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.

*Attempt any **five** questions from the remaining **six** questions.*

Question 1

Skyair is an airline company operating with in-house developed software till now. Its profit margins are under pressure due to inefficiency and disorganized work culture.

To survive in the highly competitive environment, it has to improve the efficiency of its internal processes and synchronize isolated functions into streamlined business processes so that work culture is improved. Hence it has decided to purchase and implement a real time ERP package. In order to improve its margin, it wants to transact with suppliers and customers electronically and maintain all records in electronic form. Security of information is a key activity of this process which must be taken care of from the beginning. As a member of implementation team you are required to answer the following:

(a) What issues you would like to raise during the technical feasibility of new proposed system? *(5 Marks)*

(b) Describe the provisions for authentication of electronic records under Information Technology (Amendment) Act, 2008. *(5 Marks)*

(c) Suggest the controls that need to be in place at the time of application software acquisition or selection process. *(5 Marks)*

(d) Describe any five major types of information security policy which company must maintain to meet the security objectives. *(5 Marks)*

Answer

(a) During the technical feasibility of new proposed system, the following issues may be raised:

- Does the necessary technology exist to do 'what is suggested (and can it be acquired)'?
- Does the proposed equipment/s have the technical capacity to hold the data required to be used by the new system?
- Can the proposed application be implemented with existing technology?
- Will the proposed system provide the adequate responses to inquiries, regardless of the number or location of users?
- Can the system be expanded, if developed?
- Are there technical guarantees of accuracy, reliability, ease of access, and data security?

(b) Provisions of authentication of electronic records are given under Section 3 of Information Technology (Amendment) Act, 2008, which is given as follows:

[Section 3] Authentication of Electronic Records:

(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 sub-section, "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.

(c) The following are the major controls that are required to be in place at the time of application software acquisition or selection process:

- Information and system requirements are needed to meet the business and system goals, system processes to be accomplished, and the deliverables and expectations for the system. The techniques are interviews, deriving requirements from existing systems, identifying characteristics from related system, and discovering them from a prototype or pilot system.
- A feasibility analysis should be done to define the constraints or limitations for each alternative system from technical as well as business perspective. It should also include economic, technical, operational, schedule, legal or contractual, and political feasibility of the system within the organization scope.
- A detailed Request for Proposal (RFP) document needs to specify the acceptable requirements (functional, technical, and contractual) as well as the evaluation criteria used in the vendor selection process. The selection criteria should prevent any misunderstanding or misinterpretation.

- While identifying various alternatives, software acquisition involves the critical task of vendor evaluation. The vendor evaluation process considers the following:
  - ♦ Stability of the supplier company,
  - ♦ Volatility of system upgrades,
  - ♦ Existing customer base,
  - ♦ Supplier's ability to provide support,
  - ♦ Cost-benefits of the hardware/software in support of the supplier application, and
  - ♦ Customized modifications of the application software.

(d) Major Information Security Policies, which company must maintain to meet the security objectives, are given as follows:

- Information Security Policy: This policy provides a definition of Information Security, its overall objective and the importance applies to all users.
- User Security Policy: This policy sets out the responsibilities and requirements for all IT systems' users. It provides security terms of reference for Users, Line Managers and System Owners.
- Acceptable Usage Policy: This sets out the policy for acceptable usage of email and Internet services.
- Organizational Information Security Policy: This policy sets out the Group policy for the security of its information assets and the IT systems, processing this information.
- Network & System Security Policy: This policy sets out detailed policy for system and network security and applies to IT department users.
- Information Classification Policy: This policy sets out the policy for the classification of information.
- Conditions of Connection: This policy sets out the Group policy for connecting to their network. It applies to all organizations connecting to the Group and relates to the conditions that apply to different suppliers' systems.

