DISCLAIMER

The Suggested Answers hosted on 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 any way 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

ABC is a leading company in the manufacturing of food items. The company is in the process of automation of its various business processes. During this phase, technical consultant of the company has highlighted the importance of information security and has suggested to introduce it right from the beginning. He has also suggested to perform the risk assessment activity and accordingly, to mitigate the assessed risk. For carrying out all these suggestions, various best practices have been followed by the company. In addition, after each activity, appropriate standards' compliances have been tested to check the quality of each process. Various policies related with business continuity planning and disaster recovery planning have been implemented to ensure three major expectations from the software, namely, resist, tolerate and recover.

Read the above carefully and answer the following:

(a) What are the major suggestions given by the technical consultant? How the company is implementing these suggestions? (5 Marks)

(b) Discuss risk assessment with the help of risk analysis framework in brief. (5 Marks)

(c) Out of various types of plans used in business continuity planning, discuss recovery plan in brief. (5 Marks)

(d) What should be the major components of a good information security policy, as per your opinion? (5 Marks)

Answer

(a) During the automation of various processes of ABC Company, the technical consultant of the company has given the following major suggestions:

- By realizing the importance of information security, he suggested to introduce it *right from the beginning*.
- In addition, he also suggested to perform the risk assessment activity.
- Finally, he advised to mitigate the assessed risk.

For the implementation of all the above mentioned suggestions, the company took the following steps:

- The company followed various best practices for each process for the proper implementation of the suggestions.
- In addition, the company also tested the compliance of appropriate standards' after each activity, to check the quality of each process.

- Further, the company also implemented the policies related to business continuity planning and disaster recovery to ensure three broad expectations from the software: resist, tolerate and recover.

(b) 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.

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.

A risk analysis can provide an effective approach that will serve as the foundation for avoiding the disasters. Through risk analysis, it is possible to identify, assess, and then mitigate the risk. Such an analysis entails the development of a clear summary of the current situation and a systematic plan for risk identification, characterization, and mitigation.

The framework of risk analysis is given as follows:

(c) Recovery Plan: The backup plan is intended to restore operations quickly so that the information system function can continue to service an organization, whereas, *recovery plans set out procedures to restore full information system capabilities.* Recovery plans should identify a recovery committee that will be responsible for working out the specification of the recovery to be undertaken.

The plan should specify the responsibilities of the committee and provide guidelines on priorities to be followed. The plan might also indicate '*which applications are to be recovered first*'. Members of a recovery committee must understand their responsibilities.

Here, there is a major issue that they will be required to undertake unfamiliar tasks. Periodically, they must review and practice for executing their responsibilities so that they are prepared for a disaster. If committee members leave the organization, new members must be appointed immediately and briefed about their responsibilities.

(d) A good Information Security Policy should clearly state the following:

- 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 (BCP),
- Legal compliances,
- Monitoring and auditing requirements, and
- Underlying technical policy.

Question 2

(a) What do you understand by unauthorized intrusion? What is hacking and what damage can a hacker do ? (6 Marks)

(b) What are the guidelines to be followed before starting the implementation of an ERP package? (6 Marks)

(c) Describe the power to make rules by Central Government in respect of Electronic Signature under Section 10 of Information Technology (Amended) Act 2008. (4 Marks)

Answer

(a) Unauthorized Intrusion: Intrusion detection is an attempt to monitor and possibly prevent the attempts to intrude into or otherwise compromise the system and network resources of an organization. The computer systems of an organization are

attached to a network, and also to the internet. The organization would allow access to that computer system from the network, by authorized people, for acceptable reasons.

For example; if there is a web server, attached to the internet, only clients, staff, and potential clients, are allowed to access the web pages stored on that web server. It does not allow unauthorized access to the system by anyone, be that staff, customers, or unknown third parties. For example, it does not want people (other than the web designers that the company has employed) to be able to change the web pages on that computer. Typically, a firewall or authentication system of some kind will be employed to prevent unauthorized access.

Hacking: Hacking is an act of penetrating computer systems to gain knowledge about the system and how it works. Technically, a hacker is someone, who is enthusiastic about computer programming and all things relating to the technical workings of a computer.

