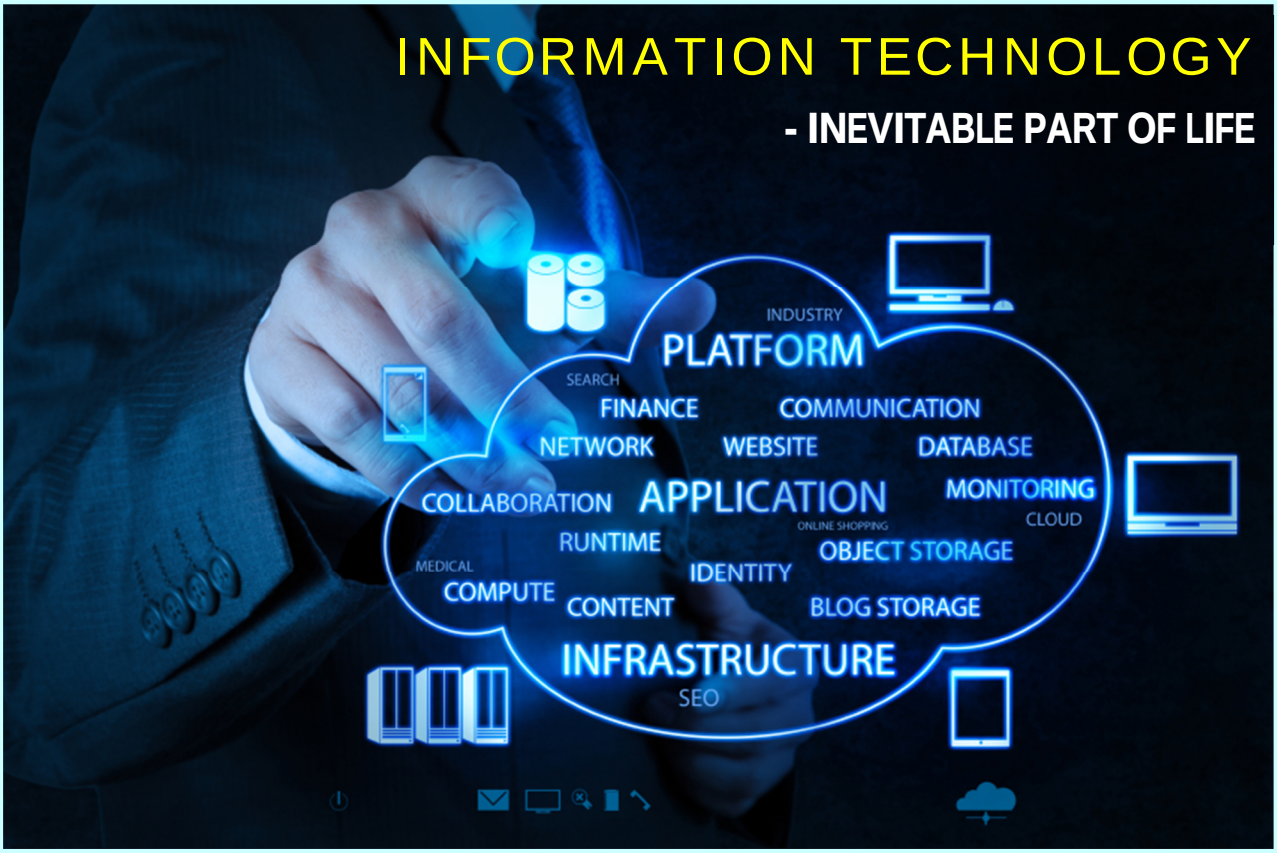


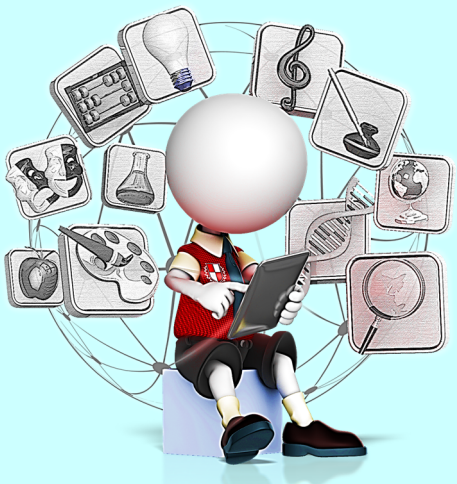
CA Final : Group – II

Paper – 6 – ISCA

Information System Control & Audit

Fast Track Notes

For - May 2017



We Need to Control Technology,
Otherwise, Technology will Control us.

VR Talsaniya
(CA. Vijay R. Talsaniya)

Contact : (+91) 8671866086
Email : ca.vrtalsaniya.com
Slide-share : VR Talsaniya
Linkedin : Vijay Talsaniya
Facebook : VR Talsaniya

Chapter – 1 : Governance & Management of ISs

Objectives of ISCA:

1) Identify & review IT Risks & controls
2) Assess Impact on organizational structure of technology integration
3) Understand & apply IT Best practices
4) Assess Information system acquisition, development and implementation strategy
5) Assess BCP of organization from Going concern perspective
6) Understand key Concepts of Governance, Risk and Compliance (GRC)
7) Understand how to perform Audit - collection and evaluation of evidence in IT environment

1. Explain - Key concepts of Governance

Ans.:

Various definitions related to governance:

A. Governance :

Stakeholders evaluate options set directions monitor compliance to meet objectives

B. Enterprise Governance :

Set of responsibilities exercised by board or executive management

For…

a. Providing strategic direction
b. Ensuring objective achieved
c. Risk managed property
d. Organization's resources are used responsibly

C. Corporate Governance :

A system by which a company / enterprise is directed & controlled to achieve the objective of increasing shareholder value by enhancing economic performance.

D. IT Governance:

A system by which IT activities in a company on enterprise are directed & controlled to achieve business objectives with the ultimate objective of meeting stakeholder needs.

2. What is the Relationship between Corporate governance and IT governance?

Ans.:

A. **Strategic alignment** of IT & business objectives is critical success factor
B. IT **provide inputs and information** to meet enterprise objective
C. **Objectives** of IT governance **is similar** to Corporate governance but with focus on IT
D. **Inseparable** relationship between both

3. What are the Benefits of Governance?

Ans.:

A. Relationship improvement among customers, business and internal relationship
B. Aligned decision making for IT principles
C. Achieving objective of enterprise by ensuring each element assigned with decision rights and accountability
D. Encouraging Desired behavior in the use of IT
E. Integrating desired business processes into enterprise
F. Overcoming limitations of the organizational structure

4. What are the Benefits of IT Governance?

Ans.:

A. Increased **value** delivered through enterprise IT
B. Increased user **satisfaction** with IT services
C. Increased **agility** in supporting business needs
D. Increased **management & mitigation** of IT related business risk
E. Increased **transparency & understanding** of IT's contribution to the business
F. Better **cost** performance of IT
G. IT becoming an **enabler for change**
H. **Improved compliance** with law, regulations & policies
I. More **optimal utilization** of IT resources

5. Explain - Governance Dimensions

Ans.:

A. Conformance Dimensions :
(Corporate Governance Dimension)

1) Focus on regulatory requirements - **Historic**
2) Covers areas of Role and composition of Board, Board committees
3) Regulatory requirements and standards are addressed in this dimension. Example Sarbanes Oxley Act of US and Clause 49 listing requirement of SEBI

B. Performance Dimensions :
(Business Governance Dimension)

1) Focus on strategy and value creation – **Forward Looking**
2) Helping the board to make strategic decisions, understand risk appetite
3) This dimension not governed by any standard

C. Comparisons :

1) Conformance dimension monitored by audit committee
2) No such dedicated mechanism for Performance dimension. It is the responsibility of full board

6. What are the Key Functions of IT Steering committees?

Ans.:

A. Long & short range IT plans in tune with enterprise objective
B. Measuring results of IT projects in terms of ROI
C. Size and scope of IT functions
D. Approve Deployment of major IT projects
E. Viable communication system between IT and its users
F. Approve Standard policy & procedures
G. Review the status of IS Budget and IT performance
H. Facilitates Implementation of IT security within enterprise
I. Report to the board of directors on IT activities
J. Decisions on key aspects of IT deployment

7. What are the Benefits of GEIT (Governance of Enterprise IT)?

Ans.:

A. IT Processes are **effective and transparent**
B. **Confirm Compliance** with legal and regulatory requirements
C. Consistent Approach **aligns** with enterprise governance approach
D. Governance **Requirement for board member** are met
E. IT related Decisions are **in line with enterprise objectives**

8. What are the Key practices for status of IT Governance determination?

Ans.:

A. **Who** makes IT Management related decisions? (Directing, Controlling etc.)
B. **What information** is required to make decision?
C. **What approach** is used for DM? OR How the decisions are made?
D. What **DM mechanisms** are required?
E. How the **exceptions are handled**?
F. How the IT governance results are **monitored & improved**?

9. Explain - Key practices of GEIT?

Ans.: (EDM)

A. **E**valuate governance system
B. **D**irect governance system
C. **M**onitor governance system

10. What are the Key practices to evaluate business value from IT?

Ans.: (EDM)

A. **E**valuate value optimization
B. **D**irect value optimization
C. **M**onitor value optimization

11. Which Key Metrics can be used for evaluating benefits realized from IT enabled investments?

Ans.:

Key metrics for value optimization monitor:

Business value is achieved by the benefit (in the form of 'Optimal value') to the business from the business processes and IT enabled investments at acceptable cost.

Metrics:

A. **% of IT enabled Investments** – where benefits monitored
B. **% of IT Services** – where benefits realized
C. **% of IT enabled Investments** – where benefits met /exceeded
D. **% of IT enabled Investments** – where IT cost & benefits defined
E. **Satisfaction survey** of key stakeholders
F. **% of IT services** – where **O**perational cost & benefits defined

12. Explain - Key Governance practices - Risk Management?

Ans.: (EDM)

A. **E**valuate – Risk Management
B. **D**irect – Risk Management
C. **M**onitor – Risk Management

13. What are the Best practices of corporate governance?

Ans.:

A. Assignment of responsibilities and decision making from individual to board of directors
B. Mechanism for interaction among board of directors and senior management
C. Implementing strong Internal control and risk management functions
D. Monitoring of Risk exposure in areas of conflict of interest
E. Incentives to senior management and employees in form of compensation, promotion
F. Information flow internally and to the public in appropriate manner

14. Explain - Enterprise Risk Management (ERM)

Ans.:

Definition of ERM:

"Enterprise Risk Management is process affected by entity's Board of directors and applied across the enterprise to identify potential events that may affect the entity and to manage risk within risk appetite and provide assurance of achieving entity objective.

15. What are the Components of internal controls as COSO?

Ans.:

(As per COSO – Same concept in Audit) – **CRC IM**

A. **Control Environment**:
   The control consciousness of organization i.e. atmosphere
B. **Risk Assessment**:
   Identify & analyze risks faced by an org. to manage them.
C. **Control Activities**:
   Actions to manage & Reduce risk assessed
D. **Monitoring**:
   Elements that ensure internal controls operate reliably over a time
E. **Information & Communication**:
   Information Identified, captured & exchanged in timely & appropriate form to discharge responsibility.

16. What are the Categories of Strategic Planning:

Ans.: (I – ERA)

A. **IS** Strategic plan
B. **E**nterprise Strategic plan
C. IS **R**equirements plan
D. IS **A**pplications & facilities plan

17. Which are the Enablers of IS Strategic Plan?

Ans.:

A. Business strategy of enterprise
B. How IT support business objective
C. Assessment of existing system
D. Inventory of technological solutions & current infrastructure
E. Enterprise Position on Risk
F. Need for senior management support, critical review

18. Which are the Enablers of IS Requirement Plan?

Ans.:

A. Data Syntax rules
B. Automated data repository and dictionary
C. Information Model representing business
D. Data Ownership and security classification
E. Information Architectural Standard

19. Explain - Key management practices for aligning IT strategy with Enterprise strategy?

Ans.:

A. **Understand** enterprise Direction
B. **Assess the Current** Environment, capabilities and performance
C. **Define the Target** IT capabilities
D. Conduct **Gap** analysis
E. **Define** the Road map and strategic plan
F. **Communicate** IT strategy and direction

20. Explain - Risk Management: (also covered in chapter – 4)

Ans.:

- ✓ IS Risks can be in the form inadequate disclosure, increasing electronic frauds etc.
- ✓ IT based Information system is subject to Inherent risks.
- ✓ *Inherent risks are risks which cannot be eliminated but can be mitigated by appropriate security*
- ✓ Risk management is 'Assessing risks' and 'Reducing to an acceptable level' through appropriate security/ controls.
- ✓ *Controls are classified as Preventive, Detective and Corrective* appropriate security/ controls assures that –
  A. **CIA** (Confidentiality, Integrity and Availability) of data is maintained
  B. Access to data is restricted to authorized users only
  C. Computer facilities are available at all times

21. What are the Sources of Risks?

Ans.:

Common sources are... (NEP TC MIH)

A. **N**atural events
B. **E**conomic events
C. **P**olitical Circumstances
D. **T**echnology & Technological issue
E. **C**ommercial & legal Relationship
F. **M**anagement activity & Control (Internal Factor)
G. **I**ndividual Activities
H. **H**uman Behavior

22. Explain - Reasons for Gap between Need to protect system and protection applied?

Ans.:

1) External dangers from **H**ackers
2) **I**nter connectivity of systems
3) **D**evolution of management & control
4) **E**limination of Time, Distance, Space constraints
5) Widespread **U**se of technology
6) Unevenness of technological **C**hanges
7) Growing potentials fir **M**isuse

23. Explain - Risk Management Strategies

Ans.:

A. **Turn back / ignore** – When very low impact
B. **Tolerate / Accept** – When minor, Periodical review required
C. **Terminate / Eliminate** – by Replacement
D. **Transfer / Share** – by Sharing with partner
E. **Treat / Mitigate** – Eliminate from the origin

24. Explain - Key Management practices - Risk Management:

(Check Q-12: if Key Governance Practices, than, Ans. = EDM)

Ans.:

A. Collect Data
B. Analyze Risk
C. Maintain Profile of Risk
D. Articulate Risk
E. Define Action Portfolio of Risk management
F. Respond to Risk

25. Explain - Key Metrics of Risk Management (RM)

Ans.:

A. % of **C**ritical business process covered by risk assessment
B. Numbers of IT related **I**ncidents not identified in risk assessment
C. % of **E**nterprise risk assessments
D. Frequency of **U**pdating risk profile

26. What are the Key Management practices of IT Compliance?

Ans.: (I O C O)

A. **Identify** External compliance **Requirement**
B. **Optimize** response to External **Requirement**
C. **Confirm** External **Compliance**
D. **Obtain** assurance of External **Compliance**

27. Explain - Key Metrics for assessing compliance with External laws?

Ans.:

A. Cost of IT non-compliance (settlement fines)
B. Reporting to the board of IT non-compliance
C. Non-compliance related to Agreement with IT service providers
D. Coverage of compliance assessment

28. Explain - Key Metrics for compliance with Internal Policies?

Ans.:

1) Incidents related to non-compliance to policy
2) % of stake holders who Understand policies
3) % of policies supported by effective Standards
4) Frequency of policies review

29. What are the needs for use of COBIT 5 by enterprises?

Ans.: GEIT Framework - COBIT 5 (**C**ontrol **OB**jective for **I**nformation & related **T**echnology)

Need for use of COBIT 5 by enterprises:

A. Development of Business focused IT solutions
B. Reduce IT related risks
C. Enterprise wide involvement in IT related activities
D. Value creation from use of IT
E. Compliance with Laws & regulations

30. Explain - 5 Principles of COBIT 5:

Ans.:

A. **Meeting** Stakeholders needs
B. **Covering** Enterprise End –to-End
C. **Applying** a Single Integrated framework
D. **Enabling** a Holistic approach
E. **Separating** Governance from Management

31. Explain - 7 Enablers of COBIT 5:

Ans.:

A. **Principles, Policies and Framework** - translates desired behavior into practical guidance for day-to-day management
B. **Processes** - describes organized set of practices to achieve certain objectives
C. **Organizational structure -** are key decision making entities in enterprise
D. **Culture, Ethics and Behavior** - of the individuals often underestimated as a success factor
E. **Information -** is pervasive throughout the organization
F. **Services, Infrastructure and Applications** - provides enterprise with information technology processing and services
G. **People, Skills and Competencies** - are linked to people and are required for successful completion of all activities and taking corrective decisions

32. What are the Components of COBIT 5?

Ans.:

A. **Framework** - Organize It governance objectives, good practices and links them to business requirement
B. **Process Description** – 'Reference process model' and 'Common language' for everyone in organization
C. **Control Objectives** – Provide set of high level requirements for effective control of each IT process
D. **Management guidelines** - Helps assign responsibilities, agree on objectives and measure performance
E. **Maturity Models** - Assesses maturity and capability per process and helps to address gaps

33. Explain - Benefits of COBIT 5

Ans.:

A. Enables It to be governed in Holistic manner for entire organization taking full end-to-end business
B. Comprehensive Framework enables enterprise in achieving objectives
C. Enables increased Business user satisfaction and clear policy development
D. Enables enterprise to create Optimal value from IT by maintaining balance between realizing benefits and optimizing risks levels
E. Enables enterprise to Manage IT related risks and ensure compliance
F. Generic Framework hence useful for enterprises of all sizes, whether Commercial, Non-profit or Public sector

34. Goals used to measure successful Implementation of GRC:

Ans.:

A. Redundant (extra) controls - Reduction
B. Control failures in key areas - Reduction
C. Expenditure related to Legal, Regulatory areas - Reduction
D. Overall time for audit of key business areas - Reduction
E. Streamlining of processes and time reduction through automation
F. Reporting of compliance issues and remediation in timely manner
G. Compliance status and key issues to senior management on real time basis

35. Several Key components evaluated by Internal auditor for Effective IT governance:

Ans.: (L O PR PC)

1) **L**eadership -
2) **O**rganizational structure –
3) **P**rocesses –
4) **R**isks -
5) **P**erformance Measurement -
6) **C**ontrols –

---- XXXX ---- XXXX ----

Chapter – 2 : ISs Concepts

1. What is information?

Ans.:

In simple term, Processed data = Information

Information is the data that has been processed into the form that is meaningful to recipient and is of real & perceived value in current and progressive decision.