Question 2

(a) Define Transaction Processing System (TPS). List out the salient features of a TPS. *(6 Marks)*

(b) Describe the Agile Methodology of system development. Describe its strength. *(6 Marks)*

(c) What are the grounds on which a certifying authority may revoke a digital certificate issued by it, in accordance with section 38 of Information Technology (Amendment) Act, 2008 ? *(4 Marks)*

Answer

(a) Transaction Processing System (TPS): TPS at the lowest level of management is an information system that manipulates data from business transactions. Any business activity such as sales, purchase, production, delivery, payments or receipts involves transaction and these transactions are to be organized and manipulated to generate various information products for external use. TPS records and manipulates transaction data into usable information.

The salient features of a TPS are given as follows:

- Large volume of data: As TPS is transaction – oriented, it generally consists large volumes of data and thus requires greater storage capacity. Their major concern is to ensure that the data regarding the economic events in the organizations are captured quickly and correctly.
- Automation of basic operations: Any TPS aims at automating the basic operations of a business enterprise and plays a critical role in day-to-day functioning of the enterprise. Any failure in the TPS for a short period of time can play havoc with the functioning of the enterprise. Thus, TPS is an important source of up-to-date information regarding the operations in the enterprise.
- Benefits are easily measurable: TPS reduces the workload of the people associated with the operations and improves their efficiency by automating some of the operations. Most of these benefits of the TPS are tangible and easily measurable. Therefore, cost benefit analysis regarding the desirability of TPS is easy to conduct. As the benefits from TPS are mainly tangible, the user acceptance is easy to obtain.
- Source of input for other systems: TPS is the basic source of internal information for other information systems. Heavy reliance by other information systems on TPS for this purpose makes TPS important for tactical and strategic decisions as well.

(b) Agile Methodology: This is a group of software development methodologies based on the *iterative and incremental* development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams.

It promotes adaptive planning, evolutionary development and delivery; time boxed iterative approach and encourages rapid and flexible response to change. It is a conceptual framework that promotes foreseen interactions throughout the development life cycle.

Major strengths of agile methodology are given as follows:

- Agile methodology has the concept of an adaptive team, which is able to respond to the changing requirements.
- The team does not have to invest time and efforts and finally find that by the time they delivered the product, the requirements of the customer have changed.
- Face-to-face communication and continuous inputs from customer representative leaves no space for guesswork.
- The documentation is crisp and to-the-point to save time.
- The end result is the high quality software in least possible time duration and satisfied customer.

(c) Section 38 of Information Technology (Amendment) Act, 2008 provides certain grounds for the *revocation of Digital Signature Certificates* under certain circumstances, which is given as follows:

[Section 38] Revocation of Digital Signature Certificate

A Certifying Authority may revoke a Digital Signature Certificate issued by it

(i) where the subscriber or any other person authorized by him makes a request to that effect; or

(ii) upon the death of the subscriber; or

(iii) upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.

Subject to the provisions of sub-section (3) and without prejudice to the provisions of sub- section (1), a Certifying Authority may revoke a Digital Signature Certificate which has been issued by it at any time, if it is of opinion that -

(i) a material fact represented in the Digital Signature Certificate is false or has been concealed;

(ii) a requirement for issuance of the Digital Signature Certificate was not satisfied;

(iii) the Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability;

(iv) the subscriber has been declared insolvent or dead or where a subscriber is a firm or a company, which has been dissolved, wound-up or otherwise ceased to exist.

A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.

Question 3

(a) Explain, briefly, the six categories of controls classified on the basis of nature of IS resources. *(6 Marks)*

(b) How an auditor will determine whether the disaster recovery plan was developed using a sound and robust methodology? Explain. *(6 Marks)*

(c) With reference to ERP package (SAP), briefly explain three modules of Enterprise Controlling. *(4 Marks)*

Answer

(a) Six categories of controls classified on the basis of the nature of IS resources are given as follows:

(i) *Environmental Controls:* Controls relating to the housing of IT resources such as power, air-conditioning, UPS, smoke detection, fire-extinguishers, dehumidifiers etc.

(ii) *Physical Access Controls:* Controls relating to physical security of the tangible IS resources and intangible resources stored on tangible media etc. Such controls include Access control doors, Security guards, door alarms, restricted entry to secure areas, visitor logged access, video monitoring etc.

(iii) *Logical Access Controls:* Controls relating to logical access to information resources such as operating systems controls, Application software boundary controls, networking controls, access to database objects, encryption controls etc.

