Question - 1:

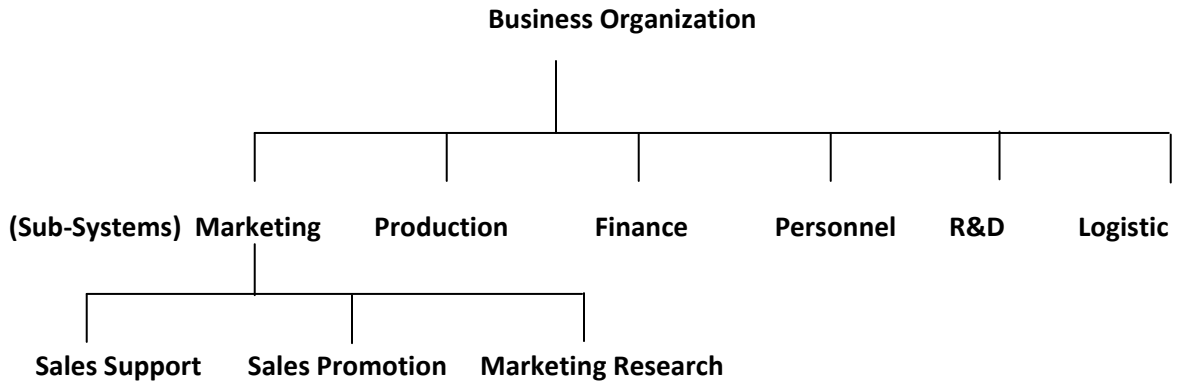
As a member of the system development team, explain the process of decomposition of an organization into various functional blocks to comprehend the information processing system with the help of an example:

Answer -1:

Any system can be divided into smaller systems known as sub-systems and a sub-system can further be divided into smaller systems known as sub-sub-system. ***The process of dividing the system into smaller systems is known as system decomposition.***

This process continues until the smallest sub-systems are of manageable size. The concept of sub-system is an important aspect and considered as basis for analysis and design of information systems, because it is difficult to manage a complex system when considered as whole. Therefore, for the sake of convenience and clarity, a system is divided into smaller systems. The process of dividing or factoring a system into smaller system is known as decomposition. The sub-systems resulting from this process usually form hierarchical structures. In a hierarchy, a sub-system is one element of a ***supra-system*** (the system above it).

The figure below provides decomposition of organization various functional blocks, which ultimately get converted into information sub-systems.



System Decomposition

Question - 2:

An organization is in the stage of systems development to implement an enterprise wide information system, where the following conditions exist:

The new system is mission critical and there is hasty need
End users are not aware of the information needs

The business risks associated in implementing the wrong system are high
Read the above case carefully and answer the following with proper justifications:

(a) Indetify the system development approach and steps to be followed in the above stated conditions.
(b) State the reasons for choosing the particular approach for system development
(c) Indentify the risks, when end-users are involved in the system development process.

Answer -2:

There are three important elements in the above case

(1) System is immediately required
(2) End user involvement is required at high level because users are not aware of the information needs
(3) The business risks of implementing wrong system are high

Based on these elements, given below are the answers to the questions raised in the above case.

(a) Considering the above conditions, I would suggest to use the RAD (Rapid Application Development) approach. The key objective of this approach is fast development of high quality system.

(b) There are many reasons for selection of this approach:

- Provides quick development of required information system
- Allows incremental prototyping which help to understand users requirements better.
- Allows the extensive involvement of end users through Joint application development (JAD) workshops which reduces the risks of wrong system implementation
- Allows the use of CASE (Computer Aided Software Engineering) tools which help to develop mission critical applications with high quality

(c) Normally, end-users involvements help to develop right system; however, end-users involvement may cause the following risks:

- End-users involved are not knowledgeable enough to provide the right suggestions, this may cause system is developed with wrong specifications
- End-users involved are not given adequate delegations which may cause delay in decision making

