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

Page No. of SHAYVIDZ Book : 2.27

Answer :

This phase includes a **thorough and detailed understanding of the current system**, identifies the **areas that need modification to solve the problem**, the **determination of user/managerial requirements** and to have fair idea about various systems 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** 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 activities such as **developing models** to document Data Flow Diagrams, E-R Diagrams.
- To **document activities** such as interview, questionnaires, reports etc. and development of a system (data) dictionary to document the modeling activities.

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

Page No. of SHAYVIDZ Book : 3.24

<u>Boundary Controls:</u>

The three classes of information with respect to the corresponding input to the boundary control are summarized in the table below.

Class of Information		***Types of Input***
Personal Information	:	Name, Birth date, account number, password, PIN
Personal Characteristics	:	Fingerprint, voice, hand size, signature, retinal pattern.
Personal Objects	:	Identification cards, badge, key, finger ring.

Boundary control techniques are:

- **Personal Identification Numbers (PIN):** The personal identification number 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.
- **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.

- **Cryptography:** This 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).

- **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.

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

Page No. of SHAYVIDZ Book : 7.19

Answer:

There are certain general guidelines, which are to be followed before starting the implementation of an ERP package.

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

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

Page No. of SHAYVIDZ Book : 9.16

Answer :

A business continuity management process should be designed, implemented and periodically tested to reduce the disruption caused by disasters and security failures. This begins by identifying all events that could cause interruptions to business processes and depending on the risk assessment, preparation of a strategy plan. In Business Continuity planning, following points should be addressed:

- 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.

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

Page No. of SHAYVIDZ Book : 2.8 & 2.10

Answer :

The Prototyping Model

- The traditional approach sometimes may take years to analyze, design and implement a system. In order to avoid such delays, organizations are increasingly using prototyping techniques to develop smaller systems such as DSS, MIS and Expert systems.
- The goal of prototyping approach 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

Strengths

1. Improves both user participation in system development and communication among project stakeholders.
2. 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.
3. Potential exists for exploiting knowledge gained in an early iteration as later iterations are developed.
4. Helps to easily identify confusing or difficult functions and missing functionality.
5. May generate specifications for a production application.
6. Encourages innovation and flexible designs.
7. Provides quick implementation of an incomplete, but functional, application.
8. Prototyping requires intensive involvement by the system users. Therefore, it typically results in a better definition of these user's needs and requirements than does the traditional systems development approach.
9. 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.

10. 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) What activities are involved in system conversion? Explain them briefly.

Page No. of SHAYVIDZ Book : 2.55

Answer :

Activities for Successful Conversion

(i) **Procedure conversion :** Operating procedures should be completely documented for the new system. Written operating procedures must be supplemented by oral communication during the training sessions on the system change.

(ii) **File conversion :** The cost and related problems of file conversion are significant whether they involve online files (common data base) or offline files. In order for the conversion to be as accurate as possible, file conversion programs must be thoroughly tested. Adequate controls, such as record counts and control totals, should be the required output of the conversion program.

(iii) **System conversion :** A cut-off point is established so that database and other data requirements can be updated to the cut-off point. 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. The old system can be dropped as soon as the data processing group is satisfied with the new system's performance.

(iv) **Scheduling personnel and equipment :** Schedules should be set up by the system manager in conjunction with departmental managers of operational units serviced by the equipment. Just as the equipment must be scheduled for its maximum utilisation, so must be personnel who operate the equipment.

(v) **Alternative plans in case of equipment failure:** Alternative-processing plans must be implemented in case of equipment failure. A written manual of procedures concerning what steps must be undertaken will help expedite the unfavourable situation. Otherwise, panic will result in the least efficient methods when time is of the essence.

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

Page No. of SHAYVIDZ Book : 1.44 (Class Notes) + PM 1.29 Q.No.10

Answer :

Executive Information System (EIS) is a tool that provides direct on-line access to relevant information, in a useful and navigable format, about aspects of a business that are of particular interest to the senior manager.

These systems are designed in such a format so that they can be used by individuals with limited time, and limited knowledge of operating computers to search information relating to broad strategic issues and then explore the information to find the root causes of those issues.

Executive information systems differ from traditional information systems in the following ways.