(iv) *IS Operational Controls:* Controls relating to IS operation, administration and its management such as day begin and day end controls, IS infrastructure management, Helpdesk operations etc.

(v) *IS Management Controls:* Controls relating to IS management, administration, policies, procedures, standards' and practices, monitoring of IS operations, Steering committee etc.

(vi) *SDLC Controls:* Controls relating to planning, design, development, testing, implementation and post implementation, change management of changes to application and other software.

(b) An auditor may determine whether the disaster recovery plan was developed by using a sound and robust methodology by evaluating the following elements:

- Identification and prioritization of the activities, which are essential for continue functioning.
- The plan is based upon a business impact analysis that considers the impact of the loss of essential functions.
- Operations managers and key employees participated in the development of the plan.
- The plan identifies the resources that will likely to be needed for recovery and the location of their availability.

- The plan is simple and easily understood so that it will be effective when it is needed.
- The plan is realistic in its assumptions.

(c) With reference to ERP package (SAP), three modules of Enterprise Controlling (EC) are given as follows:

- EC-CS,
- EC-PCA, and
- EC-EIS.

These are briefly discussed as follows:

- EC-CS: This component is used for financial statutory and management consolidation, which also allows fully automated consolidation of investments even for many companies and complex investment structures.
- EC-PCA: This allows to work with internal transfer prices and at the same time to have the right values from company, profit center, and enterprise perspectives in parallel. Any transaction that touches an object such as customer order, plant or cost center allocated to a profit center will be automatically posted to EC-PCA.

  It is also possible to take data directly from EC-PCA to EC-CS consolidation to prepare complete financial statutory statements and management reports in parallel. This provides the management with a consistent view of external and internal financial management reports.
- EC-EIS (Executive Information System): Executive Information System allows to take financial data from EC-PCA, EC-CS or any other application and combine with any external data such as market data, industry benchmarks and/or data from non-SAP applications to build a company specific comprehensive enterprise information system .

Question 4

(a) As an auditor, how will you determine whether the control is cost effective or not ? Describe the five types of costs, which are required to be considered while implementing the operating controls in a system. *(6 Marks)*

(b) 'Real time information system needs real time audit techniques like Integrated Test Facility (ITF) to provide continuous assurance.' Define and explain the ITF methodology. *(6 Marks)*

(c) What do you mean by 'Sys Trust' and 'Web Trust' ? List out the principles used by these services. *(4 Marks)*

Answer

(a) To determine whether a control is cost effective, an auditor must compare the reduction in expected losses that will occur by virtue of having the control with the costs of designing, implementing, operating and maintaining the control. The benefit of a control procedure is the difference between the expected loss with the control procedure(s) and the expected loss without it. The benefit of a control procedure must exceed its cost; then only it will be cost effective.

Five types of costs, which are required to be considered while implementing and operating controls in a system are given as follows:

(i) *Initial setup Cost*: This cost is incurred to design and implement controls. For example, a security specialist must be employed to design a physical security system.

(ii) *Executing Cost*: This cost is associated with the execution of a control. For example, the cost incurred in using a processor to execute input validation routines for a security system.

(iii) *Correction Cost*: The control has operated reliably in signalling an error or irregularity, the cost associated with the correction of error or irregularity is termed as Correction Cost.

(iv) *Failure Cost:* This refers to the cost if the control malfunctions or not designed to detect an error or irregularity. These undetected or uncorrected errors cause losses.

(v) *Maintenance Cost:* The cost is associated in ensuring the correct working of a control. For example, rewriting input validation routines as the format of input data changes.

(b) Integrated Test Facility (ITF): ITF technique involves the creation of a dummy entity in the application system files and the processing of audit test data against the entity as a means of verifying processing authenticity, accuracy, and completeness. This test data would be included with the normal production data used as input to the application system. In such cases, the auditor has to decide what would be the method to be used to enter test data and the methodology for removal of the effects of the ITF transactions.