2. Explain - Attributes of Information

Ans.: (A PM VRT C Frequently Quality of CRV)

A. Availability
B. Purpose / Objective
C. Mode & Format
D. Validity
E. Reliability
F. Transparency
G. Current / Updated
H. Frequency
I. Qualitative (Presentation, Timeliness, Place & Possession – Utility)
J. Completeness & Adequacy
K. Rate of Transmission
L. Value of Information (CBA – Cost Benefit Analysis)

3. Explain - Role of Information in Business

Ans.: Factors decide Information requirements

A. Operation Functions

Production, Finance& Marketing

B. Types of DM

Structured, Unstructured and Semi-Structured

C. Level of Business: (As follow)

No	Level	Info. Required	Role of Info.	Types of DM	Exp. of IS
1	**Top**	Strategic Info.	Essential for long term planning (Major Policy Decision) Exp. For Launching new product, 1. Customer buying habit , 2. Combination / Type 3. Location / Area 4. Price, Profit etc.	For Unstructured DM	EIS, DSS
2	**Middle**	Tactical Info.	1. Help in Smoothen implementation of decision taken by Top Mgt 2. Short term planning	For Semi Structured DM	MIS

3	**Bottom**	Operational Info.	1. For smooth running of day to day activity 2. Improve operational efficiency & effectiveness	For structured DM	TPS, PCS, ECS

4. What are the dimension / Value of Information?

Ans.: (EBT)

A. **Economic** –
Cost Benefit Analysis (Benefit of from Info. – Cost of deriving Info. = Net Benefit)

B. **Business** –
Different types of info. Used at difference level of management (as above)

C. **Technical** –
Concern for security of info, relating to DBMS, Storage, Process & Retrieval etc.

5. Explain - Types of Information

Ans.:

A. **External / Environmental Info.** –
Derived from outside the organizational boundary. Primarily from… **(MET-G)**
I. Major factors of Production
II. Economic trends
III. Technological Environment
IV. Government Policies

B. **Internal Info.** –
Derived from internal functions of the organization (Main source is TPS)

6. Explain - System

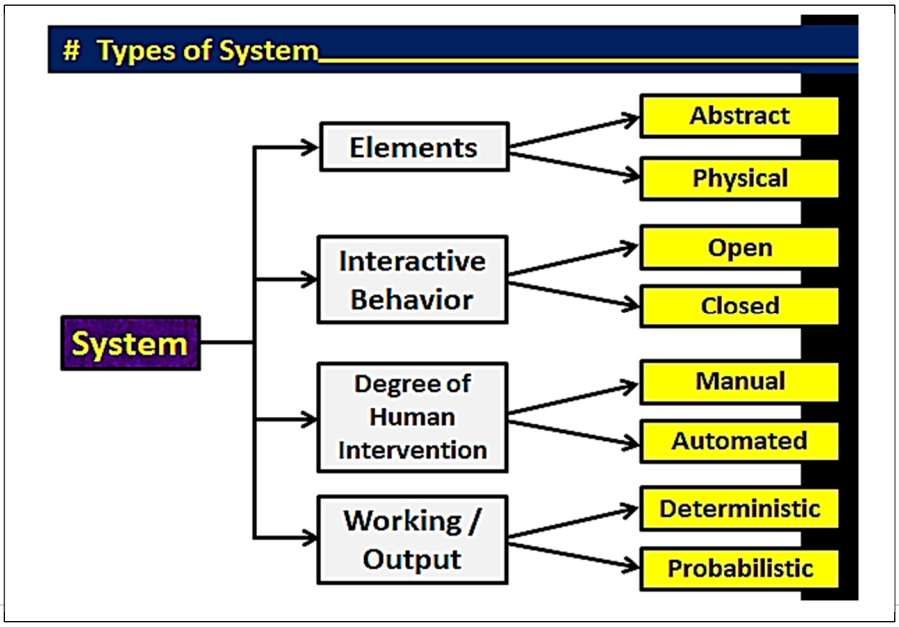
Ans.:

A system is a group of interrelated and interdepended components, working together, to achieve common goal of the system, by accepting inputs, processing it & providing desired outputs.

7. What are the Types of System?

Ans.:

There 8 types
Based on 4 bases



8. What are the types of system based on output from system?

Ans.:

Deterministic System:

- ✓ A deterministic system operates in a predictable manner wherein the interaction among the parts is known with certainty.
- ✓ If one has a description of the state of the system at a given point in time plus a description of its operation, the next state of the system may be given exactly, without error.
- ✓ **Example:-**
  A computer program, which performs exactly according to a set of instructions.

Probabilistic System:

- ✓ The probabilistic system can be described in terms of probable behavior, but a certain degree of error is always attached to the prediction of what the system will do.
- ✓ **Example:-**
  A set of instructions given to a human who, for a variety of reasons, may not follow the instructions exactly as given.

9. Sub-system & Supra System

Ans.:

Sub-system: A system is divided into smaller system (Decomposition Concept)

Supra System: A system immediately above a sub-system (Integration Concept)

10. Information System / Computer Based Information System (CBIS)

Ans.:

IS is a combination of people, HW, SW, Communication Devices, Data Sources , Network etc that processes data& information for specific purpose.

Components of CBIS

A. Peoples – IT Professional, Programmers, System Administration & Users
B. Computer System – HW & SW
C. Data
D. Network

11. Characteristics of CBIS

Ans.:

A. Includes no. of sub-system & cannot work in isolation
B. One sub system fails = whole system may fails
C. Sub system with other = interaction, for common goal
D. All system has common goal, even system designed and developed accordingly
E. Works in integration & common goal is more important than individual goal

12. Major area of computer based applications

Ans.:

A. Finance & Accounting
B. Marketing & Sales
C. HRM

D. Inventory / Stores Management
E. Production / Manufacturing

13. Applications of IS in business OR Vital roles in business firm

Ans.: i.e. to support..

A. An organization's Business Processes & Operations
B. Business DM
C. Strategic Competitive Advantages

14. To manage IS effectively & efficiently, Manager should have knowledge of following

Ans.:

Managers are not required complete understanding of complex, technologies, concepts & specific application but know knowledge…

A. Fundamental Concepts
B. Information Technology (Operation & Development of HW/SW/data etc.)
C. Business application of IT
D. Development Processes (Business IT solutions to the problems)
E. Management challenges

15. Difference of IS & IT

Ans.:

IT is sub system / component of IS, i.e. To produce, store, communicate & manage the information by using computer / CPU.

16. TPS – Transaction Processing System

Ans.:

- ✓ At the lowest level of management
- ✓ Manipulates data from business transactions
- ✓ Activities:
- ✓ Capturing, Processing, Generate Report & Processing of Queries

TPS – Component

1. Input, 2. Processing, 3. Storage 4. Output

17. Features of TPS (SAB-L)

Ans.:

A. Source of input from other system
B. Automation of basic operation
C. Benefits are easily measurable
D. Large volume of data

18. PCS – Process Control System

Ans.:

- ✓ Computer is used to control on going physical process
- ✓ Automatic decision for control (may be by AI)

19. ECS – Enterprise Collaboration System

Ans.:

This system uses a variety of technologies to help people work together.

It supports - Communication of ideas, share resources, Co-ordinate co-operative work efforts.

20. MIS – Management Information System

Ans.:

An integrated user-machine system designed for providing information to support Operational Control, Management Control & Decision Making (DM) functions in an organization.

21. Characteristics of effective MIS

Ans.:

A. Management Oriented
B. Management Directed
C. Computerized
D. Common Data Flow
E. Common Database
F. Sub-system concepts
G. Integrated
H. Long term / Heavy planning element
I. Need based system
J. Exception based (flexible for exception)

22. What are the misconceptions about MIS?

Ans.:

A. CBIS = MIS
B. Benefits of technologies
C. Study of MIS = use of computers
D. Any Reporting system = MIS
E. Accuracy in Reporting = Prime Importance of MIS
F. More Data = More Information
G. MIS = Management Technique
H. Implementation of organizational system & procedures
I. It is file structure

23. Prerequisites of effective MIS

Ans.:

A. Database
B. Qualified 'System & Management Staff'
C. Support from Top-M (Top Management)
D. Control & Maintenance of MIS

24. Evaluation of MIS (Points to be considered while evaluating MIS)

Ans.:

A. Examine flexibility to cope with expected / unexpected future change
B. View about – Capabilities & Deficiencies
C. Guiding – Appropriate authority about steps to be taken for maintenance of effective MIS

25. Constrains in the way operating MIS

Ans.:

A. Non availability of Experts
B. Co-operation from staff
C. Varied objective = not standard objective
D. Experts usually face the problem of selecting subsystem

26. Limitation of MIS

Ans.:

A. Quality of output is governed by quality of input.
B. MIS may not have requisite flexibility.
C. Less useful for unstructured / semi structured problem (non-programmed decisions)
D. MIS cannot provide tailor-made information packages
E. Considered only quantitative details
F. MIS is not a substitute for effective management
G. Hoarding culture = Reduce effectiveness
H. Changes in Top-M = Reduce effectiveness

27. DSS – Decision Support System

Ans.:

Computerized information System that supports 'Business & Organizational DM Activities'

28. Characteristics of DSS

Ans.:

A. Supports DM
B. Focuses on DM
C. Used for DM
D. Used for group DM
E. Flexible & adaptable
F. Extensive & evolve over a time
G. Can be used for 'Structured Problem' (Effective at Top-M)
H. User friendly
I. Easy to use

29. Components of DSS

Ans.:

1. Users, 2. Database, 3. Planning Language 4. Model Base

30. Examples of DSS in Accounting

Ans.:

A. Costing
B. Capital Budgeting
C. Capital variance analysis system
D. General DSS

31. Difference between DSS & Traditional MIS

Ans.:

No	*Points*	*DSS*	*MIS*
1	Focus	DM Process	Information requirement analysis
2	Used for	Unstructured / Semi-structured DM	Structured DM
3	Orientation	External	Internal
4	Flexibility	High	Relatively Low
5	Analytical	High	Low
6	Provide	Integrated tools, data models & language to users	Structured information to end users

32. EIS – Executive Information System

Ans.:

Used specifically by Top-M

The powerful focus of an EIS is due to the saying "what gets measured gets done."

33. Characteristics of EIS

Ans.:

A. Future orientation
B. Informal source
C. Lack of structure
D. Low level of details
E. High level of uncertainly

34. Content of EIS

Ans.:

Whatever is appropriate to include in EIS (interesting to executives)

For that we have 6 Principles to guide design of EIS:

A. Easy to understand & collect
B. Based on balanced view
C. Encourage to Management & Staff – to share Ownership
D. Evolve to meet changing demands
E. Performance indicator must reflect 'Everyone's contribution'
F. Information available to Everyone

35. OAS – Office Automation System

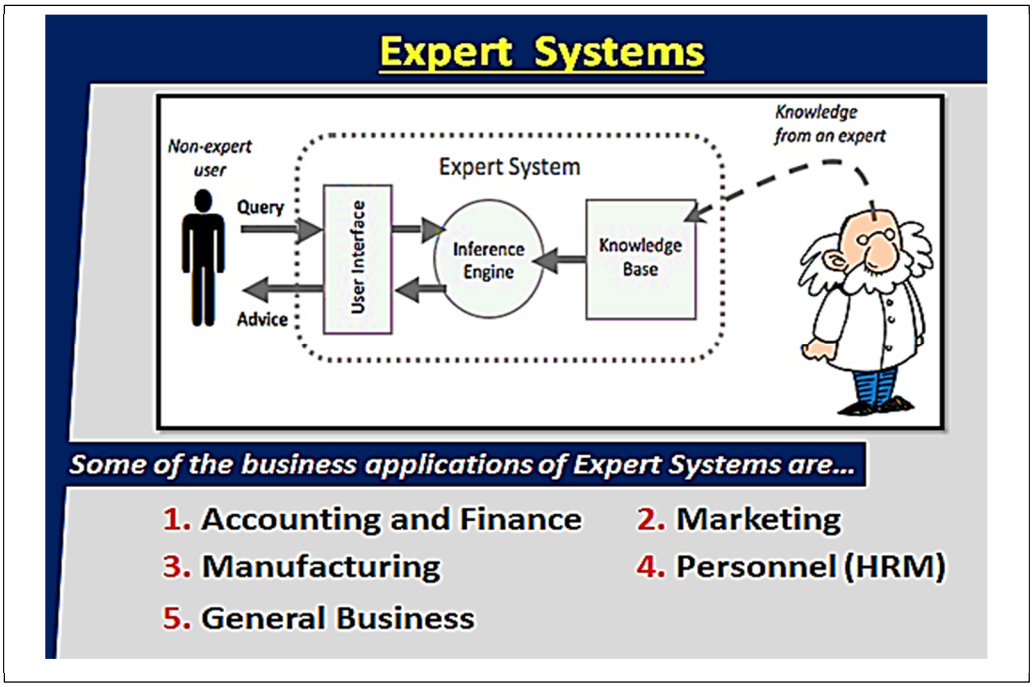
Ans.:

Activities for OAS

A. Document Capture
B. Document Creation
C. Receipts & Distribution i.e. Correspondence
D. Filling, Search, Retrieval & Follow up
E. Calculations
F. Recording Utilization of Resources

36. ES – Expert system

- ✓ An Expert System is highly developed DSS that utilizes knowledge generally possessed by an expert to share a problem.
- ✓ Expert Systems are software systems that imitate the reasoning processes of human experts and provide decision makers with the type of advice they would normally receive from such expert systems.



Need of Expert System:

1. **Expert labor is expensive** and scarce. Knowledge workers employee, who routinely work with data and information to carry out their day-to-day duties are not easy to find and keep and companies are often faced with a shortage of talent in key positions.
2. Moreover, **no matter how bright or knowledgeable** certain **people are**, they often can handle only a few factors **at a time**.
3. Both these limitations imposed by **human information processing capability** and the **rushed pace** at which **business** is conducted today put a **practical limit on the quality of human decision making** this putting a **need** for expert systems.