1. They are specifically tailored to executive's information needs.
2. They are able to access data about specific issues and problems as well as aggregate reports.
3. They provide extensive on-line analysis tools including trend analysis and exception reporting etc.
4. They can access a broad range of internal and external data.
5. They are particularly easy-to-use (typically mouse or touch-screen driven).
6. They are used directly by executives without assistance.
7. All EISs are delivered through terminals using easy-to-use software.
8. Information tends to be presented by pictorial or graphical means, whereas in most traditional information systems, information is usually presented in numerical or textual form, usually in printed report format.
9. Information is presented in summary format e.g. sales for the whole company. There is the facility to drill down to the other levels of information to see how the sales figures were arrived at–by geographical location, by product group etc.
10. The ability to manipulate data, to project `what if' outcomes and to work with modeling tools within the system are also evident in EIS. This is particularly so with external information that can be super imposed on to the company's information e.g. sales forecasts with information from the meteorological office about the weather.

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

Page No. of SHAYVIDZ Book : 3.27

Answer :

Scope of Output Controls :

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.

Output Controls: This ensure that the data delivered to users will be presented, formatted and delivered in a consistent and secured manner. Output can be in any form, it can either be a printed data report or a database file in a removable media such as a floppy disk or CDROM or it can be a Word document on the computer's hard disk. Output controls have to be enforced both in a batch-processing environment as well as in an online environment.

- **Spooling/Queuing:** "Spool" is an acronym for "Simultaneous Peripherals Operations Online". 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.

- **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.

- **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. The state of a transaction at a point of time with before and after images. Check/restart helps in recovery when a hardware problem causes a program that prints customer invoices to abort in midstream.

- **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. Various factors ranging from the need of the output, use of the output, to legislative requirements would affect the retention period.

- **Storage 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.

- **Report distribution and collection controls:** Distribution of reports should be made in a secure way to ensure unauthorized disclosure of data, it should be made immediately after printing to ensure that the time gap between generation and distribution is reduced. 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 timey 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.

- **Printing Controls:** 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.

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

Page No. of SHAYVIDZ Book : 1.34 & 1.35

Answer :

An **Expert System** is highly developed DSS that utilizes knowledge generally possessed by an expert to share a problem. Expert System 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? And so on.

Properties that potential applications should posses to qualify for Expert System

Some of the properties that potential applications should posses to qualify for Expert System development are as follows:

1. **Availability** : One or more experts are capable of communicating how they go about solving the problems to which the Expert System will be applied.

2. **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.

3. **Domain** : The domain, or subject area, of the problem is relatively small and limited to a relatively well-defined problem area.

4. **Expertise** : Solutions to the problem require the efforts of experts. That is, only a few possess the knowledge, techniques, and intuition needed.

5. **Structure** : The solution process must be able to cope with ill-structured, uncertain, missing, and conflicting data, and a dynamic problem-solving situation.

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

Page No. of SHAYVIDZ Book : 3.6

Answer :

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

Weaknesses associated with packet filtering firewalls include the following:

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

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

Page No. of SHAYVIDZ Book : 4.21

Answer :

System Control Audit Review File (SCARF):

The system control audit review tile (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 onto a special audit file the SCARF master files. Auditors then examine the information contained on this file to see if some aspect of the application system needs follow-up.

Auditors might use SCARF to collect the following types of information:

i. 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.

ii. Policy and procedural variances

Organisations have to adhere to the policies, procedures and standards of the organisation 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.

iii. 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.

iv. 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.

v. Snapshots and extended records

Snapshots and extended records can be written into the SCARF file and printed when required.

vi. 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.

vii. Performance measurement

Auditors can use embedded routines to collect data that is useful for measuring or improving the performance of an application system.

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

Page No. of SHAYVIDZ Book : 6.7

BUSINESS IMPACT ANALYSIS (BIA)

The business impact analysis is intended to help understand the **degree of potential loss** (and various other unwanted effects) which could occur. This will cover not just direct **financial loss**, but **other issues, such as reputation damage, regulatory effects,** etc.

A number of **TASKS** are to be undertaken in this phase as enumerated under :

(i) Identify organisational **risks** - This includes single point of failure and infrastructure risks. The objective is to identify risks and opportunities and to minimise potential threats that may lead to a disaster.

(ii) Identify **critical business processes**.

(iii) Identify and quantify threats/ risks to critical business processes both in terms of outage and financial impact.

(iv) Identify dependencies and interdependences of critical business processes and the order in which they must be restored. (Order of Recovery)

(v) Determine the maximum allowable downtime for each business process. (Tolerance Time)

(vi) Identify the type and the quantity of resources required for recovery e.g. tables chairs, faxes, photocopies, safes, desktops, printers, etc.

