

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

QUESTIONS

Information Systems Concepts

1. (a) What do you mean by a Transaction Processing System (TPS)? Explain important features of a TPS.
(b) Discuss major misconceptions about MIS in brief.
2. There is a practical set of principles to guide the design of measures and indicators to be included in an EIS. Describe these principles in brief.

Software Development Life Cycle Methodology

3. What is agile methodology? Explain its basic principles in brief.
4. (a) Discuss the major aspects, which are required to be kept in mind while eliciting information to delineate the scope during SDLC.
(b) What do you understand by Operational Feasibility? Describe the questions, which help in testing the operational feasibility of a project.
5. (a) Discuss Black Box, White Box and Gray Box testing in brief.
(b) Describe major characteristics of a good coded program.

Control Objectives

6. (a) What are the controls that are required to be in place in case of acquisition of a software system?
(b) Describe auditor's role in authorization controls.
7. Discuss Application Level Firewalls along with its primary disadvantages.
8. (a) What is hacking? Explain the ways, which can be used by a hacker for hacking.
(b) What do you understand by Corrective Controls? Discuss with the help of examples. Also explain the main characteristics of these controls.

Testing – General and Automated Controls

9. (a) Discuss major advantages of continuous auditing techniques.
(b) During the review of hardware, what are the tasks, which should be accomplished by a reviewer to evaluate the adequacy and the timeliness of preventive maintenance?

Risk Assessment Methodologies and Applications

10. (a) Discuss major threats due to cyber crimes.
(b) Describe Delphi approach of risk evaluation in brief.

Business Continuity Planning and Disaster Recovery Planning

11. (a) Explain the tasks to be undertaken in 'Vulnerability assessment and definition of requirement' phase of a Business Continuity Plan.
- (b) Discuss various back-up techniques in brief.

An Overview of Enterprise Resource Planning (ERP)

12. (a) An ERP system is not only the integration of various organization processes. Any system has to possess few key characteristics to qualify for a true ERP solution. Discuss these characteristics.
- (b) Discuss various steps involved in the implementation of a typical ERP Package.

Information Systems Auditing Standards, Guidelines, Best Practices

13. What are various phases of Information Security Management System (ISMS)? Explain the major activities of the first phase of ISMS.
14. Describe various categories of enablers under COBIT 5.

Drafting of IS Security Policy, Audit Policy, IS Audit Reporting- A Practical Perspective

15. What should be the components of a good Information Security Policy in your opinion? Explain in brief.
16. What are the major points that are required to be taken into consideration for the proper implementation of Physical and Environmental Security with reference to Information Security Policy?

Information Technology (Amendment) Act 2008

17. (a) Discuss the 'Powers to make rules by Central Government in respect of Electronic Signature' under Section 10 of Information Technology (Amendment) Act 2008.
- (b) Describe 'Secure Electronic Signature' in the light of Section 15 of Information Technology (Amendment) Act, 2008.
18. Discuss the 'Acceptance of Digital Signature Certificate' under Section 41 of Information Technology (Amendment) Act, 2008.

Questions based on Short Notes

19. Write short notes on the following:
 - (a) Weaknesses of Spiral Model
 - (b) Data Dictionary
 - (c) Cryptosystem
20. Write short notes on the following:
 - (a) Test Plan
 - (b) Cold Site and Hot Site

- (c) Final Acceptance Testing
- 21. Write short notes on the following:
 - (a) Benefits of COBIT 5
 - (b) Level 1- Initial Level of CMM
 - (c) Power of Controller to give directions in the light of Section 68 of Information Technology (Amendment) Act, 2008

Questions based on the Case Studies

22. At one point of time, the term 'Software Development' was used in a very limited scope and it was only relating to a programmer, writing code to solve a problem or automate a procedure of a business process. Contrary to this, in the current scenario, systems are so wide and complex that teams of architects, analysts, programmers, testers and users must work together to create the millions of lines of custom-written code that drive our enterprises. To manage all these activities, a number of System Development Life Cycle (SDLC) models have been created: waterfall; spiral, prototyping, RAD and Agile etc. The oldest of these, and the best known, is the waterfall: a sequence of stages in which the output of each stage becomes the input for the next. These stages can be characterized and divided into different ways, known as various phases of the SDLC.

Read the above carefully and answer the following:

- (a) What is SDLC? Explain the advantages of SDLC from the perspective of the IS Audit.
 - (b) Along with several strengths, there are some weaknesses also in case of Waterfall Model. Explain those weaknesses in brief.
 - (c) How accountants can be involved in the development work? Give your opinion.
23. ABC Ltd. is a company engaged in the business of manufacturing and supplying of various automobile parts. The company has implemented an information system for the proper management of its various processes and sub-processes. The company is eager to improve its day-to-day operating efficiency and assurance that its data remains available in case of a disaster. To achieve these objectives, the company asked its technical consultant to develop a disaster recovery strategy that would keep the business functional when a major disruption occurs. To meet this challenge, the company needed to upgrade its legacy primary storage, add additional storage resources at its disaster recovery locations so that storage-to-storage replication may be utilized, and also to upgrade to the latest version of the related software. The technical consultant suggested that the company must need the assistance for integrating a range of technologies in addition to the plan for the appropriate storage capacity.

Read the above carefully and answer the following:

- (a) What are the different phases of the methodology for developing a Business Continuity Plan?