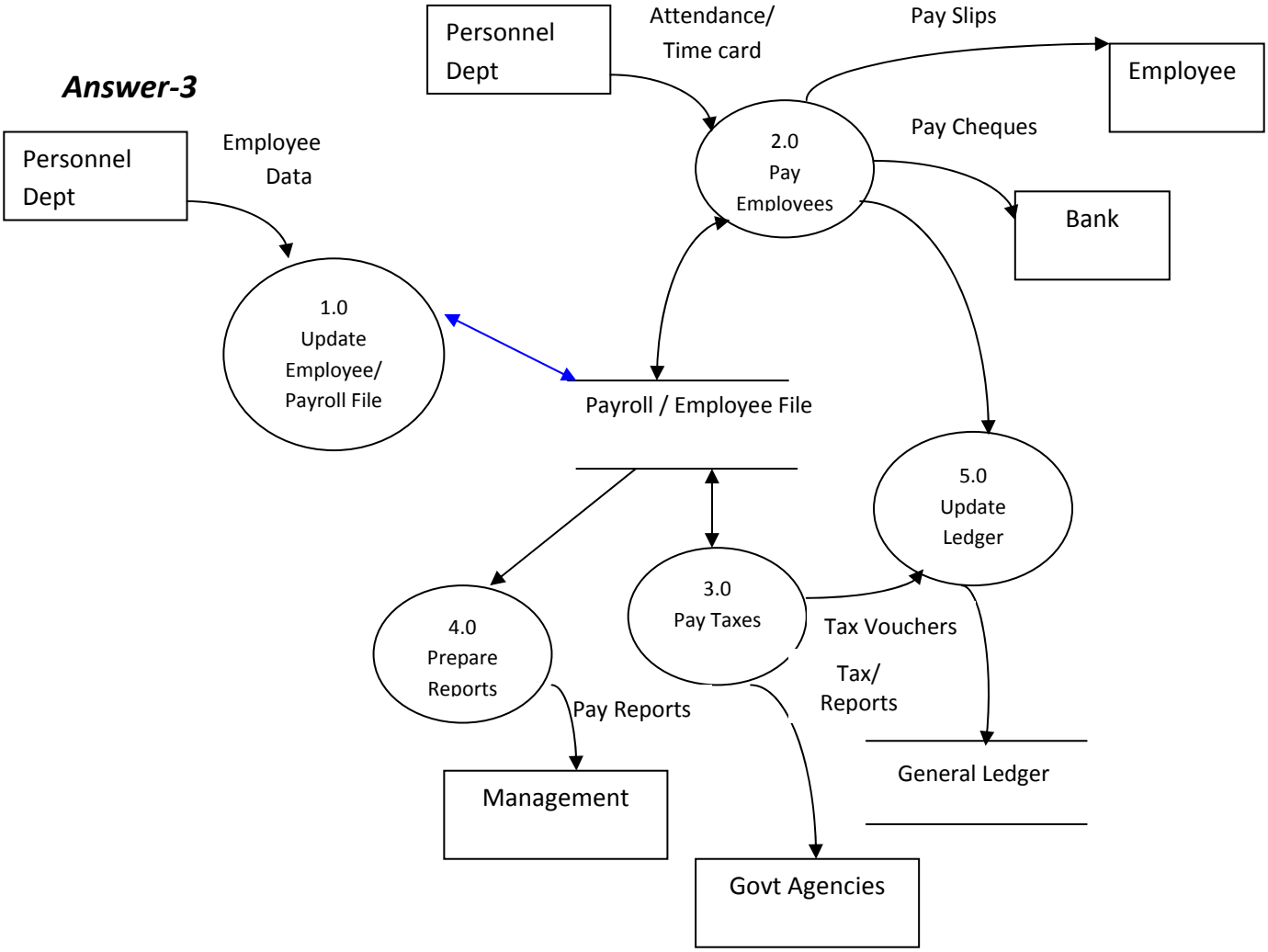
Question - 3:

Read the data flow and activities listed in the table below carefully and draw the data flow diagram for the payroll processing system.

