INFOSECTRAIN

CISA Domain 1

The Process On

Auditing Information Systems

sales@infosectrain.com

https://www.infosectrain.com

Overall understanding of the domain:

- Weightage - This domain constitutes 21 percent of the CISA exam (approximately 32 questions)
- Covers 11 Knowledge statements covering the process of auditing information systems

1. ISACA IS Audit and Assurance Standards, Guidelines, and Tools & Techniques, Code of Professional Ethics & other applicable standard
2. risk assessment concepts and tools and techniques in planning, examination, reporting and follow-up
3. Fundamental business processes & the role of IS in these processes
4. Control principles related to controls in information systems
5. Risk-based audit planning and audit project management techniques
6. Applicable laws and regulations which affect the scope, evidence collection and preservation and frequency of audits
7. Evidence collection techniques used to gather, protect and preserve audit evidence
8. Different sampling methodologies & other substantive/data analytical procedures
9. Reporting and communication techniques
10. Audit quality assurance (QA) systems and frameworks
11. Various types of audits & methods for assessing and placing reliance on the work of other auditors or control entities

Important concepts from exam point of view:

1. Audit Charter:

- Audit Charter outlines the overall authority, scope and responsibilities of audit function
- Audit charter should be approved by Audit committee, senior management
- Internal audit function is always independent of management committee

Points to remember:

- When CISA question is on the approval of audit charter, the answer should be senior most management, based on the options available.
- IS auditor's role being more of reporting of audit observations and giving an "independent audit opinion"

2. Audit planning:

- Step 1 – Understanding of business mission, vision, objectives, process which includes information requirements under CIA trait (Confidentiality, Integrity and Availability of data)
- Step 2 – Understanding of business environment
- Step 3 - Review prior work papers
- Step 4 - Perform Risk analysis
- Step 5 - Set audit scope and objectives
- Step 6 - Develop audit plan/strategy
- Step 7 - Assign audit personal/resources

Point to remember: The first step in the audit planning is always understanding the business mission, objectives and business environment, then analyzing the risk involved based in the audit scope.

- **Audit planning includes –**

1. **Short term planning** – considers audit issues that will be covered during the year
2. **Long term planning** - audit plans that will take into account risk-related issues regarding changes in the organization's IT strategic direction that will affect the organization's IT environment.

3. Risk analysis:

- Risk is a combination of the probability of an event and its consequence (International Organization for Standardization [ISO] 31000:2009)
- Risk analysis is part of audit planning, and help identify risk and vulnerabili ties so the IS auditor can determine the controls needed to mitigate those risk

Point to remember: CISA candidate should be able to differentiate between threat and vulnerability. Threat is anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset. Vulnerability is Weakness or gap in a security program that can be exploited by threats to gain unauthorized access to an asset

- **Risk analysis covers Risk Management Framework** – ISO 27005, ISO 31000
- **Risk Assessment Process** –The process starts with identifying the source & events, then identifying the vulnerabilities associated with the sources, & then analyzing the probability of the occurrence and the impact.
- **Risk Management Process** - It begins with identifying the business object ives, the information assets that are associated with business, assessmen t of risk, how to mitigate the risk (either to avoid or transfer or mitigate/ reduce the risk) and implementing controls to mitigate the risk)

Point to remember:

- CISA candidate should be aware of the difference between Risk assessment and Risk management. Risk assessment is the process of finding where the risk exists. Risk management is the second step after performing risk assessment.
- Risk can be mitigated/reduced through implementation of controls/ third-party insurance, etc.

4. Internal Controls:

- Internal controls are normally composed of policies, procedures, practices & organizational structures which are implemented to reduce risks to the organizations

- The board of directors are responsible for establishing the effective inter nal control system

Point to remember: When CISA question is on the responsibility of internal controls, the answer should be senior most management (BoD, CEO, CIO, CISO etc) , based on the options available

- **Classification of internal controls:**

a. Preventive controls
b. Detective controls
c. Corrective controls

Point to remember: CISA question will be scenario based, where the candidate should have a thorough understanding of all the three controls and able to differentiate between preventive, detective and corrective controls

- **Preventive controls:** are those internal controls which are deployed to pre vent happening of an event that might affect achievement of organization al objectives. Some examples of preventive control activities are:

- Employee background checks
- Employee training and required certifications
- Password protected access to asset storage areas
- Physical locks on inventory warehouses
- Security camera systems
- Segregation of duties (i.e. recording, authorization, & custody all handled by separate individuals)

- **Detective controls**: Detective controls seek to identify when preventive controls were not effective in preventing errors and irregularities, particu larly in relation to the safeguarding of assets. Some examples of detect- ive control activities are:

- bank reconciliations
- control totals
- physical inventory counts
- reconciliation of the general ledgers to the detailed subsidiary ledgers
- Internal audit functions

- **Corrective controls:** When detective control activities identify an error or irregularity, corrective control activities should then see what could or should be done to fix it, & hopefully put a new system in place to prevent it the next time around. Some examples of corrective control activities are:

- data backups can be used to restore lost data in case of a fire or other disaster
- data validity tests can require users to confirm data inputs if amounts are outside a reasonable range
- insurance can be utilized to help replace damaged or stolen assets
- management variance reports can highlight variances from budget to actual for management corrective action
- training and operations manuals can be revised to prevent future errors and irregularities

5. COBIT 5:

- Developed by ISACA
- A comprehensive framework that assist enterprises in achieving their objectives for the governance & management of enterprise IT (GEIT)
- COBIT 5 based on 5 principles and 7 enablers

5 Principles	7 Enablers
1. Meeting Shareholders needs	1. Principles, Policies and Frameworks
2. End-to-End coverage	2. Processes
3. Holistic Approach	3. Organizational Structures
4. Integrated Framework	4. Culture, Ethics and Behaviour
5. Separate governance from management	5. Information
	6. Services, Infrastructure, Application
	7. People, Skills and Competencies

(Note: A CISA candidate will not be asked to specifically identify the COBIT process, the COBIT domains or the set of IT processes defined in each. However, candidates should know what frameworks are, what they do and why they are used by enterprises)

6. Risk based auditing

- **Audit Risk** - the risk that information may contain a material error that may go undetected during the course of the audit.

- The audit approach should be as follows:

- Step 1 – Gather available information and plan through review of prior year's audit results, recent financial information, inherent risk assessments
- Step 2 – Understanding of existing internal controls by analyzing control procedures, detection risk assessment
- Step 3 – Perform compliance testing by identifying key controls to be tested
- Step 4 – Perform substantive testing by test of account balances, analytical procedures
- Step 5 – Conclude the audit - Audit report with independent audit opinion

- **Factors which influence audit risk**

a. **Inherent risk** – Risk that an activity would pose if no controls/ other mitigating factors were in place.
b. **Control risk** - Risk that a material error exists that would not be prev ented or detected on a timely basis by the system of internal control
c. **Detection risk** - The risk that material errors or misstatements that have occurred will not be detected by the IS auditor
d. **Residual risk** – Risk that remains after controls are taken into account

Point to remember: A CISA candidate should know the differences between preventive, detective and corrective controls. An example of a question in the exam would be: Which of the following controls would BEST detect

7. Risk Treatment

- Risk identified in the risk assessment needs to be treated.
- Possible risk response options include:

- **Risk mitigation**—Applying appropriate controls to reduce the risk
- **Risk acceptance**—Knowingly and objectively not taking action, providing the risk clearly satisfies the organization's policy and criteria for risk acceptance
- **Risk avoidance**—Avoiding risk by not allowing actions that would cause the risk to occur
- **Risk transfer/sharing**—Transferring the associated risk to other parties (e.g., insurers or suppliers)

8. Compliance testing Vs. substantive testing

- Compliance testing - determines whether controls are in compliance with management policies and procedures
  Examples:
- User access rights
- Program change control procedures
- Review of logs
- Software license audit

- Substantive testing - gathers evidences to evaluate the integrity of individual transactions, data or other information
  Examples:
- performance of a complex calculation on sample basis
- testing of account balances

Point to remember:

- CISA question will be scenario based and the candidate should able to differentiate between substantive testing & compliance testing.
- statistical sampling is to be used when the probability of error must be objectively quantified (i.e no subjectivity is involved). Statistical sampling is an objective method of sampling in which each item has equal chance of selection

9. Audit Evidence

- any information used by the IS auditor to determine whether the entity or data being audited follows the established criteria or objectives & supports audit conclusions

- **Techniques for gathering evidence:**

- Review IS organization structures
- Review IS policies and procedures
- Review IS standards
- Review IS documentation
- Interview appropriate personnel
- Observe processes and employee performance
- Walkthrough

Point to remember: A CISA candidate, given an audit scenario, should be able to determine which type of evidence gathering technique would be best

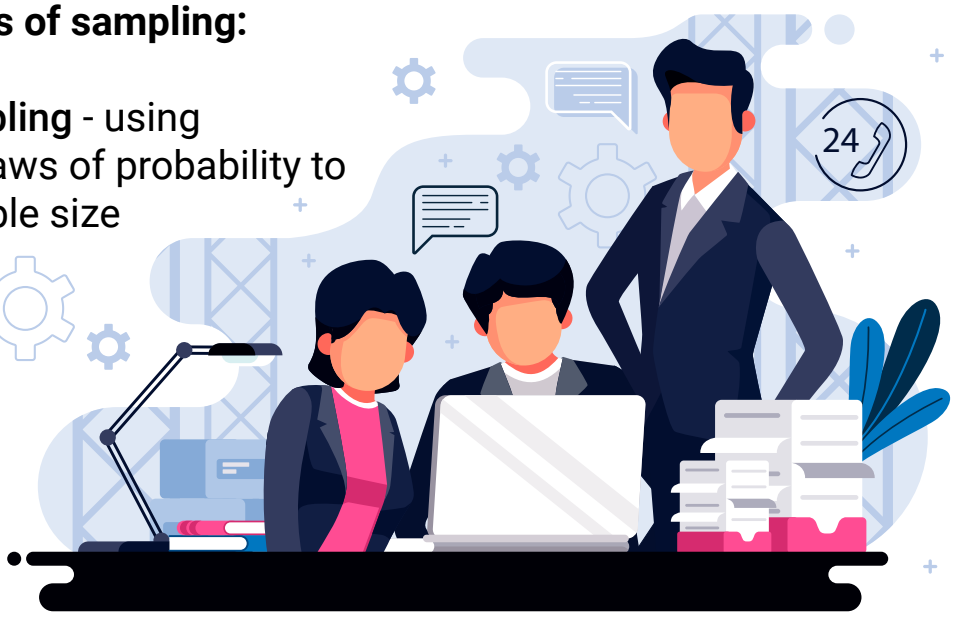
10. Audit Sampling

- The subset of population members used to perform testing

- **Two approaches of sampling:**

a. **Statistical sampling** - using mathematical laws of probability to create the sample size

b. **Non-Statistical sampling** - Uses auditor judgment to determine the method of sampling



- **Methods of sampling**

a. **Attribute sampling** - Applied in compliance testing situations, deals with the presence or absence of the attribute & provides conclusions that are expressed in rates of incidence. Involves three types:

- **Attribute sampling** - selecting a small number of transactions & making assumptions about how their characteristics represent the full population of which the selected items are a part
- **Stop-or-Go Sampling** - This model help prevents excessive sampling of an attribute by allowing an audit test to be stopped at the earliest possible moment. It is mostly used when auditor believes that relatively few errors will be found in populations
- **Discovery sampling** – It is mostly used when the objective of audit is to discover fraud

b. Variable sampling - Applied in substantive testing situations, deals with population characteristics that vary, such as monetary values & weights or any other measurement and provides conclusions related to deviations from the norm. Involves three types:

- **Stratified mean per unit** – It a statistical model in which population is divided into groups and samples are drawn from the various groups
- **Un-stratified mean per unit** – A statistical model in which sample mean (Average) is calculated and projected as an estimated total.
- **Difference estimation** – Statistical model used to estimate the total difference between audited values and unaudited values based on differences obtained from sample observations.

c. Important statistical terms:

- **Confident coefficient (CC)** – A percentage expression of the probabil ity that the characteristics of sample are true representation of the population.
  Stronger the internal control, lower the confident coefficient
- **Level of risk** – Equal to one minus the confidence coefficient [if confident co-efficient is 95%, the level of risk is (100-95= 5%)]
- **Expected error rate (ERR)** – An estimate stated as a percent of the error that may exist. The greater the ERR, greater the sample size

Point to remember: The IS auditor should be familiar with the different types of sampling techniques and when it is appropriate to use each of them

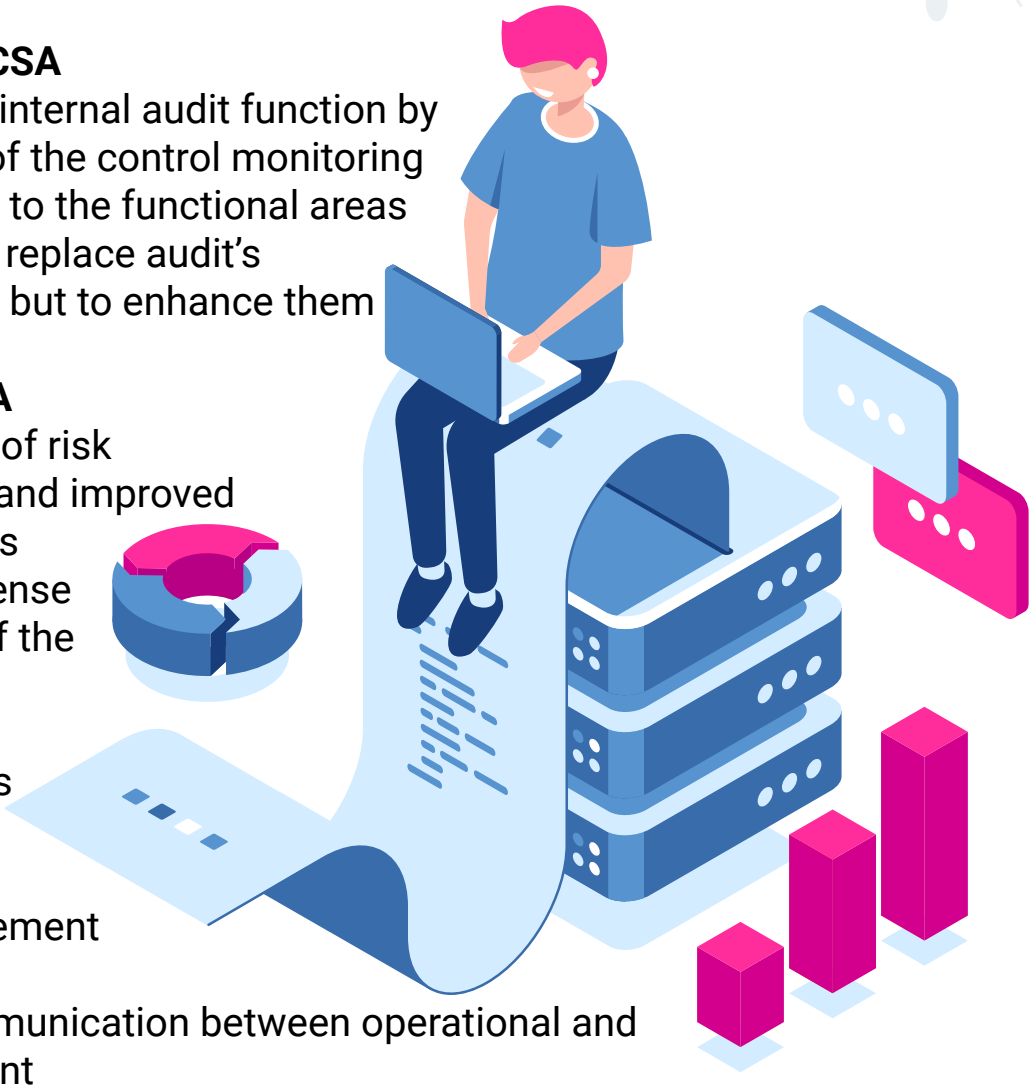
11. Control Self-assessment (CSA)

a. What is CSA?