There are many ways in which a hacker can hack. Some of them are given as follows:

- NetBIOS,
- ICMP Ping,
- FTP ,
- rpc.statd, and
- HTTP.

What damage can a Hacker do?

This depends upon 'what backdoor program(s) are hiding on the PC'. Different programs can do different amounts of damage. However, most of them allow a hacker to smuggle another program onto our PC. This means that if a hacker can't do something using the backdoor program, s/he can easily put something else onto the computer.

Hackers can see everything we are doing, and can access any file on the disk. Hackers can write new files, delete files, edit files, and do practically anything to a file that could be done to a file. A hacker can install several programs on to the system without our knowledge. Such programs can also be used to steal personal information such as passwords and credit card information.

(b) There are certain general guidelines, which are to be followed before starting the implementation of an ERP package. These are given as follows:

- Understanding the corporate needs and culture of the organization and then adopting 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 minimal customization;
- Training end users; and
- Adapting the new system and making the required changes in the working environment to make an effective use of the system in future.

(c) [Section 10] Power to make rules by Central Government in respect of Electronic Signature (Modified Vide ITAA 2008):

The Central Government may, for the purposes of this Act, by rules, prescribe

(a) the type of Electronic Signature;

(b) the manner and format in which the Electronic Signature shall be affixed;

(c) the manner or procedure which facilitates identification of the person affixing the Electronic Signature;

(d) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(e) any other matter which is necessary to give legal effect to Electronic Signature.

Question 3

(a) What are the tangible and intangible benefits that can result from the development of a computerized system? *(6 Marks)*

(b) What is Decision Support System? Discuss its characteristics in brief. *(6 Marks)*

(c) What are the major activities involved in the design of a database? *(4 Marks)*

Answer

(a) The benefits, which result from developing new or improved information systems that utilize computers can be subdivided into tangible and intangible benefits. Tangible benefits are those that can be accurately measured and are directly related to the introduction of a new system, such as decrease in data processing cost. Intangible benefits such as improved business image are harder to measure and define. Both these aforementioned benefits that can result from the development of a computerized system are summarized below:

(i) Increase in sales or profit (improvement in product or service quality);

(ii) Decrease in data processing costs (elimination of unnecessary procedures and documents);

(iii) Decrease in operating costs (reduction in inventory carrying costs);

(iv) Decrease in required investment (decrease in inventory investment required);

(v) Increased operational ability and efficiency (improvement in production ability and efficiency);

(vi) New or improved information availability (more timely and accurate information and new types and forms of information);

(vii) Improved abilities in computation and analysis;

(viii) Improved customer service (more timely service);

(ix) Improved employee morale (elimination of burdensome and boring job tasks);

(x) Improved management decision-making (better information and decision analysis);

(xi) Improved competitive position (faster and better response to actions of competitors); and

(xii) Improved business and community image (progressive image as perceived by customers, investors etc.).

(b) A Decision Support System (DSS) can be defined as a system providing tools to the decision making managers to address unstructured/ partially structured problems in their own personalized manner. It empowers the managers with a set of capabilities that enable them to generate the information required by them in decision making process. A DSS does not require any high technology. It is considered as more flexible and adaptable for changing decision making requirements than traditional Management reporting system.

There are three major characteristics of a Decision Support System, namely:

(i) Semistructured or unstructured decision-making;

(ii) Adaptable to the changing needs of decision makers; and

(iii) Ease of learning and use.

Each of these characteristics is briefly discussed below:

(i) *Semistructured and Unstructured Decisions*: Unstructured decisions and semistructured decisions are made when information obtained from a computer system is only a portion of the total knowledge needed to make the decision. DSS is well adapted to help with semistructured and unstructured decisions. A well-designed DSS helps in decision making process with the depth to which the available data can be tapped for useful information.

(ii) *Ability to adapt to changing needs*: Semistructured and unstructured decisions often do not conform to a predefined set of decision-making rules. DSS provides flexibility to enable users to model their own information needs. Rather than locking the system into rigid information producing requirements, capabilities and tools are provided by DSS to enable users to meet their own output needs.