37. ERP – Enterprise Resource Planning

Ans.:

- ✓ Now, firms are replascing legacy stems with newer client / server based solutions
- ✓ Main feature is integrated software.
- ✓ ERP is one of the latest high end solutions that seek to streamline & integrate operation processes & information flows in the company to synergize five major resources of organization i.e. Men, Money, Market, Machine & Material.
- ✓ ERP is ***a fully integrated business management system*** that integrates the core business & management processes to provide an organization a structured environment in which decisions about demand, supply, personnel, finance, logistics etc. are fully supported by **Accurate & Reliable Real time information**.
- ✓ An ERP system is multi-module software that integrates all business processes & functions of the entire enterprise in "**A single Software System**" using **a single integrated database**.
- ✓ **Modules of ERP**:
  1. Finance & Accounting System
  2. Production
  3. Marketing
  4. Payroll
  5. Quality Control
  6. CRM – Customer Relationship Management
  7. Logistic & SCM – Supply Chain Management
  8. Cost Controls & Investment Management etc.
- ✓ **Components of ERP Module**:
  1. Software Component
  2. Process Flow
  3. Customer Mindset
  4. Change Management

---- XXXX ---- XXXX ----

Chapter – 3 : Protection of IS

1. What is information security?

Ans.:

The protection of valuable assets against loss, damage & disclosure

Where valuable assets = Data /information recorded, processed, stored, shared, transmitted / retrieved from an e-medium.

i.e. Security of data / info. While transmitted through e-medium.

2. What is the Information security objective?

Ans.:

The protection of the interest of those relying on information &

Protect 'the IS & Communications that deliver information' from harm resulting from failure of CIA – Confidentiality, Integrity & Availability.

3. What information is sensitive? OR

Provide best examples of critical information for organization.

Ans.:

A. Strategic Plans
B. Business Operations
C. Finance

4. What is Information Security Policy?

Ans.:

- The statement…
  of intention by management about
  'How to protect a company's information assets'.
- Should be in written form.
- This is a formal statement of Rules.
- Does not specify technologies / specific solutions but it defines "set of intentions & conditions that help to protect company's information assets & its ability to conduct business".
- The essential foundation for an effective & comprehensive information security program.

5. How to implement policy in any organization?

Ans.:

Tools to implement policy in any organization… **(SGP)**

A. Standards (Uniform & Compulsory)

Specify technologies & methodologies to be used to secure systems

B. Guidelines (Best Practices & Optional)

Help in smooth implementation of information security policy & Standards

C. Procedures (Detailed Steps to be followed)

More detailed steps to be followed to accomplish particulars security related tasks

Such procedure normally assists in implementing applicable Info. Sec. Policy

Operational & Compulsory instructions to be followed

6. For what aspects policy is required?

Ans.:

A. Use of IS resources
B. Physical Security
C. Data Security
D. Online Security
E. Micro computer use
F. Review, evaluate & purchase of Hardware & Software
G. System Development Method
H. Application Program Changes

7. What is the objective of controls?

Ans.:

To reduce / if possible eliminate
The causes of the exposure to potential loss
i.e. **A.** Error & Omission
B. Improper Authorization & Accountability
C. Inefficient Activity

Two Main Purposes:

A. Outline policies of the organization as laid down by Management
B. A benchmark for evaluation 'Whether control objectives are achieved?'

8. Which controls is lack in CBIS?

Ans.: Lack of controls in CBIS:

A. Lack of Management understanding of IS Risks
B. Absence / inadequate 'Framework for IS controls / general controls
C. Absence of / Weak IS controls / general controls
D. Lack of awareness & knowledge of IS controls / general controls
E. Complexity of implementation of controls in distributed computing environment
F. Lack of control feature / their implementation in highly technology driven environment
G. Inappropriate technology implementation / inadequate security functionality in technologies implemented.

9. Explain - Types of control

Ans.:

Based on objectives of controls...

Types	Preventive Controls	Detective Controls	Corrective Controls
Meaning	Designed for / to **Prevent from Occurring** – Any error / omission & malicious act	Designed for / to **Detect & Report** – Any error / omission & malicious act	Designed for / to **Identify & Reduce impact / Correct** – Any error / omission & malicious act

Characteristics	A. Clear-cut understanding of vulnerabilities of the assets B. Probability of threats C. Prior for controls	A. Identify in progress B. Understanding of lawful activity C. Report unlawful D. Interaction with preventive & corrective controls E. Surprise check	A. Identify cause of problem B. Provide Remedy / medicines C. Reduce Impact D. Correcting Error E. Modify system for future F. Feedback from Preventive & Detective Controls
Example	A. Firewall B. Password C. Antivirus SW D. Qualified Staff E. Segregation of duty F. Employee training	A. Hash total B. IDS C. BRS D. Variance Analysis E. Audit F. Monitoring	A. BCP & DRP B. Re-run procedure C. Back-up procedure
Compensatory Controls			
Meaning	A. Designed to reduce probability of threats B. Based on "Cost of lock of asset should not be more than value of asset" i.e. implement **not appropriate control but compensatory measure** in this case, Due to difference constraints. C. Not as effective / efficient as Appropriate control		

Based on objectives of Nature of IS Resources…

A. Environmental Controls
B. IS Operational Controls
C. IS Management Controls
D. SDLC Controls
E. Physical Access Controls
F. Logical Access Controls

Based on objectives of Nature of function…

A. Internal Accounting Controls
B. Operational Controls
C. Administrative Controls

10. What are the major control techniques in organization?

Ans.:

A. Organizational Controls
B. Management Controls
C. Financial Controls

D. Data Processing Environment Controls
E. Physical Access Controls
F. Logical Access Controls
G. SDLC Controls
H. BCP Controls
I. Application Controls

11. Explain - Job Descriptions

Ans.:

- It establish…
  A. Instructions on "How to do the job?"
  B. Policy define the authority of the employee.
- It communicate "Management's specific expectation from job performance".
- All jobs must have a current documented job description readily available to employee
- Establish responsibility & accountabilities.

12. What is 'Segregation of duties'?

Ans.:

A. Common control technique aimed at "**Separating Conflicting Job Duties**" (i.e. Distribution of work responsibilities – ***Maker cannot be checker***)
B. Main purpose – to prevent / detect errors / irregularities, serves check on work done by others, make collusion necessary to commit a fraud.
C. Organizational controls structures should be designed in a manner that ensure 'Highest level of separation of duties'.
D. Factors to be considered –
   I. Nature of business operations
   II. Managerial policy
   III. Organizational structure with job description
   IV. IS resources deployed

13. Explain - Management controls

Ans.: Management controls shall include…

A. Responsibility
B. An official IT Structure
C. An IT Steering Committee

14. Explain - Financial Controls

Ans.:

A. Authorization
B. Budgets
C. Documentation
D. Cancellation of Documents
E. Input / Output variation
F. Serially numbered Docs (Sequentially)
G. Safekeeping

H. Supervisory Review
I. Segregation of Duties
J. Dual Controls (2 people have Simultaneously access on an asset)

15. What is Audit Trails?

Ans.:

Audit trails are logs (i.e. chronological list of the activities performed) that are designed to record activity at the system, application & user level.

It is type of detective controls and generally, used in every organization.

16. Who are the members of Security Policy?

Ans.: Comprises of…

A. **Managerial** – Management member, who have budget & policy authority
B. **Technological** – Technical group, who know what can / cannot be supported
C. **Legal** – Legal Expert, who know the legal ramification of various policy changes

17. Explain - Types of Security Policy

I) **User Security Policy** ***(i.e. for secure use of the system by users)***

Set Responsibilities & Requirements and provide reference to all users

A. User Security Policy

B. ***Acceptable Usage Policy*** - Set out the policy for acceptable use of email & internet services

II) **Organizational Security Policy** ***(i.e. for security of organizational information systems, network & information resources)***

A. Organizational Information Security Policy

Group Policy for security of information assets & IT system processing information and it is main IT security policy documents

B. Network & System Security Policy

Detailed policy for system & network security and apply to IT department users.

C. Information Classification Policy

Policy for classification of information

III) **Conditions of Connection**:

Group policy for connecting their network

Applies to all organization connecting to group & relates to conditions that apply to different systems of supplier.

18. What are the components of security policy?

Ans.:

A. Security policy infrastructure
B. Security organization Structure
C. Description of technologies & computing structure
D. Inventory & classification of assets
E. Physical & Environmental security
F. Identity Management Access Control
G. SD & Maintenance Controls

H. IT Operations Management
I. IT Communications
J. BCP
K. Legal Compliances
L. Security policy document maintenance & compliance requirement
M. Purpose & scope of document & intended audience
N. Monitoring & Auditing Requirement
O. Underlying Technical Policy
P. Incident Management – Response & Reporting

19. What is IS Controls / Internal Controls?

Ans.:

Control = Policies, Procedures, Practices & enterprise structure that designed to provide reasonable assurance that

A. The business objective will achieved
B. Undesired events are prevented / detected & corrected.

20. Explain - Impact of technology on internal controls

Ans.:

(RMC Access SAP)

A. **R**ecord keeping
B. **M**anagement Supervision & Review
C. **C**oncentration of programs & data (Centralization)
D. **Access** to Assets & Records (Physical & Logical Controls)
E. **S**egregation of Duties
F. **A**uthorization Procedure
G. **P**ersonnel (Competent & Trust worthy – Appropriate skills & training required and know "What they are doing?")

21. What are the Components of internal controls?

Ans.:

(As per COSO – Same concept in Audit) – **CRC IM**

A. **Control Environment**:
The control consciousness of organization i.e. atmosphere
B. **Risk Assessment**:
Identify & analyze risks faced by an org. to manage them.
C. **Control Activities**:
Actions to manage & Reduce risk assessed
D. **Monitoring**:
Elements that ensure internal controls operate reliably over a time
E. **Information & Communication**:
Information Identified, captured & exchanged in timely & appropriate form to discharge responsibility.

22. Explain - Boundary Controls

Ans.:

A. **Major Boundary Controls** – ACM: Access Control Mechanism

Access control is implemented with ACM, link authentic user & access to authorized resources they are permitted.

ACM = IAA

No	IAA	What You	Class of info.	Example
1	Identification	Know?	Personal Info.	Name, DOB, PW, Pin
2	Authentication	Are?	Personal Characteristics	Voice, Signature, Fingerprint
3	Authorization	Have?	Personal Objectives	ID Card, Badge, Key, Smart Card

B. **Boundary Control Technique**:

I) Cryptography

It is a process of Transforming '**data** into **codes / cypher text**' that are meaningless to anyone, who does not possess the authentication to access the resource/file.

(i.e. encryption & decryption)

II) Password

III) Identification

IV) Biometric Card

C. Input Controls

Ensuring accuracy & completeness of data & instruction input entered into an application system

Those controls are 'Preventive in nature' and called 'Front end application controls'.

D. Processing Controls

Perform validation checks to identify errors during process and detective in nature

Ensure accuracy & completeness of data being processed.

Generally, this control enforced by DMBS.

E. Output Controls

Ensure data delivery to users will be preventive, formatted & delivered in consistent & secured manner and ensure CIA of data.

F. Database Controls

Designed to protect integrity of DB, when application software acts as interface, to interact, between user & DB.

I) **Update Controls** –

All record processed, sequence check, maintain suspense account and etc.

II) **Report Controls** –

Print run to run control totals, standing data (updated), Existence / recovery controls, Print suspense account and etc.

Chapter – 3 : Protection of IS

23. Explain - Information Classification

Classification is based on sensitivity or confidentiality of information and not based on value or cost of information.

No	Class	Meaning	Control / Security Req.	Example
1	Top Secret	That can cause serious damage to organization, if lost / made public	Highest Level	Formula of Coca-Cola
2	Highly Confidential	Critical for ongoing business operation & can cause serious impediment (Slow down) if share around organization	Very high	Product related decision etc.
3	Proprietary	Relating to procedures, operational, routine works, project plans, designs etc. (only for authorized personal)	High	Payroll Data
4	Internal Use only	Cannot be circulated outside the organization & if disclosed, will created inconvenience to organization but not result in financial loss	Normal	Manager going to retire in future
5	Public Docs	Information published in public domain i.e. (of public use etc.) [Control - only for integrity is Req.]	Minimal / No Control	B/S, P&L, FS etc.

24. What are the data integrity controls?

Ans.:

They protect data from accidental / malicious – alternation / destruction & provide assurance to user that information meets expectations about its quality & integrity.

Categories of integrity controls:

A. Source data controls
B. Input validation routines
C. Online data entry controls
D. Data processing & data storage controls
E. Output controls
F. Data transmission controls

25. What are the data integrity policies?

Ans.:

A. Virus signature updating (Automatic)
B. Software testing
C. Division of environment
D. Offsite backup storage (older than 1 month to permanent storage)
E. Quarter & year-end backup
F. DRP – Disaster Recovery Planning

26. Explain - Logical Access Control

Ans.:

LAC are implemented to ensure that only authorized users have access to system, data & programs, So as to safeguard information from unauthorized disclosure, modification & use i.e. maintain CIA.

Steps to be followed = ACM = IAA

27. What are the Logical Access paths in any system?

Ans.:

A. Online Terminals:

- For access has to provide valid login ID & PW
- Additional authentication mechanism is also required
- Operator Console:
- The crucial place where any intruder can play havoc, therefore, must be restricted.
- Keep it at location = visible to all + accessible by only authorized personnel

B. Dial-up Ports:

- User at one location can connect remotely to another computer present at unknown location via telecommunication media
- Modem act as interface between remote terminal & telephone line.
- Security is achieved by providing ID & PW for access.

C. Telecommunication Network

- It is a number of computer terminals, PC etc. are linked to host computer through network / telecommunication lines.
- That can be private / public & security required = same as in online terminals.

28. Explain - Technical Exposure (need to remember all the points)

Ans.:

i.e. ***Unauthorized implementation / modification of data & SW.***

i) **Data Diddling** –

- ✓ Changing data **before / as & when** entered into the system
- ✓ Limited technical knowledge required
- ✓ Worst Part = Occurs before computer security can protect data

ii) **Bombs** –

- "A piece of bad code" deliberately planted / entered by insider / supplier of software.
- When gets triggered – causing the damage immediately but cannot infect other programs.

A. Time Bomb: (Triggered by Time)

- Computer clock initiates it.
- Time bomb causes perverse activities. i.e. disruption of computer system, modification or destructions of stored information etc on particular date & time.

B. Logical Bomb: (Triggered by Combination of events)

- Activated - by combination of events.

iii) **Trojan Horse**:
- ✓ Bomb but no need to be triggered = Trojan Horse
- ✓ Malicious programs hidden under any authorized program
- ✓ Or else "**illicit coding in legitimate program**"
- ✓ Hide in host program & do not damage host program
- ✓ Cannot copy themselves to other software or program but can be transferred to other system only if unsuspecting user copies the Trojan.

iv) **Worms**:
- ✓ **Does not require host program like Trojan / Bomb**
- ✓ Therefore, Worm program copies itself to another machine on network.
- ✓ Since, it is standalone program = detected easily.
- ✓ Sabotage (Deliberately Destroy) the system & they can also be used to perform some useful task s (like, check connectivity of the network)

v) Rounding Down: (10032.05 = 10032)
- ✓ Small **fractions of denomination** & transfer to authorized account (rarely noticed)

vi) Salami Techniques: (10032.05 = 10030)
- ✓ Slicing of small **amount of money** (here, last few digits – Rounded off)

vii) Trap Doors (Back Door):
- ✓ They are exists "**out of an authorized program**" & allow insertion of specific logic, such as program interrupts that permit a review of data.
- ✓ They also permit access to unauthorized logic in program.

29. What is Asynchronous Attacks (AA)?

Ans.:
- ✓ Generally on telecommunication lines, numerous transmissions must wait for clearance of line before data being transmitted.
- ✓ Data that are waiting to be transmitted are liable to unauthorized access called AA.
- ✓ AA is Hard to detect because very small.

Forms:
A. Data leakage
B. Wire Tapping
C. Piggybacking – (Unauthorized person behind authorized person in Org.)
D. DOS – Denial of Service Attack

30. Explain - Computer Crime Exposure

Ans.:
A. Financial loss
B. Legal repercussions
C. Loss of credibility (Consequence)
D. Blackmail / industrial espionage – Process to learn secret info. With illicit purpose
E. Disclosure of confidential / sensitive / embarrassing info.
F. Sabotage
G. Spoofing (Steal identity of other)

31. What are the Logical access controls across the system?

Ans.:

A. User Access Management –

- ✓ User Registration,
- ✓ Privilege Management,
- ✓ User Password Management,
- ✓ Review of user access rights

B. User Responsibility –

- ✓ Password use,
- ✓ Unattended user equipment

C. Network Access Controls –

- ✓ Policy on use of network services,
- ✓ Enforced path,
- ✓ Segregation of networks,
- ✓ Network connection and routing control,
- ✓ Security of network services

D. OS Access Controls –

- ✓ Automated terminal identification,
- ✓ Terminal log-on procedures,
- ✓ User identification and authentication,
- ✓ Password management system,
- ✓ Use of system utilities,
- ✓ Duress alarm to safeguard users,
- ✓ Terminal time out,
- ✓ Limitation of connection time

E. Application & Monitoring System Access Control –

- ✓ Information access restriction,
- ✓ Sensitive system isolation,
- ✓ Event logging,
- ✓ Monitor system use,
- ✓ Clock synchronization

F. Mobile Computing

G.