- (b) What should be the major backup tips to be followed by the company in your opinion?
 - (c) Explain the goals of a business continuity plan in brief.
24. PQR Enterprises is engaged in a business of manufacturing of electronic products. The company is in the process of automation of its various business processes. During this automation, technical consultant of the company suggested to perform the risk assessment activity and accordingly, to mitigate the assessed risks. Basically, risk assessment seeks to identify 'which business processes and related resources are critical to the business', 'what threats or exposures exists, that can cause an unplanned interruption of business processes', and 'what costs accrue due to an interruption'. There are various analytical procedures that are used to determine various risks, threats, and exposures, faced by an organization. These are known as Business Impact Analysis (BIA), Risk Impact Analysis (RIA) and so on.

Read the above carefully and answer the following:

- (a) Define Systematic Risks and Unsystematic Risks with the help of examples.
 - (b) There are various techniques that are available to assess and evaluate risks, namely, Judgment and Intuition, Delphi Approach, Scoring, Qualitative Techniques, and Quantitative Techniques. Explain Scoring and Quantitative approaches in brief.
 - (c) In automation of the business modules, retention of electronic records is an important activity. How Information Technology (Amendment) Act 2008 addresses this issue with reference to its Section 7?
25. ABC Technologies is a leading company in the BPO sector. Its most of the business processes are automated. The company is relying on Information Technology for information and transaction processing. The growth of E-commerce supported by the growth of the Internet has completely revolutionized and reengineered business processes. The company's new business models and new methods presume that the information required by the business managers is available all the time; it is accurate, it is reliable and no unauthorized disclosure of the same is made. Further, it is also presumed that the virtual business organization is up and running all the time on 24×7 basis. However, in reality, the technology-enabled and technology-dependent organizations are more vulnerable to security threats than ever before.

Read the above carefully and answer the following:

- (a) Discuss the major security objectives of an organization.
- (b) There are certain basic ground rules that must be addressed sequentially, prior to know the details of 'how to protect the information systems'. Explain those rules in brief.
- (c) Briefly explain the tasks that are to be performed during the post-implementation period of an ERP package.

SUGGESTED ANSWERS / HINTS

1. (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 transactions and these transactions are to be organized and manipulated to generate various information products for external use. Transaction processing system records and manipulates transaction data into usable information.

Some of the important features of a TPS are given as follows:

- **Large volume of data:** As TPS is transaction – oriented, it generally consists of 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 the 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) Major misconceptions about MIS are given as follows:

- The study of MIS is about the use of computers. This statement is not true. MIS may or may not be computer based; computer is just a tool, like any other machine. Installing a MIS depends largely on several factors such as – how critical is the response time required for getting an information; how big is the organization; and how complex are the needs of the information processing.
- More data in reports means more information for managers. This is a misapprehension. It is not the quantity of data, but its relevance, which is

important to the managers in process of decision-making. Data provided in reports should meet the information requirements of managers. It is the form of data and its manner of presentation that is having an importance to business managers. Unorganized mass of data creates confusion.

- Accuracy in reporting is of vital importance. The popular belief is that accuracy in reporting should be of high order. At the operating level, it is true. Other examples, where accuracy is really important, can be the dispensing of medicine; the control of aircraft; the design of a bridge etc. Accuracy, however, is a relevant but not an absolute ideal. Higher levels of accuracy involve higher cost. At higher decision levels, great accuracy may not be required. The degree of accuracy is closely related to the decision problem. Higher management is concerned with broad decisions on principles and objectives. A fairly correct presentation of relevant data often is adequate for top management decisions. For a decision on a new project proposal, top management is not interested in knowing the project cost in precise rupee terms. A project cost estimated at a fairly correct figure is all what it wants.
2. A practical set of principles to guide the design of measures and indicators to be included in an EIS is given as follows:
- EIS measures must be easy to understand and collect. Wherever possible, data should be collected naturally as part of the process of work. An EIS should not add substantially to the workload of managers or staff.
 - EIS measures must be based on a balanced view of the organization's objective. Data in the system should reflect the objectives of the organization in the areas of productivity, resource management, quality and customer service.
 - Performance indicators in an EIS must reflect everyone's contribution in a fair and consistent manner. Indicators should be as independent as possible from variables outside the control of managers.
 - EIS measures must encourage management and staff to share ownership of the organization's objectives. Performance indicators must promote both team-work and friendly competition. Measures will be meaningful for all staff; people must feel that they, as individuals, can contribute to improving the performance of the organization.
 - EIS information must be available to everyone in the organization. The objective is to provide everyone with useful information about the organization's performance. Information that must remain confidential should not be part of the EIS or the management system of the organization.
 - EIS measures must evolve to meet the changing needs of the organization.

3. **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.

Basic principles of agile methodology are given as follows:

- Customer satisfaction by rapid delivery of useful software;
 - Welcomes changing requirements, even late in development;
 - Working software is delivered frequently (weeks rather than months);
 - Working software is the principal measure of progress;
 - Sustainable development, able to maintain a constant pace;
 - Close, daily co-operation between business people and developers;
 - Face-to-face conversation is the best form of communication (co-location);
 - Projects are built around motivated individuals, who should be trusted;
 - Continuous attention to technical excellence and good design;
 - Simplicity;
 - Self-organizing teams; and
 - Regular adaptation to changing circumstances.
4. (a) Major aspects, which are required to be kept in mind while eliciting information to delineate the scope during SDLC are given as follows:
- Different users will represent the problem and required solution in different ways. The system developer should elicit the need from the initiator of the project alternately called champion or executive sponsor of the project, addressing his/her concerns should be the basis of the scope.
 - While the initiator of the project may be a member of the senior management, the actual users may be from the operating levels in an organization. An understanding of their profile helps in designing appropriate user interface features.
 - While presenting the proposed solution for a problem, the development organization has to clearly quantify the economic benefits to the user organization. The information required has to be gathered at this stage. For example - when a system is proposed for Road tax collection, data on the

extent of collection and defaults is required to quantify benefits that will result to the Transport Department.