(iii) *Ease of Learning and Use*: DSS software tools employ user-oriented interfaces such as grids, graphics, non-procedural fourth – generation languages (4GL), natural English, and easily read documentation. These interfaces make it easier for users to conceptualize and perform the decision-making process.

(c) The designing of a database involves four major activities, which are given as follows:

- Conceptual Modeling: These describe the application domain via entities/objects, attributes of these entities/objects and static and dynamic constraints on these entities/objects, their attributes, and their relationships.
- Data Modeling: Conceptual Models need to be translated into data models so that they can be accessed and manipulated by both high-level and low-level programming languages.
- Storage Structure Design: Decisions must be made on how to linearize and partition the data structure so that it can be stored on some device. For example-tuples (row) in a relational data model must be assigned to records, and relationships among records might be established via symbolic pointer addresses.
- Physical Layout Design: Decisions must be made on how to distribute the storage structure across specific storage media and locations –for example, the cylinders, tracks, and sectors on a disk and the computers in a LAN or WAN.

Question 4

(a) What is IT Infrastructure Library? Discuss the configuration management under ITIL framework. (6 Marks)

(b) List any six ERP vendors and describe the ERP packages offered by them. (6 Marks)

(c) Discuss the parameters that would help in planning a documentation process of IS audit. (4 Marks)

Answer

(a) ITIL (IT Infrastructure Library): ITIL is a collection of books (standards); each covering a specific 'practice' within IT management. After the initial published works, the number of publications quickly grew (within ITIL v1) to over 30 books. In order to make ITIL more accessible (and affordable) to those wishing to explore it, one of the aims of the ITIL v2 project was to consolidate the works into a number of logical 'sets' that aimed to group related sets of process guidelines for different aspects of the management of Information Technology systems, applications and services together.

The eight ITIL books and their disciplines are:

The IT Service Management sets relating to:

1. Service Delivery
2. Service Support

Other operational guidance relating to:

3. ICT Infrastructure Management
4. Security Management
5. The Business Perspective
6. Application Management
7. Software Asset Management
8. Planning to Implement Service Management

Configuration Management: It is a process that tracks all of the individual Configuration Items (CI) in a system. A system may be as simple as a single server, or as complex as the entire IT department. Configuration Management includes:

- Creating a parts' list of every CI (hardware or software) in the system;
- Defining the relationship of CIs in the system;
- Tracking of the status of each CI, both its current status and its history;
- Tracking all Requests for Change to the system; and
- Verifying and ensuring that the CI parts list is complete and correct.

There are five basic activities in configuration management:

- Planning,
- Identification,
- Control,
- Status accounting, and
- Verification and Audit.

(b) There are quite a few ERP packages available in the market these days. Out of these, most popular six ERP packages along with the vendors are listed below:

Vendor	Brief Description of ERP Package offered
Baan Corporation	Baan: Initially developed for an aircraft company, it was subsequently launched as a generalized package in 1994. It offers sound technology and coverage of broad functional scope.

Oracle	Oracle ERP Solutions: It gives Internet-enabled, network-centric computing. It also offers database, tools, implementation, applications and UNIX operating systems under one stop-shop umbrella. It is currently running on wide choice of hardware.
Marcam Corporation	Prism: Prism is a specialist process manufacturing solution for the AS/400. Its production model, which is similar to a flowchart, handles process industry problems elegantly. Although out dated, it does the job.
SAP	SAP R/3: It is a market leader with excellent philosophy of matching business processes with its modules. It covers almost all business segments.
JBA	JBA System 21: Its software license revenues are small compared to other major ERP vendors. It offers a rugged, reliable manufacturing solution.
Microsoft	Axapta (AX) and Navision (NAV): Microsoft Dynamics AX is an adaptable business management solution to streamline the business practices. Microsoft Dynamics NAV is basically designed for small and medium size companies. It is a cost effective solution that can be customized for organizations.