Activities	**Data inputs**	**Data output**
Update employee/ roll file	New employee form Employee change form Employee/pay roll file	Update employee/ pay roll

Pay employees	Time cards Employee/pay roll file Tax table	Employee cheques Pay roll register update employee/ pay roll file pay roll cheques pay roll cash disbursements voucher
Prepare reports	Employee / pay roll file	Pay roll reports
Update general ledger	Payroll tax cash disbursements voucher pay roll cash disbursements voucher	Update general ledger

Answer-3



DFD for Payroll Processing (Level-1)

Question-4:

As a system analyst, you need to assess the successful implementation and stake holder's actual requirement of an enterprise system in retail chain organization across its braches to provide the following features:

- Lower operational costs,
- Better information for managers, and
- Smooth operation for users or better levels of service to customers.

Justify your answer with the necessary techniques used to determine the requirement of a system:

Answer -4:

System analysis is very important phase of system development, since any error in this phase would affect all subsequent phases of development. The aim of the system analysis phase is to thoroughly understand the user requirements and remove any inconsistencies and incompleteness in these requirements. This phase help to design the system with best possible features as mentioned above in the question i.e. lower operational cost, better information for managers and smooth operation for users or better levels of service to customers:

The following techniques can be used to determine the requirements from the systems:

(1) Collection of Detail Information: In this step, detail information about the requirement from the new retail system will be collected. The following fact finding techniques can be used for information collection:

(a) Review and collection of documents being used in the retail chain

(b) Interview with users

(c) Questionnaire for users to provide response to set of questions incase users can not provide time for interview

(d) Personal Observations of users working

(2) Analysis of the Existing System: In this step, the analysts perform a detail analysis of users' existing system which in turn helps to define the users' requirements from the proposed system in a better manner.

(3) System Analysis of Proposed System: Once the analysis of existing system is completed, the analysis of the proposed system starts. The proposed system analysis is done by using the data collected in "Collection of Detail Information" step and models prepared during the "Analysis of Existing System".

With the above analysis the analysts can design the system which can provide the following features:

- Lower operational costs,
- Better information for managers, and
- Smooth operation for users or better levels of service to customers.

Question-5.

An auditor while evaluating the reliability of a control implemented in a transaction process had to estimate the reliability per transaction. A test was undertaken and result indicated that control was unreliable. The reliability of the process was 0.15 when control was in place and was 0.09 when the control was absent. The management had estimated the cost of reprocessing the errors as Rs.1000 per transaction procedure. Evaluate the net benefit of the control procedure if the cost implementation of the control is Rs. 10,000.

Answer-5:

It seems this question is not clearly defined in the practice manual but I am providing the possible answer for this:

Cost of reprocessing an error	= Rs. 1000
Chances of error without control	= 1- 0.09
	= 0.91
Therefore, expected error cost without control	= 1000*0.91
	= Rs. 910
Cost of implementing the control	= Rs 10,000
Chances of error with control	= 1 – 0.15
	= 0.85
Therefore, expected error cost with control	= 1000*0.85
	=Rs. 850
Net benefit per transaction with control	= 910 – 850
	= Rs. 60

The system will achieve benefits with control if more than =10000/60

=167 transactions will have errors

Question-6:

A company is engaged in the stores stock taking data activities. Whenever, input data error occurs, the entire stock data is reprocessed at a cost of Rs. 50,000. The management has decided to introduce a data validation step that would reduce errors from 12% to 0.5% at a cost of Rs.2,000 per stock taking period. The time taken for validations causes an additional cost of Rs. 200

(i) Evaluate the percentage of cost-benefit effectiveness of the decision taken by the management and

(ii) Suggest preventive control measures to avoid errors for improvements

Answer-6:

(i) Evaluate the percentage of cost-benefit effectiveness of the decision taken by the management

Without Control:

Chances of Error	=12%
Cost of one error	= Rs. 50,000

Expected cost of error	=Rs. 12% * 50,000
	=Rs. 6,000

With Data Validation Control:

