic signature certificate under Section 22 of the Information Technology (Amendment) Act, 2008. (4 Marks)*

Answer

(a) System Control Audit Review File (SCARF): SCARF technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. The information collected is written on a special audit file-the SCARF master files. Afterwards, auditors examine the information contained on this file to see if some aspect of the application system needs follow-up. In many ways, the SCARF technique is like the snapshot technique along with other data collection capabilities.

Auditors 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 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. For example, salespersons might be given some leeway in the prices they charge to customers. SCARF can be used to see how frequently salespersons override the standard price.
- 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 - Auditors 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.

(b) Business Impact Analysis: Business Impact Analysis (BIA) is a means of systematically assessing the potential impacts resulting from various events or incidents. It enables the business continuity team to identify critical systems, processes and functions, assess the economic impact of incidents and disasters that result in a denial of access to the system, services and facilities, and assess the "pain threshold," that is, the length of time business units can survive without access to the system, services and facilities.

Major tasks, which are to be undertaken in this analysis, are given as follows:

- Identifying organisational risks - This includes single point of failure and infrastructure risks. The objective is to identify risks and opportunities and to minimize potential threats that may lead to a disaster.
- Identifying critical business processes.
- Identifying and quantifying threats/ risks to critical business processes both in terms of outage and financial impact.
- Identifying dependencies and interdependencies of critical business processes and the order in which they must be restored.
- Determining the maximum allowable downtime for each business process.
- Identifying the type and the quantity of resources required for recovery e.g. tables chairs, faxes, photocopies, safes, desktops, printers, etc.
- Determining the impact to the organization in the event of a disaster, e.g. financial reputation, etc.

(c) *[Section 22] Application for license* of Information Technology (Amended) Act, 2008:

(1) Every application for issue of a license shall be in such form as may be prescribed by the Central Government.

(2) Every application for issue of a license shall be accompanied by-

(a) a certification practice statement;

(b) a statement including the procedures with respect to identification of the applicant;

(c) payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government;

(d) such other documents, as may be prescribed by the Central Government.

Question 5

(a) Briefly explain the control and objectives of 'Asset Classification and Control' in information security management system. *(6 Marks)*

(b) What is the purpose of risk evaluation ? Give some of the techniques that are available for risk evaluation. *(6 Marks)*

(c) What is Information Security Policy ? What are the issues it should address ? *(4 Marks)*

Answer

(a) 'Asset Classification and Control' in Information Security Management System (ISMS):

The detailed controls and objectives are given as follows:

- *Information Classification*: To ensure that information assets receive an appropriate level of protection, and
- *Accountability for Assets*: To maintain appropriate protection of organizational assets.

These are briefly discussed as follows:

(i) Information Classification: One of the most laborious but essential task is to manage inventory of all the IT assets, which could be information assets, software assets, physical assets or other similar services. These information assets need to be classified to indicate the degree of protection. The classification should result into appropriate information labeling to indicate whether it is sensitive or critical and what procedure, which is appropriate for copy, store, and transmit or destruction of the information asset.

(ii) Accountability for assets: It is achieved using IAR and Contracts Register. An Information Asset Register (IAR) should be created with the details of every information asset within the organization. For example: Databases, Personnel records, Scale models, Prototypes, Test samples, Contracts, Software licenses, Publicity material.

The Information Asset Register (IAR) should also describe 'who is responsible for each information asset' and 'whether there is any special requirement for confidentiality, integrity or availability'. For administrative convenience, separate register may be maintained under the subject head of IAR e.g. 'Media Register' will detail the stock of software and its licenses.

Similarly, 'Contracts Register' will contain the contracts signed and thus other details. The impact that is an addendum to mere maintenance of a register is control and thus protection of valuable assets of the corporation. The value of each asset can then be determined to ensure appropriate security is in place.

(b) 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.

Following are the major techniques, which are available for risk evaluation:

(i) Judgment and intuition: In many situations, the auditors have to use their judgment and intuition for risk assessment. This mainly depends on the personal and professional experience of the auditors and their understanding of the system and its environment. Together with it, systematic education and ongoing professional updating is also required.

(ii) The Delphi Approach: This technique is used for obtaining a consensus opinion. A panel of experts is engaged and each expert is asked to give his opinion in a written and independent method. They enlist the estimate of the cost benefits and the reasons why a particular system is to be chosen, the risks and exposures of the system. These estimates are then complied together. The estimates falling within a pre-decided acceptable range are taken. The process may be repeated four times for revising estimates falling beyond the range. Then a curve is drawn taking all the estimates as points on the graphs. The median is drawn and this is the consensus opinion.