(c) The following three parameters would help in planning a documentation process of IS Audit:

(i) The importance of planning and understanding the planning process requires identifying three planning questions:

- *Knowing Your Resources*: The three basic resources are: time, people, money. One has to check for their availability and affordability.
- *Defining the Scope and Audience*: The same report may undergo significant changes depending on the character of the report and nature of the audience. Presentation on Balance Sheet made to bankers and to investors would be quite different in content and focus.
- *Using a Scope Definition Report*: It is critical to know how to complete a Scope Definition Report. This report helps in developing a workable schedule for completing the project.

(ii) The Documentation Writer: The qualities and skills that the documentation writer would need. The requirement may often be legal in nature.

(iii) Rules to guide documentation writing: The four steps of writing documentation namely, writing in active voice, giving the consequences, writing from general to specific, consistency and writing online documentation.

Question 5

(a) *What is a Virus? What policy and procedure controls can be recommended for ensuring control over virus proliferation and damage?* *(6 Marks)*

(b) *How is the term 'Electronic Record' defined in IT (Amended) Act 2008? What is the provision given in the IT Act for the retention of Electronic Records?* *(6 Marks)*

(c) *Discuss the constraints in operating a MIS.* *(4 Marks)*

Answer

(a) Virus: A virus is a program (usually destructive) that attaches itself to a legitimate program to penetrate the operating system. The virus destroys application programs, data files, and operating systems in a number of ways. One common technique for the virus is to simply replicate itself over and over within the main memory, thus destroying whatever data or programs are resident. One of the most insidious aspects of a virus is its ability to spread throughout the system and to other systems before perpetrating its destructive acts.

The policy and procedural controls that can be recommended for ensuring control over virus proliferation and damage are given as follows:

- The Security Policy should address the virus threats, systems vulnerabilities and controls. A separate section on anti-virus is appropriate to address the various degrees of risks and suitable controls thereof.
- Anti-virus awareness and training on symptoms of attacks, methods of reducing damage, cleaning and quarantining should be given to all employees.
- Hardware installations and associated computing devices should be periodically verified for parameter settings.
- As a part of SDLC Controls, the development area should be free of viruses and sufficient safeguards must be in place to secure the area from viruses.
- Provision of drives to read media should be restricted to certain controlled terminals and should be write-protected.
- Network access to the Internet should be restricted preferably to stand-alone computers.
- Networks should be protected by means of firewalls that can prevent entry of known viruses.
- The servers and all terminals must have rated anti-virus software installed with sufficient number of user licenses.
- Procedures should ensure that systematic updates are applied to all anti-virus installations at frequent intervals.

- External media such as disks, CDs, tapes need to be avoided. If necessary such media should be scanned on a stand-alone machine and certified by the department.
- Vendors and consultants should not be allowed to run their demonstrations and presentations on organizational systems.
- All new software acquisitions should follow a controlled procedure of centralized acquisition and testing for viruses.
- Patches to operating systems and other software and upgrades thereof should be acquired from authentic sources and scanned before installation.
- Reporting and incident handling procedures should be in place to suitably handle virus incidents and eradicate them at the earliest.
- An effective backup plan must be implemented and monitored to ensure that back-up media is not infected and preferably encrypted. Only new media must be used for back-up purposes.

(b) "Electronic Record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.

[Section 7] Retention of Electronic Records:

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

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

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

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

However,

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

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

(c) Major constraints, which come in the way of operating a MIS are given as follows:

- Non-availability of experts, who can diagnose the objectives of the organization and provide a desired direction for installing and operating a system. This problem may be overcome by grooming internal staff, which should be preceded by proper selection and training.
- Experts usually face the problem of selecting the sub-system of MIS to be installed and operated upon. The criteria, which should guide the experts, depending upon the need and importance of a function for which MIS can be installed first.
- Due to varied objectives of business concerns, the approach adopted by experts for designing and implementing MIS is a non-standardized one.
- Non-availability of cooperation from staff is a crucial problem, which should be handled tactfully. This task should be carried out by organizing lecturers, showing films and also explaining to them the utility of the system. Besides this, some persons should also be involved in the development and implementation of the system.