- assessment of controls made by the staff and management of the unit or units involved
- management technique that assures stakeholders, customers and other parties that the internal control system of the organization is reliable.
- Ensures that employees are aware of the risk to the business & they conduct periodic, proactive reviews of controls

b. Objectives of CSA

- to leverage the internal audit function by shifting some of the control monitoring responsibilities to the functional areas
- not intended to replace audit's responsibilities but to enhance them



c. Benefits of CSA

- Early detection of risk
- More effective and improved internal controls
- Developing a sense of ownership of the controls in the employees and process owners
- reducing their resistance to control improvement initiatives
- Increased communication between operational and top management
- Highly motivated employees

d. Disadvantages of CSA

- mistaken as an audit function replacement
- considered as an additional workload
- Failure to act on improvement suggestions could damage employee morale
- Lack of motivation may limit effectiveness in the detection of weak controls

e. Auditor's role in CSA

- The auditor's role in CSAs should be considered enhanced when audit departments establish a CSA program.
- Auditors internal control professionals & assessment facilitators

INFOSECTRAIN

CISA Domain 2

Governance & Management of IT

sales@infosectrain.com

https://www.infosectrain.com

Overall understanding of the domain:

Weightage - This domain constitutes 16 percent of the CISA exam (approximately 24 questions)

Covers 17 Knowledge statements covering the process of auditing information systems

1. Knowledge of the purpose of IT strategy, policies, standards & procedures for an organization and the essential elements of each
2. Knowledge of IT governance, management, security and control frameworks and related standards, guidelines and practices
3. Knowledge of organizational structure, roles, and responsibilities related to IT, including segregation of duties (SoD)
4. Knowledge of relevant laws, regulations and industry standards affecting the organization
5. Knowledge of the organization's technology direction and IT architecture and their implications for setting long-term strategic directions
6. Knowledge of the processes for the development, implementation and maintenance of IT strategy, policies, standards and procedures
7. Knowledge of the use of capability and maturity models
8. Knowledge of process optimization techniques

9. Knowledge of IT resource investment & allocation practices, including prioritization criteria (e.g., portfolio management, value management, personnel management)
10. Knowledge of IT supplier selection, contract management, relation management & performance monitor processes including third party outsourcing relationships

11. Knowledge of enterprise risk management (ERM)
12. Knowledge of practices for monitoring and reporting of controls performance (e.g., continuous monitoring, quality assurance [QA])
13. Knowledge of quality management & quality assurance systems
14. Knowledge of practices for monitoring reporting of IT performance (balanced scorecards [BSCs], key performance indicators [KPIs])
15. Knowledge of business impact analysis (BIA)
16. Knowledge of the standards and procedures for the development, maintenance and testing of the business continuity plan (BCP)
17. Knowledge of procedures used to invoke and execute the business continuity plan and return to normal operations

Important concepts from exam point of view:

1. Corporate Governance:

- It is a system by which entity is controlled and directed
- Set of responsibilities and practices who provide strategic directions, thereby ensuring that
  - Goals are achievable,
  - Risk are properly addressed and
  - Organizational resources are properly utilized
- Involves a set of relationships between a company's management, its board, its shareholders and other stakeholders

Points to remember:

- To have an effective IT Governance, IT plan should be consistent with overall business plan
- To improve information security alignment with business the best practice is to involve top management to mediat-e between business and information systems.

2. Governance of Enterprise IT (GEIT):

- GEIT is one of the domains of Corporate governance
- GEIT is a system in which all stakeholders, including the board, senior management, internal customers & departments such as finance, provide input into the decision-making process.
- GEIT is the responsibility of the board of directors and executive management.
- Purposes of GEIT are:

a. to direct IT endeavors to ensure that IT performance meets the ob jectives of aligning IT with the enterprise's objectives & the realiza tion of promised benefits

b. enable the enterprise by exploiting opportunities and maximizing benefits

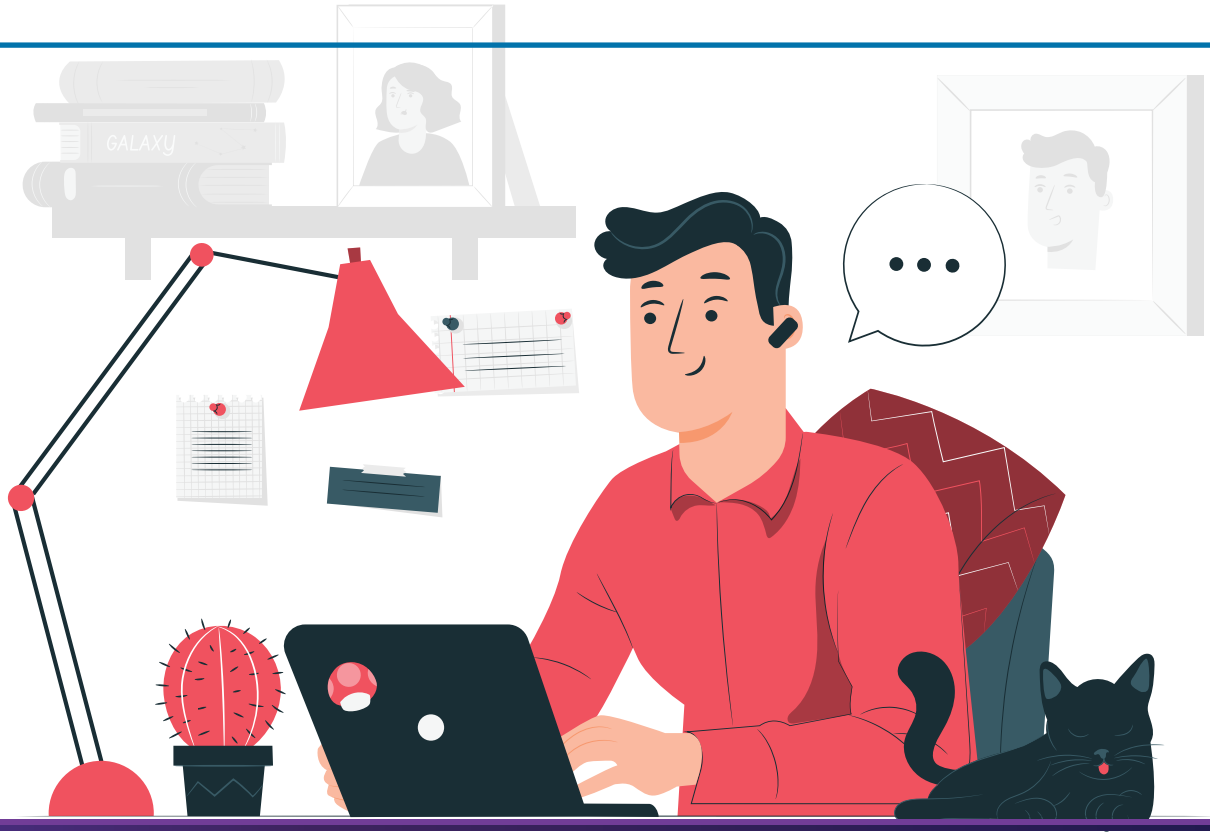
c. IT resources should be used responsibly, and IT-related risk should be managed Appropriately

- Key element of GEIT is the alignment of business and IT, leading to the achievement of business value.
- Examples of GEIT includes the following:
- COBIT 5 is developed by ISACA, which includes five principles, five domains, 37 processes and 210 practices
- The International Organization for Standardization (ISO)/Internati-onal Electro-technical
  Commission (IEC) 27001 (ISO 27001) - provides guidance to organizations implementing and maintaining information security programs.
- The Information Technology Infrastructure Library (ITIL) was devel oped by the UK
  Office of Government Commerce (OGC)
- ISO/IEC 38500:2008 Corporate govern of information technology
- ISO/IEC 20000 is a specification for service management that is aligned with ITIL's service management framework

Points to remember:

- Though ISACA does not test on ISO numbers, it is good to know the ISO numbers and standards and their scope /description, to understand the subject better
- ISO 27001 (BS7799) - ISO for information security man agement system (ISMS)(Requirements - 0 t 10; Controls – 114; Control objectives – 35; Domains -14)
- ISO 38500 -Information technology–Security techniques – Code of practice for information security controls.
- ISO 20000 - ISO for Information technology service man - agement (ITSM) system. The standard was developed to mirror the best practices described – ITIL

- Relationship between COBIT and ITIL - COBIT defines IT goals, whereas ITIL provides the process-level steps on how to achieve them
- how to achieve them



3. Auditor's Role in Governance of Enterprise IT (GEIT):

- To provide leading practice recommendations to senior management to help improve the quality and effectiveness of the IT governance initiatives implemented.
- Helps ensure compliance with GEIT initiatives implemented within an organization
- continuous monitoring, analysis & evaluation of metrics associate with GEIT initiatives require an independent and balanced view to ensure a qualitative assessment that subsequently facilitates the qualitative improvement of IT processes & associated GEIT initiatives
- To check on alignment of the IT function with the organization's mission, vision, values, objectives and strategies
- To ensure compliance with legal, environmental, information quality, fiduciary, security and privacy requirements

4. IT Balanced Score Card (BSC):

- BSC is a process management evaluation technique that can be applied to the GEIT process in assessing IT functions & processes
- BSC is the most effective means to aid the IT strategy committee management in achieving IT governance through proper IT and business alignment

Points to remember:

- The purpose of IT Balance Score card is to evaluate & monitor performance indicators – Customer satisfaction, internal processes, innovation capacity, etc.
- The IT BSC does not measure the financial performance of the enterprise

5. IT Governing committees:

- Organizations, broadly have two committees

1. IT Strategy committee
2. IT Steering committee

- There should be a clear understanding of both the IT strategy & IT steering committee

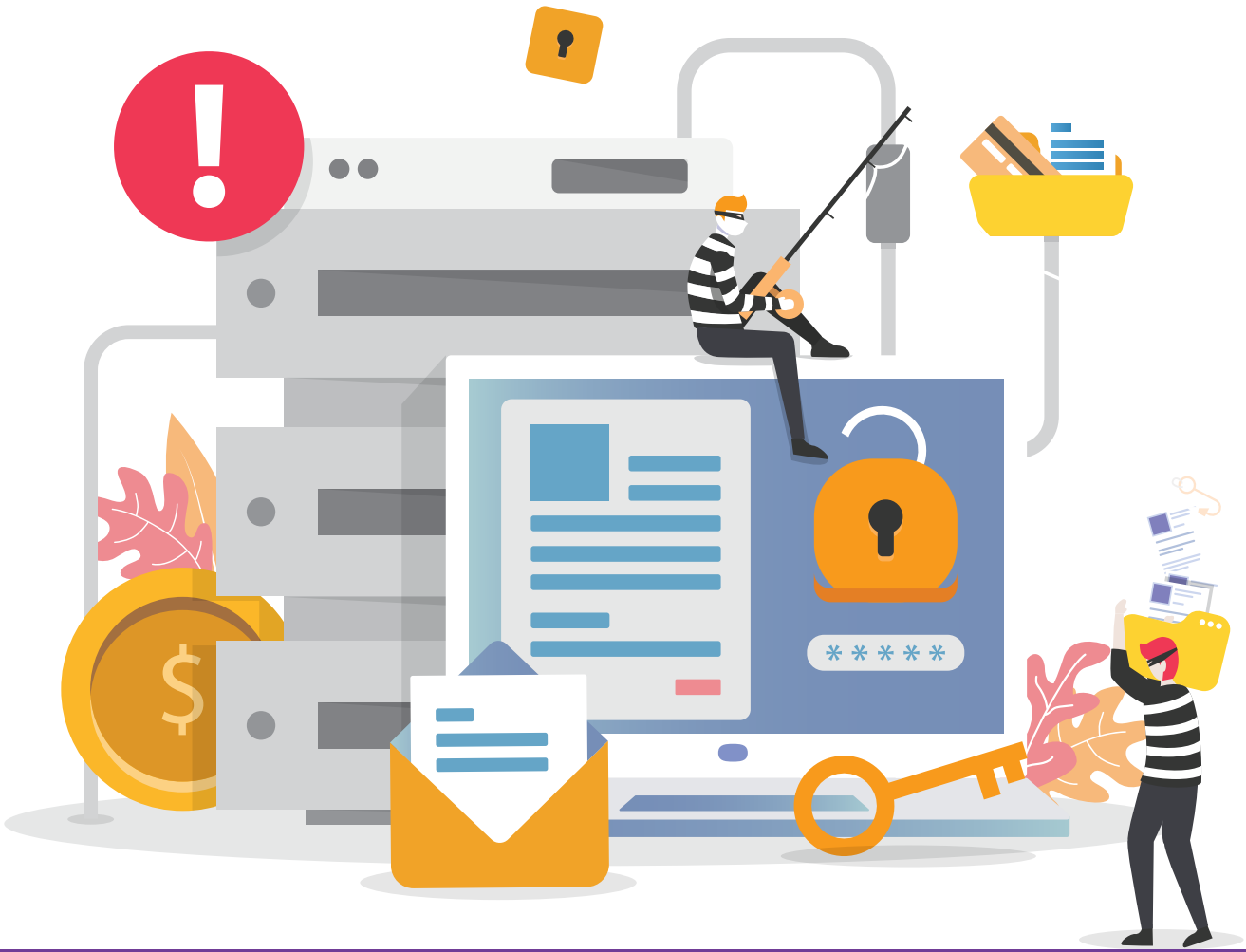
- **Role of IT strategy committee:**
- Advises the board and management on IT strategy
- Is delegated by the board to provide input to the strategy & prepare its approval
- Focuses on current and future strategic IT issues
- Provides insight and advice to the board on topics such as:
- The alignment of IT with the business direction
- The availability of suitable IT resources, skills and infrastructure to meet the strategic objectives
- The achievement of strategic IT objectives

- **Membership of IT Strategy committee:**
- Board members, and
- Specialist non-board members

- **Role of IT Steering committee:**
- Assists the executive in the delivery of the IT strategy
- Oversees day-to-day management of IT service delivery, IT projects
- Focuses on implementation
- Decide the overall level of IT spending & how costs will be allocate
- Approves project plans & budgets, setting priorities & milestones
- Communicates strategic goals to project teams
- Monitors resource & priority conflict between enterprise divisions and the IT function as well as between projects
- Report to the board of directors on IS activities.
- Make decisions regarding centralization versus decentralization & assignment of responsibility.

Points to remember: The enterprise's risk appetite is best established by IT Steering committee.

- **Membership of IT Strategy committee:**
- Sponsoring executive
- Business executive (key users)
- Chief information officer (CIO)
- Key advisors as required (IT, audit, legal, finance)



6. Maturity and Process Improvement Models:

- Implementation of IT governance requires ongoing performance measurement of an organization's resources that contribute to the execution of processes that deliver IT services to the business

- **Some of the process improvement models are:**
- The IDEAL model is a software process improvement (SPI) program model in planning & implementing an effective software process improvement program and consists of five phases:

1. Initiating,
2. Diagnosing,
3. Establishing,
4. Acting and
5. Learning

- The COBIT Process Assessment Model (PAM), using COBIT 5,
- Capability Maturity Model Integration (CMMI) - is a process improvement approach that provides enterprises with the essential elements of effective processes. It is based on ISO/IEC 15504 Information Technology—Process Assessment standard. CMMI have five maturity levels

- **Level 1** – Initial – This is a riskiest stage an organization can find itself- unpredictable environment that increases risk, inefficiency.
- **Level 2** – Managed – Projects are planned & performed, however there are lot of issues to be addressed
- **Level 3** – Defined – Organizations are proactive at this level, rather than reactive. Processes are tailored for the organization. Organization is aware of their shortcomings, how to address and plans for improvement.
- **Level 4** - Quantitatively managed – This level is more measured & controlled. The organization is ahead of risks, with more data-driven insight into process deficiencies.
- **Level 5** – Optimised – At this stage, the processes are stable and flexible. The organization will be in constant state of improving & responding to changes or other opportunities.