- It is also necessary to understand the impact of the solution on the organization- its structure, roles and responsibilities. Solutions, which have a wide impact are likely to meet with greater resistance. ERP implementation in organizations is a classic example of change management requirement. Organizations that have not been able to handle this have had a very poor ERP implementation record, with disastrous consequences.
- While economic benefit is a critical consideration when deciding on a solution, there are several other factors that have to be given weight-age too. These factors have to be considered from the perspective of the user management and resolved. For example- in a security system, how foolproof it is, may be a critical a factor like the economic benefits that entail.

(b) Operational Feasibility: It is concerned with ascertaining the views of workers, employees, customers and suppliers about the use of computer facility. A system can be highly feasible in all respects except the operational and fails miserably because of human problems.

The important questions, which help in testing the operational feasibility of a project are given as follows:

- Is there sufficient support for the system from management and from users?
- Are current business methods acceptable to users?
- Have the users been involved in planning and development of the project?
- Will the proposed system cause harm? Will it produce poorer results in any respect or area? Will loss of control result in any areas? Will accessibility of information be lost?
- Will individual performance be poorer after implementation than before?

This analysis may involve a subjective assessment of the political and managerial environment in which the system will be implemented. In general, the greater the requirements for change in the user environment in which the system will be installed, the greater the risk of implementation failure will exist.

5. **(a) Black Box Testing:** Black Box Testing takes an external perspective of the test object to derive test cases. These tests can be functional or non-functional, though usually functional. The test designer selects valid and invalid inputs and determines the correct output. There is no knowledge of the test object's internal structure.



This method of test design is applicable to all levels of software testing: unit,

integration, functional testing, system and acceptance. The higher the level, hence the bigger and more complex the box, the more one is forced to use black box testing to simplify. While this method can uncover unimplemented parts of the specification, one cannot be sure that all existent paths are tested. If a module performs a function, which is not supposed to, the black box test does not identify it.

White Box Testing: White box testing uses an internal perspective of the system to design test cases based on internal structure. It requires programming skills to identify all paths through the software. The tester chooses test case inputs to exercise paths through the code and determines the appropriate outputs. Since, the tests are based on the actual implementation, if the implementation changes, the tests probably will need to change, too. It is applicable at the unit, integration and system levels of the testing process, it is typically applied to the unit. While it normally tests paths within a unit, it can also test paths between units during integration, and between subsystems during a system level test. After obtaining a clear picture of the internal workings of a product, tests can be conducted to ensure that the internal operation of the product conforms to specifications and all the internal components are adequately exercised.

Gray Box Testing: Gray box testing is a software testing technique that uses a combination of black box testing and white box testing. In gray box testing, the tester applies a limited number of test cases to the internal workings of the software under test. In the remaining part of the gray box testing, one takes a black box approach in applying inputs to the software under test and observing the outputs.

(b) Major characteristics of a good coded program are given as follows:

- **Reliability:** It refers to the consistence, which a program provides over a period of time. However, poor setting of parameters and hard coding of some data subsequently could result in the failure of a program after some time.
- **Robustness:** It refers to the process of taking into account all possible inputs and outputs of a program in case of least likely situations.
- **Accuracy:** It refers not only to 'what program is supposed to do', but should also take care of 'what it should not do'. The second part becomes more challenging for quality control personnel and auditors.
- **Efficiency:** It refers to the performance, which should not be unduly affected with the increase in input values.
- **Usability:** It refers to a user-friendly interface and easy-to-understand document required for any program.
- **Readability:** It refers to the ease of maintenance of program even in the absence of the program developer.

6. (a) The following are the major controls that are required to be in place in case of acquisition of a software system:
- Information and system requirements need to meet 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 to define the constraints or limitations for each alternative system from a technical as well as a 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:
 - o Stability of the supplier company,
 - o Volatility of system upgrades,
 - o Existing customer base,
 - o Supplier's ability to provide support,
 - o Cost-benefits of the hardware/software in support of the supplier application, and
 - o Customized modifications of the application software.
- (b) Auditor's role in authorization controls are given as follows:
- Transactions in an application system are manually authorized, the controls that ensure that no unauthorized modifications take place after authorization and prior to establishing input controls? Determine if the proper level of management is authorizing the transaction activity.
 - If transaction authorization is facilitated by logical access restrictions, select a sample of access rules applying to transaction input and update, and verify if the appropriate people have these capabilities.
 - Identify any allowable overrides or bypasses of data validation and edit checks (authorization, monitoring, etc.). Determine who can do the overrides and verify that they are in a management position that should have this authority.

Are all uses of the override features automatically logged so these actions can be subsequently analyzed for appropriateness?