Question 6

(a) The unique nature of each LAN makes it difficult to define standard testing procedures to effectively perform a review. So, what information a Reviewer / IS Auditor should identify and understand prior to commencing a LAN review? (6 Marks)

(b) As an IS Auditor, what are the steps to be followed by you while conducting IT auditing? (6 Marks)

(c) What are the two types of Service Auditor's Reports under SAS 70? Describe the contents of each type of report. (4 Marks)

Answer

(a) The unique nature of each LAN makes it difficult to define standard testing procedures to effectively perform a review. The reviewer/IS Auditor should identify the following prior to commencing a LAN review:

- LAN topology and network design;
- Significant LAN components (such as servers and modems);
- Network topology (including internal LAN configuration as well as interconnections to other LANs, WANs or public networks);
- LAN uses, including significant traffic types and main applications used over the network;
- LAN administrator; and
- Significant groups of LAN users.

In addition, the reviewer should gain an understanding of the following:

- Functions performed by the LAN Administrator;
- The company's division or department procedures and standards relating to network design support, naming conventions and data security; and
- LAN transmission media and techniques, including bridges, routers and gateways.

Understanding the above information should enable the reviewer to make an assessment of the significant threats to the LAN, together with the potential impact and probability of occurrence of each threat. Having assessed the risks to the LAN, the reviewer should evaluate the controls used to minimize the risks.

(b) Steps in Information Technology Audit: Different audit organizations go about IT auditing in different ways and individual auditors have their own favourite ways of working. However, it can be categorized into six major stages:

(i) *Scoping and pre-audit survey*: Auditors determine the main area/s of focus and any areas that are explicitly out-of-scope, based normally on some form of risk-based assessment. Information sources at this stage include background reading and web browsing, previous audit reports, pre audit interview, observations and, sometimes, subjective impressions that simply deserve further investigation.

(ii) *Planning and preparation:* During this stage, the scope is broken down into greater levels of detail, usually involving the generation of an audit work plan or risk-control-matrix.

(iii) *Fieldwork:* It is related to gathering the evidence by interviewing staff and managers, reviewing documents, printouts and data, observing processes etc.

(iv) *Analysis*: This step involves desperately sorting out, reviewing and trying to make sense of all that evidence gathered earlier. SWOT (Strengths, Weaknesses, Opportunities, and Threats) or PEST (Political, Economic, Social, Technological) techniques can be used for analysis.

(v) *Reporting:* Reporting to the management is done after analysis of data gathered and analysis.

(vi) *Closure*: Closure involves preparing notes for future audits and following up management to complete the actions they promised after previous audits.

(c) Service Auditor's Report under SAS 70: The most effective ways a service organization can communicate information about its controls is through a service Auditor's Report.

There are two types of Service Auditor's Report: Type I and Type II.

A Type I report describes the service organizations description of controls at a specific point in time (e.g. June 30, 2011). A type II report not only includes the service organization description of controls, but also includes detailed testing of the service

organization's controls over a minimum six month period (e.g. January 1, 2011 to June 30, 2011). The contents of each type of report are described in the following table:

S. No.	Report Contents	Type I Report	Type II Report
1.	Independent service auditor's report (i.e. opinion)	Included	Included
2.	Service organization's description of controls	Included	Included
3.	Information provided by the independent service auditor; includes a description of the service auditor's tests of operating effectiveness and the results of those tests.	Optional	Included
4.	Other information provided by the service organization (e.g. glossary of terms)	Optional	Optional

In a Type I report, the service auditor will express an opinion on (1) whether the service organization's description of its controls presents fairly, in all material respects, the relevant aspects of the service organizations controls that had been placed in operation as of a specific data and (2) whether the controls were suitably designed to achieve specified control objectives.

In a type II report, the service auditor will express an opinion on the same items noted above in a type I report, and (3) whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period specified.