(iii) The Scoring Approach: In this approach, the risks in the system and their respective exposures are listed. Weights are then assigned to the risks and to the exposures depending on the severity, impact of occurrence and costs involved. The product of the risk weight with the exposure weight of every characteristic gives the weighted score. The sum of these weighted score gives the risk and exposure score of the system. System risks and exposures are then ranked according to the scores.

(iv) Quantitative Techniques: Quantitative techniques involve the calculating of an annual loss exposure value based on the probability of the event and the exposure in terms of estimated costs. This helps the organization to select cost effective solutions. It is the assessment of potential damage in the event of occurrence of unfavorable events, keeping in mind how often such an event may occur.

(v) Qualitative Techniques: These are by far the most widely used approach to risk analysis. Probability data is not required and only estimated potential loss is used. Most qualitative risk analysis methodologies make use of a number of interrelated elements, namely, threats, vulnerabilities, and controls.

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

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

The policy should address the following major issues:

- a definition of information security,
- reasons for 'why information security is important to the organization', and its goals and principles,
- a brief explanation of the security policies, principles, standards and compliance requirements,

- definition of all relevant information security responsibilities, and
- reference to supporting documentation.

Question 6

(a) Under the IT Infrastructure Library (ITIL) framework, discuss the importance of following :

(i) Release management

(ii) ICT infrastructure management (6 Marks)

(b) Mr. A has received some information about Mr. B on his cellphone. He knows that this information has been stolen by the sender. He not only retained this information but also sends it to Mr. B and his friends. Because of this act Mr. B is annoyed and his life is in danger.

Mr. B seeks your advice, under what sections of Information Technology (Amendment) Act, 2008, he can file an FIR with police? Advise Mr. B detailing the applicable sections of the Act. (6 Marks)

(c) 'Every company that intends to implement ERP has to Re-engineer its processes in one form or other.' In the light of this statement, describe any four processes that needs to be re-engineered. (4 Marks)

Answer

(a) (i) Release Management under ITIL: Release Management is used for platform-independent and automated distribution of software and hardware, including license controls across the entire IT infrastructure. Proper Software and Hardware Control ensure the availability of licensed, tested, and version certified software and hardware, which will function correctly and respectively with the available hardware. Quality control during the development and implementation of new hardware and software is also the responsibility of Release Management. This guarantees that all software can be conceptually optimized to meet the demands of the business processes. The goals of release management are:

- ♦ Plan to rollout of software,
- ♦ Design and implement procedures for the distribution and installation of changes to IT systems,
- ♦ Effectively communicate and manage expectations of the customer during the planning and rollout of new releases, and
- ♦ Control the distribution and installation of changes to IT systems.

(ii) ICT Infrastructure Management under ITIL: ICT Infrastructure Management processes recommend best practices for requirements analysis, planning, design, deployment and ongoing operations of management and technical support of an ICT

Infrastructure. The Infrastructure Management processes describe those processes within ITIL that directly relate to the ICT equipment and software that is involved in providing ICT services to customers; these are given as follows:

- ♦ ICT Design and Planning,
- ♦ ICT Deployment,
- ♦ ICT Operations, and
- ♦ ICT Technical Support.

(b) It is not clear whether Mr. B wants to file an FIR with police against Mr. A or sender, who has stolen his information or both.

Considering the most feasible assumption that if Mr. B wants to file an FIR against Mr. A then he may file the same under the following Section of Information Technology (Amendment) Act, 2008:

- Section 66 A: Punishment for sending offensive messages through communication service, etc.;
- Section 66 B: Punishment for dishonestly receiving stolen computer resource or communication device; and
- Section 66 E: Punishment for violation of privacy.

All these applicable sections in this case are given as follows:

[Section 66 A] Punishment for sending offensive messages through communication service, etc.

Any person who sends, by means of a computer resource or a communication device,-

(a) any information that is grossly offensive or has menacing character; or

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently by making use of such computer resource or a communication device,

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation: For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

[Section 66 B] Punishment for dishonestly receiving stolen computer resource or communication device.

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

[Section 66E] Punishment for violation of privacy

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

However, the answer may also be written considering the other two assumptions, accordingly.