32. Explain - Physical Access Controls

Ans.:

Control over tangible resources & intangible stored in tangible media.

Issues & exposures:

Results of accidental / intentional violation of access path...

A. Abuse of data processing resources
B. Blackmail
C. Embezzlement

D. Damage / theft to equipment / document
E. Public disclosure of sensitive information
F. Unauthorized entry

33. Explain concept of Access Control Mechanism (ACM).

Ans.:

Associates with identify & authorize the users, the resources they are allowable to access & action privileges.

A. Identification

Users have to identify themselves + intent request for usage of system resources

B. Authentication

User must authenticate & mechanism must authenticate itself

C. Authorization

Check user request resources are allowed to access, then provided access.

Two approaches:

I) Ticket Oriented Approach:

- Assigns a ticket for each resource they are permitted to access.
- Operates by row in matrix
- Holds action privileges + Resources
- Advantage = Run time efficiency, can be used for large number of users efficiently.

II) A List Oriented Approach:

- Associates with each resource a list of users who can access the resources & privileges.
- Allows efficient admin of capabilities
- Large number of users then = inefficient (i.e. for small no. of users)

34. What are the Physical Access Controls?

Ans.:

i. Locks on doors

A. Cypher lock

- Push button panel
- Computer coded with person's handprint

B. Bolting Door Locks – Open by only Metal key + Avoid to be duplicated

C. Electronic Door Locks

Gain:

i) Identity specie individual
ii) Restricted to specific area + specific hours
iii) Degree of duplication
iv) Deactivate on termination / stolen etc.
v) Accounting & Provide card = IMP part of admin.

D. Biometric Door Locks

ii. Physical Identification Medium:

PIN, Plastic Card, Identification Badges

iii. Logging on Facilities:

Manual Logging, Electronic Logging

iv. Other means of Controlling Physical Access –

Video Cameras, Security Guards, Controlled Visitor, Bonded Personnel, Dead Main Doors, Non-Exposure of Sensitive Facilities, Computer Single Entry Point, Alam System, Perimeter Fencing, Control of out of hours of employee, Secured Report/Document Distribution Cart.

35. What is cyber fraud?

Ans.:

Fraud enabled by technology = cyber fraud

With the advancements in the technology, cyber frauds are also increasing day-by-day across the world.

One of the **major reasons behind the rise of such frauds** are:

- ✓ Failure of internal control system,
- ✓ Failure of organizations to update themselves to new set of risk, and
- ✓ Smart fraudsters: These are people who are able to target the weaknesses in system, lacunae's in internal controls, even before the organization realizes that such gaps are there.

36. What are the major techniques to commit cyber fraud?

Ans.:

A. Hacking – *White hat hacker*
B. Cracking – *Black hat hacker*
C. Phishing
D. Spoofing / Masquerading / impersonation
E. Data Digging
F. Data Leakage
G. DOS – Denial Of Service
H. Time / Logical Bombs
I. PassWord Cracking
J. Rounding Down
K. Slami Technique
L. Severing / Dumpster Diving / Data Dumping
M. Social Engineering Techniques
N. Super Zapping
O. Trap Door etc.

---- XXXX ---- XXXX ----

Contact : (+91) 8671866086
Email : ca.vrtalsaniya@gmail.com
Slide-share : VR Talsaniya

Chapter – 4 : BCP & DRP

Chapter covers following topics...

A. **DRP – Disaster Recovery Planning**
B. **CM / IM – Crisis Management / Incident Management**
C. **BCP – Business Continuity Planning**
D. **BCM – Business Continuity Management**

---

1. What is DRP?

Ans.:

Disaster = Event which is very destructive

DRP = Technologies aspect of BCP

i.e. the advance planning & preparation ...
Necessary to minimize losses &
Ensure continuity of critical business function of organization
in the event of disaster.

2. What are the components of DRP (Plans of BCM / BCP / DRP)?

Ans.:

DRP = Combination of 4 plans

Emergency Plan + Backup Plan + Recovery Plan + Test Plan

A. Emergency Plan:

Specify the actions to be undertaken immediately, when disaster occurs.
Management must identify those situations that require the plan to be invoked.
Covered four aspects...

i) Person to be called & notified
ii) Actions to be taken
iii) Evaluation Procedure
iv) Return (to business Place) Procedure

B. Backup Plan:

i) Type of backup
ii) Frequency (i.e. period) of backup
iii) Procedure for backup
iv) Location of backup resources
v) Site – Where resource can be assembled & operation can continue
vi) Personnel – Responsible for gathering backup
vii) A time frame for recovery of each system

Types of backup:

i) **Full Back up**:
- ✓ Backup contains "**Every file in backup set** ".
- ✓ Large amount of time & space required + expensive than other
- ✓ Restoration of data is faster.

ii) **Differential Back up**:
- ✓ Backup contains "**That all files changed since LAST FULL Backup**".
- ✓ Faster & Economic than full backup and most efficient one.

iii) **Incremental Back up**:
Backup contains "**That all files changed since LAST ANY TYPE of Backup**".
i.e. last full backup / differential backup / incremental backup.
It is most economical but difficult to restore & take little bit more time.

iv) **Mirror Backup**:
It is full back up as name suggest.
Except: Not compressed in Zip & Not password protected.

Alternate Processing Facilities Arrangement / Site:

i) Cold Site: (0%)
(When we can tolerate downtime)
Need to install all facilities on the event of disaster.
No mainframe will be installed by organization.

ii) Worm Site: (50%)
Cold site + Hardware facilities installed
i.e. installed hardware that might be difficult to obtain / install (on disaster).
It is intermediate level of backup.

iii) Hot Site: (100%)
(When faster recovery is critical)
All hardware, Software, Data & Supplies = Installed = Ready to use.
It is most expensive one.
Generally, it is shared with other organization.

iv) Reciprocal Agreement:
Two / more organization - Agree to provide back facilities to each other on the event of disaster.
Cheap but both should have sufficient capacity for the same.

v) 3rd Party Arrangement / Outsourced:
Must have contract for following…
A. How soon site will be available
B. No. of organizations – allowed concurrent use
C. Priority to be given
D. Time period – site can be used
E. Condition for use of site
F. Facilities & Services – that will make available
G. Controls will be placed.

Contact : (+91) 8671866086
Email : ca.vrtalsaniya@gmail.com
Slide-share : VR Talsaniya

C. Restore Plan:

Setout – procedure to restore full is capabilities.

I) Identify recovery committee – responsible for recovery
II) Specifies the responsibilities of committee & guidance on priorities to be followed
III) Members of committee – understand their 'Responsibilities'
IV) Might indicate – 'Applications are to be recovered first'

D. Test Plan:

The plan = still unfamiliar, need to test!!!

Therefore, final step = Test the DRP.

Purpose of test –

i) To identify difficulties in all above 3 plans
ii) Readiness of organization & its personnel for facing disaster.

It must enable organization –

i) To simulate effect of disaster
ii) Specify criteria by which 3 plans results satisfactory.

But Management may be unwilling for periodically test –

i) Daily operation disrupted
ii) Test = may results Real Disaster

3. What is Crisis Management / Incidental Management Planning?

Ans.:

CM/IM means the overall co-ordination of organization's response to a crisis in effective & timely manner with a view to avoiding / minimizing damage to organization's profitability, reputation & ability to operate.

4. Explain - Risk Management (From Chapter – 1)

Ans.:

RM = Process of identifying & assessing risk, taking steps to reduce risk to the acceptable level & maintaining that level.

Process = Risk Assessment Procedure...

A. Identify information assets & category of information
B. Valuation of that assets
C. Identify vulnerability & threats
D. Risk Assessment = Probability of Occurrence + Potential Loss
E. Strategies for Risk Management:
   i. **Turn back / ignore** – When very low impact
   ii. **Tolerate / Accept** – When minor, Periodical review required
   iii. **Terminate / Eliminate** – by Replacement
   iv. **Transfer / Share** – by Sharing with partner
   v. **Treat / Mitigate** – Eliminate from the origin

5. **What is Asset?**

Ans.:

Asset = Something of value to organization.

Include any of the following…

i. Value to organization
ii. Not easily replaceable
iii. Organization's corporate identity & without which organization may threatened
iv. Data classification of these asset – Top Secret OR Highly Confidential OR Proprietary

6. **What is Vulnerability?**

Ans.:

Vulnerability = Inherent weakness in system safeguards that exposes the system to threats.

Any one of the following condition…

Allow attackers

i. To execute commands as another user
ii. To access data that is contrary (Unauthorized)
iii. To pose as another entity (Spoofing)
iv. To conduct DOS (Denial of Service – Attack)

7. **What is Threat?**

Ans.:

It is an event that exploits the vulnerability of asset to cause serious damage to asset.

i.e. Any entity, circumstances / event through, unauthorized access, destruction, modification, DOS etc.

It has capability to attack on a system with intent to harm.

Asset & threats are closely correlated without target asset threat cannot exist.

8. **What is Likelihood / Pi of threat?**

Ans.:

Likelihood of threat occurring is the "Estimation of Probability (Pi) that the threat will succed to achieve undesirable event

i.e. Pi of threat materialized.

9. **What is Exposure (i.e. impact)?**

Ans.:

Extent of loss the organization has to face when a risk / threat materialized

Not just immediate impact but a "Real Harm" long run, also.

10. **What is a Risk?**

Ans.:

Risk = The potential harm caused if a particular threat exploits the vulnerability to cause damage to the asset

Risk Analysis = **The process** of **identifying** security risks & **determining** their magnitude & **impact** on organization.

Risk Assessment = Procedure as already done above

11. What is Countermeasure?

Ans.:

Action, procedure, technique / other measure that "**Reduces the vulnerability of component or system is countermeasure**".

12. What is Residual Risk?

Ans.:

Any risk still remaining after the counter measure analyzed & implemented = Residual Risk

13. Explain - Sources of risk

Ans.:

Most important step of risk management to identify sources of risk
i.e. area from where risk can occur.

Common sources are... (NEP TC MIH)

A. **N**atural events
B. **E**conomic events
C. **P**olitical Circumstances
D. **T**echnology & Technological issue
E. **C**ommercial & legal Relationship
F. **M**anagement activity & Control (Internal Factor)
G. **I**ndividual Activities
H. **H**uman Behavior

14. Explain – Business continuity Planning (BCP)

Ans.:

- ✓ It is creation & validation of "A practical logistical plan"
- ✓ **For how an organization will...**
  - A. Recover & restore partially / completely
  - B. Interrupted critical functions (CBF)
  - C. Within predetermined time after disaster / extended disruption.
- ✓ Plan = for running business under stressful & time compressed situations.
- ✓ Plan lays out steps to be initiated on occurrence of disaster, combating (fight) it & returning to normal operations.

15. Explain - Objectives & Goals of BCP

Ans.:

A. Provide safety & well-being of people on premise on disaster
B. Critical business lines & functions
C. Continue Critical Business Operations
D. Reduce duration of serious disruption to operation & resource
E. Reduce immediate damage & losses
F. Facilitate effective Co-Ordination of recovery tasks
G. Reduce complexity of recovery efforts / tasks.

Contact : (+91) 8671866086
Email : ca.vrtalsaniya@gmail.com
Slide-share : VR Talsaniya

16. What are the goals of BCP?

Ans.:

A. Identify "Weakness" & implement "A disaster Prevention Program"
B. Reduce duration of a serious disruption to business operations
C. Facilitate effective Co-Ordination of Recovery Tasks
D. Reduce Complexity of Recovery Tasks

17. Explain - Phases of BCP

Ans.:

A. Pre-planning Activities (Understand – Existing & Projected System)
B. Vulnerabilities Assessment & General Definition Requirement
C. BIA
D. Detailed Definition of Requirement
E. Plan Development
F. Testing Program
G. Maintenance Program
H. Initial plan testing & plan implementation

18. Explain - Business Impact Analysis (BIA)

Ans.:

Essentially, a means of systematically assessing the potential impact resulting from various incident / event / disaster…

A. Identify critical system, process & functions
B. Assess economic impact of incident & disaster that result in denial of access to the system, services & facilities.
C. Assess "Pain Threshold = Length of time Business unit can survive without system, services & facilities"
D. Identity & understand – The degree of potential loss

Steps:

i) Identify organizational risk
ii) Identify critical business function
iii) Identify + Quantify threats / risks to critical business functions (CBF)
iv) Identify dependencies & interdependencies of CBF
v) Determine maximum allowable "Down Time" i.e. Pain Threahold
vi) Type & Quantity of resources required for recovery tasks
vii) Determine impact

Ways to gathering information:

A. Examination of Documents
B. Interviews
C. Examination of Documents
D. Workshops

BIA Report should be presented to "Steering Committee", specify CBF & Pain Threshold

19. What are the objectives of Plan Development?

Ans.:

Objective

A. To determine the available options & formulation of appropriate alternative operating strategies,

B. To provide timely recovery for all critical process & their dependencies.

i.e. two tiered strategy

A. Business – Logistics, Accounting & HRM etc

B. Technical – IT = PC, LAN, Network, DBMS etc.

20. Explain - Business Community Management (BCM)

Ans.:

BCM = Planning + Develop + Running + Maintaining + Monitoring

BCM – business owned & business driven process that establishes "A fit for purpose strategic & operational framework"

A. Improves enterprise's resilience against disruption

B. Rehearsed method of restoring enterprise's ability to supply its key products & services to agreed level within an agreed time after disaster.

C. Delivers proven capabilities to manage a business disruption & protect reputation & brand.

21. What is BCM Policy?

Ans.:

It defines processes of setting up activities for establishing a BC capability & ongoing Management & Maintenance of BC Capability.

Objective = A structure through which...

A. CBF – identified

B. Plan developed for continuity of CBF

C. Manage IM & BCP

D. Subject – IM & BCP to ongoing testing, revision & updates as required.

E. Assign – Planning & Management responsibility to a number of relevant senior management team.

22. Explain - Components of BCM Process

Ans.:

A. BCM Management Process

B. Information Collection

C. Strategy Process

D. Development & Implementation Process

E. Testing & Maintenance Process

F. Training Process

23. Explain - BCM Management Process

Ans.:

- ✓ Address "the objectives" defined in "BC Policy" by providing organization structure with responsibilities & authority for implementation & maintenance (I&M) of BCM.
- ✓ Organization should nominate a person / team with appropriate seniority & authority to be accountable

  i.e. Clearly defines person responsible for I & M of BCM in organization.
- ✓ Top Management should appoint the manager (BCM) responsible for ongoing I & M of BCM within their area of responsibility.

  i.e. system manager responsible for their functional area.
- ✓ **Implementation should include following activities**
  A. Defining the scope & context
  B. Defining the role & responsibility
  C. Regular testing of program
  D. Maintaining up to date & appropriate BCP
  E. Reviewing, reworking & updating BCP, RA & BIAS
  F. Convert policies & strategies into actions
  G. Managing costs & benefits
  H. Engaging & involving stakeholders
- ✓ **BCM documents required to be maintain (for minimum One Year)**
  A. BC Policy
  B. BIA Report
  C. BCM System
  D. RA Report etc… (Complete from SM/PM)

24. How to classify the critical activities?

Ans.:

A. BIA – same as above

B. Classification of critical activity (CBF):

BIA will be used in categorization (DEV) of infrastructure & business function by disaster scenario (Trivial, Minor, Major & Catastrophic) for various disaster causes.