Detailed explanation of ITF technique is given as follows:

Methods of Entering Test Data: The transactions to be tested have to be tagged. The application system has to be programmed to recognize the tagged transactions and have them invoked two updates, one to the application system master file record and one to the ITF dummy entity. Auditors can also embed audit software modules in the application system programs to recognize transactions having certain characteristics as ITF transactions. Tagging live transactions as ITF transactions has the advantages of ease of use and testing with transactions representative of normal system processing. However,

use of live data could mean that the limiting conditions within the system are not tested and embedded modules may interfere with the production processing.

The auditors may also use test data that is specially prepared. Test transactions would be entered along with the production input into the application system. In this approach, the test data is likely to achieve more complete coverage of the execution paths in the application system to be tested than selected production data and the application system does not have to be modified to tag the ITF transactions and to treat them in a special way. However, preparation of the test data could be time consuming and costly.

Methods of Removing the Effects of ITF Transactions: The presence of ITF transactions within an application system affects the output results obtained. The effects of these transactions have to be removed. The application system may be programmed to recognize ITF transactions and to ignore them in terms of any processing that might affect users. Another method would be the removal of effects of ITF transactions by submitting additional inputs that reverse the effects of the ITF transactions. Another less used approach is to submit trivial entries so that the effects of the ITF transactions on the output are minimal in which the effects of the transactions are not really removed.

(c) SysTrust and WebTrust are two specific services developed by the AICPA that are based on the Trust Services Principles and criteria. SysTrust engagements are designed for the provision or advisory services or assurance on the reliability of a system. WebTrust engagements relate to assurance or advisory services on an organization's system related to e-commerce.

Following are the major principles and related criterion, which have been developed by the AICPA to be used by the practitioners in the performance of trust services engagements such as SysTrust and WebTrust:

- Security: The system is protected against unauthorized access (both physical and logical).
- Availability: The system is available for operation and use as committed or agreed.
- Processing Integrity: System processing is complete, accurate, timely and authorized.
- Online Privacy: Personal information obtained as a result of e-commerce is collected, used, disclosed and retained as committed or agreed.
- Confidentiality: Information designated as confidential is protected as committed or agreed.

Question 5

(a) Describe any six business processes which can be integrated using ERP. (6 Marks)

(b) State the components of a security policy to protect information system of an organization. (6 Marks)

(c) Define the term 'Risk Mitigation'. Explain the common risk mitigation techniques. (4 Marks)

Answer

(a) Major business processes, which can be integrated by using an ERP system, are given as follows:

- Business System: It includes the following aspects - Business Forecasting for product/market groups; Target fixing and allocation by key parameters; Strategy formulation and implementation; Resource allocation to key result areas; Strategy monitoring and control and Information based management for management applications.
- Production: It includes the following aspects - Production planning and control; Work processes; Purchasing and procurement system; Inventory management; Inventory analysis and valuation; Excise/ custom interface; and Production information systems for production applications.
- Maintenance: It includes the following aspects - Plant maintenance planning; Breakdown, preventive, and conditional maintenance; Maintenance management – initiation, execution, control and costing; Monitoring performance of maintenance action; Maintenance contract management; and Maintenance information systems for maintenance applications.
- Quality Control: It includes the following aspects - Quality assessment against standards; Quality assessment by process, materials, and work center location; Analysis of quality by reasons and actions taken; Building quality assurance data for equipment/process/technology selection; Monitoring quality across the organization from input to output for operating decisions and business decisions; and Quality control information systems for quality control applications.
- Marketing: It includes the following aspects - Market/customer/product analysis; Sales forecasting and budgeting; Marketing research information; Distribution and channel management; Order processing and analysis; Finished goods store management; Dispatching and invoicing; Accounts receivable analysis and management; and Marketing information systems for marketing applications.
- Finance : It includes the following aspects - Financial planning and control; Management of long-term funds and working capital management; Ledgers, payables and receivables; Financial statement analysis; Cost accounting – cost center accounting and product / process costing; Cost analysis for management decisions; Tax management; Finance information systems for finance applications.
- Personnel: It includes the following aspects - Human resource planning, recruitment, and training; Employee performance appraisal and up-gradation; Job evaluation and compensation management; Employee benefits and incentives;

Employee health and safety; Disciplinary measures; Maintaining industrial peace; Personnel information systems for personnel applications.