(c) In the light of the statement given in the question, the following are the major processes that need to be re-engineered:

- Forecasting: Shows sales, Fund Flows etc. over a long period of time say next two years.
- Fund Management: The necessity of funds and the way to raise these funds. Uncertainty and Risk factors to be considered. Simulation with `What if" type analysis.
- Price Planning: Determines the price at which products are offered. It involves application of technology to pricing support such as commercial database services. Also performs feedback and sensitivity analysis.
- Budget Allocation: Using computerized algorithms to estimate desirable mix of funds allocated to various functions.
- Material Requirement Planning: Process of making new products from raw materials and include production scheduling, requirement planning. Also includes activities for monitoring and planning of actual production.
- Quality Control: Takes care of activities to ensure that the products are of desired quality.

Question 7

Write short notes on any four of the following:

(a) Purpose of IS Audit Policy (4 Marks)

(b) Audit Tools and Techniques used in Disaster Recovery Plan. (4 Marks)

(c) Risk Assessment (4 Marks)

(d) Reasons for failure of ERP projects (4 Marks)

(e) *Recognition of Foreign, certifying authorities as per under Section 19 of Information Technology (Amendment) Act, 2008* *(4 Marks)*

Answer

(a) Purpose of IS Audit Policy: Purpose of the audit policy is to provide the guidelines to the audit team to conduct an audit on IT based infrastructure system. The Audit is done to protect entire system from the most common security threats such as access to confidential data, unauthorized access of the department computers, password disclosure compromise, virus infections, denial of service attacks etc.

Audits may be conducted to ensure integrity, confidentiality and availability of information and resources. The IS Audit Policy should lay out the objective and the scope of the audit. An IS audit is conducted to:

- safeguard the Information System Assets/Resources,
- maintain the Data Integrity,
- maintain the System Effectiveness,
- ensure System Efficiency, and
- comply with Information System related policies, guidelines, circulars, and any other instructions requiring compliance in whatever name called.

(b) Audit Tools and Techniques in Disaster Recovery Plan: The best audit tool and technique is a periodic simulation of a disaster. Other audit techniques would include observations, interviews, checklists, inquiries, meetings, questionnaires and documentation reviews. These tools and methods may be categorized as under:

- Automated Tools: Automated tools make it possible to review the 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.
- 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.
- 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.
- Penetration Testing: Penetration testing can be used to locate vulnerabilities.

(c) Risk Assessment: A risk assessment activity can provide an effective approach, which acts as the foundation for avoiding the disasters. Risk assessment is also termed as a critical step in disaster and business continuity planning. Risk assessment is necessary for developing a well-tested contingency plan. In addition, Risk assessment is the analysis of threats to resources (assets) and the determination of the amount of

protection necessary to adequately safeguard the resources, so that vital systems, operations, and services can be resumed to normal status in the minimum time in case of a disaster. Disasters may lead to vulnerable data and crucial information suddenly becoming unavailable. The unavailability of data may be due to the non-existence or inadequate testing of the existing plan.

Risk assessment is a useful technique to assess the risks involved in the event of unavailability of information, to prioritize applications, identify exposures and develop recovery scenarios.

(d) Reasons for failure of ERP projects: At its simplest level, ERP is a set of best practices for performing the various duties in the departments of a company, including finance, manufacturing and the warehouse. To get the most from the software, we have to get people inside our company to adopt the work methods outlined in the software. If the people in the different departments that will use ERP don't agree that the work methods embedded in the software are better than the ones they currently use, they will resist using the software or will want IT to change the software to match the ways they currently do things. This is where ERP projects break down.

Political fights erupt over how or even whether the software will be installed. IT gets bogged down in long, expensive customization efforts to modify the ERP software to fit with powerful business barons' wishes. Customizations make the software more unstable and harder to maintain when it finally does come to life. Because ERP covers so much of 'what a business does'; a failure in the software can bring a company to a halt, literally.

The mistake companies make is assuming that changing people's habits will be easier than customizing the software. It's not the case. Getting people inside the company to use the software to improve the ways they do their jobs is by far the harder challenge. If people are resistant to change, then the ERP project is more likely to fail.

(e) [Section 19] Recognition of foreign Certifying Authorities: Section 19 provides the power of the Controller with the previous approval of the Central Government to grant recognition to foreign Certifying Authorities subject to such conditions and restrictions as may be imposed by regulations. As per ITAA 2008, Section 19 is given as under:

(1) Subject to such conditions and restrictions as may be specified by regulations, the Controller may with the previous approval of the Central Government, and by notification in the Official Gazette, recognize any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.

(2) Where any Certifying Authority is recognized under sub-section (1), the Electronic Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.

(3) The Controller may if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub- section (1) he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.