(vii) Determine the impact to the organisation in the event of a disaster, e.g. financial reputation, etc.

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

Page No. of SHAYVIDZ Book : 10.16

Answer :

Application for license

- Every application for issue of a license shall be **in such form** as may be prescribed by the Central Government.
- Every application for issue of a license shall be accompanied by -
  - a **certification practice statement**;
  - a statement including the procedures with respect to **identification of the applicant**;
  - payment of such fees, **NOT EXCEEDING Rs. 25000,** as may be prescribed by the C.G.
  - **such other documents**, as may be prescribed by the Central Government

5. (a) Briefly explain the control and objective of 'Asset Classification and Control' in information security management system?

Page No. of SHAYVIDZ Book : 8.4

Answer :

Asset Classification and Control

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 info appropriate information **labeling to indicate** whether it is **sensitive or critical and** what **procedure**, is appropriate to copy, store, transmit or destruction of the information asset.

An **Information Asset Register (IAR)** should be created detailing each of the following information assets within the organization:

- Databases
- Personnel records
- Scale models
- Prototypes
- Test samples
- Contracts
- Software licenses
- Publicity material

The detailed control and objectives thereof are as follows:

• ***Accountability for assets***

To maintain appropriate protection of organizational assets.

• ***Information Classification***

To ensure that information assets receive an appropriate level of protection.

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

Page No. of SHAYVIDZ Book : 5.20

Answer :

The PURPOSE OF A RISK EVALUATION is to

(i) identify the probabilities of failures and threats,

(ii) calculate the exposure, i.e., the damage or loss to assets, and

(iii) make control recommendations keeping the cost-benefit analysis in mind.

TECHNIQUES FOR RISK EVALUATION

I. Judgement and intuition

II. The Delphi approach

III. Scoring Approach

IV. Quantitative Techniques

V. Qualitative Techniques

I. Judgement 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 is required a systematic education and ongoing professional updating.

II. Delphi Technique

- 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 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.

III. Scoring approach

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

IV. Quantitative techniques

- Quantitative techniques involve the calculating an annual loss exposure value based on the probability of the event and the exposure in terms of estimated costs. This helps the organisation to select cost effective solutions.

- It is the assessment of potential damage in the event of occurrence of unfavourable events, keeping in mind how often such an event may occur.

V. Qualitative techniques

Qualitative techniques 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:

- **Threats** : These are things that can go wrong or that can 'attack' the system. Examples, might include fire or fraud. Threats are ever present for every system.

- **Vulnerabilities** : These make a system more prone to attack by a threat or make an attack more likely to have some success or impact. For example, for fire, vulnerability would be the presence of inflammable materials (e.g. paper).

- **Controls** : These are the countermeasures for vulnerabilities. There are four types:
  (i) **Deterrent controls** reduce the likelihood of a deliberate attack
  (ii) **Preventative controls** protect vulnerabilities and make an attack unsuccessful or reduce its impact
  (iii) **Corrective controls** reduce the effect of an attack
  (iv) **Detective controls** discover attacks and trigger preventative or corrective controls.

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

Page No. of SHAYVIDZ Book : 9.7

Answer :

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.

ISSUES TO ADDRESS

- This policy does not need to be extremely extensive, but clearly state senior management's commitment to information security, be under change and version control and be signed by the appropriate senior manager. **The policy should at least address the following issues:**
  - a definition of information security,
  - reasons why information security is important to the organisation, and its goals and principles,
  - a brief explanation of the security policies, principles, standards and compliance requirements,
  - definition of all relevant information security responsibilities
  - reference to supporting documentation.
- The auditor should ensure that the policy is readily accessible to all employees and that all employees are aware of its existence and understand its contents.
- The policy may be a standalone statement or part of more extensive documentation (e.g. a security policy manual) that defines how the information security policy is implemented in the organization.
- In general, most if not all employees covered by the ISMS scope will have some responsibilities for information security, and auditors should review any declarations to the contrary with care.
- The auditor should also ensure that the policy has an owner who is responsible for its maintenance and that it is updated responding to any changes affecting the basis of the original risk assessment.

6. (a) Under the IT Infrastructure Library (ITIL) framework, discuss the importance of following:
(i) Release Management
(ii) ICT infrastructure Management

Page No. of SHAYVIDZ Book : 8.21 & 8.23

Answer :

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
- Control the distribution and installation of changes to IT systems

ICT Infrastructure Management processes recommend best practice 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.