Question 7

Write short notes on any four of the following:

(a) Data Dictionary *(4 Marks)*

(b) Risk Mitigation Measures *(4 Marks)*

(c) Software Process Maturity *(4 Marks)*

(d) Preventative and Restorative Information Protection *(4 Marks)*

(e) Objectives of Information Technology Act 2000 *(4 Marks)*

Answer

(a) Data Dictionary: A data dictionary is a computer file that contains descriptive information about the data items in the files of a business information system. Thus, a data dictionary is a computer file about data. Each computer record of a data dictionary contains

information about a single data item used in a business information system. This information may include:

- Codes describing the data item's length (in characters), data type (alphabetic, numeric, alphanumeric, etc.), and range (e.g., values from 1 to 99 for a department code)
- The identity of the source document(s) used to create the data item.
- The names of the computer files that store the data item.
- The names of the computer programs that modify the data item.
- The identity of the computer programs or individuals permitted to access the data item for the purpose of file maintenance, upkeep, or inquiry.
- The identity of the computer programs or individuals not permitted to access the data item.

(b) Risk Mitigation Measures: In risk mitigation, there is a term called, Cause analysis, which identifies events and their impact on losses. Cause models help in the implementation of risk mitigation measures. In addition to establishing causal relationship, other risk mitigation measures are:

- Self assessment;
- Calculating reserves and capital requirements;
- Creating culture supportive of risk mitigation;
- Strengthening internal controls, including internal and external audit of systems, processes and controls, including IS audit and assurance);
- Setting up operational risks limits (so business will have to reduce one or more of frequency of loss, severity of loss or size of operations);
- Setting up independent operational risk management departments;
- Establishing a disaster recovery plan and backup systems;
- Insurance; and
- Outsourcing operations with strict service level agreements so that operational risk is transferred.

Out of these afore mentioned measures, generally the following common mitigation techniques are used:

- 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.
- Service Level Agreements: Some of risks can be mitigated by designing the service level agreement. This may be entered into 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.

  Here, it is noteworthy that the organization should not be so obsessed with mitigating the risk that it seeks to reduce the systematic risk - the risk of being in business. The risk mitigation tools available should not eat so much into the economics of business that the organization may find itself in a position where it is not earning adequate against the efforts and investments made.

(c) Software Process Maturity: This is the extent to which a specific process is explicitly defined, managed, measured, controlled, and effective. Maturity implies a potential for growth in capability and indicates both the richness of an organization's software process and the consistency with which it is applied in projects throughout the organization.

As a software organization gains in software process maturity, it institutionalizes its software process via policies, standards, and organizational structures. Institutionalization entails building an infrastructure and a corporate culture that supports the methods, practices, and procedures of the business so that they endure after those who originally defined them have gone.

(d) Preventative Information Protection: It is based on the use of security controls, which itself is a group of three types of controls such as Physical, Logical, and Administrative. Theses are briefly given as follows:

- Physical controls deal with Doors, Locks, Guards, Floppy Disk Access Locks, Cables locking systems to desks/walls, CCTV, Paper Shredders, Fire Suppression Systems,
- Logical controls deal with Passwords, File Permissions, Access Control Lists, Account Privileges, Power Protection Systems, and
- Administrative controls deal with Security Awareness, User Account Revocation, and Policy.

Restorative Information Protection: If an organization cannot recover or recreate critical information systems in an acceptable time period, the organization will suffer and possibly have to go out of business. Hence, the key requirement of any restorative information system protection plan is that the information systems can be recovered. The

claim of back program to backup data automatically cannot be reliable. It has so many problems. The restorative information protection program must address the following:

- Whether the recovery process has been evaluated and tested recently?
- The time taken for restoration,
- The quantum of productivity loss,
- The strict adherence of plan, and
- The time needed to input the data changes since the last backup.

(e) Objectives of Information Technology Act 2000: The objectives of Information Technology Act 2000 are given as follows:

- To grant legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication commonly referred to as "electronic commerce" in place of paper based methods of communication;
- To give legal recognition to Digital signatures for authentication of any information or matter, which requires authentication under any law;
- To facilitate electronic filing of documents with Government departments;
- To facilitate electronic storage of data;
- To facilitate and give legal sanction to electronic fund transfers between banks and financial institutions;
- To give legal recognition for keeping of books of accounts by banker's in electronic form; and
- To amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934.