D – Desirable

E – Essential

V – Vital

For following chart,

A. Axis – X: Business Categories

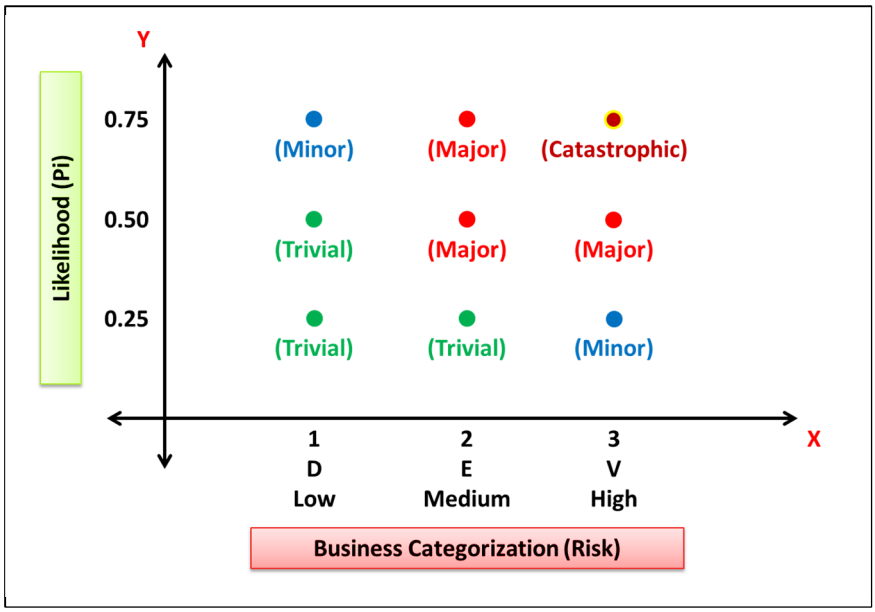
Based on Loss of Revenue, Loss of Reputation, Loss of Productivity and Reduction in satisfaction

Determine – Grade i.e. 123 / DEV / LMH

B. Axis – Y = Pi of occurrence of disaster

C. Catastrophic, Major, Minor & Trivial = Disaster Scenario decided from graph

D. RA – same as above



25. Explain - Documentation required for BCM

Ans.:

All documents that form the BCM are subject to the document control and record control processes.

The following documents (representative only) are classified as being part of the business continuity management system:

A. The business continuity policy;
B. The business continuity management system;
C. The business impact analysis report;
D. The risk assessment report;
E. The aims and objectives of each function;
F. The activities undertaken by each function;
G. The business continuity strategies;
H. The overall and specific incident management plans;
I. The business continuity plans;
J. Change control, preventative action, corrective action, document control and record control
K. processes;
L. Local Authority Risk Register;
M. Exercise schedule and results;
N. Incident log;
O. Training Program.

---- XXXX ---- XXXX ----

Contact : (+91) 8671866086
Email : ca.vrtalsaniya@gmail.com
Slide-share : VR Talsaniya

Chapter covers following topics...

A. Business Process Design
B. System Development Process
C. Reasons for failure to achieve SD Objective
D. System Development Team
E. Roles in SDLC
F. Approaches for SD (How to Develop?)
G. Methodology for SD
H. SDLC (Benchmark Steps, to develop any system)

---

1. Explain - Business Process Design OR Business Process Re-engineering (BPR)

Ans.:

- ✓ It involves improving the existing business system by restructuring the business tasks, functions & activities etc.
- ✓ Example: Conversion from legacy IS to ERP, it will require restructuring of business tasks, function etc.
- ✓ **3 Steps:**
  - A. Understanding & Documenting the existing system
  - B. Proposed business Processes documentation
  - C. Implementing new business processes

2. What is the System Development Process?

Ans.:

- ✓ It is identification of existing business situation with an aim for improving those situations & then putting up an IS in place for achieve that aim.
- ✓ Key important phases:
  - A. **System Analysis** – Requirement Analysis (Thoroughly) to improve existing system
    - **Existing System**
    - \+ **Problem in Existing (Remove)**
    - \+ **Additional Proposed Requirements**
    - **Total Requirements Analyzed**
  - B. **System Design** –
    Based on requirement analyzed
    Convert into the System Design i.e. Flow Chart, Data Flow Diagrams etc...

3. Reason for failure – to achieve System development objectives

Ans.:

User Related Issues:

- A. Shifting / Changing user needs
- B. Resistance to change
- C. Lack of user participation
- D. Inadequate testing & user training

Developer Related Issues:

A. Difficult to define the exact requirements particularly for unstructured / strategic system.
B. New Technologies
C. Lack of senior management support & involvement
D. Lack of standard project management & system development methodologies
E. Over worked / Under trained development staff

4. System Development Team:

Ans.:

A. Steering Committee:

Usually consists of a group of key IS Plans & Application developments
It ensures that ongoing systems development activities are consistently aimed at satisfying the information requirement of managers & users.
i.e. by Review of "Progress of Project"

B. IS Department:

Responsible to Develop system

C. Project Management:

Co-ordinate Development Activities of system i.e. computer professional & Key users

D. System Analysts:

Assigned to determined user requirements, design the system and assist in development & implementation activities.

5. Roles of SDLC

Ans.:

A. Steering Committee
B. Project Manager
C. Project leader
D. System Analyst / Business Analyst
E. Module leader / Team leader
F. Programmer / Coder / Developer
G. DBA – Database Administrator
H. Quality Assurance
I. Tester
J. Domain Specialist
K. IS Auditor:

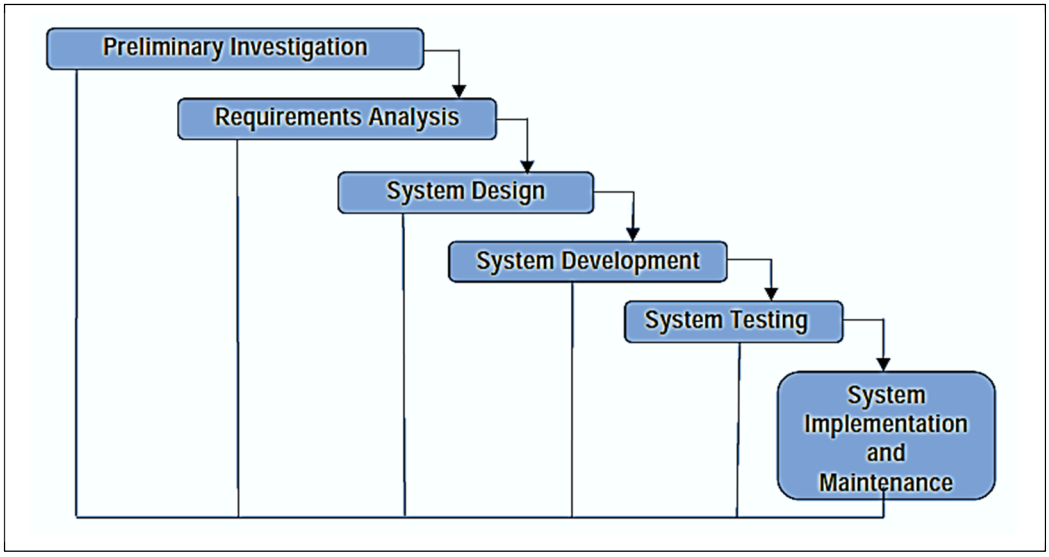
Ensure that application development also focuses control perspective.
Need to involve in design phase & final testing phase to ensure existence & operations of controls in new software.

6. System Development Approaches

Ans.:

A. Traditional / Waterfall Approach –

- ✓ Phases of SDLC – one by one
- ✓ Many refinements are provided
- ✓ Initial model organized in liner order output of one phase become input of next phase and assumes no defect is introduced during any phases of life cycle
- ✓ **Refinements:**
  - i. In actual SD, the defect / error, get introduced in any of the phase of LC. It is preferable to detect & correct in the same phase But it is not always possible i.e. provision of feedback path introduced.
  - ii. Two/more phases to be conducted, simultaneously. i.e. not one by one but parallel



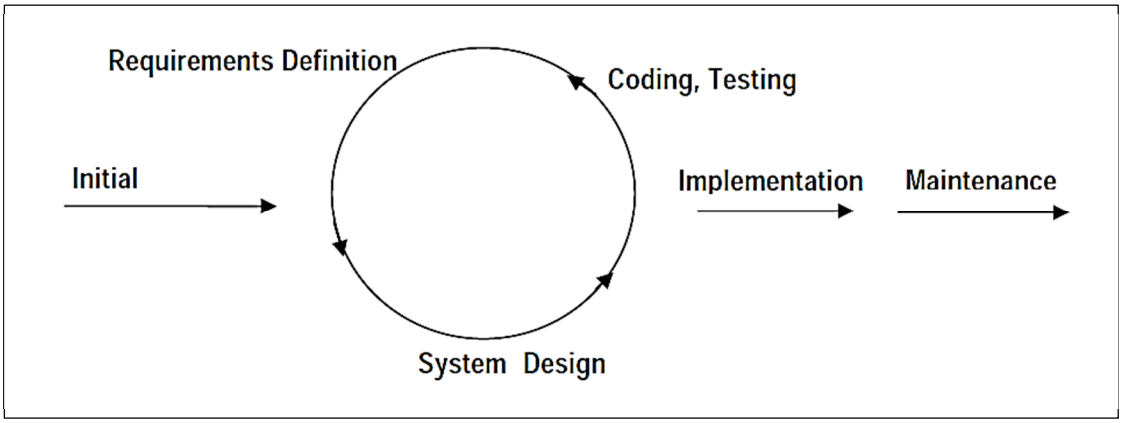
B. Prototype Model –

- ✓ Before development of actual software a working prototype of system should be build, first.
- ✓ Toy implementation of system, provides…
  - i. Limited functional capabilities
  - ii. Low reliabilities
  - iii. Inefficient performance

But help to understand the exact requirement from system.

Generic Phases of Prototype Model:

- i. Identify information system requirement
- ii. Develop the initial prototype
- iii. Test & Revise
- iv. Obtain user signoff of the Approved Prototype



C. Incremental Approach –

- ✓ **Combine both Waterfall & Prototype model**.
- ✓ Software product is built incrementally through different iterations.
- ✓ Does not attempt to start with full specification of requirements but develop by iteration of review.

D. Spiral Model/ Evolutionary Model –

- ✓ Similar to incremental model
- ✓ But with more thrust on risk analysis & resolution.
- ✓ It also combines waterfall & prototype models.
- ✓ Activities represented as Spiral rather than sequence of the activities.
- ✓ Each loop in spiral is phase in process & no fixed phases like other but selected based on requirement.
- ✓ Risk is explicitly assessed in each spiral's loops & risks are resolved throughout Spiral process.

E. Agile Methodologies –

- ✓ System development is human activity, therefore, there will be variation in inputs & process.
- ✓ Therefore, **SD should flexible enough & agile for required changes**.
- ✓ Plan activities as nature of project.
- ✓ Follow iterative cycle, advocates to work user and management
- ✓ People oriented approach
- ✓ No one by one systematical steps required.
- ✓ Rapid & Flexible – Response to change.

F. RAD – Rapid Application Development

- ✓ Designed to give – faster development & high quality result.
- ✓ **Maximum advantage of already developed powerful software for development of new software**. ***(Copy old one & make required changes)***
- ✓ i.e. use already developed "Software code / Programs" maximum possible.

- ✓ **Key feature:**
  i. Low cost
  ii. Quick development
  iii. Right quality
- ✓ Useful when less time available & otherwise 'requirement of business get changed.'
- ✓ **Components:**
  i. JAD – Joint Application Development
  ii. Rapid Development Project
  iii. Clean Rooms
  iv. Time Boxing
  v. Incremental Prototyping
  vi. Tools, like – CASE, DBMS etc.

7. SDLC – System Development Life Cycle:

Ans.:

- ✓ SDLC is a popular system development framework, which sequence steps to system designer & developers for efficient system development.
- ✓ It is document driven framework i.e. at every stage of SDLC documentation is produced.
- ✓ A phase of SDLC is not completed until appropriate documentation &work product is produced.
  Known as 'Deliverables'.
- ✓ Does produced by previous phase is important for next phase activity, based on it all decision will be taken.

8. Advantages of SDLC

Ans.:

General

A. Better planning & control by project managers
B. Compliance with prescribed standard & ensure better quality
C. Documents of SDLC are important measure of communication & control
D. The phases are milestones i.e. help project manager review & signoff.

Audit Perspective:

A. Clear cut understanding of all steps & phases
B. Can state in report about compliance by IS Management
C. If IS Auditor has technical knowledge & capability
D. Evaluation of methods & techniques used in SDLC

9. Risk & Shortcomings of SDLC

Ans.:

A. Time consuming
B. Rigidity of approach may delay / prolong duration
C. Development team may find cumbersome
D. End product – may not be for long term
E. May not be suitable for small & medium sized projects

Contact : (+91) 8671866086
Email : ca.vrtalsaniya@gmail.com
Slide-share : VR Talsaniya

10. Explicit knowledge & Tacit Knowledge

Ans.:

Explicit knowledge

- ✓ It can be formalized easily & as a consequence is easily available the organization
- ✓ It is articulated, represented by spoken words, written material & complied data.
- ✓ This type of knowledge is codified, easy to document, transfer & reproduce.

Example:

A. Online Tutorials
B. Policy & Procedural manuals

Tacit knowledge

- ✓ It resides in a few often in just one person & has not been captured by organization
- ✓ It is unarticulated & represented as intuition, perspective, beliefs & values that individuals form based on their experiences.
- ✓ It is difficult to document & communicate the tacit knowledge.

Example:

Hand on skills, Special knowhow, Employee Experiences etc.

-----: Phases of System Development Life Cycle (SDLC) :------

---

P1. Preliminary Investigation

A. Problem Definition

B. Conduct Investigation

i. Review internal documents
ii. Conduct interview

C. Identify – Viable Options

D. Feasibility Study – Need to conduct

i. **Technical** : Required HW & SW available in the market?
ii. **Financial** : Financially viable – Affordability of Org.
iii. **Economical** : Cost Benefit Analysis – Profit / Loss
iv. **Operational** : Operational in org. by users – employees, customers, supplies
v. **Schedule/Time** : Estimated time – Proposed time acceptable or not
vi. **Resource** : Preliminarily related to availability of HR
vii. **Legal** : Conflict between proposed system & Org. legal obligation / license etc.
viii. **Behavior** : Adverse effect on quality of work life?

E. Submit 'Report' to management with recommendation

Contact : (+91) 8671866086
Email : ca.vrtalsaniya@gmail.com
Slide-share : VR Talsaniya

P2. System / Requirement Analysis

A. Information Collection (Fact Finding Technique)

i. Collection of Documents
ii. Interviews
iii. Questionnaires
iv. Observations

B. Analysis of current system

i. History of organization
ii. Data file maintain
iii. Inputs
iv. Method / Procedures
v. Output
vi. Internal Controls

+ Documentation for following Two:

i. Modeling of existing logical & physical system
ii. Undertake overall analysis of Current system

C. Analysis of Proposed system

Therefore, Problem in Current system + New Req. in Proposed System = Specifications
i.e. Specifications for Proposed System:
For input, method/procedure, database, output, workload & time efficiency.

D. Reporting – SRS – System Requirement Specifications

a. Introduction -
b. Information Description (for input / output) – Information content requirement
c. Functional Description (Process / Database) – all function parameters
d. Behavioral Description (Controls) – Connectivity to External & Internal Org.
e. Validation Description (Controls) – Tests to be formed
f. Appendix – All tools of system development i.e. DFD, Flow chart etc.

---------- System Development Tools ----------

a. System flow & component

For flow:

i. **Flow Chart** –
Physical flow of System

ii. **Data Flow Diagram** –
Logical flow of data within organization
Four basic elements:
1. Data source & destination, **2.** Data Flows, **3.** Processes **4.** Data Stores

For component :

iii. **Component Matrix**
Matrix framework to document resources used, activities performed & information produced.

Contact : (+91) 8671866086
Email : ca.vrtalsaniya@gmail.com
Slide-share : VR Talsaniya

b. User interface

i. Layout forms & screens

They are used to construct the formats & contents of input / output media & methods

ii. Dialog flow diagrams

They are used to depict flow of dialogue between computer & people, based on response to menus & prompts.

c. Data Attributes & Relationship

i. File Layout Forms

Document type, size & name of data element in system

ii. Data Dictionary

Description of information of data in files of IS (i.e. data about data, metadata)

It contains –

a) Name of the company file store data
b) Codes of data item length / type / range
c) Source documents used to create data
d) Individual / program to permit access or not permitted
e) Name of the computer host programs that modify the data items

iii. Gird charts

Identifying use of each type of data element

iv. E-R Diagrams

To document number & type of relationship among the entities in a system

d. Detailed system process

i. Decision Tree

Network / tabular form for decision

ii. Decision Table

To document complex conditional logic involving among information processing alternatives in system

e. PDL (Program Design Language) / Pseudo code

- ✓ Use of English language with syntax of structure of programming language
- ✓ **Benefit:**

  English = convenience of 'Spoken English Languages'
  Structured Programming = To obtain Precision as programming.

f. CASE Tools (Computer Aided Software Engineering Tools)

- ✓ These tools are used for **the automation of anything** that 'Human to do' to develop the system / software.

Q - What are the characteristics of Good system designs?