- Consolidation of Business Operations: It includes the following aspects - Accounting by units and divisions with local focus; Consolidation by accounts in corporate functions; Comprehensive reporting systems for business decisions.

(b) The components of a good Information Security Policy to protect information systems of an organization are given as follows:

- Purpose and Scope of the Document and the intended audience,
- The Security Infrastructure,
- Security policy document maintenance and compliance requirements,
- Incident response mechanism and incident reporting,
- Security organization Structure,
- Inventory and Classification of assets,
- Description of technologies and computing structure,
- Physical and Environmental Security,
- Identity Management and access control,
- IT Operations management,
- IT Communications,
- System Development and Maintenance Controls,
- Business Continuity Planning,
- Legal Compliances,
- Monitoring and Auditing Requirements, and
- Underlying Technical Policy.

Aforementioned components are the major contents of a typical security policy. However, the policy is always organization specific and accordingly, a study of the organizations' functions, their criticality and the nature of the information would determine the content of the security policy.

(c) Risk Mitigation: A systematic reduction in the extent of exposure to a risk and/or the likelihood of its occurrence is termed as 'Risk Mitigation'. Typically, in cases of risk mitigation, there is a particular threshold that is acceptable below which the risk is attempted to be mitigated.

A risk mitigation strategy is an organization's plan for 'how it will address its identified risks'. Some of the common risk mitigation techniques are given as follows:

- Insurance: An organization may buy insurance to mitigate such risk. Under the scheme of the insurance, the loss is transferred from the insured entity to the insurance company in exchange of a premium. However, while selecting such an insurance policy, one has to look into the exclusion clause to assess the effective coverage of the policy.
- Outsourcing: The organization may transfer some of the functions to an outside agency and transfer some of the associated risks to the agency. One must make careful assessment of whether such outsourcing is transferring the risk or is merely transferring the management process. For example, outsourcing of telecommunication line viz. subscribing to a leased line does not transfer the risk. The organization remains liable for failure to provide service because of a failed telecommunication line. Consider the same example where the organization has outsourced supply and maintenance of a dedicated leased line communication channel with an agreement that states the minimum service level performance and a compensation clause in the event failure to provide the minimum service level results in to a loss. In this case, the organization has successfully mitigated the risk.
- Service Level Agreements: Some of risks can be mitigated by designing the service level agreements. This may be entered with the external suppliers as well as with the customers and users. The service agreement with the customers and users may clearly exclude or limit responsibility of the organization for any loss suffered by the customer and user consequent to the technological failure.

Question 6

(a) What is CoCo Model? Give the four important concepts lay down about 'control' in CoCo Model. *(6 Marks)*

(b) Describe any six characteristics of an effective management information system.(6 Marks)

(c) With reference to Information Security policy, explain the following :

(i) Incident handling

(ii) Business continuity management *(4 Marks)*

Answer

(a) CoCo Model: The Criteria of Control (CoCo) model was published by the Canadian Institute of Chartered Accountants (CICA). CoCo describes internal control as actions that foster the best result for an organization and those elements of an organization (including its resources, systems, processes, culture, structure and tasks) that, taken together, support people in the achievement of the organization's objectives. CoCo is “guidance,” that means it is not intended as “prescriptive minimum requirements” but rather as “useful in making judgments” about “designing, assessing and reporting on the control systems of organizations.” CoCo’s generality is one of its key strengths.

Four important concepts about "control" in CoCo Model are given as follows:

- Control is affected by people throughout the organization, including the Board of Directors (or its equivalent), management and all other staff.
- People who are accountable as individuals or teams for achieving objectives should also be accountable for the effectiveness of control that supports achievement of those objectives.
- Organizations are constantly interacting and adapting.
- Control can be expected to provide only reasonable assurance, not absolute assurance.