7. Risk Management:

- The process of identifying vulnerabilities & threats to the information resources used by an organization in achieving business objectives & what countermeasures to take in reducing risk to an acceptable level.
- encompasses identifying, analyzing, evaluating, treating, monitoring and communicating the impact of risk on IT processes
- The Board may choose to treat the risk in any of the following ways

1. **Avoid**—Eliminate the risk by eliminating the cause
2. **Mitigate**—Lessen the probability or impact of the risk by defining, implementing and monitoring appropriate controls
3. **Share/Transfer (deflect, or allocate)**—Share risk with partners or transfer via insurance coverage, contractual agreement or other means
4. **Accept**—Formally acknowledge the existence of the risk & monitor it.

Points to remember: The best to assess IT risks is achieved by - evaluating threats associated with existing IT assets and IT projects.

- The steps of Risk Management process involve:

- **Step – 1:** Asset identification – Examples: Information, Data, Soft ware, Hardware, documents, personnel.
- **Step – 2:** Evaluation of threats and vulnerabilities:

a. **Threat** - A threat is a person or event that has the potential for im pacting a valuable resource in negative manner. Common clauses of threats are:

- Errors
- Malicious damage/attack
- Fraud
- Theft
- Equipment/software failure

b. **Vulnerability** - Vulnerability refer to weaknesses in a system. They make threat outcomes possible and potentially even more dangerous. Examples are:

- Lack of user knowledge
- Lack of security functionality
- Inadequate user awareness/education (e.g., poor choice of passwords)
- Untested technology
- Transmission of unprotected communications

- **Step 3 – Evaluation of the impact** – The result of a threat agent exploiting a vulnerability is called an impact
- In commercial organizations, threats usually result in

a. a direct financial loss in the short term or
b. an ultimate (indirect) financial loss in the long term

- **Examples of such losses include:**

- Direct loss of money (cash or credit)
- Breach of legislation (e.g., unauthorized disclosure)
- Loss of reputation/goodwill
- Endangering of staff or customers
- Breach of confidence
- Loss of business opportunity
- Reduction in operational efficiency/performance
- Interruption of business activity

- **Step 4 – Calculation of Risk** – A common method of combining the elements is to calculate for each threat:probability of occurrence × magnitude of impact. This will give a measure of overall risk.
- **Step 5 – Evaluation of and response to Risk**

- After risk has been identified, existing controls can be evaluated or new controls designed to reduce the vulnerabilities to an accept level.
- These controls are referred to as countermeasures or safeguards and include actions, devices, procedures or techniques
- Residual risk, the remaining level of risk after controls have been applied, can be used by management to further reduce risk by identifying those areas in which more control is required.

8. Human Resource Management:

- **On Hiring process**, the first step before hiring a candidate is back ground checks (e.g., criminal, financial, professional, references, qualifications)

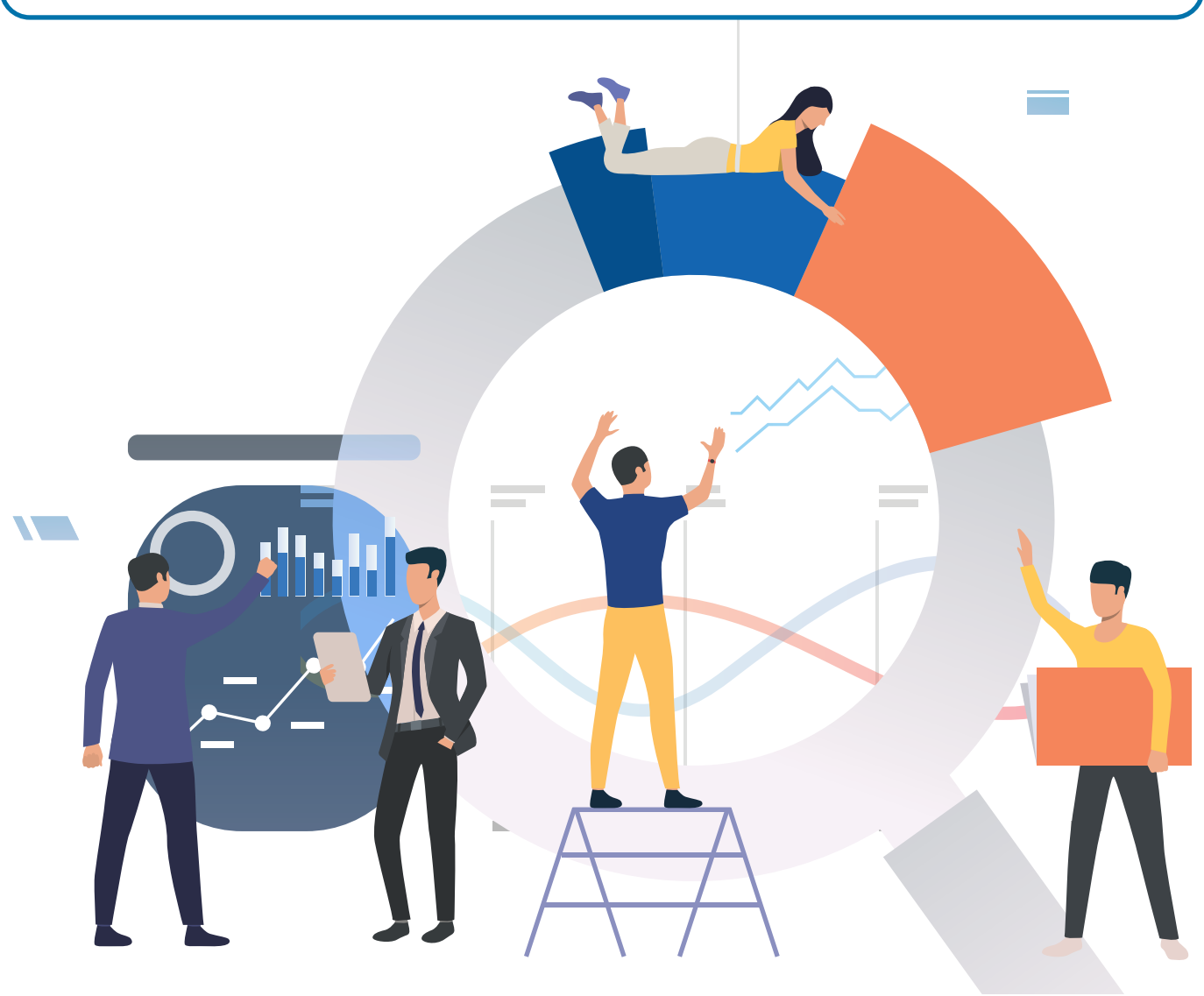
- **A required vacation** (holiday) ensures that once a year, at a minimum, someone other than the regular employee will perform a job function. This reduces the opportunity to commit improper or illegal acts. During this time, it may be possible to discover fraudulent activity as long as there has been no collusion between employees to cover possible discrepancies (Mandatory leave is a control measure)

- **Job rotation** provides an additional control (to reduce the risk of fraudulent or malicious acts) because the same individual does not perform the same tasks all the time. This provides an opportunity for an individual other than the regularly assigned person to perform the job and notice possible irregularities.

- **On Termination policies**, policies be structured to provide adequate protection for the organization's computer assets & data. The following control procedures should be applied:
  - Return of all devices, access keys, ID cards and badges
  - Deletion/revocation of assigned logon IDs and passwords
  - Notification to appropriate staff and security personnel regarding the employee's status change to "terminated"
  - Arrangement of the final pay routines
  - Performance of a termination interview

Points to remember:

- The CISA candidate should be aware of the above process – from hiring to termination. ISACA tests on the knowledge at each step – on what the enterprise should/should not do.
- The employees should be aware of the enterprise IS policy. If not, the lack of knowledge would lead to unintentional disclosure of sensitive information
- When an employee is terminated, the immediate action/ most important action/first step that the enterprise should do is – disable the employee's logical access and communicate on the termination of the employee



9. Sourcing Practices:

- **Delivery of IT functions can include:**
- **Insourced** - Fully performed by the organization's staff
- **Outsourced** - Fully performed by the vendor's staff
- **Hybrid** - Performed by a mix of the organization's and vendor's staffs; can include joint ventures/supplemental staff

- IT functions can be performed across the globe, taking advantage of time zones and arbitraging labor rates, and can include:
- **Onsite** - Staff work onsite in the IT department.
- **Offsite** - Also known as nearshore, staff work at a remote location in the same geographic
- **Offshore**—Staff work at a remote location in a different geographic region

- **Objective of outsourcing** - to achieve lasting, meaningful improvement in business processes and services through corporate restructuring to take advantage of a vendor's core competencies

- The management should consider the following areas for moving IT functions offsite or offshore:
- Legal, regulatory and tax issues
- Continuity of operations
- Personnel
- Telecommunication issues
- Cross-border and cross-cultural issues

Points to remember:

- The most important function of IS management in outsourcing practices is - monitoring the outsourcing provider's performance
- The enterprise cannot outsource the accountability for IT security policy. The accountability always lies with the senior management/Board of directors
- When the outsourcing service is provided in another country, the major concern for the IS auditor is–the legal jurisdiction can be questioned
- The clause in outsourcing contract that can help in improving the service levels and minimize the costs is – Gain-sharing performance bonuses.

10. Information Security – Roles and Responsibilities:

Role	Responsibilities
a. Systems development manager	Responsible for programmers and analysts who implement new system and maintain existing systems
b. Project management	Responsible for planning & executing IS projects and may report to a project management office or to the development organization
c. Help desk (service desk)	Responds to technical questions and problems faced by users
d. Quality assurance (QA) manager	Responsible for negotiating and facilitating quality activities in all areas of information technology.
e. Information security management	Separate IT department, headed by a CISO. The CISO may report to the CIO or have a dotted-line (indirect reporting) relationship to the CIO
f. Systems administrator	Responsible for maintaining major multiuser computer systems, including LAN, WLANs, WANs, etc.
g. Database Administration	Maintains the data structures in the corporate database system

Business Continuity Planning (BCP):

- The purpose of business continuity/disaster recovery is to enable a business to continue offering critical services in the event of a disruption and to survive a disastrous interruption to activities.

- The first step in preparing a BCP is to identify the business processes of strategic importance—those key processes that are responsible for both the permanent growth of the business and for the fulfillment of the business goals
- Based on the key processes, the risk management process should begin with a risk assessment
- The result of the risk assessment should be the identification of the following:

a. The human resources, data, infrastructure elements and other resources (including those provided by third parties) that support the key processes
b. A list of potential vulnerabilities—the dangers or threats to the organization
c. The estimated probability of the occurrence of these threats
d. The efficiency and effectiveness of existing risk mitigation control (risk countermeasures)

- BCP is primarily the responsibility of senior management
- ISO for BCP – ISO 22301

- The IT business continuity plan should be aligned with the strategy of the organization. If the IT plan is a separate plan, it must be con sistent with and support the corporate BCP.
- **Business Continuity policy:**
- Is a document approved by top management that defines the extent and scope of the business continuity effort (a project or an ongoing program) within the organization
- Should be pro-active
- Is a most critical corrective control
- The business continuity policy serves several other purposes:
- Its internal portion is a message to internal stakeholders (i.e., employees, management, board of directors) that the company is undertaking the effort, committing its resources and expecting the rest of the organization to do the same.
- Its public portion is a message to external stakeholders (share holders, regulators, authorities, etc.) that the organization is treat its obligations (e.g., service delivery, compliance) seriously.

- **Business Continuity Planning (BCP) Incident Management:**
- An incident is
- any unexpected event, even if it causes no significant damage
- Dynamic in nature
- Depending on an estimation of the level of damage to the organi- zation, all types of incidents should be categorized. A classifica- tion system could include the following categories:
- **Negligible** - incidents are those causing no perceptible or signific- ant damage
- **Minor** - events are those that, while not negligible, produce no neg ative material (of relative importance) or financial impact
- **Major** - incidents cause a negative material impact on business processes and may affect other systems, departments or even outside clients
- **Crisis** - major incident that can have serious material (of relative importance) impact on the continued functioning of the business and may also adversely impact other systems or third parties.

12. Business Impact Analysis (BIA):

- critical step in developing the business continuity strategy and the subsequent implementation of the risk countermeasures and BCP in particular.
- used to evaluate the critical processes (IT components supporting them) and to determine time frames, priorities, resources and inter dependencies
- **Different approaches for performing BIA:**
  - Detailed questionnaire
  - Interview groups of key users
  - Bring relevant IT personnel and end users (i.e., those owning the critical processes) together in a room to come to a conclusion regarding the potential business impact of various levels of disruptions.

13. Classification of systems and criticality analysis:

- **Critical** - These functions cannot be performed unless they are replaced by identical capabilities
- **Vital** - These functions can be performed manually, but only for a brief period of time (usually five days or less)
- **Sensitive** - These functions can be performed manually, at a tolera ble cost & for an extended period of time. While they can be perfo- rmed manually, it usually is a difficult process and requires additi- onal staff to perform.
- **Non-sensitive** - These functions may be interrupted for an extend ed period of time, at little or no cost to the company, and require little or no catching up when restored.

Points to remember:

- The first resource to be protected when designing continui ty plan provisions and processes – Human Resource/ People
- The first step in business continuity life cycle is – BCP scope, followed by Risk assessment
- The insurance that covers loss incurred from dishonest or fraudulent acts by employees – Fidelity coverage

14. Components of Business Continuity Planning (BCP):

- **Business Continuity Planning (BCP)** – Provides procedures for sustaining mission/business operations while recovering from a significant disruption
- **Continuity of Operations Plan (COOP)** - Provides procedures and guidance to sustain an organization's MEFs (Mission Essential Functions) at an alternate site for up to 30 days;
- **Business resumption plan** - Provides procedures for relocating information systems operations to an alternate location.
- Continuity of support plan / IT contingency plan
- Crisis communications plan
- Incident response plan
- Transportation plan
- Occupant emergency plan (OEP)
- Evacuation and emergency relocation plan

Points to remember:

- The authority to make a disaster declaration is Business Con tinuity Coordinator or backup personnel identified in the suc cession plan
- The primary responsibility for establishing organization-wide contingency plans lies with the Board of Directors.

15. Plan Testing:

- Should be scheduled during a time that will minimize disruptions to normal operations
- Key recovery team members be involved in the test process and allotted the necessary time to put their full effort into it
- Should address all critical components and simulate actual prime time processing conditions, even if the test is conducted in off hours.
- **Plan Execution**: Pre-test, Test, Post-Test
- **Types of tests:**

- **Desk-based evaluation/paper test** - A paper walk-through of the plan, involving major players in the plan's execution who reason out what might happen in a particular type of service disruption.
- **Preparedness test** - Usually a localized version of a full test, wherein actual resources are expended in the simulation of a system crash
- **Full operational test**—This is one step away from an actual service disruption. The organization should have tested the plan well on paper and locally before endeavoring to completely shut down operations.