Chances of Error:	=0.5%
Cost of one Error	=Rs. 50,000
Expected cost of error	=Rs.0.5% * 50,000
	=Rs. 250
Cost of per stock taking with control	=Rs. 2000
Additional cost per stock taking	=Rs. 200

Total expected cost with data validation control= Rs. 2,450

Percentage of cost-benefit

Benefit with data validation	= 6,000- 2,450 = Rs. 3,550
Benefits % with data validation	= (3550/6000)
	=60%

(ii) Suggest preventive control measures to avoid errors for improvements

Preventive Controls:

These controls as name suggest are designed to prevent an error or any malicious activity in the system, for example using login-id and password is a preventive control. Preventive controls are implemented for both computerized and manual environment; but techniques and implementation may differ depending upon the type of threats and exposure. Below list provides some examples of preventive controls.

- Employ qualified personnel
- Segregation of duties
- Proper Documentation
- Authorization of transactions
- Validation of transactions through various checks

Question -7:

Identify and briefly discuss the necessary data integrity control techniques for the following processes in a payroll system:

(a) addition/deletion/updating of employee data by the HR department:

b) Payroll processing and storage

(c) Pay-slip generation and consolidated pay-report department wise

Answer -7:

Hint:

(a) Describe input/source document controls of data integrity

(b) Describe processing and storage controls of data integrity controls

(c) Describe output controls of data integrity controls

Question -8:

A retail company has been in the process of converting its manual sales into a computerized system with the implementation of a Point of Sales system for the last 6 months. The company needs to evaluate the software application system for its completeness, correctness and quality.

Read the scenario carefully and answer the following:

(a) State the test plant to be performed to check if the different modules of the application are integrated seamlessly
(b) Indentify the testing method to verify that the application is efficient to handle about 500 POS counters concurrently
(c) Explain the testing method used to test the consistency between different versions of the same application.

Answer -8:

(a) ***The test plan for this task will be "INTEGRATION TEST PLAN":***
In this test plan, functionalities which link one unit with another are tested. This test plan includes activities for testing of integrated functionalities.

(b) For this we will use two testing methods:
(1) Volume Testing: It is the testing of the system to check whether system will work efficiently when 500 POS counters will be simultaneously active and when the database contains the greatest data volume load.
(2) Stress Testing: This testing helps to determine how many numbers of POS can be simultaneously active without compromising the system performance.

(c) For this we will use a testing method known as regression testing (you can read about this from reference book)

Question -9:

An automobile spare parts production company has 10 distribution centers, each of which maintain their inventory status through the company's inventory application software on its Virtual Private Network (VPN). Managers across the distribution centers have identified different types of frauds / errors committed during data entry, transaction processing and fake users' logins in the inventory system.
The managers on one of the distribution center has asked you (IS auditor) to prepare a report on "how the risk appraisal can be undertaken". Indicate the appropriate approach in this situation and give reasons for your answers.

Answer-9:

Here the major problem is frauds committed during data entry and transaction processing. Also, the fake users login into the inventory system. These problems seem to be due to absence of adequate controls and security policy. In the risk appraisal of these problems the following approach can be mentioned by auditor:

- Identification of types errors and frauds in the system.

- Determination of possible losses due to these errors and frauds in the systems
- Review of existing applied controls and security policy to avoid these errors and frauds (which seem to be inadequate)
- Identification of types of controls which can be applied to avoid these frauds and errors
- Cost of implementation of these controls vs. benefits from controls
- Implementation of controls
- Monitoring/review of applied controls for potential corrections
- Suggestion to develop and implement an effective information security policy

Question -10:

Briefly explain the control measures to ensure confidentiality, integrity, and availability of data.