(b) Major characteristics for an effective Management Information System (MIS) are given as follows:

- Management Oriented: It means that efforts for the development of the information system should start from an appraisal of management needs and overall business objectives. Such a system is not necessarily for top management only; it may also meet the information requirements of middle level or operating levels of management as well.
- Management Directed: Because of management orientation of MIS, it is necessary that management should actively direct the system's development efforts. For system's effectiveness, it is necessary for management to devote their sufficient time not only at the stage of designing the system but for its review as well to ensure that the implemented system meets the specifications of the designed system.
- Integrated: Development of information should be an integrated one, which means that all the functional and operational information sub-system should be tied together into one entity. An integrated Information system has the capability of generating more meaningful information to management by taking a comprehensive view or a complete look at inter locking sub-systems that operate within a company.
- Common Data Flows: It means that the use of common input, processing and output procedures and media whenever required. Data is captured by system analysts only once and as close to its original source as possible. Afterwards, they try to utilize a minimum of data processing procedures and sub-systems to process the data and strive to minimize the number of output documents and reports produced by the system. This eliminates duplication in data collections, simplifies operations and produces an efficient information system.
- Heavy Planning Element: An MIS usually takes 3 to 5 years and sometimes even longer period to get established firmly within a company. Therefore, a MIS designer must be present in MIS development who should keep in view future objectives and requirements of firm's information in mind.

- Sub System Concept: Even though the information system is viewed as a single entity, it must be broken down into digestible sub-systems which can be implemented one at a time by developing a phasing plan. The breaking down of MIS into meaningful sub-systems sets the stage for this phasing plan.
- Common Database: Database is the mortar that holds the functional systems together. It is defined as a "super-file" which consolidates and integrates data records formerly stored in many separate data files. The organization of a database allows it to be accessed by several information sub-systems and thus, eliminates the necessity of duplication in data storage, updating, deletion and protection.
- Computerized: Though MIS can be implemented without using a computer, the use of computers increases the effectiveness of the system. In fact, its use equips the system to handle a wide variety of applications by providing their information requirements quickly. Other necessary attributes of the computer to MIS are accuracy and consistency in processing data and reduction in clerical staff. These attributes make computer a prime requirement in management information system.

(c) With reference to Information Security Policy, the brief explanation of the given terms is given as follows:

(i) Incident Handling: For incident handling, following are the major points to be addressed:

- Security incident reporting times and approach must be consistent at all the times. Specific procedures must be introduced to ensure that incidents are recorded and any recurrence is analyzed to identify weaknesses or trends.
- Procedures for the collection of evidence relating to security incidents should be standardized. All staff must be made aware of the process. Adequate records must be maintained and inspections facilitated to enable the investigation of security breaches or concerted attempts by third parties to identify security weaknesses.

(ii) Business Continuity Management: In Business Continuity Management, 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.

Question 7

Write short notes on any four of the following:

(a) *Function of Controller of Certifying Authority u/s 18 of Information Technology (Amendment) Act, 2008* *(4 Marks)*

(b) *Systematic and Unsystematic risk* *(4 Marks)*

(c) *Goals of the business continuity plan* *(4 Marks)*

(d) *Five levels of software process maturity* *(4 Marks)*

(e) *Types of System Testing* *(4 Marks)*

Answer

(a) Functions of Controller of Certifying Authorities under Section 18 of Information Technology (Amendment) Act, 2008:

Section 18 lays down the *functions which the Controller may perform* in respect of activities of Certifying Authorities. The Controller may perform all or any of the following functions, namely:

(i) exercising supervision over the activities of the Certifying Authorities;

(ii) certifying public keys of the Certifying Authorities;

(iii) laying down the standards to be maintained by the Certifying Authorities;

(iv) specifying the qualifications and experience which employees of the Certifying Authorities should possess;

(v) specifying the conditions subject to which the Certifying Authorities shall conduct their business;

(vi) specifying the content of written, printed or visual material and advertisements that may be distributed or used in respect of an Electronic Signature Certificate and the Public Key;

(vii) specifying the form and content of an Electronic Signature Certificate and the key;

(viii) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;

(ix) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;

(x) facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;

(xi) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;

(xii) resolving any conflict of interests between the Certifying Authorities and the subscribers;