INFOSECTRAIN

CISA Domain 3

Information Systems Acquisition, development & implementation

Overall understanding of the domain:

Weightage - This domain constitutes 18 percent of the CISA exam (approximately 27 questions)
Covers 14 Knowledge statements covering the process of auditing information systems

1. Knowledge of benefits realization practices, (e.g., feasibility studies, business cases, total cost of ownership [TCO], return on investment [ROI])
2. Knowledge of IT acquisition & vendor management practices (e.g., evaluation & selection process, contract management, vendor risk and relationship management, escrow, software licensing) including third-party outsourcing relationships, IT suppliers and service providers.
3. Knowledge of project governance mechanisms (e.g., steering committee, project oversight board, project management office)
4. Knowledge of project management control frameworks, practices and tools
5. Knowledge of risk management practices applied to projects
6. Knowledge of requirements analysis & management practices (e.g., requirements verification, traceability, gap analysis, vulnerability management, security requirements)
7. Knowledge of enterprise architecture related to data, applications, technology (e.g., web-based applications, web services, n-tier applications, cloud ser vices, virtualization)
8. Knowledge of system development methodologies & tools including their strengths & weaknesses (e.g, agile development practices, prototyping, rapid application development [RAD], object-oriented design techniques, secure coding practices, system version control)
9. Knowledge of control objectives & techniques that ensure the completeness, accuracy, validity and authorization of transactions and data
10. Knowledge of testing methodologies & practices related to the information system development life cycle (SDLC)
11. Knowledge of configuration & release management relating to the development of information systems
12. Knowledge of system migration & infrastructure deployment practices & data conversion tools, techniques and procedures
13. Knowledge of project success criteria and project risk
14. Knowledge of post-implementation review objectives & practices (e.g., - control implementation, benefits realization, performance measurement)

Important concepts from exam point of view:

1. Benefits realization:

The objectives of benefits realization are

- is to ensure that IT & business fulfill their value management responsibilities
- IT-enabled business investments achieve the promised benefits and deliver measurable business value
- Required capabilities (solutions & services) are delivered on time and within budget

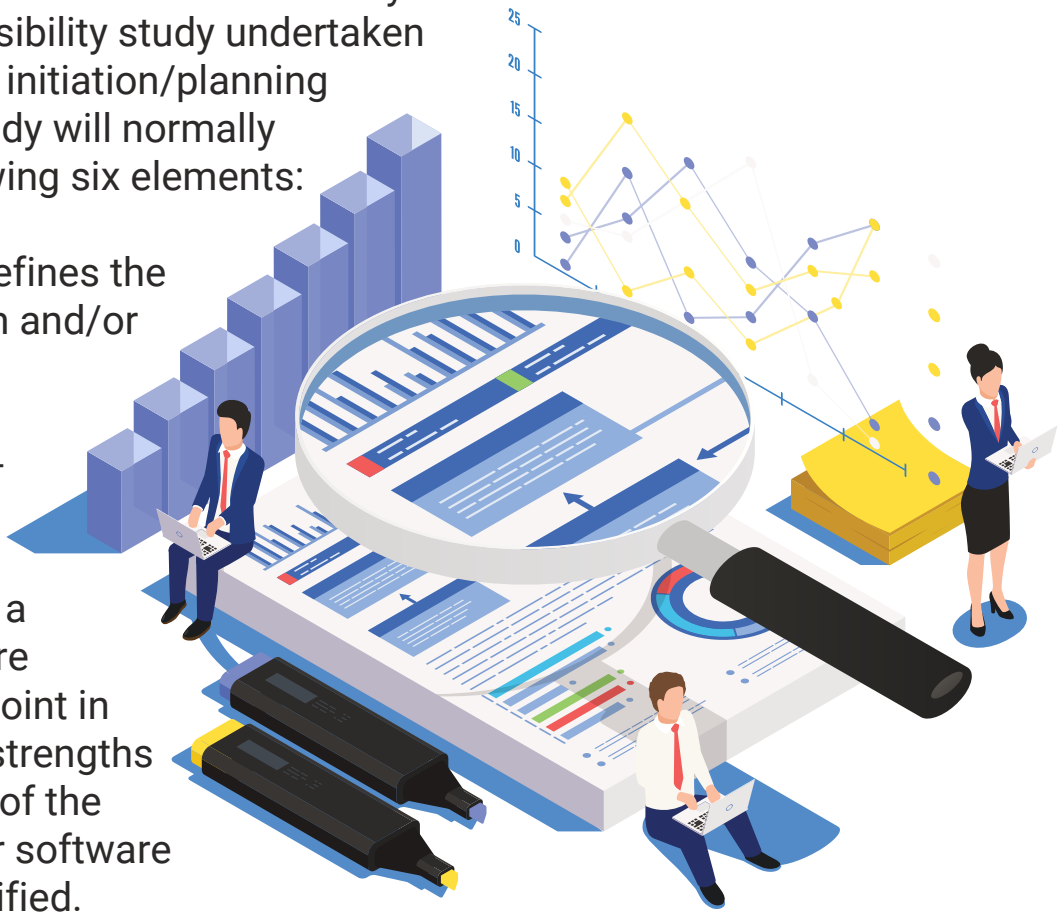
2. Portfolio/Program Management:

The objectives of project portfolio management are:

- Optimization of results of the project portfolio (not of the individual project)
- Prioritizing and scheduling projects
- Resource coordination (internal and external)
- Knowledge transfer throughout the projects

3. Business case development and approval:

- A business case provides the information required for an organization to de cide whether a project should proceed
- A business case is the first step in a project or a precursor to the commenc- ement of the project
- The business case should also be a key element of the decision process th- roughout the life cycle of any project
- The initial business case would normally derive from a feasibility study undertaken as part of project initiation/planning
- The feasibility study will normally include the following six elements:



I. **Project Scope** - defines the business problem and/or opportunity to be addressed
II. **Current Analysis** - defines and establishes an understanding of a system, a software Product. At this point in the process, the strengths and weaknesses of the current system or software product are identified.
III. **Requirements** - defined based upon stakeholder needs and constraints
IV. **Approach** - Recommended system and/or software solution to satisfy the Requirements
V. Evaluation is based upon the previously completed elements within the feas ibility study. The final report addresses the cost-effectiveness of the appro- ach selected
VI. **Review** – A formal review of feasibility study report is conducted with all stakeholders

4. Benefit realization techniques:

- COBIT 5 provides the industry accepted framework under which IT governance goals & objectives are derived from stakeholder drivers with the intent of enterprise IT generating business value from IT-enabled investments
- COBIT 5 based on 5 principles and 7 enablers

5 Principles	7 Enablers
1. Meeting Shareholders needs	1. Principles, Policies & Frameworks
2. End-to-End coverage	2. Processes
3. Holistic Approach	3. Organizational Structures
4. Integrated Framework	4. Culture, Ethics and Behaviour
5. Separate governance from management	5. Information
	6. Services, Infrastructure & Applications
	7. People, Skills and Competencies

5. Project Management structure:

- Project management is business process in a project-oriented organization
- Some of the most prominent standards and organizations - PRINCE2TM
- The project management process begins with the project charter and ends with the completion of the project
- Project Charter provides a preliminary delineation of roles & responsibilities, outlines the project objectives, identifies the main stakeholders, and defines the authority of the project manager

6. Project Organizational forms:

- Three major forms of organizational alignment for project management are

- **Influence project organization –**
  - The project manager has only a staff function without formal management authority
  - The project manager is only allowed to advise peers and team members as to which activities should be completed

- **Pure project organization –**
  - The project manager has formal authority over those taking part in the project
  - providing a special working area for the project team that is separated from their normal office space

- **Matrix project organization -**
  - Management authority is shared between the project manager and the department heads.

7. Project communication and culture:

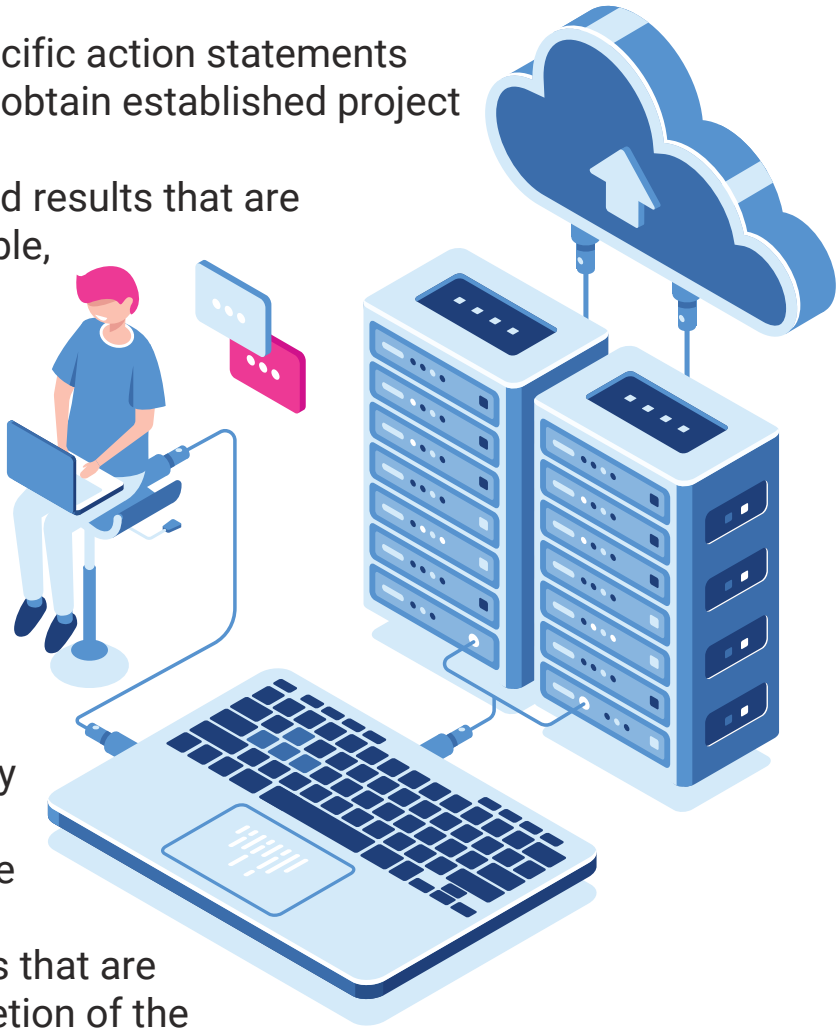
- Project communication can be achieved by

- **One-on-one meetings** - One-on-one meetings and a project start workshop help to facilitate two-way communication between the project team members and the project manager
- **Kick-off meetings** - A kick-off meeting may be used by the project manager to inform the team of what has to be done for the project
- **Project start workshops** - communication is open & clear among the project team to use a project start workshop to obtain cooperation from all team members and buy-in from stakeholders. This helps develop a common over view of the project & communicates the project culture early in the project.
- **A combination of the three**

- A project culture is comprised of shared norms, beliefs, values & assumptions of the project team.

- A key success factor for establishing the correct project culture is defining and adapting the unique characteristics of a project

8. Project objectives:



- Project objectives are the specific action statements that support the road map to obtain established project goals
- A project needs clearly defined results that are specific, measurable, attainable, realistic and timely (SMART)
- These objectives are broken down into three –

  - **Main objectives** are the primary reason for the project and will always be directly coupled with business success
  - **Additional objectives** are objectives that are not directly related to the main results of the project but may contribute to project success
  - **Non-objectives** are the results that are not to be expected on completion of the project.

- A commonly accepted approach to define project objectives is to start off with an object breakdown structure (OBS).

- After the OBS has been compiled or a solution is defined, a work breakdown structure (WBS) is designed to structure all the tasks that are necessary to build up the elements of the OBS during the project

9. OBS – Object based Structure:

- It represents the individual components of the solution and their relationships to each other in a hierarchical manner, either graphically or in a table.
- An OBS can help, especially when dealing with nontangible project results such as organizational development, to ensure that a material deliverable is not overlooked.

10. WBS – Object based Structure:

- WBS is designed to structure all the tasks that are necessary to build up the elements of the OBS during the project.
- The WBS represents the project in terms of manageable and controllable units of work, serves as a central communications tool in the project, and forms the baseline for cost and resource planning.

11. Roles and Responsibilities:

- **Senior Management** - Demonstrates commitments to the project & approve the resources
- **User management** – Assumes ownership of the project & resulting systems, allocates qualified resources, and actively participates in business process redesign, system requirement definitions, test case development, acceptance testing and user training
- **Project steering committee**–It provides overall directions & also responsible for all deliverables, project cost, and schedules
- **Project sponsor** – Providing funding for the project.
- **Systems development management** – Provides technical supports for hard ware and software environment by developing, installing User project team

  Completes assigned task, communicates effectively with user by actively involving them in the development process as a subject matter expert.
- **Security officer** – Ensures that systems controls and supporting processes provide an effective level of protection based on data classifications
- **Quality assurance** – person who review results and deliverables within each phase & at the end of each phase and confirm compliance requirement & operating the requested systems.
- **Project manager** – Day to day management and leadership of the project
- **Systems development project team** – Completes assigned task, communicates effectively with user by actively involving them in the development process.

Points to remember:

- The CISA candidate should be familiar with general roles and responsi bilities of groups or individuals involved in the systems development process.

12. Project Management practices:

- Project management is the application of knowledge, skills, tools & techniques to a broad range of activities to achieve a stated objective such as meeting the defined user requirements, budget and deadlines for an IS project

- Project management knowledge and practices are best described in terms of their component processes of

a. initiating,
b. planning,
c. executing and controlling and
d. closing a project

- **Initiation of the project**
  - Initiated by project manager or sponsor
  - often be compiled into terms of reference or project charter that states the objective of the project, the stakeholders in the system to be produced, & the project manager and sponsor
  - Approval of a project initiation document (PID) or a project request document (PRD) is the authorization for a project to begin

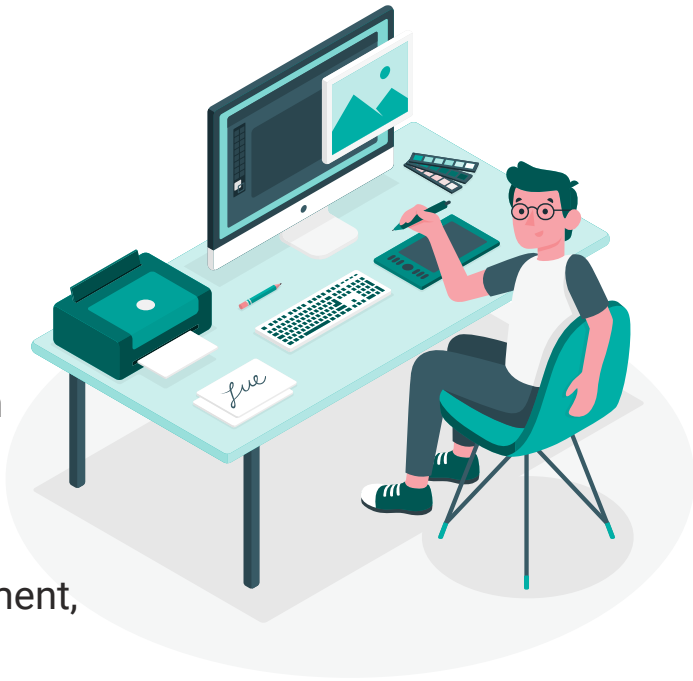
- **Project planning**
  - The project manager should determine the following as part of project planning

  - Project scope
  - The various tasks that need to be performed to produce the expected business application system
  - The sequence or the order in which these tasks need to be performed
  - The duration or the time window for each task
  - The priority of each task
  - The IT resources that are available and required to perform these tasks
  - Budget or costing for each of these tasks
  - Source and means of funding

- **System Development Project Cost Estimation**

  The following are the four methods in determining the cost of system development project:

  1. Analogous estimating
  2. Parametric estimating
  3. Bottom-up estimating
  4. Actual costs



- **Software size estimation**
  - Relates to methods of determining the relative physical size of the application software to be developed
  - Can be used as a guide for the allocation of resources, estimates of time and cost required for its development, and as a comparison of the total effort required by the resources available
  - Methods of software sizing

- **Single line of code (SLOC) –**
  - The traditional and simplest method in measuring size by counting the number of lines of source code, measured in SLOC, is referred to as kilo lines of code (KLOC)

- **Functional Point Analysis (FPA) –**
  - Indirect measurement of software size
  - It is based on the number & complexity of inputs, outputs, files, interfaces and queries.
  - a multiple point technique widely used for estimating complexity in developing large business applications.
  - Five functional points - user inputs, user outputs, user inquiries, files and external interfaces.

Points to remember:

- The CISA candidate should be familiar with concepts of SLOC & FPA & should be able to differentiate between the two. CISA question will be based on a scenario where the candidate should be able to justify on the method of software estimation
- A reliable technique for estimating the scope & cost of a software-development project – Functional Point Analysis (FPA)

- **Scheduling and establishing the time frame**
- While budgeting involves totaling the human and machine effort involved in each task, scheduling involves establishing the sequential relationship among tasks.

- The schedule can be graphically represented using various techniques such as
  a. Gantt charts,
  b. Critical Path Methodology (CPM) or
  c. Program Evaluation Review Technique (PERT) diagrams.