Ans.:

A. Capture all functionalities of the system – correctly
B. Easy to understand
C. Efficient design
D. Flexible design
E. Based on extensive analysis
F. Flow prescribed standards of design
G. Modular
H. Directly relevant to business activities

P3. System Design

A. Architectural Design

B. Design of data / information flow

C. Database Design

i. Conceptual modeling: (Design)

DBA design the database by E-R diagram & other tools

It describes – application domain via. Entity, attributes, static & dynamic constraints, relationship among them.

ii. Data modeling: (Readable by Program)

Design prepared as above need to translate into data model so that it can be accessed & manipulated by high & low level PL.

iii. Storage structure design (modeling): (How to store?)

How linearize & partition the data structure as in data modeling to store on device.

iv. Physical layout design (modeling): (Where to store?)

How distributed the storage structure across specified storage device & locations like, tack, cylinder& sector on disk.

D. Design of interface input & output

1. Format, **2**. Content, **3**. Form, **4**. Timeliness, **5**. Media, **6**. Volume

E. Physical Design

F. Design of Acquisition of Hardware / Software

P4. System Acquisition & Software Development

A. Hardware Acquisition

B. Software Acquisition

Benefit of Application packages

i. Rapid implementation
ii. Low risk
iii. High Quality
iv. Low Cost

Limitation of Application packages:

i. Lack of flexibility
ii. Partially useful application
iii. Low quality of documents
iv. Continuity

C. Contract & SW license

D. Vendors' proposal validation

Points to be considered for the validation of proposal…

i. Performance – CBA
ii. Maintainability / Adaptability of each proposal
iii. Compatibility with existing system
iv. Support services by vendors

E. Methods of validation proposals

i. Checklist:

Most Common, Simple Method, List of required specification for HW/SW/ Support

ii. Point scoring:

Criteria with maximum points & allocate points based on performance

iii. Evaluating public report:

Magazines & manuals for the same – Published Periodically

iv. Bench marking test:

Job mix of possible transactions executed on acquiring system and then results will be compared with benchmark.

F. Software Development

Characteristics of good Program code:

i. Reliabilities
ii. Readability
iii. Robustness – Strong enough (should not get hang out)
iv. Accuracy
v. Efficient
vi. Usability

Stages in software Development

i. Program Analysis
ii. Program Design
iii. Program Coding
iv. Debug the Program
v. Program Documentation
vi. Program Maintenance

Programming Language (PL):

✓ **Set of instruction** in programming language = Program code = source program
✓ It is converted in **Object Program** (executable binary program) by Compiler.

✓ Debugging of Software

i. **Complier**
Syntax / logical errors if any – check by complier while converting program

ii. **Structured Walk through**
Sometime, there will be wrong business logic with correct syntax, so that, we need to check Object Program (Executable Program) as Structured walk through.

iii. **Test**
Finally, testing of whole software is done by test data to find 'Run Time Errors'.

P5. Testing Phase

A. Unit Testing

i. **Functional Testing** : Process/function – correct supposed to be
ii. **Performance Testing** : Avg. response time
iii. **Stress Testing** : Maximum load a system can handle (Users simultaneous access)
iv. **Structural Testing** : Internal logic of programs
v. **Parallel Testing** : same data for old & new – compare results from both

Types of Unit Testing –

Static (Non Execution)

i. **Desk Check**: by Programmer himself
ii. **Structured Walk Through**: by other programmers through the text of program
iii. **Code Inspection**: reviewed by a formal committee with formal checklists.

Dynamic (Execution)

i. **Black Box Testing**:
External Perspective – no relevance with internal codes
Test designer selects valid & invalid inputs & determines the correct output

ii. **White Box Testing:**
Internal Perspective – need to test whole system & codes
Need to ensure internal operation of the product conforms to specifications & all internal components are adequately exercised.

iii. **Gray Box Testing:**
Combination = **Black** + **White** (i.e. based on Modules)

B. Integration Testing

i. **Bottom Up Testing** – Traditional strategy
ii. **Top Down Testing**
iii. **Regression Testing** (when new Module introduced)

C. System Testing

i. Recovery ii. Security iii. Stress iv. Performance

D. Final Acceptance

i. Quality Assurance Test
ii. User Acceptance Test
   a. **Alpha Test** – α – By internal Staff
   b. **Beta Test** – β – By External Expert

P6. System Implementation

A. Equipment installation

i. Site preparation
ii. Install
iii. Check

B. Training

i. System Operators
ii. User training

C. Conversion

i. Procedure conversion
ii. File conversion
iii. System conversion
   a. **Direct conversion** : Immediately change system from next day
   b. **Parallel conversion** : Old system continue until new system work properly
   c. **Modular conversion** : Start to change system module wise
   d. **Pilot conversion** : Change system at one location, than at all.
iv. Scheduling conversion
v. Alternative conversion

P7. System Implementation

A. PIR – Post Implementation Review (PIR)

Did we get what we have set out to do in terms of business?
(If No, than now, what should we need to do?)
For That - DOI Evaluation Required…

i. Development Evaluation
ii. Operation Evaluation
iii. Information Evaluation

B. Maintenance –

i. Schedule Maintenance:
Anticipated & planned for operational continuity & avoidance of anticipated risk

ii. Rescue Maintenance:
Previously non-detected malfunctions that were not anticipated but require immediate troubleshooting solution

iii. **Corrective Maintenance**:
Fixing bugs in code/defects found during the executions (initiated by bug report & drawn up by end user)

iv. **Adoptive Maintenance**:
Adapting software to changes in environment, such as hardware/OS

v. **Perfective Maintenance:**
The system runs satisfactorily, but for accommodating to new/changed user requirement & activities to increase performance.

vi. **Preventive Maintenance:**
Activities aimed at increasing system maintainability & improving modular structure of system.

C. Operational Manual

It is typical user's guide, also commonly known as Operations Manual.

The section of an operation manual will include the following:

1) A cover page, a title page and copyright page;
2) A preface, containing details of related documents and information on how to navigate the user guide;
3) A contents page;
4) A guide on how to use at least the main functions of the system;
5) A troubleshooting section detailing possible errors or problems that may occur, along with how to fix them;
6) A FAQ (Frequently Asked Questions);
7) Where to find further help, and contact details;
8) A glossary and, for larger documents, an index.

D. Auditor's Role in SDLC:

- ✓ The audit of systems under development can have three main objectives.
- ✓ It is primarily aimed to provide **an opinion** on the **efficiency**, **effectiveness**, and **economy** of project management.
- ✓ An auditor's role is **to assess** the extent to which the system being developed provides for **adequate audit trails and controls to ensure the integrity of data** processed and stored; and the effectiveness of controls being enacted for the management of the system's operation.
- ✓ In order to achieve these goals, an auditor has to attend project and steering committee meetings and examine project control documentation and conducting interviews.

---- XXXX ---- XXXX ----

Chapter – 6 : Auditing of ISs

1. What are needs of audit of information system?

Ans.:

Due to absence of control, following results may be there…

A. Organizational costs of data loss
B. Cost of computer abuse
C. Incorrect Decision Making cost
D. Loss of value of Hardware, Software & personnel
E. High cost of computer errors
F. Maintenance of privacy may compromise
G. Due to control – we can evaluate the use of computer

2. What are the Objectives of IS Audit?

Ans.: (Sieeeeee)

(Safeguard, Integrity, Effectiveness & Efficiency)

A. Improve data security & safeguard of the assets
B. Improve data integrity
C. System effectiveness objectives – Improve Performance
D. System efficiency objectives – Reputation & Customer Loyalty

3. Explain – Effects of computers on audit

Ans.:

For evidence collection (for Audit Purpose)–

A. Absence of input documents
B. Lack of visible output
C. Lack of visible output trail
D. Data retention & storage
E. Audit evidence – system generated
F. Legal issues

For evidence evaluation (for Audit Purpose)–

A. System generated transaction (due to backend processing)
B. System errors (Systematic Errors – Coding Errors)

4. Who is responsible for implementing the controls in organization?

Ans.:

Responsible = Management

A. Develop & implement 'Cost Effective Internal Control (IC)'
B. Assess adequacy of IC in programs & operations
C. Separately assess adequacy of IC over IS in consistent with security policy
D. Identify the need & improvements
E. Take – corresponding corrective actions
F. Report annually on IC through management assurance statement

5. What auditor needs to do?

Ans.:

Responsibility of auditor:

A. Validate the implemented IC
B. Also provide recommendations for improvements in IC (if any).

6. What are the 'Set of skills' expected from the IS Auditor?

Ans.:

A. Knowledge of **business practices & compliance**
B. Knowledge of **IT policy or security policy**
C. Knowledge of **professional standards & best practices**
D. Adequate – **Professional Technical qualification**
E. **Ability to Understand** – Technical controls
F. U**nderstanding of IS Risks & Controls**

7. What are the Categories of IS Audit / Types of IS Audit / Area required to be audited in the IS Audit?

Ans.:

A. System (Operation System) & Application
B. Information processing facilities
C. System Development (SD)
D. Management of IT & enterprise architecture
E. Telecommunication, intranets & extranets.

8. What are the steps of IT Audit?

Ans.:

A. Scoping & Pre-audit survey - **Scope**
B. Planning & Preparation - **Plan**
C. Audit & Field Work - **Fieldwork**
D. Analysis - **Analysis**
E. Audit Reporting - **Report**
F. Closure Notes – **Closure**

9. Factors / critical factors should be considered in preliminary review by IS Auditor

Ans.:

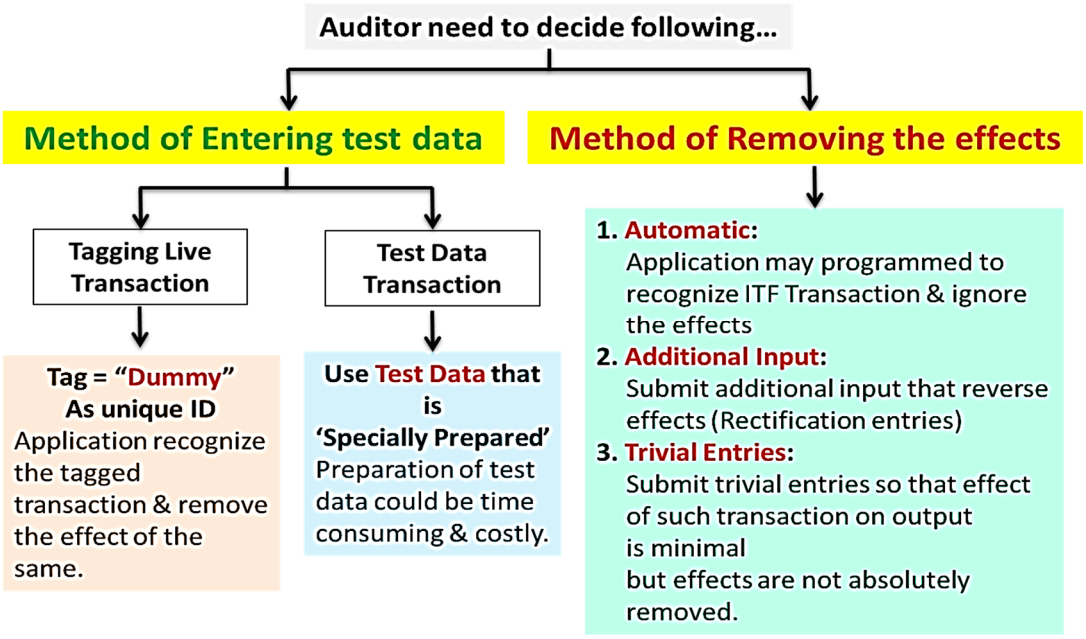
A. Knowledge of the business
B. Understanding of the technology
C. Understanding of IC System
D. Legal consideration & audit standards
E. Risk Assessment (RA) & Materiality
(i.e. Inherent Risk, control Risk, Detection Risk & Material or not?)

10. Explain - Concurrent / Continuous & embedded audit modules in IS Audit

Ans.:

A. ITF – Integrated Test Facility

- ✓ Embedded audit module as ITF is used in IS to be audited.
- ✓ Auditor can open 'Dummy A/c' or 'Branch' in IS through ITF audit module, then enter test dummy transaction & review the processing & output of these transactions.
- ✓ Compare, the processed & expected result to verify the system.
- ✓ Such dummy record does not have effect on the actual records.
- ✓ Best part is automatic removal of dummy transaction impact by IS.



B. Snapshot Technique:

- ✓ Audit software will take snaps/pictures of transaction as flows through out an application system.
- ✓ Provide efficient audit trails
- ✓ Embedded audit software module is used for "Those Points", where material impact can be observed for processing.
- ✓ To validate the correctness of the processing snapshots of both before & after processing of transaction are captured.
- ✓ Auditor needs to check authenticity, accuracy & completeness by comparing both images of transaction.
- ✓ However, auditor needs to take decision about...
  - A. Location of snapshot points
  - B. Time of capturing of snapshot
  - C. Reporting of snapshot data captured
- ✓ All snapshots data can be collected in records at one place for the efficient audit evaluation work.

C. SCRAF (System Control Audit Review File):

i.e. Log file of transactions of special audit significance.

- ✓ Embedded audit software module within the Host Application System to provide
- ✓ Continuous monitoring of system's transactions is SCRAF file / audit log.
- ✓ That…
  Collect the data on transaction with 'Special Audit Significance' by maintaining log of transactions.
- ✓ Note that:
  Only these transactions are recorded in SCARF file that are of Special Audit Significance.
  Like: Exceeds the specific limit/ Related to Special Account.
- ✓ Periodical printout taken by the auditor & identify the questionable transactions & perform the audit follow up investigation.

Auditor need to decide…

a) What information to be collected
   (What should be considered as of Special Audit Significance?)
b) Reporting system to be used.

SCARF Collect the following data:

a) Policy & procedural variances
b) System exception
c) Profiling data
d) Statistical sample
e) Application system errors
f) Performance measurement
g) Snapshots & extended records

D. CIS – Continuous & Intermittent Simulation:

- ✓ Continuous = All Transaction are simulated
- ✓ Intermittent = only Significant Transaction are simulated
- ✓ CIS is used to trap exceptions whenever the application system uses the DBMS.
- ✓ Embedded audit module in DBMS = CIS
- ✓ Variation on SCRAF Method.
- ✓ Validation the correctness of processing using audit module in DBMS.
- ✓ DBMS used to trap exceptions that are of interest to the auditors
- ✓ Same transactions are processed in both in CIS Module & Application SW in a way uses parallel simulation, then both result compared.

Process:

1. DBMS reads an application system transaction & passed to CIS
2. **CIS decide – Further Examine?**
   No = Wait for further data
   Yes = Next steps are followed for the same
3. CIS simulate the application system processing
4. Then, update the database:
   Selected transactions will be checked by CIS to find out the material discrepancies between result produced & result simulated to be produced by application.
5. Exceptions identified by CIS & then written to 'Exception Log File'.

11. Explain - Advantages & Disadvantages of continuous audit:

Ans.:

Advantages –

A. Timely audit
B. Detailed auditing
C. Surprise test
D. Information meets the set of objectives
E. Training for new users

Disadvantages –

A. Availability of resources
B. Involvement in System Development
C. Expert knowledge
D. Missing audit trail
E. Stable application system required

12. What are Audit trail controls?

Ans.:

Audi trail = Logs that can be designed to record the activities at the system, application & user level.

It is a chronological record of all the activities that have occurred in a system.

Three major ways by which audit trail can be used…

A. Detecting unauthorized access to the system
B. Facilitating the reconstruction of events
C. Promoting personal accountability

13. What are the Layers & related Audit issues for the organization?

Ans.:

A. Operation layers

i. User A/c & Access Rights
ii. Password Controls
iii. Segregation of duties

B. Tactical layers

i. Interface security
ii. Audit logging & monitoring

C. Strategic

14. Types of control - General controls

Ans.:

A. **OS controls**:

OS control objectives –

a) Protect itself from users
b) Protect users from each other
c) Protect user's one program from another
d) OS should be protected from environment
e) Must be protected from itself.

OS Security Components –

a) Login Procedure: identity & authenticity
b) Access token – Authorization
c) Access control list
d) Discretionary access control

B. Data Management Controls:

i. Data Access Control:

a. **User Access Control** – by Password, Token etc.
b. **Data Encryption** – keeping the data in DB in encrypted form

ii. Data Backup control:

a. **Dual Recording of Data** –
Two complete copies of DB are maintained
b. **Periodical Dumping of data** –
Backup of entire DB at periodical interval
c. **Logging input transactions** –
Backup of data between dates on which periodical dumping done
d. **Logging changes to data** –
Copying a record each time, it is changed by an update action.