(xiii) laying down the duties of the Certifying Authorities;

(xiv) maintaining a data-base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

(b) Systematic Risks: These are unavoidable risks; constant across majority of technologies and applications. For example, the probability of power outage is not dependent on the industry but is dependent on external factors. Systematic risks would remain, no matter what technology is used. Thus, efforts to seek technological solution to reduce systematic risks would essentially be unfruitful activity and needs to be avoided. Systematic risks can be reduced by designing management control process and does not involve technological solutions. For example, the solution to non-availability of consumable is maintaining a high stock of the same. Thus, a systematic risk can be mitigated not by technology but by management process. Hence, one would not make any additional payment for technological solution to the problem. To put in other words, there would not be any technology linked premium that one should pay trying to reduce the exposure to systematic risk.

Unsystematic Risks: These are the risks, which are peculiar to the specific applications or technology. One of the major characteristics of these risks would be that they can be generally mitigated by using an advanced technology or system. For example, one can use a computer system with automatic mirroring to reduce the exposure to loss arising out of data loss in the event of failure of host computer. Thus, by making additional investment one can mitigate these unsystematic risks.

(c) Goals of a Business Continuity Plan: Major goals of a business continuity plan should be to:

- identify weaknesses and implement a disaster prevention program;
- minimize the duration of a serious disruption to business operations;
- facilitate effective co-ordination of recovery tasks; and
- reduce the complexity of the recovery effort.

(d) Five Levels of Software Process Maturity: A maturity level is a well-defined evolutionary plateau toward achieving a mature software process. Each maturity level comprises a set of process goals that, when satisfied, stabilize an important component of the software process. Achieving each level of the maturity framework establishes a different component in the software process, resulting in an increase in the process capability of the organization.

Capability Maturity Model (CMM) provides a framework for organizing these evolutionary steps into five maturity levels that facilitates successive foundations for continuous process improvement. The levels also help an organization to prioritize its improvement efforts. These five levels are given as follows:

- Level 1 - The Initial Level: This is the starting point for use of a new or undocumented repeat process. It is characteristic of processes at this level that they are (typically) undocumented and in a state of dynamic change, tending to be driven in an adhoc, uncontrolled and reactive manner by users or events. This provides a chaotic or unstable environment for the processes.
- Level 2 - The Repeatable Level: At this level, some processes are repeatable, possibly with consistent results. Process discipline is unlikely to be rigorous, but where it exists it may help to ensure that existing processes are maintained during times of stress.
- Level 3 - The Defined Level: At this level, there are sets of defined and documented standard processes established and subject to some degree of improvement over time. These standard processes are in place (i.e., they are the AS-IS processes) and used to establish consistency of process performance across the organization.
- Level 4 - The Managed Level: At this level, using process metrics, management can effectively control the AS-IS process (e.g., for software development). In particular, management can identify ways to adjust and adapt the process to particular projects without measurable losses of quality or deviations from specifications. Process Capability is established from this level.
- Level 5 - The Optimizing Level: At this level, the focus is on continually improving process performance through both incremental and innovative technological changes/improvements.

(e) Types of System Testing: System testing is a process in which software and other system elements are tested as a whole. Major types of system testing that might be carried out, are given as follows:

- Recovery Testing: This is the activity of testing 'how well the application is able to recover from crashes, hardware failures and other similar problems'. Recovery testing is the forced failure of the software in a variety of ways to verify that recovery is properly performed.
- Security Testing: This is the process to determine that an Information System protects data and maintains functionality as intended or not. The six basic security concepts that need to be covered by security testing are – confidentiality, integrity, availability, authentication, authorization and non-repudiation. This testing technique also ensures the existence and proper execution of access controls in the new system.
- Stress or Volume Testing: Stress testing is a form of testing that is used to determine the stability of a given system or entity. It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results.

Stress testing may be performed by testing the application with large quantity of data during peak hours to test its performance.

- Performance Testing: Software performance testing is used to determine the speed or effectiveness of a computer, network, software program or device. This testing technique compares the new system's performance with that of similar systems using well defined benchmarks.