- **Gantt charts:**
  a. constructed to aid in scheduling the activities (tasks) needed to complete a project
  b. The charts show when an activity should begin and when it should end along a timeline.
  c. Gantt charts can also reflect the resources assigned to each task and by what percent allocation.
  d. Gantt charts can also be used to track the achievement of milestones or significant accomplishments for the project such as the end of a project phase or completion of a key deliverable.

- **Critical Path Methodology (CPM):**
  a. the critical path is the sequence of activities whose sum of activity time is longer than that for any other path through the network
  b. Critical path are important because if everything goes according to the schedule, their duration gives the shortest possible completion time for the overall project
  c. Activities that are not in the critical path have slack time
  d. Slack time - It is defined as the amount of time a task can be delayed without causing another task to be delayed or impacting the completion date of the overall project.
  e. Activities on a critical path have zero slack time, and conversely, activities with zero slack time are on a critical path

- **Program Evaluation Review Technique (PERT):**
  a. CPM-type technique which uses three different estimates of each activity duration in lieu of using a single number for each activity duration.
  b. The three estimates are then reduced (applying mathematical formula) to a single number and then the classic CPM algorithm is applied
     1. **First one** - Most optimistic one (if everything went well)
     2. **Second one** – Most likely scenario
     3. **Third one** – Most pessimistic or worst-case scenario

Points to remember:

- A program evaluation review technique that considers different scenarios for planning & control projects – Program Evaluation Review Technique (PERT)

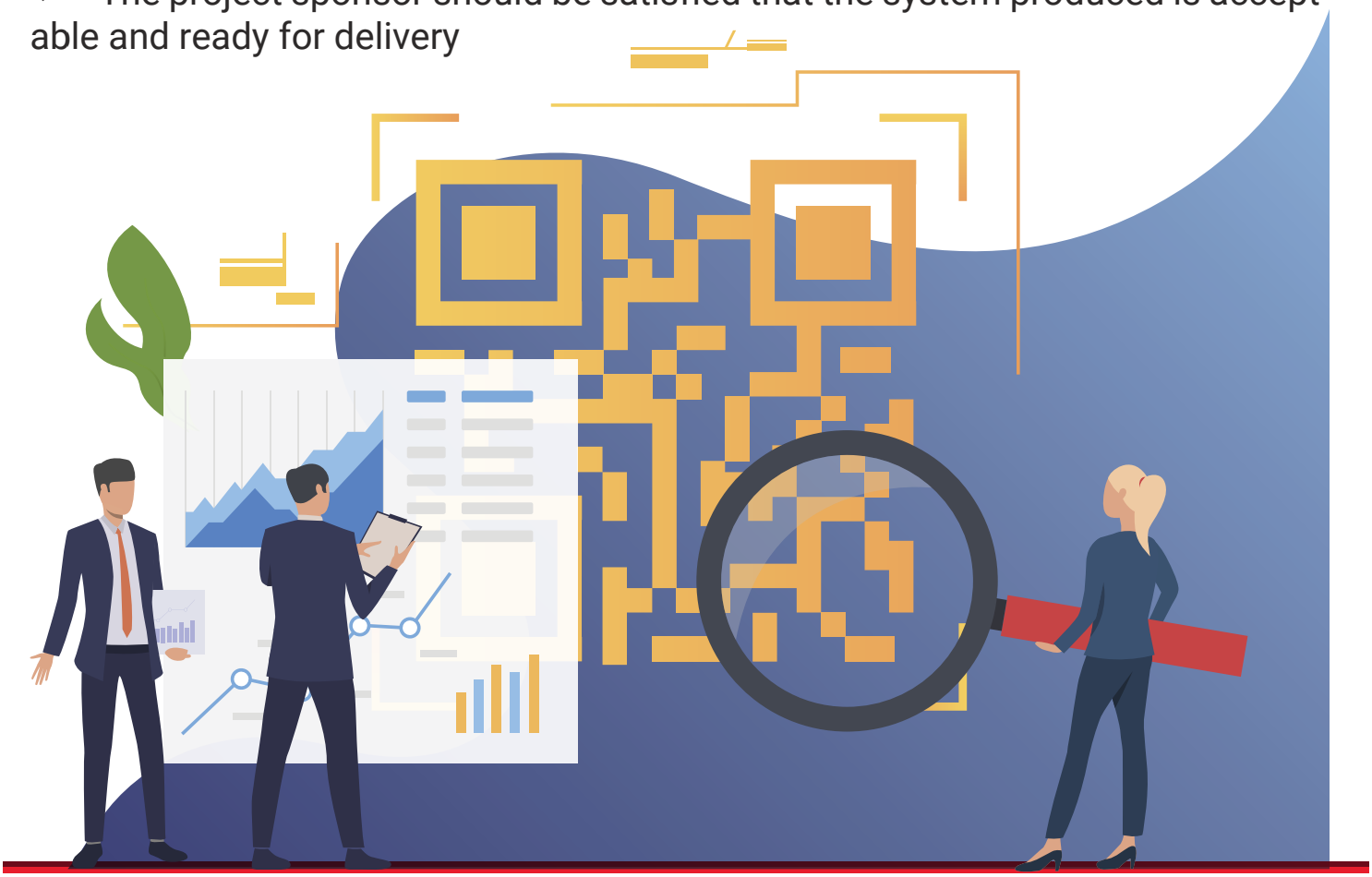
- **Project executing and controlling:**
  - The controlling activities of the project includes:

1. Management of scope changes
2. Management of resource usage
3. Management of risk

  - The risk management process consists of five steps:

1. Identify risk
2. Access and evaluate risk
3. Manage risk
4. Monitor risk
5. Evaluate the risk management process

- **Closing a project:**
  - A Project should have a finite life so, at some point, it is closed and the new or modified system is handed over to the user
  - When closing a project, there may still be some issues that need to be resolved, ownership of which needs to be assigned
  - The project sponsor should be satisfied that the system produced is acceptable and ready for delivery



13. Traditional SDLC approach:

- Also referred to as the waterfall technique
- Traditional system Development Life Cycle Approach

- **Phase 1 – Feasibility Study:**

1. Includes development of a business case, which determine the strategic benefits of implementing the system either in productivity gains or in future cost avoidance
2. Intangible factors such as readiness of the business users and maturity of the business processes will also be considered and assessed.
3. This business case provides the justification for proceeding to the next phase.

- **Phase 2 – Requirements definition** - Define the problem or need that requires resolution & define the functional & quality requirements of the solution system

- **Phase 3A – Software selection and acquisition (Purchased systems)** - Based on requirements defined, prepare a request for proposal outlining the entity requirements to invite bids from suppliers

- **Phase 3B – Design (In-house development)** - Based on the requirements defined, establish a baseline of system and subsystem specifications that describe the parts of the system, how they interface, & how the system will be implemented using the chosen hardware, software & network facilities.

- **Phase 4A – Configuration (purchased systems)** - Configure the system, if it is a packaged system, to tailor it to the organization's requirements. This is best done through the configuration of system control parameters, rather than changing program code.

- **Phase 4B – Development (In-house development)** - Use the design specifications to begin programming & formalizing supporting operational processes of the System

- **Phase 5 – Final testing and implementation** - The system also may go through a certification and accreditation process to assess the effectiveness of the business application in mitigating risk

- **Phase 6 – Post implementation** - Following the successful implementation of a new or extensively modified system, implement a formal process that assesses the adequacy of the system and projected cost benefit or ROI measurements vis-à-vis the feasibility stage findings and deviations

Points to remember:

- The CISA candidate should be familiar with the phases of traditional SDLC.
- The candidate should be aware of what IS auditor should look for when reviewing the feasibility study

14. Approaches of test plans:

- **Bottom-up approach:**
- a testing strategy in which the modules at the lower level are tested with higher modules until all the modules and aspects of the software are tested properly

- **Benefits of bottom-up approach:**
- No need for stubs or drivers
- Can be started before all programs are complete
- Errors in critical modules are found early

- **Top-down approach:**
- High-level modules are tested first and then low-level modules & finally integrating the low-level modules to a high level to ensure the system is working as intended.

- **Benefits of top-down approach:**
- Tests of major functions and processing are conducted early
- Interface errors can be detected sooner
- Confidence is raised in the system because programmers & users actually see a working system

Points to remember:

- The type of approach to the development of organizational policies is often driven by risk assessment – **Bottom-up approach**
- The MOST appropriate method to ensure that internal application inter face errors are identified as soon as possible – **Top-down approach**

15. Testing classifications:

- **Unit testing:**
- The testing of an individual program or module.
- Unit testing uses a set of test cases that focus on the control structure of the procedural design.
- These tests ensure that the internal operation of the program performs according to specification.

- **Interface or integration testing**
- The tests that verify & validate the functioning of the application under test with other systems, where a set of data is transferred from one system to another
- A hardware or software test that evaluates the connection of two or more components that pass information from one area to another
- The objective is to take unit-tested modules & build an integrated structure dictated by design.

- **System testing:**
- The testing of the software application as a whole to check if the system is complaint with the user requirements.
- It is an end to end user perspective testing intended to find defects in the software system.

- **Final acceptance testing**:
- After the system staff is satisfied with their system tests, the new or modified system is ready for the acceptance testing, which occurs during the implementation phase.

- Final acceptance testing has two major parts:

1. **Quality assurance testing (QAT):**
- QAT focuses on the documented specifications & the technology employed.
- QAT is performed primarily by the IT department.
- The participation of the end user is minimal and on request.
- QAT does not focus on functionality testing.

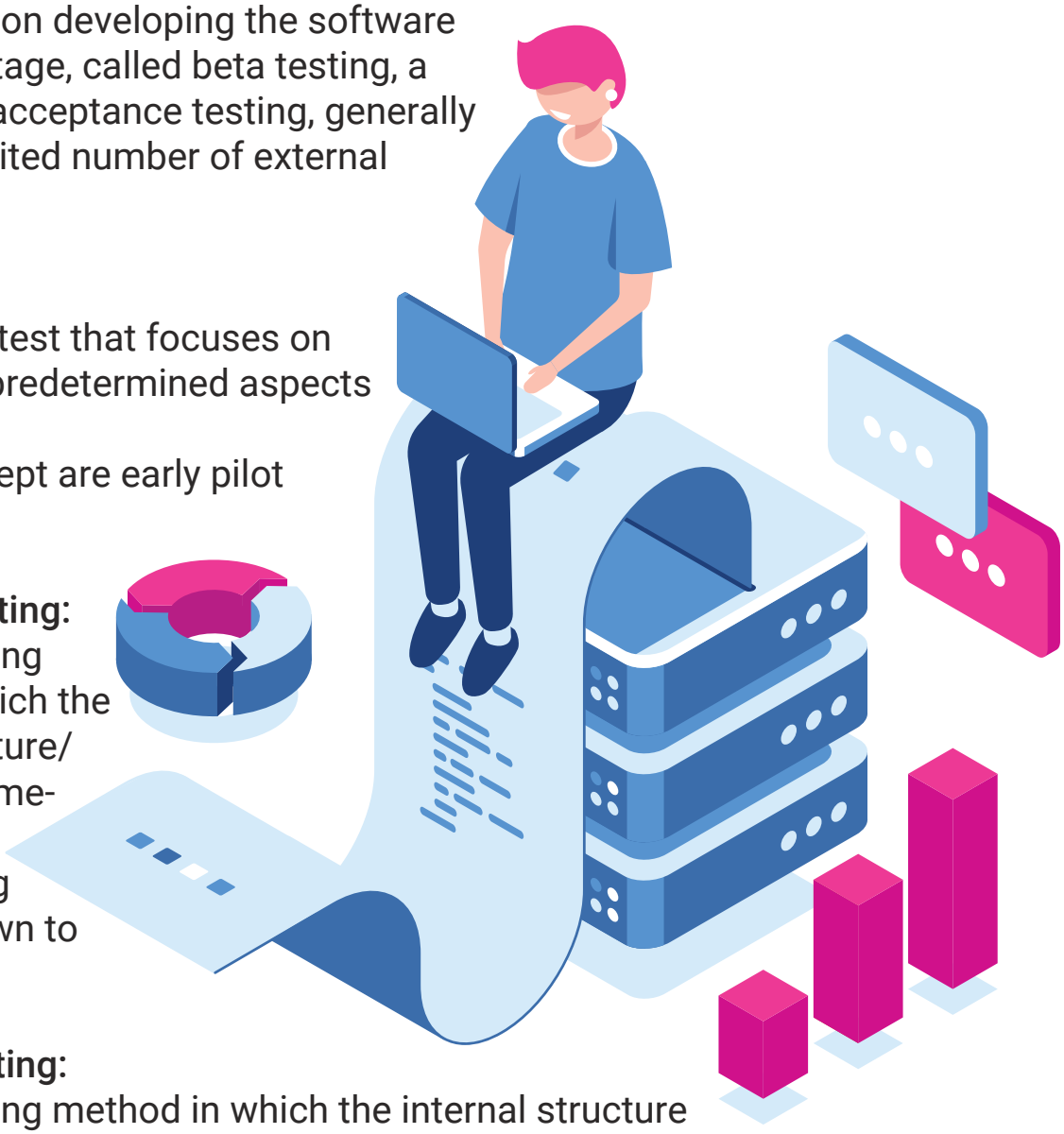
2. **User acceptance testing (UAT):**
- UAT should be performed in a secure testing or staging environment
- On completion of acceptance testing, the final step is usually a certification and accreditation process

Points to remember:

- Failure in this testing stage would have the GREATEST impact on the implementation of new application software – Acceptance testing

16. Other types of testing

- **Alpha and beta testing:**
- An alpha version is an early version of the application system (or software product) submitted to internal users for testing.
- The first stage, called alpha testing, is often performed only by users within the organization developing the software
- The second stage, called beta testing, a form of user acceptance testing, generally involves a limited number of external users.

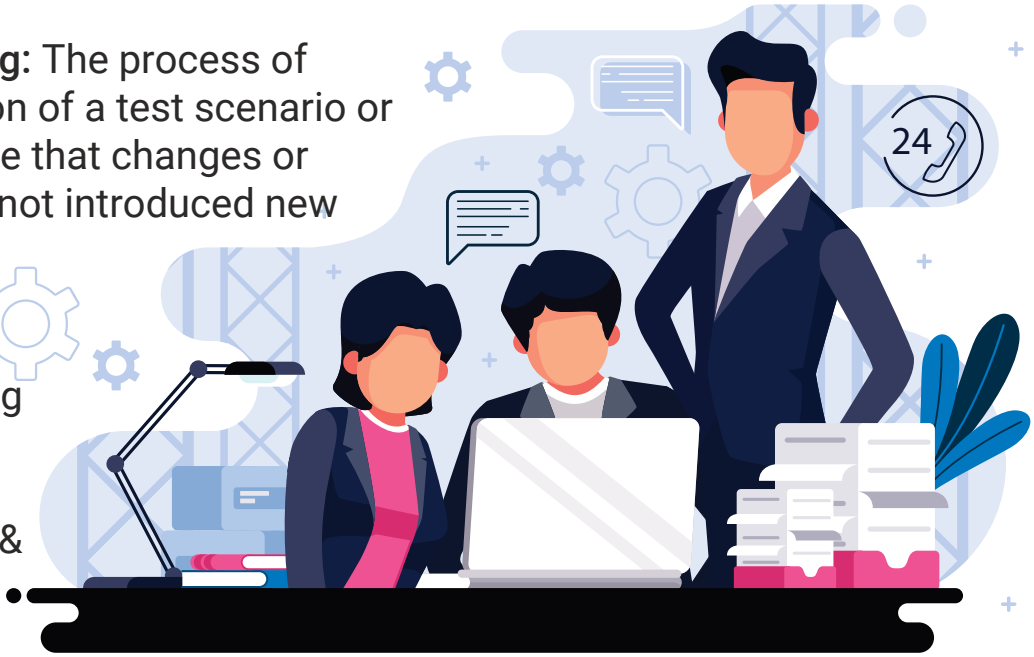


- **Pilot testing:**
- A preliminary test that focuses on specific and predetermined aspects of a System
- Proof of concept are early pilot testing.