Answer - 10:

Please explain in this the below 10 domains of BS 7799 or Focus area of ISMS

- *SECURITY POLICY*
- *ORGANISATIONAL SECURITY*
- *ASSET CLASSIFICATION & CONTROL*
- *PERSONNEL SECURITY*
- *PHYSICAL AND ENVIRONMENTAL SECURITY*
- *COMMUNICATIONS AND OPERATIONS MANAGEMENT*:
- *ACCESS CONTROL*
- *SYSTEM DEVELOPMENT AND MAINTENANCE*
- *BUSINESS CONTINUITY MANAGEMENT*
- *COMPLIANCE*

Question-11:

A backup plan is to be prepared for XYZ company in order to specify the type of backup to be kept, frequency with which backup is to be undertaken, procedures for making a backup, location of backup resources, sites where these resources can be assembled and operations restarted, personnel who are responsible for gathering backup resources and restarting operations, priorities to be assigned to recover various systems and a time frame for the recovery of each system. But the most difficult part in preparing the backup plan is to ensure that all the critical resources are backed up. List the resources that are to be considered in a backup plan.

Answer: -11:

Backup plan is the most crucial plan for immediate recovery from disaster. Backup plan is considered as a supportive plan for the recovery plan. In this plan, as mentioned above various planning related to type of backup, frequency of backup and location of backup etc are decided and implemented.

In general, the following resources are considered for backup

- Personnel: Arrangement of staff to maintain information system in any emergency and also arrangement with another company for provision of staff.
- Hardware: Arrangement of backup/standby hardware
- Facilities: Arrangement of standby facilities or arrangement with another company for provision of facilities
- Documentation: Inventory of documents also at some off-site location
- Data/Information: Backup of data files at on-site, as well at off-site locations
- Application Software: Inventory of application software at on-site, as well at off-site locations
- System software: Inventory of application software at on-site, as well at off-site locations

Question: 12

ABC limited has migrated from traditional system to new real time integrated ERP systems. The technical advisor of the company advised to the owner that the company should take necessary steps to analyze several types of risks. Explain those risks in brief.

Answer: 12

Migration to real-time and integrated ERP system, from old system, is not an easy process. It involves many risks and governance issues; such as:

Risks and Issues with ERP:

Single Point Failure: ERP provides an integrated system in the organization which is managed by a single ERP application (software). Failure of ERP application/main-server may bring down the working of entire organization's information system.

Change Management: ERP implementation is not only an implementation of a computer based integrated system; it requires changes in existing processes, culture and working methods of organizations' staff/stakeholders. And adapting to new processes, culture and working method for staff is always a big challenge.

Structural Changes: Not only the implementation of ERP requires change in processes and working methods; it also requires the structural changes (re-arrangement of departments) in the organization through BPR to achieve the best practices.

Job Profile Changes: The change management and structural changes may need the change in job profiles of the staff from existing job profiles. This is also a very big risk and governance issue, as staff normally resist for change in their job profiles.

On-line and Real-time System: ERP provides an on-line and real-time data processing system which requires a continuous maintenance capability, and also requires a quick response to any system problems and new requirements. Maintaining such capabilities is always a big challenge for the organizations.

Distributed Computing: ERP provides a distributed data processing system, which helps to process data from anywhere. Inexperience with distributed computing implementation and management also put forward a big challenge.

Dependence on External Assistance: Previously, organizations used to manage information system through internal support only. But ERP management requires the support of external assistance and that may expose for security and resource management risks to organizations data and resources.

Program Interfaces and Data Conversions: ERP requires extensive interfaces with other systems (like banks, tax authorities, customers and suppliers' systems), and it also requires extensive data conversion from old (legacy) system. These tasks always pose a big challenge to organizations**.**

Audit expertise: ERP environment require expertise to implement the controls and audit those controls.

Single sign on: A single sign-in to ERP system provides access to multiple modules and applications which create a security problem to the organizations.

Data Content Quality: ERP system requires the data inputs from multiple external data sources like customers, suppliers and banks. This may affect the data quality in the system.

Privacy and Confidentiality: There is risk of disclosure of personnel information to greater extent as ERP systems are connected with multiple external data sources.

Question:-13

What is enterprise controlling? Briefly explain its modules:

Answer:-13

ERP provides a module known as ***Enterprise Controlling*** which helps to manage and control entire Enterprise in an integrated manner. This module contains accounting data prepared by subsidiaries for corporate reporting which is automatically prepared within the local books of each subsidiary but consolidated at corporate level.