C. Organization Structure Controls

i.e. only by segregation of duties

a) Segregation of assets record keeper than physical assets keeper
b) Separation of system development from computer operators
c) Separation of new system development from maintenance

D. System Development Controls

a) System Authorization
b) User Specifications
c) Technical Design
d) Internal Audit

e) Program Testing
f) User Testing & Acceptance

E. System maintenance controls

F. Computer Center Security & Controls (Data Center):

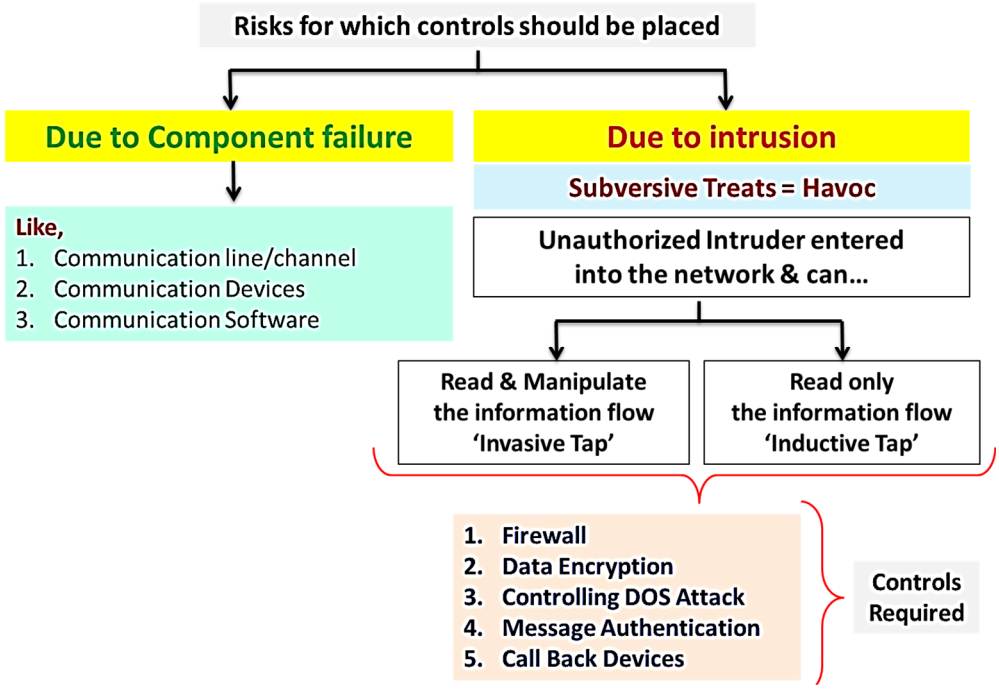
i. Physical Security –

a. Fire Damage
b. Water damage
c. Pollution Damage
d. Energy Damage
e. Unauthorized intrusion (IDS)

ii. Software & Data Security

iii. Data communication Security

G. Internet & Intranet controls:



15. What is the Role of Auditor?

Ans.:

Audit & Evaluation Technique for...

Physical controls:

1. Risk Assessment
2. Controls Assessment
3. Review of Document

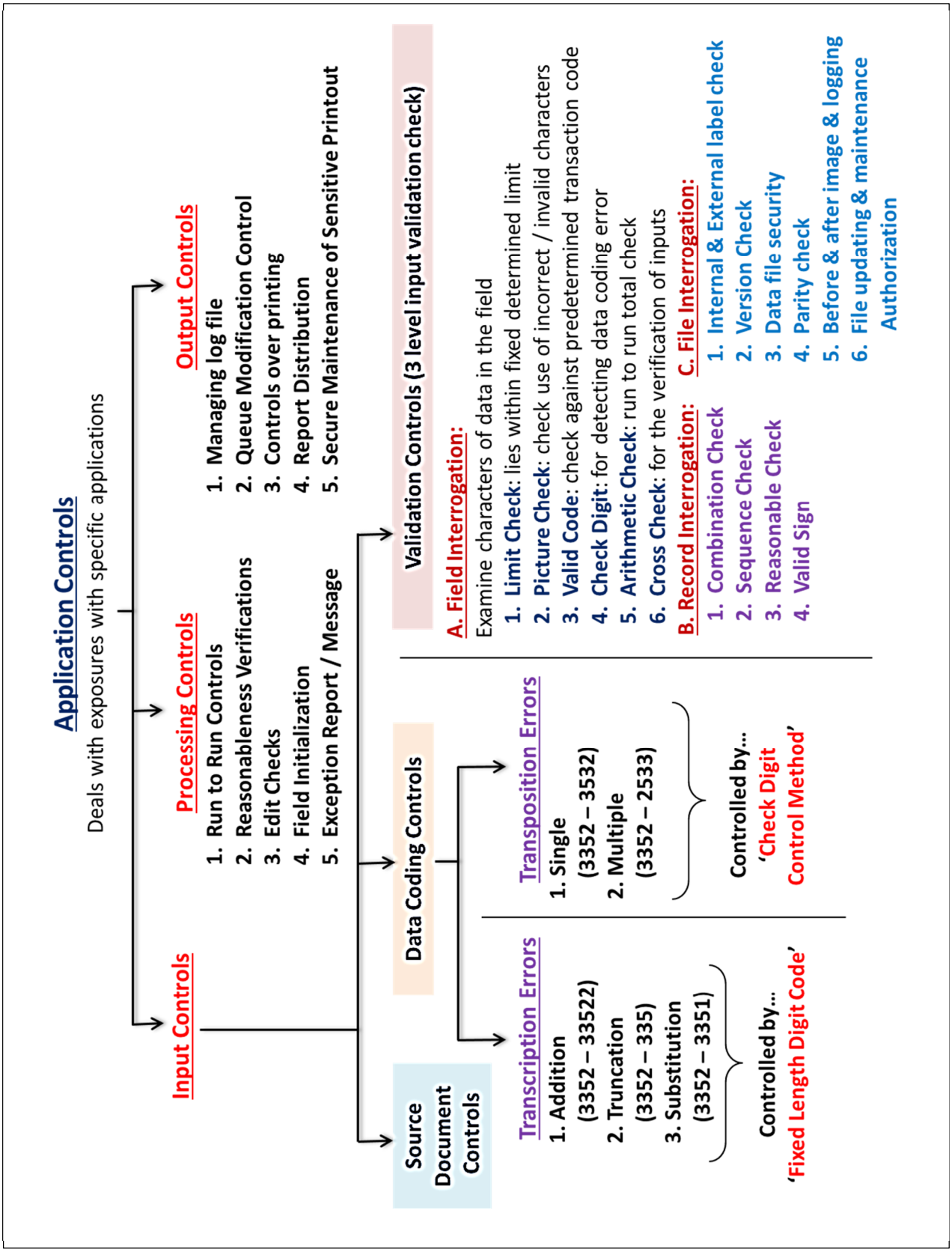
Environmental Controls:

Following should be considered by IS Auditor

1. Audit planning & assessment
2. Audit of environmental controls
3. Documentation

16. Types of control – Application Controls

Ans.:



---- XXXX ---- XXXX ----

Chapter – 7 : IT Regulatory Issues

Information Technology (Amendment) Act - 2008 [ITAA]

Our Syllabus contains, Chapter - 1, 2, 3, 5, 9, 11, 12 & 13 of ITAA.

Chapter		Section	Title of the section
1	Preliminary	1	Short Title, Extent, Commencement & Application
		2	Definitions
2	DS & ES	3	Authentication of Electronic Records
		3 - A	Electronic Signature (ES)
3	Electronic Governance	4	Legal Recognition of Electronic Records
		5	legal Recognition of Electronic Signature
		6	Use of Electronic Records & E-Signature in Government & Agencies
		6 - A	Delivery of services by Service Provider
		7	Retention of Electronic Records
		7 - A	Audit of Documents etc. in Electronic Records
		8	Publication of rules, Regulations etc. in Electronic Gazette
		9	Section 6, 7 and 8 Not to Confer Right to insist document should be accepted in E - form
		10	Power to make rule by Central Government in respect of Electronic Signature
		10 - A	Validity of contracts formed through electronic means
5	Secure e-Record & Secure ES	14	Secure Electronic Record
		15	Secure Electronic Signature
		16	Security procedures and Practices
9	Penalties, compensation & Adjudication	43	Penalty and compensation for damage to Computer, Computer System etc.
		43 - a	Compensation for failure to protect data
		44	Penalty for failure to furnish information, return, etc. **(CCA / CA – 1.50 Lakh OR 5k Per Day OR 10k Per Day)**
		45	Residuary Penalty **(Rs. 25000)**
		46	Power to Adjudicate
		47	Factors to be taken into account by the adjudicating officer
11	Offences	65	Tampering with Computer Source Documents **(3 Years OR 2 Lakh OR Both)**
		66	Computer Related Offences **(3 Years OR 2 Lakh OR Both)**
		66 - A	Punishment for sending offensive messages through communication service, etc. **(3 Years OR Unlimited Amount OR Both)**
		66 - B	Punishment for dishonestly receiving stolen computer resource or communication device **(3 Years OR 3 Lakh OR Both)**
		66 - C	Punishment for identity theft **(3 Years OR 1 Lakh OR Both)**

11	Offences	66 - D	Punishment for cheating by personation by using computer resource **(3 Years OR 1 Lakh OR Both)**
		66 - E	Punishment for violation of privacy **(3 Years OR 2 Lakh OR Both)**
		66 - F	Punishment for Cyber Terrorism **(Imprisonment up to the Life)**
		67	Punishment for publishing or transmitting obscene material in electronic form **(1st - 3 Years OR 5 Lakh)** **(2nd - 5 Years OR 10 Lakh)**
		67 - A	Punishment for publishing or transmitting of material containing sexually explicit act, etc. in e-form **(1st - 5 Years OR 10 Lakh)** **(2nd - 7 Years OR 10 Lakh)**
		67 - B	Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in e-form **(1st - 5 Years OR 10 Lakh)** **(2nd - 7 Years OR 10 Lakh)**
		67 - C	Preservation and Retention of information by intermediaries **(3 Years & Unlimited)**
		68	Power of Controller to give directions **(1 Year & 1 Lakh)**
		69	Powers to issue directions for interception or monitoring or decryption of any information through any computer source **(7 Years & Unlimited)**
		69 - A	Powers to issue directions for blocking for public access of any information through any computer resource **(7 Years & Unlimited)**
		69 - B	Power to authorize to monitor and collect traffic data or information through any computer resources for Cyber Security **(7 Years & Unlimited)**
		70	Protected System **(3 Year OR 2 Lakh OR Both)**
		70 - A	National Nodal Agency
		70 - B	India Computer Emergency Response Team to serve as national agency for incident response
		71	Penalty for misrepresentation **(2 Years OR 1 Lakh)**
		72	Breach of confidentiality and privacy **(2 Years OR 1 Lakh)**
		72 - A	Punishment for Disclosure of information in breach of lawful contract **(3 Years OR 5 Lakh)**
		73	Penalty for publishing electronic Signature Certificate false in certain particulars **(2 Years OR 1 Lakh)**

		74	Publication for fraudulent purpose **(2 Years OR 1 Lakh)**
		75	Act to apply for offence or contraventions committed outside India
		76	Confiscation
		77	Compensation, Penalties or confiscation not to interface with other punishment
		77 - A	Compounding of Offences
		77 - B	Offences with Three years' imprisonment to be cognizable
		78	Power to investigate Offences
12	Intermediaries not be liable	79	Exemption from liability of **intermediary** in certain cases **Not Liable:** A. Functions is limited to access to communication system B. Does not initiate transaction & does not modify info. C. Observe due diligence while discharging duties **Liable for:** A. Knowledge of unlawful act B. After receiving info. of unlawful act, does not take appropriate action.
13	Miscellaneous	80	Power of Police Officer and other Officers to Enter, Search, etc.
		81	Act to have Overriding effect
		81 - A	Application of the Act to Electronic cheque and Truncated Cheque
		82	Chairperson, Members, Officers and Employees to be Public Servants
		83	Power to Give Direction
		84	Protected of Action taken in Good Faith
		84 - A	Modes or methods for encryption
		84 - B	Punishment for abetment of offences
		84 - C	Punishment for attempt to commit offences
		85	Offences by companies
		86	Removal of Difficulties
		87	Power of central Government to make rules
		88	Constitution of Advisory Committee
		89	Power of Controller to make Regulations
		90	Power of State Government to make rules

- ✓ Requirement of various Authorities for system controls & audits:
  - A. IRDA (Insurance Regulatory & Development Authority of India)
  - B. RBI
  - C. SEBI
- ✓ Cyber Forensic and Cyber Fraud Investigation
- ✓ Information Security Standards & National Cyber Security Policy 2013
- ✓ ISO 270001 – Information Security Management Standard
- ✓ SA 402
- ✓ ITIL V3 (IT Infrastructure Library)

DOCUMENTS OR TRANSACTIONS TO WHICH THE ACT SHALL NOT APPLY:

1. A negotiable instrument other than a cheque.
2. A power-of-attorney.
3. A trust.
4. A will or any other document of testamentary nature.
5. Any contract for the sale or conveyance of immovable property or any interest in such property.

---

1. What are the objectives of ITAA?

Ans.:

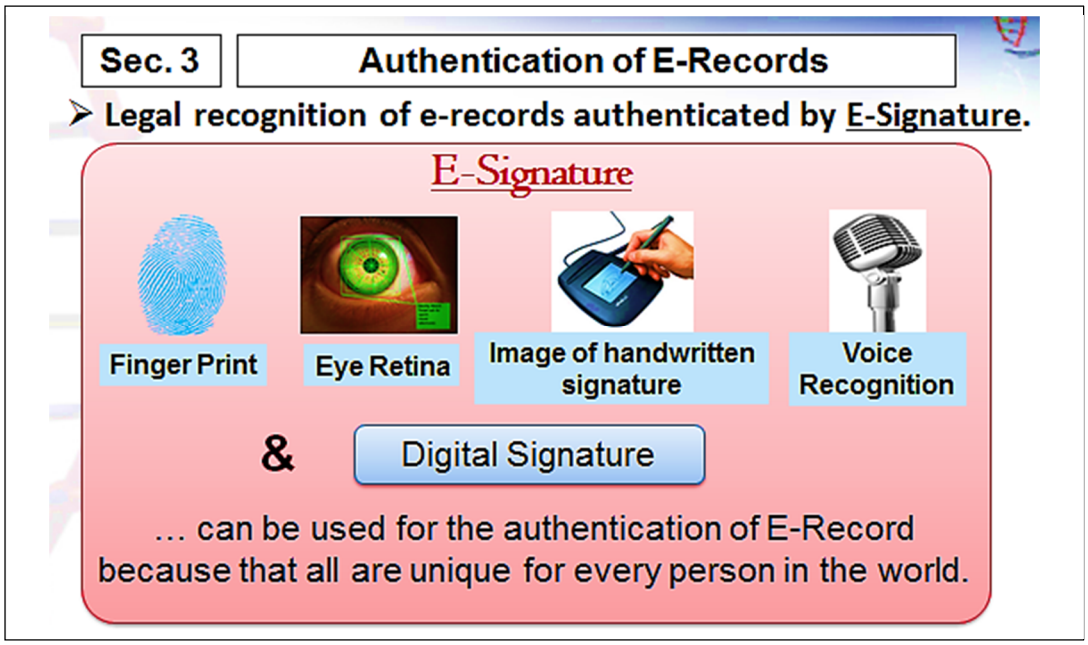
A. Legal recognition to EDI & e-commerce
B. Legal permission to EFT
C. Legal recognition to DS
D. Legal recognition to keep BOA in e-form
E. To facilitate e-storage of data
F. To facilitate e-filling with Government department
G. Legal recognition to ES
H. To include new penal provisions for new type of e-offences
I. More important to protection of IS
J. More important to protection of personal data & info.

2. What is Electronic signature (ES)?

Ans.:

Definition as per Section-2:

"Electronic Signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the 'second schedule' and includes digital signature.