- Implement specific procedures to handle urgent matter, such as logging all emergency changes that required deviations from standard procedures and having management review and approve them after the fact. Make sure there is as audit trail for all urgent matters.
- Review by IT management to monitor, and approve all changes to hardware, software, and personnel responsibilities.
- Review the assigned and authorized responsibilities to those involved in the change and monitor their work with adequate segregation of duties.

7. **Application-Level Firewalls:** Application-level firewalls perform application-level screening, typically including the filtering capabilities of packet filter firewalls with additional validation of the packet content based on the application. Application-level firewalls capture and compare packets to state information in the connection tables. Unlike a packet filter firewall, an application-level firewall continues to examine each packet after the initial connection is established for specific application or services such as telnet, FTP, HTTP, SMTP, etc. The application-level firewall can provide additional screening of the packet payload for commands, protocols, packet length, authorization, content, or invalid headers. Application level firewalls provide the strongest level of security, but are slower and require greater expertise to administer properly.

The primary disadvantages of application-level firewalls are given as follows:

- The time required to read and interpret each packet slows the network traffic. Traffic of certain types may have to be split off before the application-level firewall and passed through different access controls.
 - Any particular firewall may provide only limited support for new network applications and protocols. They also simply may allow traffic from those applications and protocols to go through the firewall.
8. (a) Hacking is an act of penetrating computer systems to gain knowledge about the system and how it works.

Some of the major ways, which can be used by a hacker for hacking are given as follows :

- **NetBIOS:** NetBIOS hackers are the worst kind, since they don't require us to have any hidden backdoor program running on the computer. This kind of hack exploits a bug in Windows 9x. NetBIOS is meant to be used on local area networks, so machines on that network can share information. Unfortunately, the bug is that NetBIOS can also be used across the Internet - so a hacker can access your machine remotely.

- **ICMP 'Ping' (Internet Control Message Protocol):** ICMP is one of the main protocols that make the Internet work. It stands for Internet Control Message Protocol. 'Ping' is one of the commands that can be sent to a computer using ICMP. Ordinarily, a computer would respond to this ping, telling the sender that the computer does exist. This is all pings are meant to do. Pings may seem harmless enough, but a large number of pings can make a Denial-of-Service attack, which overloads a computer. Also, hackers can use pings to see if a computer exists and does not have a firewall (firewalls can block pings). If a computer responds to a ping, then the hacker could launch a more serious form of attack against a computer.
 - **FTP (File Transfer Protocol):** FTP is a standard Internet protocol, standing for File Transfer Protocol. It can be used for file downloads from some websites. If you have a web page of your own, you may use FTP to upload it from your home computer to the web server. However, FTP can also be used by some hackers. FTP normally requires some form of authentication for access to private files, or for writing to files. FTP backdoor programs, such as-
 - Doly Trojan,
 - Fore, and
 - Blade Runner.simply turn the computer into an FTP server, without any authentication.
 - **RPC statd:** This is a problem specific to Linux and Unix. The problem is the infamous unchecked buffer overflow problem. This is where a fixed amount of memory is set aside for storage of data. If data is received that is larger than this buffer, the program should truncate the data or send back an error, or at least do something other than ignore the problem. Unfortunately, the data overflows the memory that has been allocated to it, and the data is written into parts of memory it shouldn't be in. This can cause crashes of various different kinds. However, a skilled hacker could write bits of program code into memory that may be executed to perform the hacker's evil deeds.
 - **HTTP –** HTTP stands for Hypertext Transfer Protocol. HTTP hacks can only be harmful if we are using Microsoft web server software, such as Personal Web Server. There is a bug in this software called an 'unchecked buffer overflow'. If a user makes a request for a file on the web server with a very long name, part of the request gets written into parts of memory that contain active program code. A malicious user could use this to run any program they want on the server.
- (b) **Corrective Controls:** Corrective controls are designed to reduce the impact or correct an error once it has been detected. Corrective controls may include the use of default dates on invoices where an operator has tried to enter the incorrect date.

A business continuity plan is considered to be a significant corrective control. Some of the examples of Corrective Controls are given as follows:

- Contingency planning,
- Backup procedure,
- Rerun procedures,
- Treatment procedures for a disease,
- Change input value to an application system, and
- Investigate budget variance and report violations.

Main characteristics of the corrective controls are given as follows:

- To minimize the impact of the threat;
- To identify the cause of the problem;
- To provide remedy for problems discovered by detective controls;
- To get feedback from preventive and detective controls;
- To correct error arising from a problem; and
- To modify the processing systems to minimize future occurrences of the problem.

9. (a) Major advantages of continuous auditing techniques are given as follows:

- **Timely, comprehensive and detailed auditing:** Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analysed rather than examining the inputs and the outputs only.
- **Surprise test capability:** As evidences are collected from the system itself by using continuous audit techniques, auditors can gather evidence without the systems staff and application system users being aware that evidence is being collected at that particular moment. This brings in the surprise test advantages.
- **Information to system staff on meeting of objectives:** Continuous audit techniques provides information to systems staff regarding the test vehicle to be used in evaluating whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency.
- **Training for new users:** Using the ITFs, new users can submit data to the application system, and obtain feedback on any mistakes they make via the system's error reports.