This data is transferred to a module called Enterprise Controlling (EC).

Date transfer to EC module automatically set up consolidated financial statements including elimination of inter-company transactions, currency translation etc.

Enterprise Controlling consists of 3 modules.

1. EC-CS: This allows the financial consolidation at corporate level.
2. EC-PCA: Implement transfer pricing rule for inter companies transactions
3. EC-EIS: Provide KPI (key performance indicators) at corporate levels to top-executive

Enterprise Controlling allows to control the whole enterprise from a corporate and a business unit perspective within one common infrastructure. It helps to speed up provision of business control information by fully automated corporate reporting from operative accounting via financial consolidation to management reporting. From EC-EIS top-level reports, end users can drill down to more detailed information within EC or any other SAP-R/3 application. EC can work with data from SAP and non-SAP sources.

Question-14

A company is developing several types of biscuits having its branches all over the country. The owner of the company wishes to centralize and consolidate the information flowing from its branches in a uniform manner across various levels of the organization. The technical advisor of the company recommended that the company should go for the implementation of the ERP package. Why the company should undertake ERP?

Answer-14

If we look at the broad perspective that why companies undertake the ERP then those can be the followings:

Integrate financial information:
Because the operation of company is located at different locations and if the owner tries to understand the company's overall financial performance, he may find the differences in the outputs given by different units and departments. For example, finance may have its own set of revenue numbers, sales may have another set, and the different business units may each have their own set for how much they contributed to revenue. ERP creates a single set of numbers that cannot be questioned because everyone is using the same system.

Integrate customer order information:
ERP systems can help to integrate the customer order information irrespective of the place from where order is inserted and executed. By having this information in one software system, rather than scattered among many different systems that can't communicate with one another helps to keep track of orders more easily, and coordinate manufacturing, inventory and shipping among many different locations simultaneously.

Standardize and speed up manufacturing processes:
Manufacturing companies-especially those with an appetite for mergers and acquisitions—often find that multiple business units across the company make the same transaction/ recording/ report using different methods and computer systems. ERP systems come with standard methods for automating some of the steps of a manufacturing process. Standardising those processes and using a single, integrated computer system can save time, increase productivity and reduce headcount.

Reduce inventory:
ERP helps the manufacturing process flow more smoothly, and it improves visibility of the order fulfilment process inside the company. That can lead to reduced inventories of the materials used to make products (work-in-progress inventory), and it can help users better plan deliveries to customers, reducing the finished good inventory at the warehouses.

Standardise HR information:
Especially in companies with multiple business units, HR may not have a unified, simple method for tracking employees' time and communicating with them about benefits and services. ERP can fix that.

Question-15:

Explain the relevance of BS 7799 (ISO 17799) for Indian Companies:

Answer-15

In the recent past, Indian companies and the Government have invested heavily in the IT infrastructure. However, theft of data and attacks on Indian sites and companies are alarming. Attacks and theft that happen on corporate websites are high and is usually kept under "strict" secrecy to avoid embarrassment from business partners, investors, media and customers. Huge losses are sometime remained un-audited and the only solution is to involve a model where one can see a long-run business led approach to Information Security Management.

BS 7799 (ISO 17799) consists of 127 best security practices (*covered under the 10 Domains which are discussed in chapter-8*) which Indian companies can adopt to build their Security Infrastructure. Even if a company decides not go in for the certification, the BS 7799 (ISO 17799) model helps companies maintain IT security through ongoing, integrated management of policies and procedures, personnel training, selecting and implementing effective controls, reviewing their effectiveness and improvement. Additional benefits of ISMS are improved customer confidence, a competitive edge, better personnel motivation and involvement, and reduced incident impact. Ultimately these factors lead to increased profitability.