- **White box testing:**
- Software testing method in which the internal structure/ design/implementation of the item being tested is known to the tester

- **Black box testing:**
- Software testing method in which the internal structure / design/implementation of the item being tested is NOT KNOWN to the tester.
- An integrity-based form of testing associated with testing components of an information system's "functional" operating effectiveness without regard to any specific internal program structure

- **Functional testing:** It ensures that the product actually meets the client's needs
- **Regression testing:** The process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors.
- **Parallel testing:** This is the process of feeding test data into two systems - the modified system & an alternative system (possibly the original system) & comparing the results
- **Sociability testing:** Purpose of this test to confirm that the new or modified system can operate in its target environment without adversely impacting existing systems.



Points to remember:

- The CISA candidate should be familiar with all the above types of test ing. CISA question will be scenario based & the candidate is expected to identify which type of testing is to be used.
- White box testing - dynamic analysis tool for the purpose of testing software modules

17. Changeover (Go-live or cutover) techniques:

- **Parallel changeover:**
- This technique includes running the old system, then running both the old & new systems in parallel, and finally, fully changing over to the new system after gaining confidence in the working of the new system.
- **Advantages:**
  - minimize the risk of using the newer system
  - help in identifying problems, issues or any concerns that the user comes across in the newer system in the beginning
- **Disadvantages:**
  - running two systems at the same time is higher costs.
  - The parallel changeover process also can be quite time-consuming.

- **Phased changeover:**
- The phased changeover technique is considered a compromise between parallel and direct changeovers.
- In a phased changeover, the new system is implemented one stage at time
- **Advantages:**
  - Low cost and
  - Isolates errors
- **Disadvantages:**
  - the process takes a long time to complete because phases need to be implemented separately.

- **Abrupt changeover:**

- In this approach the newer system is changed over from the older system on a cutoff date and time, & the older system is discontinued once change over to the new system takes place
- **Advantages:**
  - Low cost
- **Disadvantages:**
  - Asset safeguarding
  - Data integrity
  - System effectiveness
  - System efficiency
  - Change management challenges (depending on the configuration items considered)
  - Duplicate or missing records (duplicate or erroneous records may exist if data cleansing is not done correctly)

Points to remember:

- ★ The CISA candidate should be familiar with all the changeover techniques with its advantages and disadvantages.
- ★ The CISA candidate is expected to know where the use which type of changeover technique.
- ★ Most Risky changeover technique/Low cost changeover – Abrupt/Direct changeover
- ★ Costliest changeover technique/ Least risky changeover technique – Parallel changeover
- ★ Changeover in Phases – Phased changeover

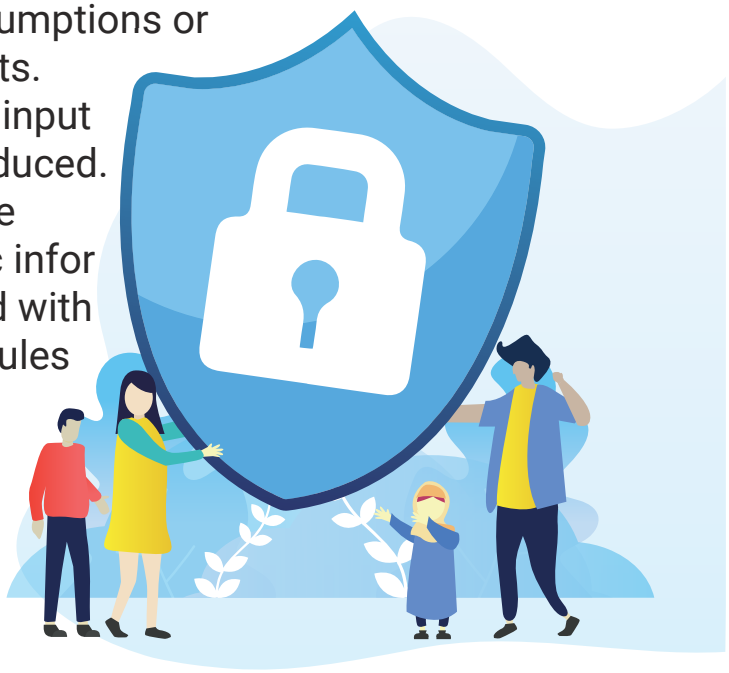
19. Artificial Intelligence (AI) and Expert Systems:

- Artificial intelligence (AI) is the study and application of the principles by which:
- Knowledge is acquired and used.
- Goals are generated and achieved.
- Information is communicated.
- Collaboration is achieved.
- Concepts are formed.
- Languages are developed.

- AI fields include, among others:
- Expert systems
- Natural and artificial (such as programming) languages
- Neural networks
- Intelligent text management
- Theorem proving
- Abstract reasoning
- Pattern recognition
- Voice recognition
- Problem solving
- Machine translation of foreign languages

- **Expert systems:**

- Expert systems are an area of AI and perform a specific function or are prev alent in certain industries.
- An expert system allows the user to specify certain basic assumptions or formulas and then uses these assumptions or formulas to analyze arbitrary events. Based on the information used as input to the system, a conclusion is produced.
- Key to the system is the knowledge base (KB), which contains specific infor mation or fact patterns associated with particular subject matter and the rules for interpreting these facts.
- Knowledge base: This component consists of data, facts & rules for certain topic, industry or skill, usually equivalent to that of a human expert. The information in the KB can be expressed in several ways:



1. **Decision trees** – Using questioners to lead the user through series of ch- oices, until a conclusion is reached.

2. **Rules** - Expressing declarative knowledge through the use of if-then rela- tionships. For example, if a patient's body temperature is over 39°C (102.2- °F) and his/her pulse is under 60, then the patient might be suffering from a certain disease.

3. **Semantic nets** - A semantic network is a system in which commonly und- erstood labeling is used to show relationships between its parts

18. Certification and Accreditation:

- **Certification:**

- Certification is the process of evaluating, testing, and examining security controls that have been pre-determined based on the data type in an information system
- The certification process ensures that security weaknesses are identified and plans for mitigation strategies are in place
- Testing laboratories may also certify that certain products meet pre-established standards, or governmental agencies may certify that a company is meeting existing regulations (e.g., emission limits).

- **Accreditation:**

- Accreditation is the formal declaration by a neutral third party that the certification program is administered in a way that meets the relevant norms or standards of certification program (e.g., ISO/IEC 17024).
- Accreditation is the official management decision (given by a senior official) to authorize operation of an information system and to explicitly accept the risk to the organization's operations, assets or individuals based on the implementation of an agreed-upon set of requirements and security controls.

Points to remember:

- The CISA candidate should be familiar with the auditor's role in the cer tification process

20. Agile development:

- The term “agile development” refers to a family of similar development pro cesses that espouse a nontraditional way of developing complex systems. One of the first agile processes, Scrum (a rugby analogy), emerged in the early 1990s

- a lightweight software engineering framework that promotes iterative devel opment throughout the life-cycle of the project, close collaboration between the development team & business side, constant communication, & tightly-knit teams

21. Software re-engineering:

- Re-engineering is a process of updating an existing system by extracting and reusing design and program components
- the act of recreating a core business process with the goal of
- improving product output,
- improving product quality, or
- reducing costs.
- The following are the steps involved in business process re-engineering
- Define objectives and framework
- Identify customer needs
- Study the existing process
- Formulate a Redesign Business plan
- Implement and monitor the redesigned process
- Establish continuous improvement process

Points to remember:

- The MOST likely to result from a business process reengineering (BPR) Project - An increased number of people using technology
- The FIRST step of Re-engineering process – Identify current/existing business processes. If option on Identifying customer needs is availabl-e, then it would be the best option

22. Reverse engineering:

- Reverse engineering is the process of studying and analyzing an application, a software application or a product to see how it functions and to use that information to develop a similar system

- **This process can be carried out in several ways:**
- Decompiling object or executable code into source code & using it to analyze the program
- Black box testing the application to be reverse-engineered to unveil its functionality

- **Advantages:**
- Faster development and reduced SDLC duration
- Possibility of introducing improvements by overcoming the reverse-engineered application drawbacks

23. Benchmarking process:

- Benchmarking is about improving business processes.
- It is defined as a continuous, systematic process for evaluating the product, services or work processes of organizations recognized as a world-class "reference" in a globalized world

- **Benchmarking process includes the following exercise:**
- Plan
- Research
- Observe
- Analyze
- Adopt
- Improve

24. Capacity Maturity Model Integration (CMMI):

- Capability Maturity Model Integration (CMMI) is a process level improvement training and appraisal program. Administered by the CMMI Institute, a subsidiary of ISACA.

- The following are the characteristics of the maturity levels:
- Level 1 – Initial – Processes are unpredictable, poorly controlled & reactive.
- Level 2 – Managed–Process is characterized for projects & is often reactive.
- Level 3 – Defined–Process characterized for the organization & is proactive
- Level 4 – Quantatively managed – Process is measured and controlled
- Level 5 – Optimizing – Focus is on process improvement.

25. Processing procedures and controls:

- Processing procedures and controls are meant to ensure the reliability of application program processing.

- IS auditors need to understand the procedures & controls that can be exercised over processing to evaluate what exposures are covered by these controls and what exposures remain.

26. Data validation edits and controls:

1. **Sequence check:**
- The control number follows sequentially & any sequence or duplicated control numbers are rejected or noted on an exception report for follow-up purposes.

- For example, invoices are numbered sequentially. The day's invoices begin with 12001 and end with 15045. If any invoice larger than 15045 is encountered during processing, that invoice would be rejected as an invalid invoice number.

2. **Limit check:**
- Data should not exceed a predetermined amount.
- For example, payroll checks should not exceed US $4,000. If a check exceed US $4,000, the data would be rejected for further verification/authorization.

3. **Range check:**
- Data should be within a predetermined range of values.
- For example, product type codes range from 100 to 250. Any code outside this range should be rejected as an invalid product type.

4. **Validity check:**
- Programmed checking of the data validity in accordance with predetermined criteria.
- For example, a payroll record contains a field for marital status and the acceptable status codes are M or S. If any other code is entered, the record should be rejected.

5. **Reasonableness check:**
- Input data are matched to predetermined reasonable limits or occurrence rates.
- For example, a widget manufacturer usually receives order for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

6. **Existence check:**
- Data are entered correctly and agree with valid predetermined criteria.
- For example, a valid transaction code must be entered in the transaction code field.

7. **Key verification:**
- The keying process is repeated by a separate individual using a machine that compares the original keystrokes to the repeated keyed input.
- For example, the worker number is keyed twice and compared to verify the keying process.

8. **Check digit:**
- A numeric value that has been calculated mathematically is added to data to ensure that the original data have not been altered or an incorrect, but valid, value substituted.
- This control is effective in detecting transposition and transcription errors.
- For example, a check digit is added to an account number so it can be checked for accuracy when it is used.

9. **Completeness check:**
- A field should always contain data rather than zeros or blanks (No Null value)
- A check of each byte of that field should be performed to determine that some form of data, not blanks or zeros, is present.
- For example, a worker number on a new employee record is left blank. This is identified as a key field and the record would be rejected, with a request that the field be completed before the record is accepted for processing.

10. **Duplicate check:**
- New transactions are matched to those previously input to ensure that they have not already been entered.
- For example, a vendor invoice number agrees with previously recorded invoices to ensure that the current order is not a duplicate and, therefore, the vendor will not be paid twice.

11. **Logical relationship check:**

- If a particular condition is true, then one or more additional conditions or data input relationships may be required to be true & consider the input valid.
- For example, the hire date of an employee may be required to be more than 16 years past his/her date of birth.

Points to remember:

- The CISA is expected to be familiar with each one of the data edit and controls
- **Check digit** - Effective in detecting transposition & transcription errors
- **Reasonableness check** – A data validation edit control that matches input data to an occurrence rate

27. Data integrity testing:

- Data integrity testing is a set of substantive tests that examines accuracy, completeness, consistency and authorization of data presently held in a system
- Two common types of data integrity tests are
- **Relational Integrity tests** – Relational integrity tests are performed at the data element and record-based levels.
- **Referential integrity tests** - tests whether the table relationships are consist ent. In other words, any foreign key field must agree with the primary key th at is referenced by the foreign key.

Points to remember:

- **Referential integrity** - will prevent dangling tuples in a database

28. Data Integrity in Online Transaction Processing Systems:

- The four online data integrity requirements known collectively as the ACID principle, which are as follows:
- **Atomicity** - From a user perspective, a transaction is either completed in its entirety or not at all. If an error or interruption occurs, all changes made up to that point are backed out.
- **Consistency** - All integrity conditions in the database are maintained with each transaction, taking the database from one consistent state into anoth- er consistent state.
- **Isolation** - Each transaction is isolated from other transactions, & hence, ea- ch transaction only accesses data that are part of a consistent database state.
- **Durability** - If transaction has been reported back to a user as complete, the resulting changes to the database survive subsequent hardware or software failures.

Points to remember:

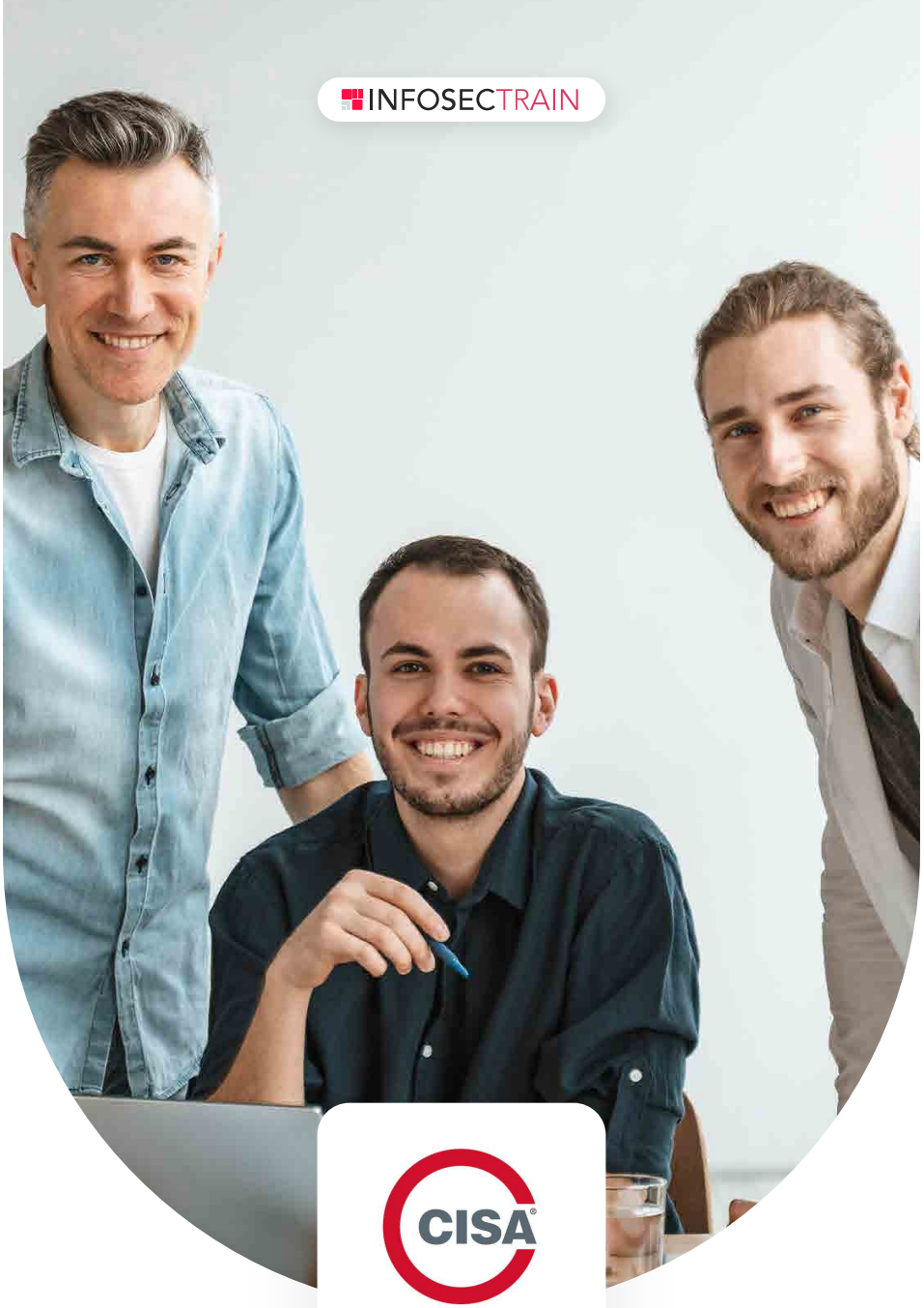
- In an online transaction processing system, data integrity is maintained by ensuring that a transaction is either completed in its entirety or not at all. This principle of data integrity is known as - Atomicity

29. Online auditing techniques:

- **Systems Control Audit Review File and Embedded Audit Modules (SCARF/ /EAM)** - The use of this technique involves embedding specially written audit software in the organization's host application system so the application systems are monitored on a selective basis
- **Snapshots** - This technique involves taking what might be termed pictures of the processing path that a transaction follows, from the input to the output stage.
- **Audit hooks** - This technique involves embedding hooks in application systems to function as red flags and to induce IS security & auditors to act before an error or irregularity gets out of hand.
- **Integrated test facility (ITF)** - It creates a fictitious entity in a database to process test transactions simultaneously with live input. It can be used to incorporate test transactions into a normal production run of a system.
- **Continuous and intermittent simulation (CIS)** – This means that the simulation is notified about each transaction that is entered to the application and accesses to database by the DBMS

Points to remember:

- An online auditing techniques is most effective for the early detection of errors or irregularities – Audit hooks
- Generalized audit software (GAS) – Used by IS auditor to detect duplicate invoice records within an invoice master file



CISA Domain 5

Protection of Information assets

INFOSECTRAIN

The article is split into 16 parts as below

Part 1: Information Security Management Systems (ISMS) - Its importance and key elements

Part 2: The Classification of Information assets, Various fraud risk factors, Information security control design

Part 3: System Access Permission, Mandatory Access Controls (MACs), and Discretionary Access Controls (DACs) and other types of Access controls.