(b) During the review of hardware, major tasks, which should be accomplished by a reviewer to evaluate the adequacy and the timeliness of preventive maintenance,

are given as follows:

- To understand the frequency of scheduled preventive maintenance work performed by the hardware vendors and the in-house staff;
- To compare this frequency to hardware maintenance contract and note any exceptions;
- To determine compliance with maintenance contractual agreements by examining maintenance log;
- To ascertain whether scheduled maintenance has had any adverse effect on the production schedule during peak season;
- To determine whether preventive maintenance logs are retained. Identify any abnormal hardware or software problems;
- To ensure that the hardware maintenance period commences on the same day as the warranty or guarantee expires; (This prevents additional maintenance charges while in warranty period and also eliminates the time gap between the expiry of the warranty period and the commencement of maintenance.) and
- To verify whether the maintenance agreement has a maintenance call response time defined. (It is the maximum time allowed between notification of a problem and the arrival of the maintenance staff.)

10. (a) Following are the major threats due to cyber crimes:

- **Embezzlement:** It is unlawful misappropriation of money or other things of value, by the person to whom it was entrusted (typically an employee), for his/her own use or purpose.
- **Fraud:** It occurs on account of intentional misrepresentation of information or identity to deceive others, the unlawful use of credit/debit card or ATM, or the use of electronic means to transmit deceptive information, to obtain money or other things of value. Fraud may be committed by someone inside or outside the company.
- **Theft of proprietary information:** It is the illegal obtaining of designs, plans, blueprints, codes, computer programs, formulas, recipes, trade secrets, graphics, copyrighted material, data, forms, files, lists, and personal or financial information, usually by electronic copying.
- **Denial of Service (DoS):** An action or series of actions that prevents access to a software system by its intended/authorized users or causes the delay of its time-critical operations or prevents any part of the system from functioning is termed as 'DoS'. There can be disruption or degradation of service that is dependent on external infrastructure. Problems may erupt through internet connection or e-mail service those results in an interruption of the normal flow

of information. DoS is usually caused by events, such as ping attacks, port scanning probes, and excessive amounts of incoming data.

- **Vandalism or sabotage:** It is the deliberate or malicious damage, defacement, destruction or other alteration of electronic files, data, web pages, and programs.
- **Computer virus:** A computer virus is a computer program that can copy itself and infect a computer without the permission or knowledge of the user.
- **Others:** Threat includes several other cases, such as intrusions, breaches and compromises of the respondent's computer networks (such as hacking or sniffing) regardless of whether damage or loss were sustained as a result.

(b) **Delphi approach:** The Delphi technique is defined as: 'a method for structuring a group communication process so that the process is effective in allowing a group of individuals as a whole to deal with a complex problem'. It was originally developed as a technique for the US Department of Defence. The Delphi Technique was first used by the Rand Corporation for obtaining a consensus opinion. Here, a panel of experts is appointed. Each expert gives his/her opinion in a written and independent manner. They enlist the estimate of the cost, benefits and the reasons why a particular system should be chosen, the risks and the exposures of the system. These estimates are then compiled together. The estimates within a pre-decided acceptable range are taken. The process may be repeated four times for revising the estimates falling beyond the range. Then a curve is drawn taking all the estimates as points on the graph. The median is drawn and this is the consensus opinion.

11. (a) The tasks to be undertaken in 'Vulnerability assessment and definition of requirement' phase of a Business Continuity Plan are given as follows:

- A thorough Security Assessment of the system and communications environment including personnel practices; physical security; operating procedures; backup and contingency planning; systems development and maintenance; database security; data and voice communications security; systems and access control software security; insurance; security planning and administration; application controls; and personal computers.
- The Security Assessment will enable the business continuity team to improve any existing emergency plans and disaster prevention measures and to implement required emergency plans and disaster prevention measures where none exist.
- Present findings and recommendations resulting from the activities of the Security Assessment to the Steering Committee so that corrective actions can be initiated in a timely manner.

- Define the scope of the planning effort.
- Analyse, recommend and purchase recovery planning and maintenance software required to support the development and maintenance of the plans.
- Develop a Plan Framework.
- Assemble business continuity team and conduct awareness sessions.

(b) Various backup techniques are given as follows:

- **Full Back-up:** This is the simplest form of back-up. With a full back-up system, every back-up generation contains every file in the backup set. However, the amount of time and space such a backup takes prevents it from being a realistic proposition for backing up a large amount of data. When it comes to restoring data, this type of backup is the simplest to use because a single restore session is needed for restoring all back-up files.
- **Differential Back-up:** A differential backup generation contains all the files that have changed since the last full backup. This is in contrast to incremental backup generation, which holds all the files that were modified since the last full or incremental backup.

Comparing with full back-up, differential back up is obviously faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved.

Restoring from a differential backup is a two-step operation. Restoring from the last full back- up; and then restoring the appropriate differential backup. The downside to using differential backup is that each differential backup will probably include files that were already included in earlier differential backups.

- **Incremental Backup:** In an incremental backup generation only the files that have changed since the last full backup / differential back up / or incremental backup are saved. This is the most economical method, as only the files that changed since the last backup are backed up. This saves a lot of backup time and space.
- **Mirror backup:** It is identical to a full backup, with the exception that the files are not compressed in zip files and they cannot be protected with a password. A mirror backup is most frequently used to create an exact copy of the backup data.

12. (a) Major characteristics for any system to qualify for a true ERP solution is given as follows:

- **Flexibility:** An ERP system should be flexible to respond to the changing needs of an enterprise. The Client Server technology enables ERP to run

across various database back ends through Open Database Connectivity (ODBC).