3. What is digital Signature (DS)?

Ans.:

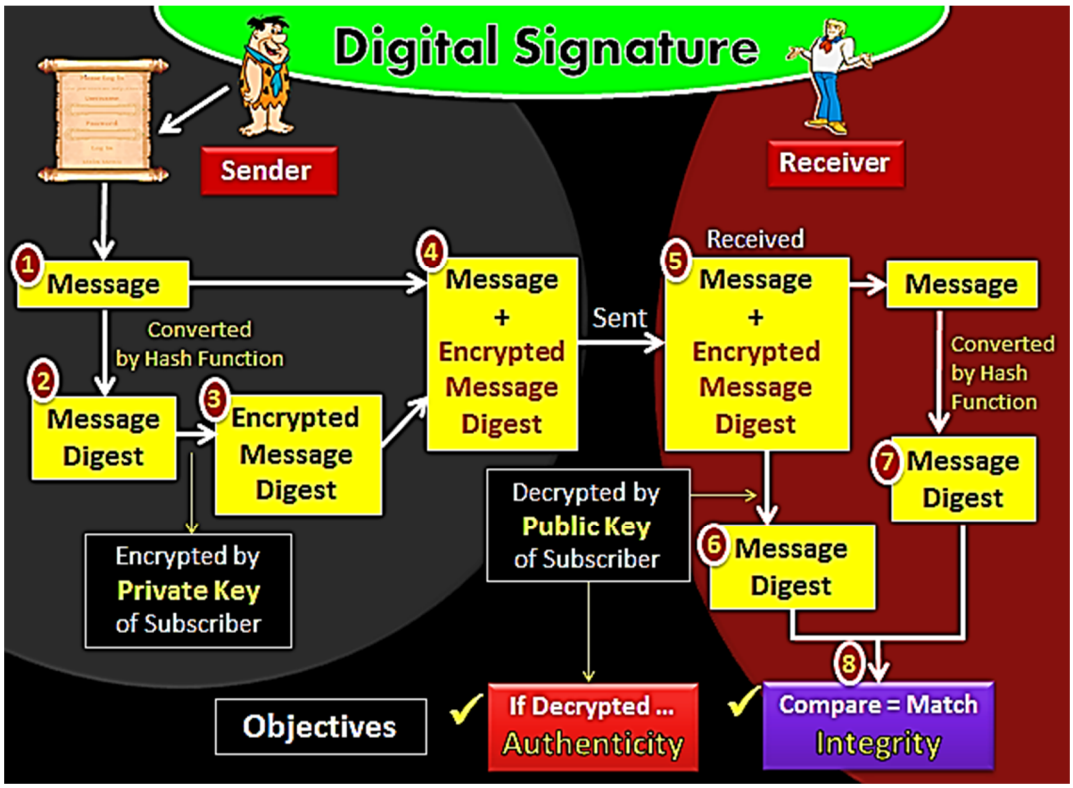
Definition as per Section-2:

"Digital Signature" means authentication of any electronic record by a subscriber by means of an electronic method / procedure in accordance with the provisions of section 3.

Steps:

1st	➢ The electronic record is converted into a message digest by using a mathematical function known as "hash function" which digitally freezes the electronic record (irreversible) thus ensuring the integrity of the content of the intended communication contained in the electronic record. ➢ Any tampering with the contents of the electronic record will immediately invalidate the digital signature (on last step).
2nd	➢ The identity of the person affixing the digital signature is authenticated through the use of a private key which attaches itself to the message digest and which can be verified by anybody who has the public key corresponding to such private key. ➢ This will enable anybody to verify whether the electronic record is retained intact or has been tampered with since it was so fixed with the digital signature. ➢ It will also enable a person who has a public key to identify the originator of the message.

Process of Digital Signature (DS):-



Section – 3:

1. Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his Digital Signature.
2. The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.
3. Any person by the use of a public key of the subscriber can verify the electronic record.
4. The private key and the public key are unique to the subscriber and constitute a functioning key pair.

For the purposes of this sub-section:

"Hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "Hash Result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible (i.e. not possible) …

a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;
b) that two electronic records can produce the same hash result using the algorithm (limitation).

4. Requirements of IRDA (Insurance Regulatory & Development Authority of India):

Ans.:

- ✓ Apex body overseeing the insurance business in India
- ✓ It protects interest of the insurance policy holders
- ✓ It regulates, promotes & ensures orderly growth of insurance business in India

Aims of IS Audit for insurance companies is to ensure…

A. Compliance with law & regulation
B. CIA of Information in IS
C. Effective & Efficient responsiveness of IS

Audit:

A. System Audit Requirements (i.e. at least once in 3 years)
B. Preliminaries
C. System Controls

5. What is Cyber Forensic & Cyber Fraud Investigation?

Ans.:

- ✓ **Investigation of internet / computer related frauds**
- ✓ One of the latest scientific techniques & emerged due to increasing internet / computer frauds.
- ✓ **Cyber + Forensic** = Internet world / computer / digital system + Scientific method of investigation

- ✓ **Cyber + Investigation** = Method of investigation together digital evidences to produce in court of law.
- ✓ Court rulings & cyber laws – Permits to rely on digital evidences
- ✓ Electronic evidences are created by using scientific techniques i.e. cyber forensic
- ✓ Follow a special method & standard method for investigation, such method is globally acceptable,
  i.e. same evidence can be checked by another expert.
- ✓ There is increasing demand for experts in cyber forensic.

6. Explain - ISO 27001 – ISMI (Information Security Management System)

Ans.:

- ✓ ISMS should establish within organization
- ✓ Purpose – organization's information is secured & properly managed
- ✓ Information like other business assets has value to organization need to be suitably protected.
- ✓ Based on key principles (Objectives of 27001) – CIA (same)
- ✓ ISO 27001 – best practice for information security management & provide systematic approach for managing confidential & sensitive information
- ✓ This standard is similar to ISO 9001 Standard which is for quality.
- ✓ ISO 27001 defines 'How to organize information security in any organization.
- ✓ i.e. standard written by "Best Security Experts" for information security & provide methodology for implementing information security in organization.

Phases of ISO 27001: (PDCA)

A. **Plan** - Identification of Risks & Vulnerabilities and selection of controls
B. **Do** - Implementation of appropriate controls from selection
C. **Check** - Monitoring the implemented controls
D. **Act** - Improve controls as find out in the check phase

7. Explain – SA 402

Ans.:

SA 402 –

Auditor's responsibility to obtain sufficient & appropriate audit evidence, when a user entity uses a service of one or more service organization (SO):

A. Understanding of services provided by service organization
B. Understanding of internal controls as SO.
C. Responding to assessed risk of material misstatement (MM)
D. Type – I & II Report
E. Fraud & Non-compliance with low & regulations
F. Uncorrected MM for activities at SO & reporting by user auditor.

8. ITIL V3 – IT Infrastructure Library

Ans.:

- ✓ ITIL is a public framework that describes best practices in IT service management (ITSM)
- ✓ Key object – Align IT services with business needs + continual measurement & improvement of quality of IT services, delivered, from both perspective business & customer.
- ✓ Now, organizations are increasing dependent on IT to achieve goal & objectives.
- ✓ Therefore, increased requirement for high quality IT services.
- ✓ **ITIL V3 consists of 5 Books:**
  - A. Service Strategy
  - B. Service Design
  - C. Service Transition
  - D. Service Operation
  - E. Continual Service Improvement

---- XXXX ---- XXXX ----

Chapter – 7 : Emerging Technologies

1. Explain - Virtualization

Ans.:

Create **A virtual version** of a device or resource (by division / consolidation) such as a server, storage device, network or even an operating system *by using specific software for the same*.

Types of Virtualization:

A. Hardware Virtualization
B. Network Virtualization
C. Storage Virtualization

2. Explain - Grid Computing

Ans.:

- ✓ **Use computing power of thousand computers**
- ✓ Grid computing is A Decentralized model, where computation could occur on many computers/domains that have already joined the grid/cluster.
- ✓ Cloud computing evolved from grid computing and provides on-demand resource provisioning.
- ✓ Grid computing requires the use of software that can divide and carve out pieces of a program as one large system image to several thousand computers (**Virtualization**).
- ✓ One concern about grid is that if one piece of the software on a node fails, other pieces of the software on other nodes may fail.
- ✓ This is improved, if that component has a failover component on another node, but problems can still arise if components rely on other pieces of software to accomplish one or more grid computing tasks.
- ✓ Large system images and associated hardware to operate and maintain them, can contribute to large capital and operating expenses.

3. Explain - Cloud computing

Ans.:

- ✓ The practice of using a network of remote servers hosted on the Internet to store, manage and process data, **rather than a local server or a personal computer**.
- ✓ CC means of computing resources as a service through networks, typically the internet.
- ✓ The internet is commonly visualized as clouds, hence the term “cloud computing” for computation done through internet.
- ✓ CC is a combination of software and hardware based computing resources delivered as a network services.
- ✓ CC is platform independent in term of computing.
- ✓ The consumers may not own the infrastructure, platform, or software in the cloud based schemes, leading to lower upfront, capital, and operating expenses.
- ✓ End users may not need to care about how severs and networks are maintained in the cloud, and can access multiple servers anywhere on the globe without knowing ‘which ones and where they are located.’

- ✓ Applications and resources can be accessed using a simple front-end interface such as a web browser.
- ✓ CC Enables anytime access to a shared pool of applications and sources.
- ✓ CC Offers services to perform operations that meet changing business needs.
- ✓ Users can access database resources, which may be highly dynamic and scalable.
- ✓ Services consumers use 'what they need on the internet' and pay only for 'what they use.'

Cloud Computing Architecture:

A. Front end Architecture
B. Back end Architecture

Cloud Computing Environment / Types of Cloud:

A. **Public Cloud** –
This environment can be used by the General Public
B. **Private Cloud** –
This cloud computing environment resides within the boundaries of an organization and is used exclusively for the organization's benefits. These are also called internal clouds.
C. **Hybrid Cloud** –
This is combination of both at least on private (internal) and at least public (external) cloud computing environments
D. **Community Clouds** -
This is the sharing of computing infrastructure in between organizations of the same community

Cloud Computing Models

1. **Infrastructure as a Service (IaaS)** – Providers/offer computers, more often virtual machines
2. **Platform as a Service (PaaS)** – Hardware + Operating System (SS)
3. **Software as a Service (SaaS)** – Provides users to access large variety of applications over internets.
4. **Network as a Service (NaaS)** – Provide Networking Services like VPN etc
5. **Communication as a Service (CaaS)** – Provide Communication Services

Potential issues relating to CC

1. Threshold Policy – Allocate & De-allocate resources on demand
2. Hidden Cost = [Cost of CC Service Provided – Cost to Company], CC provide should not disclose the same.
3. Environmental Friendly CC
4. Unexpected Behavior

5. Security Issues
6. Interoperability
   (i.e. same data format, among vendors are required, so that anyone can move to another vendor, when not satisfied with services of that one.)
7. Software Development in Cloud

What structure is used for SW Development in cloud?

1. Development Software (for Development)
2. Testing Software (for Testing)
3. Production Software (for Production)

Goals of CC

A. Efficient IT system with pooling of resources
B. Scale of IT system requirements immediately
C. Pay-Per-Use only
D. Reduced Cost
E. Access of Services from anywhere

Characteristics of Cloud Computing

A. Elasticity and Scalability (high scalability)
B. High availability & Reliability
C. Agility – Quick Responsiveness
D. Pay-per-Use (mode services)
F. Performance – loosely coupled
G. Maintenance
H. Virtualization – as above

Advantages of Cloud Computing (CA BA is Easy & Quick)

1. Cost Efficient:
2. Almost Unlimited Storage:
3. Backup and Recovery:
4. Automatic Software Integration
5. Easy Access to Information:
6. Quick Deployment:

Disadvantages of Cloud Computing

1. Confidentiality
2. Integrity
3. Availability
4. Privacy
5. Audit

6. Architecture
7. Governance
8. Trust Provided
9. Legal issues & compliance
10. Software isolation
11. Application Security
12. Data Stealing
13. Incident Response
14. Identity Management & Access Control

Similarities & Differences between GC & CC

Similarities		
1. Scalability	CPU & Network bandwidth is allocated & de-allocated on demand. i.e. Resizable	
2. Multi-tenancy & Multitasking		
3. SLAs	Guaranteed uptime availability – otherwise customer will receive credit	
Differences		
1. Computation power & Storage Capacity	Leased	Shared
2. Size	Any – 1 byte to TBs	Large size of data
3. Task	Day to day Tasks + Computational intensive	Computational intensive task
4. Cost	Low Capital & Operating Cost	Reduced Cost
5. Uptime	Very high	High

4. Explain - Mobile Computing

Ans.:

- ✓ Like mobile phone services (computing from distance)
- ✓ Mobile Computing is the use of portable computing devices (such as laptop and handheld computers) in conjunction with mobile communications technologies to enable users to access the Internet and data on their home or work computers from anywhere in the world.
- ✓ This provides ability to use computing capability without pre-defined location & connection (from anywhere, at any time) to a particular network to publish & access information.
- ✓ It is an extension of mobile phone services & related to transfer & receipt of data over cellular phone network.

- ✓ Therefore, can be used data & processing services from anywhere while moving from one location to another.

Mobile Computing Devices:

A. PDA – Personal Digital Assistance
B. Smartphone
C. Tablets
D. Ultra Mobile PC (UMPC)

Benefits:

A. Access information from anywhere & anytime
B. Update information / Process data from anywhere & anytime
C. Remote Access to knowledgebase / information
D. Help to control mobile workforce by remote access & at real time update.

5. Explain - BYOD / BYOI / BYOP / BYOPC

- ✓ Bring Your Own Device / Instrument / Phone / Personal Computer…
- ✓ This is a policy of permitting employees to bring personally owned mobile devices (like, laptop, tablet etc.) to their workplace & use these device to access company's information & applications.
- ✓ This term is also applicable for student in education institution.
- ✓ This gives right to the employees to be mobile & work beyond normal working Hours.

Emerging threats: (DANI)

A. Device Risk
B. Application Risk
C. Network Risk
D. Implementation Risk

6. Social Media & Web 2.0

Used for 2nd generation of WWW that is focused on ability for people to collaborate & share information online.

	Web 1.0	Web 2.0
1	The web	Social Web
2	Read only Web	Read & Write Web
3	Information Access	Interaction & Sharing
4	Connect to information	Connect to people
5	You find Information	Information find you
6	Static content / one way communication	Two ways communication Like, Wikis, Tagging etc.
7	Static HTML	Dynamic Web
8	Personal Website	Blogs, Facebook, Wikis etc.

Key feature of Web 2.0

A. News / information find you
B. Mostly write read web
C. Focuses on community
D. Content sharing

7. Components of Web 2.0 for social network

A. Communities:

Online space formed by a group of individual to share their thoughts, ideas & have variety of tools to promote social Networking.
Exp. – FB, WhatsApp group, CA Club Community etc.

B. Wikis:

It is a set of correlated pages on particular subject & allowed users to share content.

C. Blogging:

Blog gives users of social network the freedom to express their thoughts & generation and discussion of different topics.

D. Mash-ups:

Mash-up means "Combination of services from two or more vendors".
Like to find location any person on google map…

i. Mobile Network Service to track mobile location
ii. Map service from google to find exact location

E. Podcasting:

Sharing – files & contents = Podcasting

F. Tagging / Folksonomy:

User can tag their content / image online to any person
So that, easy to find & view content by that person, with whom intent to share.

8. Types & behavior of social network

A. Social contact network
B. Study circles
C. Social network for socialist groups
D. Social network for investors (like, Investo Pedea)
E. Networks for Fine Arts
F. Police & Military Network

9. Life cycle of social networks

A. Analyze need for social network
B. Identify initial set of members
C. Crate social network
D. Conduct regular meeting (using online tools)

E. Have discussions on important topics between members and share data with all other members
F. Interact with other network & invite other members
G. Achieve the final objective or terminate the network

10. Challenges for social network

A. Data security
B. Data Privacy
C. Cost of Advertising
D. Making sound business mode for successful operation.

11. Green IT

✓ Green IT = Use of computers in environmental friendly manner.
✓ Responsible use of computer & related resources
✓ Implementation of energy efficient CPUs, Servers, Peripheral devices

Which help to reduce...

A. Power consumptions
B. Other resources consumptions like paper etc.
C. Also includes responsible disposal of e-waste.

Best Practices in Green IT:

(i.e. What to do for best result?)

A. Involves large no. of users / members for green IT initiatives at places such as university & large IT organization campuses.
B. Partner with Government, Non-Government, Private Agencies to communication green IT benefits
C. Publish simple guidelines on using best practices for Green IT & Simple adoption of Green IT for users.
D. Provide information about ongoing commitments on Green IT & provide its economic & environmental benefits.

---- XXXX ---- XXXX ----

...Best of Luck...