Part 4: Difference between privacy and Confidentiality, privacy principles and the role of IS auditors, the privacy-related compliance requirements

Part 5: Critical Success Factors (CSFs) to Information Security Management, the different mechanisms available for raising information security awareness, the various Human Resources security.

Part 6: The various Computer crime issues and exposures, the perpetrators in computer crimes, the common attack methods, and techniques

Part 7: the various phases of incident response, the logical access exposures, Identification, and Authentication (I&A).

Part 8: The common I&A vulnerabilities, the categorization of Authentication, the various authentication techniques.

Part 9: Biometric access controls, Operation of each biometric access control, the various biometric devices/ techniques.

Part 10: The quantitative measures to determine the performance of biometric control devices, Single sign-on - its advantages and disadvantages, Firewall security systems.

Part 11: The general features of the firewall, the types of firewalls, the Packet filter firewall - its advantages and disadvantages.

Part 12: Application firewall systems - its advantages and disadvantages, a Stateful inspection firewall - its advantages and disadvantages, the various firewall implementations that are commonly used.

Part 13: Intrusion Detection Systems (IDS) - its types, its components, and its features

Part 14: The limitations of Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Honeypots and its types

Part 15: Honeynets, Cryptography, Encryption, and decryption

Part 16: Digital signature, the various environmental issues and exposures in Information security, the controls for environmental exposures, the various physical exposure issues and exposures in Information security, the controls for Physical access exposures

PART 01

CISA Domain 5
Protection of Information assets

- Overall understanding of the domain
- What is Information Security Management Systems (ISMS)?
- What is the importance of Information Security Management Systems (ISMS)?
- What are the key elements of Information security management?

Overall understanding of the domain

Weightage - This domain constitutes 25 percent of the CISA exam (approximately 38 questions)

Covers 26 Knowledge statements covering the process of auditing information systems

1. Knowledge of generally accepted practices and applicable external requirements (e.g., laws, regulations) related to the protection of information assets
2. Knowledge of privacy principles
3. Knowledge of the techniques for the design, implementation, maintenance, monitoring, and reporting of security controls
4. Knowledge of physical and environmental controls and supporting practices related to the protection of information assets
5. Knowledge of physical access controls for the Identification, Authentication, and restriction of users to authorized facilities and hardware
6. Knowledge of logical access controls for the Identification, Authentication, and restriction of users to authorized functions and data
7. Knowledge of the security controls related to hardware, system software (e.g., applications, operating systems) and database management systems.
8. Knowledge of risk and controls associated with the virtualization of systems
9. Knowledge of risk and controls associated with the use of mobile and wireless devices, including personally owned devices (bring your own device [BYOD])

10. Knowledge of voice communications security (e.g., PBX, Voice-over Internet Protocol [VoIP])
11. Knowledge of network and Internet security devices, protocols and techniques
12. Knowledge of the configuration, implementation, Operation, and maintenance of network security controls
13. Knowledge of encryption-related techniques and their uses
14. Knowledge of public key infrastructure (PKI) components and digital signature techniques
15. Knowledge of risk and controls associated with peer-to-peer computing, instant messaging and web-based technologies (e.g., social networking, message boards, blogs, cloud computing)
16. Knowledge of data classification standards related to the protection of information assets
17. Knowledge of the processes and procedures used to store, retrieve, transport and dispose of confidential information assets
18. Knowledge of risk and controls associated with data leakage
19. Knowledge of security risk and controls related to end-user computing
20. Knowledge of methods for implementing a security awareness program
21. Knowledge of information system attack methods and techniques
22. Knowledge of prevention and detection tools and control techniques
23. Knowledge of security testing techniques (e.g., penetration testing, vulnerability scanning)
24. Knowledge of processes related to monitoring and responding to security incidents (e.g., escalation procedures, emergency incident response team)
25. Knowledge of the processes followed in forensics investigation and procedures in the collection and preservation of the data and evidence (i.e., chain of custody).
26. Knowledge of fraud risk factors related to the protection of information assets

Important concepts from exam point of view

What is Information Security Management Systems (ISMS)?

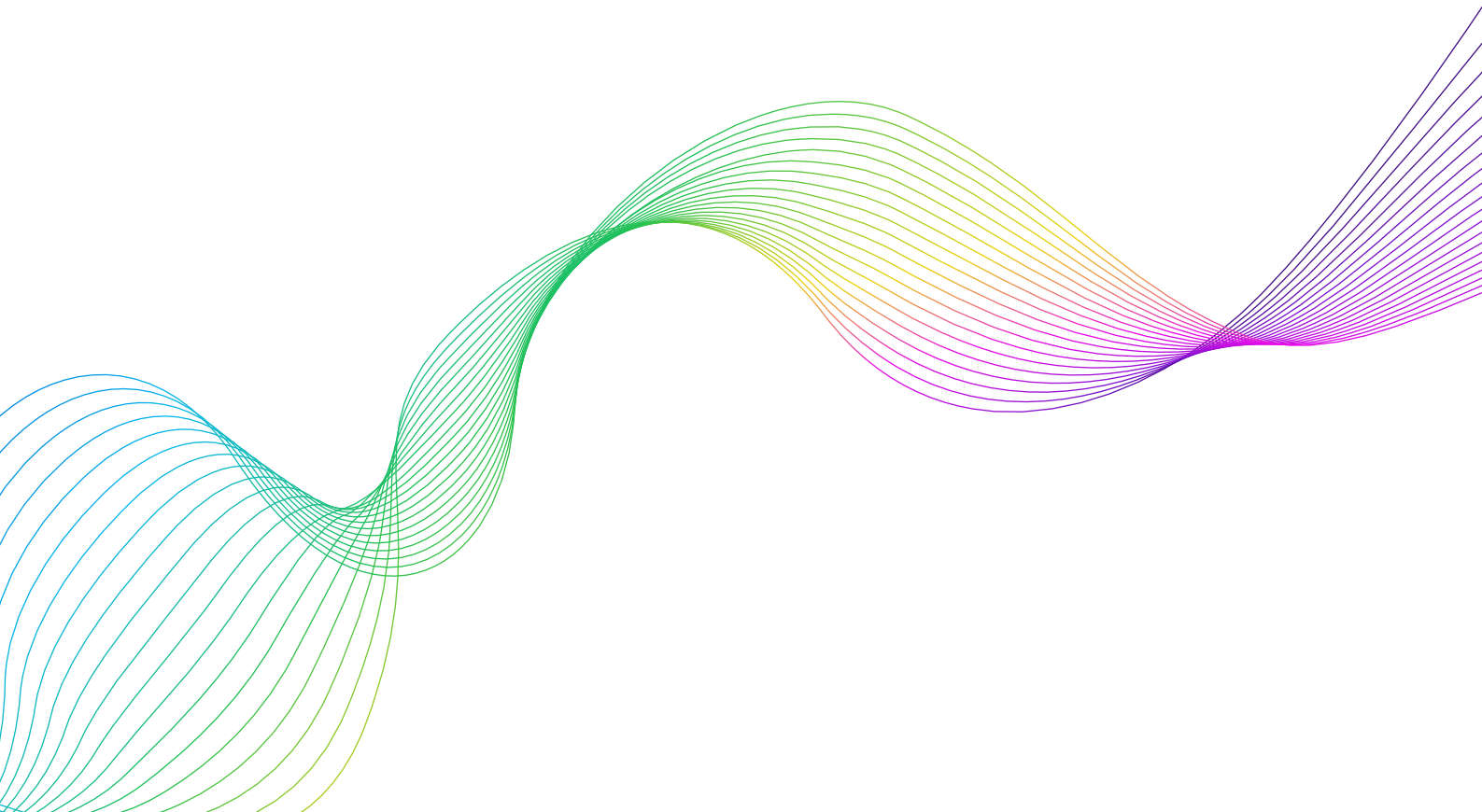
- Represents the collation of all the interrelated/interacting information security elements of an organization so as to ensure policies, procedures, and objectives can be created, implemented, communicated, and evaluated to better guarantee an organization's overall information security
- This system is typically influenced by the organization's needs, objectives, security requirements, size, and processes
- Includes and lends to effective risk management and mitigation strategies

What is the importance of Information Security Management Systems (ISMS)?

- Ensure the continued availability of their information systems and data.
- Ensure the integrity of the information stored on their computer systems and while in transit.
- Preserve the Confidentiality of sensitive data while stored and in transit.
- Ensure conformity to applicable laws, regulations, and standards.
- Ensure adherence to trust and obligation requirements in relation to any information relating to an identified or identifiable individual (i.e., data subject) in accordance with its privacy policy or applicable privacy laws and regulations.
- Ensure that sensitive data are adequately protected while stored and when in transit, based on organizational requirements.

What are the key elements of Information security management?

- An ISMS is defined in the International Organization for Standardization (ISO)/International Electro-Technical Commission (IEC) 27000 series of standards and guidelines
- The first standard in this series was ISO/IEC 17799:2000; this was a fast-tracking of the existing British Standard BS 7799 part 1:1999
- The initial release of BS 7799 was based, in part, on an information security policy manual developed by the Royal Dutch/Shell Group in the late 1980s and early 1990s
- ISO 27000 series is as follows:
    - ISO 27001
    - ISO 27002
    - ISO 27003
    - ISO 27004
    - ISO 27005



PART 02

CISA Domain 5
Protection of Information assets

- What are the classification of Information assets?
- What are the various fraud risk factors?
- What is Information Security Control design?

What is the classification of Information assets

- Effective control requires a detailed inventory of information assets.
- Creating this list is the first step in classifying assets and determining the level of protection needed for each asset.
- Information assets have varying degrees of sensitivity and criticality in meeting business objectives
- Classification of information assets reduces the risk and cost of over or under-protecting information resources in linking security to business objectives because it helps to build and maintain a consistent perspective of the security requirements for information assets throughout the organization
- Most organizations use a classification scheme with three to five levels of sensitivity.
- The number of classification categories should take into consideration the size and nature of the organization and the fact that complex schemes may become too impractical to use.
- Data classification is a major part of managing data as an asset.
- Data classification as a control measure should define:
    - The importance of the information asset
    - The information asset owner
    - The process for granting access
    - The person responsible for approving the access rights and access levels
    - The extent and depth of security controls

- If documents or media are not labeled according to a classification scheme, this is an indicator of the potential misuse of information. Users might reveal confidential information because they did not know that the requirements prohibited disclosure.
- Below is the example of classification of assets:
  - HIGHLY RESTRICTED: This classification label applies to the most private or otherwise sensitive information of the Company. Information under this classification shall be strictly monitored and controlled at all times. (e.g., merger and acquisition documents, corporate-level strategic plans, litigation strategy memos, reports on breakthrough new product research, and Trade Secrets such as certain computer programs.)
  - CONFIDENTIAL: This classification label applies to Company information, which is private or otherwise sensitive in nature and shall be restricted to those with a legitimate business need for access. (e.g., employee performance evaluations, customer transaction data, strategic alliance agreements, unpublished internally generated market research, computer passwords, identity token personal identification numbers (PINs), and internal audit reports).
  - INTERNAL USE ONLY: This classification label applies to information intended for use within the Company, and in some cases, within affiliated organizations, such as business partners of the Company. Assets of this type are widely-distributed within the Company and may be distributed within the Company without permission from the information asset owner. (e.g., telephone directory, dial-up computer access numbers, new employee training materials, and internal policy manuals.
  - PUBLIC: This classification applies to information that has been explicitly approved by the Company's management for release to the public. Assets of this type may be circulated without potential harm. (e.g., product and service brochures, advertisements, job opening announcements, and press releases.)

Points to remember

1. The MOST effectively reduce social engineering incidents is Security awareness training.
2. Non-repudiation is a message service that provides the strongest evidence that a specific action has occurred

What are the various fraud risk factors

- Fraud is the crime of using dishonest methods to take something valuable from a person or organization.
- There can be many reasons why a person commits fraud, but one of the more accepted models is the fraud triangle, which was developed by criminologist Donald R. Cressey
- Below are the three key elements in the fraud triangle:

I. Motivation - a perceived financial (or other) need

II. Rationalization - the way the fraudster justifies the crime to himself/herself

III. Opportunity - the method by which the crime is to be committed. Opportunity is created by the abuse of position and authority, poor internal controls, poor management oversight, etc.

What is Information Security Control design?

- Information security is maintained through the use of controls
- Controls can be
  - Proactive controls: Controls which attempt to prevent an incident (Safeguards)
  - Reactive controls: Controls that allow the detection, containment, and recovery from an incident (Countermeasures)
- Every organization has some controls in place, and a risk assessment should document these
  - controls and their effectiveness in mitigating risk
- Effective control is one that prevents, detects and/or contains an incident and enables recovery from an event
- Controls are divided into three categories:
  - Managerial controls: Controls related to the oversight, reporting, procedures, and operations of a process. These include policy, procedures, balancing, employee development, and compliance reporting.
  - Technical controls: Controls, also known as logical controls and are provided through the use of technology, a piece of equipment or device. Examples include firewalls, network or host-based intrusion detection systems (IDSs), passwords, and antivirus software. Technical control requires proper managerial (administrative) controls to operate correctly.
  - Physical controls: Controls that are locks, fences, closed-circuit TV (CCTV), and devices that are installed to physically restrict access to a facility or hardware. Physical controls require maintenance, monitoring, and the ability to assess and react to an alert should a problem be indicated.

- Controls are divided into three categories:
  - Managerial controls: Controls related to the oversight, reporting, procedures, and operations of a process. These include policy, procedures, balancing, employee development, and compliance reporting.
  - Technical controls: Controls, also known as logical controls and are provided through the use of technology, a piece of equipment or device. Examples include firewalls, network or host-based intrusion detection systems (IDSs), passwords, and antivirus software. Technical control requires proper managerial (administrative) controls to operate correctly.
  - Physical controls: Controls that are locks, fences, closed-circuit TV (CCTV), and devices that are installed to physically restrict access to a facility or hardware. Physical controls require maintenance, monitoring, and the ability to assess and react to an alert should a problem be indicated.