- **Modular & Open:** ERP system has to have open system architecture. This means that any module can be interfaced or detached whenever required without affecting the other modules. It should support multiple hardware platforms for the companies having heterogeneous collection of systems. It must support some third party add-ons also.
 - **Comprehensive:** It should be able to support variety of organizational functions and must be suitable for a wide range of business organizations.
 - **Beyond The Company:** It should not be confined to the organizational boundaries, rather support the on-line connectivity to the other business entities of the organization.
 - **Best Business Practices:** It must have a collection of the best business processes applicable worldwide. An ERP package imposes its own logic on a company's strategy, culture and organization.
- (b) Various steps involved in the implementation of a typical ERP package, are given as follows:
- Identifying the needs for implementing an ERP package;
 - Evaluating the 'As Is' situation of the business i.e. to understand the strength and weakness prevailing under the existing circumstances;
 - Deciding the 'Would be' situation for the business i.e. the changes expected after the implementation of ERP;
 - Reengineering the Business Process to achieve the desired results in the existing processes;
 - Evaluating the various available ERP packages to assess suitability;
 - Finalising of the most suitable ERP package for implementation;
 - Installing the required hardware and networks for the selected ERP package;
 - Finalising the Implementation consultants who will assist in implementation; and
 - Implementing the ERP package.

13. Various phases of ISMS are given as follows:

- **The Plan Phase** – This phase serves to plan the basic organization of information security, set objectives for information security and choose the appropriate security controls (the standard contains a catalogue of 133 possible controls).

- **The Do Phase** – This phase includes carrying out everything that was planned during the previous phase.
- **The Check Phase** – The purpose of this phase is to monitor the functioning of the ISMS through various “channels”, and check whether the results meet the set objectives.
- **The Act Phase** – The purpose of this phase is to improve everything that was identified as non-compliant in the previous phase.

The cycle of these four phases never ends, and all the activities must be implemented cyclically in order to keep the ISMS effective.

Major activities of the first phase of ISMS (Plan phase) are given as follows:

- Determining the scope of the ISMS;
 - Writing an ISMS Policy;
 - Identifying the methodology for risk assessment and determining the criteria for risk acceptance;
 - Identification of assets, vulnerabilities and threats;
 - Evaluating the size of risks;
 - Identification and assessment of risk treatment options;
 - Selection of controls for risk treatment;
 - Obtaining management approval for residual risks;
 - Obtaining management approval for implementation of the ISMS; and
 - Writing a Statement of applicability that lists all applicable controls, states which of them have already been implemented, and those which are not applicable.
- 14. COBIT 5 Enablers:** Enablers are factors that, individually and collectively, influence whether something will work— in this case, governance and management over enterprise IT. Enablers are driven by the goals cascade, i.e., higher-level IT-related goals define what the different enablers should achieve. The COBIT 5 framework describes seven categories of enablers (shown in Fig.):
1. Principles, policies and frameworks are the vehicle to translate the desired behaviour into practical guidance for day-to-day management.
 2. Processes describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.
 3. Organizational structures are the key decision-making entities in an enterprise.

4. Culture, ethics and behavior of individuals and of the enterprise are very often underestimated as a success factor in governance and management activities.
5. Information is pervasive throughout any organization and includes all information produced and used by the enterprise. Information is required for keeping the organization running and well governed, but at the operational level, information is very often the key product of the enterprise itself.
6. Services, infrastructure and applications include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.
7. People, skills and competencies are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions.

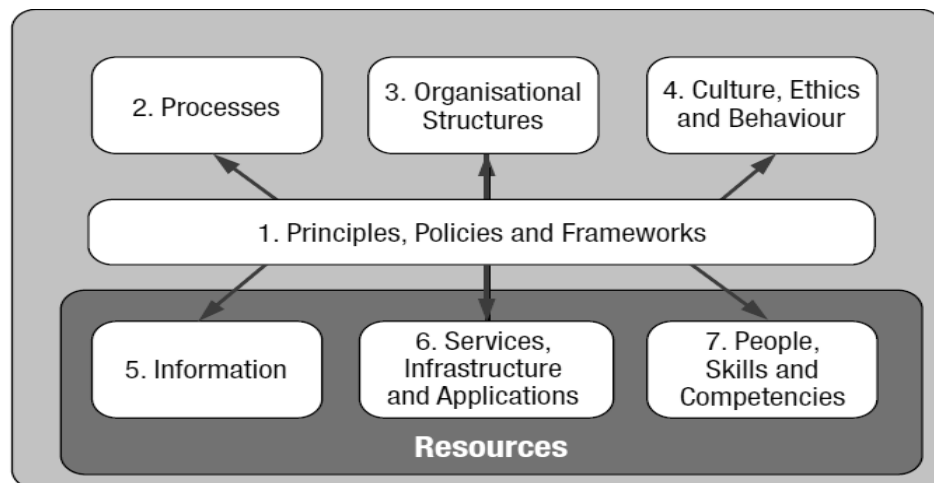


Fig.: Seven Enablers of COBIT 5

15. The components of a good Information Security Policy is 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.

16. Major points that are required to be taken into consideration for the proper implementation of Physical and Environmental Security with reference to Information Security Policy are given as follows:

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

17. (a) [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.