- ICT Design and Planning
- ICT Deployment
- ICT Operations
- ICT Technical Support

(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 friend. Because of this act Mr. B is annoyed and his life is in danger.
Mr. B seeks your advise, under what sections of Information Technology (Amendment) Act, 2008, he can file an FIR with police? Advice Mr. B detailing the applicable sections of the Act.

Page No. of SHAYVIDZ Book : 10.43 (Class Notes) w. r. t. 10.29 & 10.36

Answer :

Section 66A : 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**;

(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 message.**

shall be punishable with imprisonment upto 3 years and with fine.

Section 77B : Offences with three years imprisonment to be cognizable

Notwithstanding anything contained in Criminal Procedure Code 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bail able.

Thus, as per Section 66A (b), Mr. A shall be punishable with imprisonment upto 3 years and with fine. Further, this offence is cognizable as per section 77B as the period of imprisonment for the offence is three years. So, Mr. B is advised to file FIR with police under section 66A read with section 77B of Information Technology (Amendment) Act, 2008.

(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.

Page No. of SHAYVIDZ Book : 7.8

Answer :

ERP is a result of a modern Enterprise's concept of how the Information System is to be configured to the challenging environments of new business opportunities. However merely putting in place an information system is not enough. Every company that intends to implement ERP has to re-engineer its processes in one form or the other. This process is known as BPR. Some Typical processes are :

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. Involves application of technology to pricing support such as commercial database services. Also feedback and sensitivity analysis

Budget Allocation :

Using computerised 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 activities for monitoring and planning of actual production.

Quality control :

Takes care of activities to ensure that the products are of desired quality.

7. (a) Purpose of IS Audit Policy.

Page No. of SHAYVIDZ Book : 9.17

Answer :

Purpose of this 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 which includes the following:

- Access to confidential data,
- Unauthorized access of the department computers,
- Password disclosure compromise,
- Virus infections,
- Denial of service attacks,
- Open ports, which may be accessed from outsiders, and
- Unrestricted modems unnecessarily open ports.

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 Policy. **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 used in Disaster Recovery Plan.

Page No. of SHAYVIDZ Book : 6.33

Answer :

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 categorised as under:

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.

(c) Risk Assessment.

Page No. of SHAYVIDZ Book : 5.7

Answer :

- Risk assessment is a critical step in disaster and business continuity planning. Risk assessment is necessary for developing a well tested contingency plan.
- 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.

Page No. of SHAYVIDZ Book : 7.22

Answer :

ERP is a set of best practices for performing the various duties in the departments of your company, including in finance, manufacturing and the warehouse. To get the most from the software, you have to get people inside your 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 customisation 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.

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

Page No. of SHAYVIDZ Book : 10.15

Answer :

Recognition of Foreign Certifying Authorities

- The Controller may with the **previous approval** of the Central Government, recognize any Foreign Certifying Authority as a Certifying Authority for the purposes of this Act.
- Where any Certifying Authority is recognized, the Electronic Signature Certificate issued by such Certifying Authority shall be **valid** for the purposes of this Act.
- The Controller may if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions, he may, for reasons to be recorded in writing, by notification in Official Gazette, **revoke** such recognition.

Chapter-wise Marks Distribution of ISCA – May 2013 Exam

Chapter No.	Chapter Name	Ques No.	Marks	Total Marks
1	Information Systems Concepts	2(c) 3(b)	4 6	**10**
2	System Development Life Cycle Methodology	1(a) 2(a) 2(b)	5 6 6	**17**
3	Control Objectives	1(b) 3(a) 3(c)	5 6 4	**15**
4	Testing – General and Automated Control	4(a)	6	**6**
5	Risk Assessment Methodologies and Applications	5(a) 7(c)	6 4	**10**
6	Business Continuity Planning and Disaster Recovery Planning	4(b) 7(b)	6 4	**10**
7	An Overview of Enterprise Resource Planning (ERP)	1(c) 6(c) 7(d)	5 4 4	**13**
8	Information Systems Auditing Standards, Guidelines, Best Practices	5(a) 6(a)	6 6	**12**
9	Drafting of IS Policy, Audit Policy, IS Audit Reporting – A Practical Perspective	1(d) 5(a) 7(a)	5 4 4	**13**
10	Information Technology (Amendment) Act, 2008	4(c) 6(b) 7(e)	4 6 4	**14**
	Total			**120**