The 10 domains of BS 7799 or Focus Area of ISMS (Information Security Management Systems)

- *SECURITY POLICY*
- *ORGANISATIONAL SECURITY*
- *ASSET CLASSIFICATION & CONTROL*
- *PERSONNEL SECURITY*
- *PHYSICAL AND ENVIRONMENTAL SECURITY*
- *COMMUNICATIONS AND OPERATIONS MANAGEMENT*:
- *ACCESS CONTROL*
- *SYSTEM DEVELOPMENT AND MAINTENANCE*
- *BUSINESS CONTINUITY MANAGEMENT*
- *COMPLIANCE*

Question-16:

ABC Company is implementing the health insurance portability and accountability act (HIPPA). There is a security rule issued under the act which lays out three types of security safeguards required for compliance. What are those conditions under these safeguards for which the company should look after?

Answer -16:

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the USA promises to streamline the conduct of electronic healthcare transactions by imposing standards, and at the same time to ensure the integrity, confidentiality and availability of the individually identifiable health information involved.

There are two HIPAA titles:

Title I

- Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs.

Title II

- **Title II** of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions
- **Title –II also requires** national identifiers for health services providers, health insurance plans, and employers.
- The AS provisions also address the security and privacy of health data.
- The standards are meant to improve the efficiency and effectiveness of the US health care system by encouraging the widespread use of electronic data interchange in the US health care system.

For us the topic of interest here is the Security Rule issued under the Act

The Security Rules:

- The Security rules lays out three types of security safeguards required for compliance: administrative, physical, and technical.
- For each of these types, the rules identify various security standards.
- And for each standard, there are both required and addressable implementation specifications.
- Required specifications must be adopted. Addressable specifications are more flexible. Individual entities can evaluate their own situation and determine the best way to implement addressable specifications.

HIPPA security rules requires three types of security safeguards:

- **Administrative Safeguards**
- **Physical Safeguards**
- **Technical Safeguards**

Administrative Safeguards:

- The use of administrative procedures for security include Certification, Contingency plans, Internal audit procedures, Security management process
- Training and awareness among staff for effective use of system.
- Documentation of processes used to protect data.
- Rules are required to manage the conduct of the personnel in relation to protection of the data.

Physical Safeguards:

- There should be procedures for protecting the physical computers systems and building containing data from fire, intrusion and any form of physical damage.
- Workstations should be used in such a way to avoid their direct access or view from users
- The movement of media/devices (containing data) in and out should be in a secured manner

Technical Safeguards:

- There should be processes in place for protecting information and to control individual access of such information.

By using

- Access Control.
- Authorization Control
- Audit Control.
- Message Authentication

Question-17:

Briefly discuss end user computing policies with respect to a sample IS security policy:

Answer -17:

The Information System (IS) security policy is a set of laws, rules, and practices that regulates how information is managed, protected, and distributed within an organization.

There are different categorizations of Information System security policy:
(1) Organization Security Policy
(2) User Policies
(3) Conditions for connection

User computing policies consist of a “User Security Policy” and “Acceptable Usage Policy”.

User security Policy set out the responsibilities and requirements for IT system users. For example:

- User will be provided a unique ID
- User will use a strong password for access of system
- User will not share his/her password with other users and outsiders
- User will not use the office system for personal work
- Games may not be stored or used on computer system
- Storage of sensitive Information on Personal Computers (PCs) must be protected through encryption techniques to restrict the viewing of information to authorized users only; and through lock in key for physical protections.

Acceptable Usage Policy provides acceptable use of internet access and email. For example:

- Organization will not allow the users to use office email for personal communications.
- Internet access will be permitted only for official work.

- Any content which is obscene or sexual in nature will not allow to be downloaded into the office system.
- User can not visit the prohibited sites.
- Users not following the acceptable usage policy may be fired from the organization.

Question-18:

Differentiate between the responsibilities of a Facilities Management Security Officers and Divisional System Security Officers with respect to organizational security structure.

Answer-18:

Facilities Management Security Officer (FMSO): The Facilities Management Security Officer (FMSO) reports directly to Facilities Management (or Facilities Managers) on all security matters relating to personnel. The role involves ensuring the controls are implemented, adhered to and reviewed as necessary.