(b) [Section 15] Secure Electronic Signature (Substituted vide ITAA 2008):

An electronic signature shall be deemed to be a secure electronic signature if-

- (i) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and
- (ii) the signature creation data was stored and affixed in such exclusive manner as may be prescribed

Explanation- In case of digital signature, the "signature creation data" means the private key of the subscriber.

18. [Section 41] Acceptance of Digital Signature Certificate:

- (1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of a Digital Signature Certificate -
 - (a) to one or more persons;
 - (b) in a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.
- (2) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that –
 - (a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;
 - (b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;
 - (c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

19. (a) **Weaknesses of Spiral Model:** Major weaknesses of Spiral Model are given as follows:

- Challenges to determine the exact composition of development methodologies for each iteration around the Spiral;
- Highly customized to each project, and thus is quite complex, limiting reusability;
- A skilled and experienced project manager required to determine how to apply it to any given project;
- No established controls for moving from one cycle to another cycle. Without controls, each cycle may generate more work for the next cycle; and
- No firm deadlines - cycles continue with no clear termination condition, so there is an inherent risk of not meeting budget or schedule.

(b) **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; and
- The identity of the computer programs or individuals not permitted to access the data item.

(c) **Cryptosystem:** A cryptosystem refers to a suite of algorithms needed to implement a particular form of encryption and decryption. Typically, a cryptosystem consists of three algorithms: one for key generation, one for encryption, and one for decryption. The term *cipher* (sometimes *cypher*) is often used to refer to a pair of algorithms, one for encryption and one for decryption. Therefore, the term "cryptosystem" is most often used when the key generation algorithm is important. For this reason, the term "cryptosystem" is commonly used to refer to public key techniques; however both "cipher" and "cryptosystem" are used for symmetric key techniques.

20. (a) **Test Plan:** The final component of a disaster recovery plan is a test plan. The purpose of the test plan is to identify deficiencies in the emergency, backup, or recovery plans or in the preparedness of an organization and its personnel for facing a disaster. It must enable a range of disasters to be simulated and specify the criteria by which the emergency, backup, and recovery plans can be deemed satisfactory. Periodically, test plans must be invoked. Unfortunately, top managers are often unwilling to carry out a test because daily operations are disrupted. They also fear a real disaster could arise as a result of the test procedures.

To facilitate testing, a phased approach can be adopted. First, the disaster recovery plan can be tested by desk checking and inspection and walkthroughs, much like the validation procedures adopted for programs. Next, a disaster can be simulated at a convenient time—for example, during a slow period in the day. Anyone, who will be affected by the test (e.g., personnel and customers) also might be given prior notice of the test so they are prepared. Finally, disasters could be simulated without warning at any time. These are the acid tests of the organization's ability to recover from a catastrophe.

- (b) **Cold Site:** If an organisation can tolerate some downtime, cold-site backup might be appropriate. A cold site has all the facilities needed to install a mainframe system—raised floors, air conditioning, power, communication lines, and so on. An organisation can establish its own cold-site facility or enter into an agreement with another organisation to provide a cold-site facility.

Hot Site: If fast recovery is critical, an organisation might need hot site backup. All hardware and operations facilities will be available at the hot site. In some cases, software, data and supplies might also be stored there. A hot site is expensive to maintain. They are usually shared with other organisations that have hot-site needs.

- (c) **Final Acceptance Testing:** Final Acceptance Testing is conducted when the system is just ready for implementation. During this testing, it is ensured that the new system satisfies the quality standards adopted by the business and the system satisfies the users. Thus, the final acceptance testing has two major parts:

- **Quality Assurance Testing:** It ensures that the new system satisfies the prescribed quality standards and the development process is as per the organization's quality assurance methodology.
- **User Acceptance Testing:** It ensures that the functional aspects expected by the users have been well addressed in the new system. There are two types of the user acceptance testing :
 - o *Alpha Testing:* This is the first stage, often performed by the users within the organization.
 - o *Beta Testing:* This is the second stage, generally performed by the external users. This is the last stage of testing, and normally involves

sending the product outside the development environment for real world exposure.

21. (a) Benefits of COBIT 5: COBIT 5 helps enterprises of all sizes to:

- maintain high-quality information to support business decisions;
- achieve strategic goals and realize business benefits through the effective and innovative use of IT;
- achieve operational excellence through reliable, efficient application of technology;
- maintain IT-related risk at an acceptable level;
- optimize the cost of IT services and technology; and
- support compliance with relevant laws, regulations, contractual agreements and policies.

(b) Level 1- Initial Level of CMM: It is characteristic of processes at this level that they are (typically) un-documented 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.

At the Initial Level, the organization typically does not provide a stable environment for developing and maintaining software. Such organizations frequently have difficulty making commitments that the staff can meet with an orderly engineering process, resulting in a series of crises. During a crisis, projects typically abandon planned procedures and revert to coding and testing. Success depends entirely on having an exceptional manager and a seasoned and effective software team. Occasionally, capable and forceful software managers can withstand the pressures to take shortcuts in the software process; but when they leave the project, their stabilizing influence leaves with them. Even a strong engineering process cannot overcome the instability created by the absence of sound management practices. In spite of this ad hoc, even chaotic, process, Level 1 organizations frequently develop products that work, even though they may be over the budget and schedule. Success in Level 1 organizations depends on the competence and heroics of the people in the organization and cannot be repeated unless the same competent individuals are assigned to the next project. Thus, at Level 1, capability is a characteristic of the individuals, not of the organization.