Divisional System Security Officer (DSSO): A System Security Officer (SSO) from each division will be appointed as a DSSO. The SSO is a senior person appointed to fulfill the role of System Security Officer (SSO) for each ***major application system*** or **group of *systems.*** SSO responsibilities focus on business aspects of security thus ensuring that the information security of the system meets all relevant business control objectives.
The DSSO carries the same responsibilities as a SSO and in addition is responsible for representing the SSOs in their division at the ISMG (Information Security Management Group) and for communicating requirements and issues to/from this group.

Question-19:

It is clear from various instances that there are not only many direct and indirect benefits from the use of information systems, but many direct and indirect risks related to the use of information system. These risks have led to a gap between need to protect systems and the degree of protection applied. Briefly explain the causes of this gap.

Answer-19:

Risk: Risk is a probabilistic terms, it is likelihood that an organization may be exposed to some threats that may cause harms to organizations. For example, organizations are exposed to risks of fire and theft etc so fire and theft are the risks to organizations, which may cause harms to organization.
Information Systems are also exposed to many direct and indirect risks. These risks primarily have emerged due to technological changes of information systems, these changes always create gap between protection applied and protection required, due to:

1. Widespread use of new technologies
2. Extensive use of network applications
3. Eliminations of distance, time and space constraints i.e. use of distributed or any time anywhere processing systems
4. Frequent technological changes
5. Attractiveness of conducting electronic attacks against organizations (electronic attacks are easy to conduct and hard to detect)

6. Devolutions or decentralization of management and control
7. Some external factors such as legal and regulatory requirements

The above gaps indicate that there are always emerging new risks areas that could have significant impacts on critical business operations such as:

(a) External dangers from hackers, leading to denial of service and virus attack, extortion and leakage of corporate confidential information
(b) Growing potential for misuse and abuse of information system affecting privacy and ethical values
(c) Dangers to information system availability and robustness

Question-20:

Information Systems Audit Report contains various components: Cover and title page, Table of Contents, Summary/Executive Summary and Appendices. But after submission, the principal auditor raised the query that the report is not correct as it missed various important components. Explain the missing components in brief.

Answer-20:

IS audit report is an end product of information system audit, conducted by an IS auditor. This report is communicated to management with auditor's opinions. Though there is no standard format or guidelines for preparation of this report, but overall this report may contain the followings:

- Cover and Title Page
- Table of Contents
- Executive Summary
- Introduction
    - Background of IT Environment or Context
    - Purpose of Audit
    - Scope of Audit
    - Methodology Used for Auditing
- Findings
- Opinions
- Appendices

If we look at all the components of an audit report from the above list then the major components missing from the submitted audit report are:

- **Introduction:** This section describes briefly about IT environment in which audit was conducted, purpose of audit, scope of audit and methods used for auditing.
- **Findings:** This includes the key findings from the concluded audits on the client system
- **Opinions:** This includes auditor's opinions about the client's information system in terms of adequacy of controls and information security etc
- **Appendices:** It includes various references which helped in an effective audit of client system during the audit assignment

Question-21:

An Information System Audit Report includes various sections: Title page, Table of Contents, Summary, Introduction, Findings and Appendices. Explain various elements, included in the Introduction section.

Answer-21:

Introduction is the key section of an audit report. It describes briefly about IT environment of client's organization, purpose of audit, scope of audit and methods used for auditing.

Since readers will read "Executive Summary" section before the introduction therefore "Introduction" section should not repeat details of "Executive Summary". It includes the following elements:

- **Context or Environment:** This sub-section briefly describes about the IT environment of client's organization. This sub-section also describes size/type of information system (speed, memory capacity, network structure etc) workload on information system and changes in the program and results of previous audits, etc.

- **Purpose:** This sub-section is a short description of what components, functions and special programs were audited.

- **Scope:** The scope lists the period under review, the issues covered in each function and program, the locations visited and the on-site audit dates.

- **Methodology:** This section briefly describes sampling, data collection techniques and the basis for auditors' opinions. It also identifies any weaknesses in the methodology to allow the client to make informed decisions as a result of audit report.