(c) [Section 68] Power of Controller to give directions (Amended Vide ITAA 2008):

- (1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under.

- (2) Any person who **intentionally or knowingly** (Inserted vide ITAA 2008) fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or to a fine not exceeding one lakh rupees or to both.

22. (a) System Development Life Cycle (SDLC) framework provides system designers and developers to follow a sequence of activities. It consists of a set of steps or phases in which each phase of the SDLC uses the results of the previous one. The SDLC is document driven, which means that at crucial stages during the process, documentation is produced. A phase of the SDLC is not complete until the appropriate documentation or artifact is produced. These are sometimes referred to as deliverables.

From the perspective of the IS Audit, the following are the major advantages of SDLC:

- The IS Auditor can have a clear understanding of various phases of the SDLC on the basis of the detailed documentation created during each phase of the SDLC.
- The IS Auditor on the basis of his/her examination, can state in his/her report about the compliances by the IS management of the procedures, if any, set up by the management.
- The IS Auditor, if has a technical knowledge and ability of the area/s of SDLC, can be a guide during various phases of SDLC.
- The IS Auditor can provide an evaluation of the methods and techniques used during various development phases of the SDLC.

- (b) Major weaknesses of Waterfall model are given as follows:

- Inflexible, slow, costly, and cumbersome due to significant structure and tight controls.
- Project progresses forward, with only slight movement backward.
- Little room for use of iteration, which can reduce manageability if used.
- Depends upon early identification and specification of requirements, yet users may not be able to clearly define what they need early in the project.
- Requirement inconsistencies, missing system components and unexpected development needs are often discovered during design and coding.
- Problems are often not discovered until system testing.
- System performance cannot be tested until the system is almost fully coded, and under capacity may be difficult to correct.
- Difficult to respond to changes. Changes that occur later in the life cycle are

more costly and are thus discouraged.

- Produces excessive documentation and keeping it updated as the project progresses is time-consuming.
- Written specifications are often difficult for users to read and thoroughly appreciate.
- Promotes the gap between users and developers with clear vision of responsibility.

(c) **Accountants' involvement in Development work:** In most of the cases, accountants are uniquely qualified to participate in systems development because they may be among the few people in an organization who can combine knowledge of IT, business, accounting, and internal control, as well as behavior and communications, to ensure that new systems meet the needs of the user and possess adequate internal controls. They have specialized skills - such as accounting and auditing - that can be applied to the development project. For example, an accountant might perform the analysis of a proposed system's costs and benefits.

23. (a) Different phases of the methodology for developing a Business Continuity Plan are given as follows:

- Pre-Planning Activities (Business continuity plan Initiation),
- Vulnerability Assessment and General Definition of Requirements,
- Business Impact Analysis,
- Detailed Definition of Requirements,
- Plan Development,
- Testing Program,
- Maintenance Program, and
- Initial Plan Testing and Plan Implementation.

(b) Major backup tips to be followed by the company are given as follows:

- Draw up a simple (easy to understand) plan of who will do what in the case of an emergency.
- Keep a record of what was backed up, when it was backed up and which backup media contains what data. You can also make a calendar of which type of backup is due on a certain date.
- Select the option to verify backup, the process will take a little longer but it's definitely worth the wait.
- Create a reference point where you know everything is working properly. It will

be quicker to restore the changes from tape.

- Select the option to restrict restoring data to owner or administrator and also set the Domain Group Policy to restrict the Restore privilege to Administrators only. This will help to reduce the risk of someone being able to restore data should the media be stolen.
- Create a step-by-step guideline (a flowchart for example) clearly outlining the sequence for the retrieval and restoration of data depending on the state of the system.

(c) The goals of a business continuity plan should be to:

- identify the 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.

24. (a) **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 effort 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.

(b) **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.

Quantitative techniques: These 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.

(c) [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.

- 25. (a) Security Objectives:** The objective of information system security is “the protection of the interests of those relying on information, and the information systems and communications that deliver the information, from harm resulting from failures of confidentiality, integrity, and availability”.

For any organization, the security objective comprises three universally accepted attributes:

- **Confidentiality:** Prevention of the unauthorized disclosure of information.
- **Integrity:** Prevention of the unauthorized modification of information.
- **Availability:** Prevention of the unauthorized withholding of information.

The relative priority and significance of confidentiality, integrity and availability vary according to the data within the information system and the business context in which it is used.

- (b) Prior to know the details of 'how to protect the information systems', we need to define a few basic ground rules that must be addressed sequentially. These rules are given as follows:
- **Rule #1:** We need to know that 'what the information systems are' and 'where these are located'.
 - **Rule #2:** We need know the value of the information held and how difficult it would be to recreate if it were damaged or lost.
 - **Rule #3:** We need to know that 'who is authorized to access the information' and 'what they are permitted to do with the information'.
 - **Rule #4:** We need to know that 'how quickly information needs to be made available should and it become unavailable for whatever reason (loss, unauthorized modification, etc.)'
- (c) Major tasks that are to be performed during the post-implementation period of an ERP package are given as follows:
- To develop the new job descriptions and organization structure to suit the post ERP scenario;
 - To determine the skill gap between existing jobs and envisioned jobs;
 - To assess training requirements, and create and implement a training plan;
 - To develop and amend HR, financial and operational policies to suit the future ERP environment; and
 - To develop a plan for workforce logistics adjustment.