- Controls within the above groups can be classified into:
  - Preventive controls: internal controls which are deployed to prevent the happening of an event that might affect the achievement of organizational objectives
  - Detective controls: Detective controls seek to identify when preventive controls were not effective in preventing errors and irregularities, particularly in relation to the safeguarding of assets.
  - Corrective controls: When detective control activities identify an error or irregularity, corrective control activities should then see what could or should be done to fix it, and hopefully put a new system in place to prevent it the next time around.

PART 03

CISA Domain 5
Protection of Information assets

- What is System Access Permission?
- What are Mandatory Access Controls (MACs) and Discretionary Access Controls (DACs)?
- What are the other types of Access controls?
  - Role-based access control (RBAC)
  - Rule-based access control (RAC)
  - Organization-based access control (OrBAC)

Points to remember

1. Security administration efforts are BEST reduced through the deployment of
   - Role-based access controls (RBACs)

What is System Access Permission

- System access permission is the prerogative to act on a computer resource.
- This usually refers to a technical privilege, such as the ability to read, create, modify or delete a file or data; execute a program, or open or use an external connection
- System access to computerized information resources is established, managed and controlled at
  - the physical level and/or
  - the logical level
- Physical controls
  - The controls restrict the entry and exit of personnel to an area such as an office building, suite, data center, or room containing information processing equipment such as a local area network (LAN) server.

- There are many types of physical access controls, including badges, memory cards, guard keys, true floor-to-ceiling wall construction fences, locks, and biometrics.

- Logical system access controls
  - Restrict the logical resources of the system (transactions, data, programs, applications) and are applied when the subject resource is needed.
  - On the basis of Identification and Authentication of the user that requires a given resource and by analyzing the security profiles of the user and the resource, it is possible to determine if the requested access is to be allowed (i.e., what information users can utilize, the programs or transactions they can run, and the modifications they can make).
  - Such controls may be built into the operating system (OS), invoked through separate access control software and incorporated into application programs, database systems, network control devices, and utilities (e.g., real-time performance monitors).

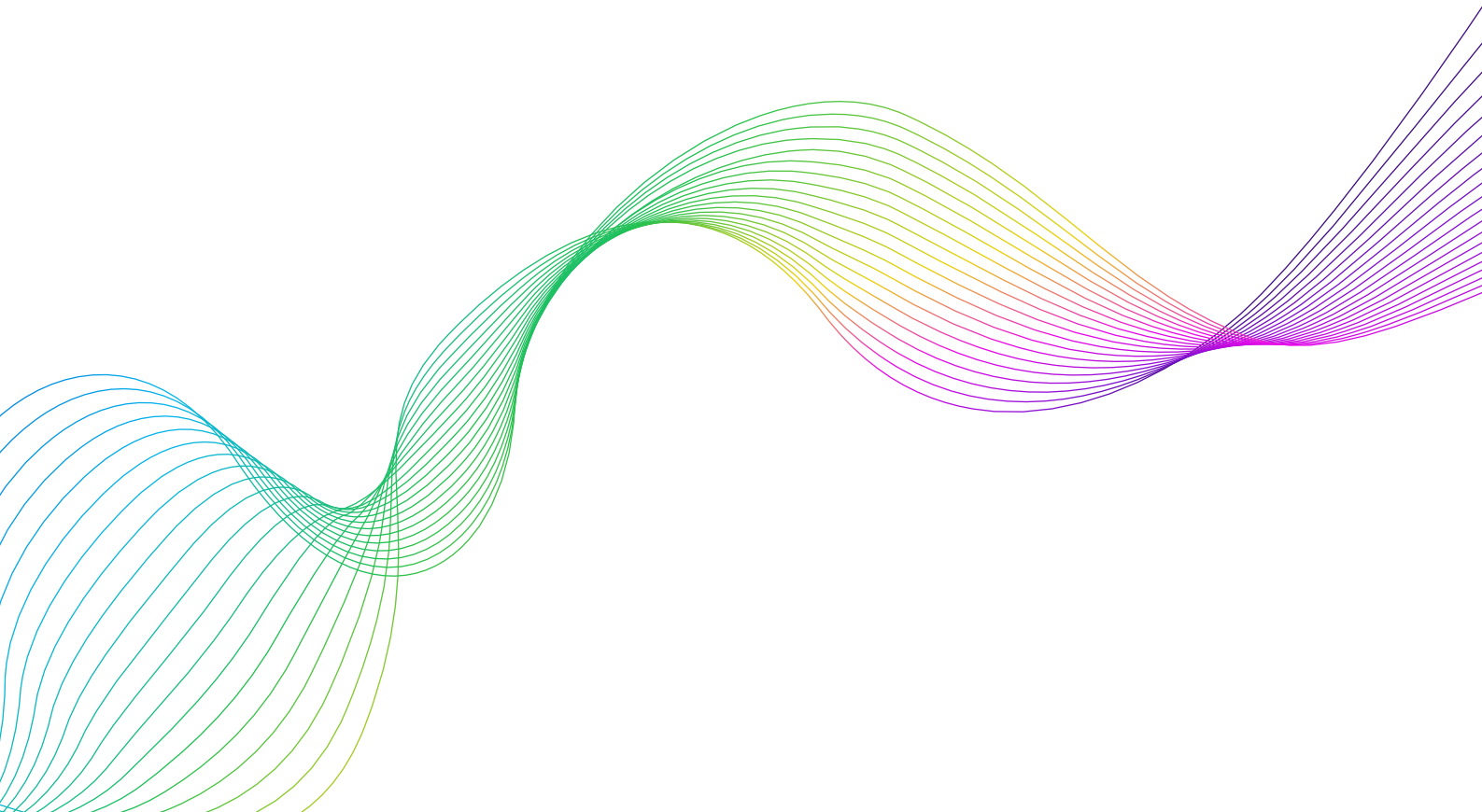
What are Mandatory Access Controls (MACs) and Discretionary Access Controls (DACs)?

- Mandatory Access Controls (MACs):
  - MACs are logical access control filters used to validate access credentials that cannot be controlled or modified by normal users or data owners; they act by default
  - With mandatory access control, the security policy is centrally controlled by a security policy administrator; users do not have the ability to override the policy and, for example, grant access to files that would otherwise be restricted

- Discretionary Access Controls (DACs):
  - Controls that may be configured or modified by the users or data owners
  - This would be the case of data owner-defined sharing of information resources, where the data owner may select who will be enabled to access his/her resource and the security level of this access.
  - DACs cannot override MACs; DACs act as an additional filter, prohibiting still more access with the same exclusionary principle

What are the other types of Access controls

- Role-based access control (RBAC): Provides access based on the position an individual hold in the organization
- Rule-based access control (RAC): Dynamically assign rules to users based on criteria defined by owner or system administrator
- Organization-based access control (OrBAC): allows the policy designer to define a security policy independently of the implementation



INFOSECTRAIN

CISA Domain 4

Information Systems Operations, Maintenance & Service Management

sales@infosectrain.com https://www.infosectrain.com

Overall understanding of the domain:

Weightage - This domain constitutes 20 percent of the CISA exam (approximately 30 questions)

Covers 23 Knowledge statements covering the process of auditing information systems

1. Knowledge of service management frameworks
2. Knowledge of service management practices and service level management
3. Knowledge of techniques for monitor third-party performance & compliance with service agreements and regulatory requirements
4. Knowledge of enterprise architecture (EA)
5. Knowledge of the functionality of fundamental technology (e.g., hardware & network components, system software, middleware, database management systems)
6. Knowledge of system resiliency tools and techniques (e.g., fault tolerant hardware, elimination of single point of failure, clustering)
7. Knowledge of IT asset management, software licensing, source code management and inventory practices
8. Knowledge of job scheduling practices, including exception handling
9. Knowledge of control techniques that ensure the integrity of system inter faces
10. Knowledge of capacity planning & related monitoring tools and techniques

11. Knowledge of systems performance monitoring processes, tools & techniques (e.g., network analyzers, system utilization reports, load balancing)
12. Knowledge of data backup, storage, maintenance & restoration practices
13. Knowledge of data base management & optimization practices
14. Knowledge of data quality (completeness, accuracy, integrity) & life cycle management (aging, retention)
15. Knowledge of problem and incident management practices
16. Knowledge of change management, configuration management, release management & patch management practices
17. Knowledge of operational risks & controls related to end-user computing
18. Knowledge of regulatory, legal, contractual and insurance issues related to disaster recovery
19. Knowledge of business impact analysis (BIA) related to disaster recovery planning
20. Knowledge of the development and maintenance of disaster recovery plans (DRPs)
21. Knowledge of benefits and drawbacks of alternate processing sites (e.g., hot sites, warm sites, cold sites)
22. Knowledge of disaster recovery testing methods
23. Knowledge of processes used to invoke the disaster recovery plans (DRPs)

Important concepts from exam point of view:

1. Information Systems operations:

- Responsible for ongoing support for an organizations computer and IS environment
- plays a critical role in ensuring that computer operations processing requirements are met, end users are satisfied & information is processed securely

2. Management of IS operations:

- COBIT 5 framework makes clear distinction between governance and management, which are as follows:

◆ **Governance:**

a. Ensures that stakeholder needs, conditions & options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved;
b. Setting direction through prioritization and decision making; & monitoring performance and compliance against agreed-on direction and objectives.
c. Overall governance is the responsibility of the board of directors under the leadership of the chairperson.
d. Specific governance responsibilities may be delegated to special organizational structures at an appropriate level, particularly in larger, complex enterprises.

◆ **Management:**

a. Management plans builds, runs & monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives
b. Management is the responsibility of the executive management under the leadership of the chief executive officer (CEO).
c. IS management has the overall responsibility for all operations within the IT department

3. IT Service Management framework (ITSM):

- Refers to the implementation & management of IT services (people, proce ss and information technology) to meet business needs
- **Two frameworks for ITSM:**

1. **IT Infrastructure Library (ITIL):**

- a reference body of knowledge for service delivery good practices
- a comprehensive framework detailed over five volumes – Service strategy, Service design, Service transition, services operations, Continual service improvement
- The main objective of ITIL is to improve service quality to the business.

2. **ISO 20000-1:2011 Information technology** – Service management

- Requires service providers to implement the plan-do-check-act (PDCA) methodology
- The main objective is to improve service quality, achievement of the stan dard certifies organizations as having passed auditable practices and pro cesses in ITSM.

4. Service Level Agreement and Operational Level Agreement:

- **Service Level Agreement:**
- The Service Level agreement is a contract between service provider and customer
- SLAs can also be supported by operational level agreements (OLAs)

- **Operational Level Agreement:**
- OLA is an agreement between the internal support groups of an institution that supports SLA
- The OLA clearly depicts the performance and relationship of the internal service groups.
- The main objective of OLA is to ensure that all the support groups provide the intended Service Level Agreement

5. Tools to monitor efficiency and effectiveness of services provided:

- **Exception reports:**
- These automated reports identify all applications that did not successfully complete or otherwise malfunctioned.
- An excessive number of exceptions may indicate:
  - Poor understanding of business requirements
  - Poor application design, development or testing
  - Inadequate operation instructions
    Inadequate operations support
  - Inadequate operator training or performance monitoring
  - Inadequate sequencing of tasks
  - Inadequate system configuration
  - Inadequate capacity management

- **System and application logs:**
- Refers to logs generated from various systems and applications
- Using this software, the auditor can carry out tests to ensure that:
- Only approved programs access sensitive data
- Only authorized IT personnel access sensitive data
- Software utilities that can alter data files and program libraries are used only for authorized purposes
- Approved programs are run only when scheduled and, conversely, that unauthorized runs do not take place
- The correct data file generation is accessed for production purposes
- Data files are adequately protected

- **Operator problem reports** – Manual report used by helpdesk to log computer operations problems & resolutions
- **Operator work schedules** – Report maintained manually by IS management to assist in human resource planning to ensure proper staffing of operation support

Points to remember:

- **Availability reports** – The report that IS auditor use to check compliance with service level agreements (SLA) requirement for uptime

6. Incident management and problem management:

- **Incident management:**
- An Incident is an event that could lead to loss of, or disruption to, an organ ization's operations, services or functions.
- Incident management is a term describing the activities of an organization to identify, analyze, and correct hazards to prevent a future re-occurrence.
- These incidents within a structured organization are normally dealt with by either an incident response team (IRT) or an incident management team (IMT)
- Incident management is reactive and its objective is to respond to & resolve issues restoring normal service (as defined by the SLA) as quickly as possible.

- **Problem management:**
- Problem management is the process responsible for managing the lifecycle of all problems that happen or could happen in an IT service.
- The primary objectives of problem management are to prevent problems and resulting incidents from happening, to eliminate recurring incidents, & to minimize the impact of incidents that cannot be prevented.

7. Support/Help desk – Roles and responsibilities:

- The responsibility of the technical support function is to provide specialist knowledge of production systems to identify and assist in system change /development and problem resolution.
- The basic function of the help desk is to be the first, single and central point of contact for users and to follow the incident management process
- The help desk personnel must ensure that all hardware & software incidents that arise are fully documented and escalated based on the priorities established by management

8. Change management and patch management process:

- **Change management:**
  - used when changing hardware, installing or upgrading to new releases of off-the-shelf applications, installing software patch & configuring various network devices
  - Changes are classified into three types:

a) Emergency changes
b) Major changes
c) Minor changes

- **Patch Management:**
  - an area of systems management that involves acquiring, testing & installing multiple patches (code changes) to an administered computer system in order to maintain up-to-date software and often to address security risk
  - Patch management tasks include the following:
    - Maintaining current knowledge of available patches
    - Deciding what patches are appropriate for particular systems
    - Ensuring that patches are installed properly; testing systems after installation
    - Documenting all associated procedures, such as specific configurations required

Points to remember:

- **Patch Management** – The BEST method for preventing exploitation of system vulnerabilities

9. Release management:

- Software release management is the process through which software is made available to users.
- The term “release” is used to describe a collection of authorized changes.
- The release will typically consist of a number of problem fixes & enhancements to the service.
- The release can be of three types:

a. **Major releases:** Normally contain a significant change or addition to new functionality. A major upgrade or release usually supersedes all preceding minor upgrades.

b. **Minor releases:** Upgrades, normally containing small enhancements and fixes. A minor upgrade or release usually supersedes all preceding emergency fixes. Minor releases are generally used to fix small reliability or func tionality problems that cannot wait until the next major release.

c. **Emergency releases:** Normally containing the corrections to a small number of known problems. Emergency releases are fixes that require implementation as quickly as possible to prevent significant user downtime to busi ness-critical functions

- While change management is the process whereby all changes go through a robust testing and approval process, release management is the process of actually putting the software changes into production.

10. Quality Assurance:

- QA personnel verify that system changes are authorized, tested & implemented in a controlled manner prior to being introduced into the production environment according to a company’s change and release management policies

11. Database management systems (DBMS):

- aids in organizing, controlling and using the data needed by application programs.
- A DBMS provides the facility to create & maintain a well-organized data-base.

- Primary functions include:

a. Reduced data redundancy,
b. Decreased access time and
c. Basic security over sensitive data.

12. DBMS Architecture:

- Database architecture focuses on the design, development, implementation & maintenance of computer programs that store & organize information for businesses, agencies & institutions.
- A database architect develops & implements software to meet the needs of users. The design of a DBMS depends on its architecture

- **Metadata:**
- the data (details/schema) of any other data (i.e. data about data)
- The word 'Meta' is the prefix that is generally the technical term for self-ref erential. In other words, we can say that Metadata is the summarized data for the contextual data.

- **There are three types of metadata:**

i. Conceptual schema,
ii. External schema and
iii. Internal schema

13. Data Dictionary/Directory system:

- Data Dictionary contains an index and descriptions all of the data stored in database. Directory describes the locations of the data and the access method

- **Some of the benefits of using DD/DS include:**
  - Enhancing documentation
  - Providing common validation criteria
  - Facilitating programming by reducing the needs for data definition
  - Standardizing programming methods

14. Database structure:

- The database structure is the collection of record type & field type definitions that comprise your database`.
- **There are three major types of database structure:**

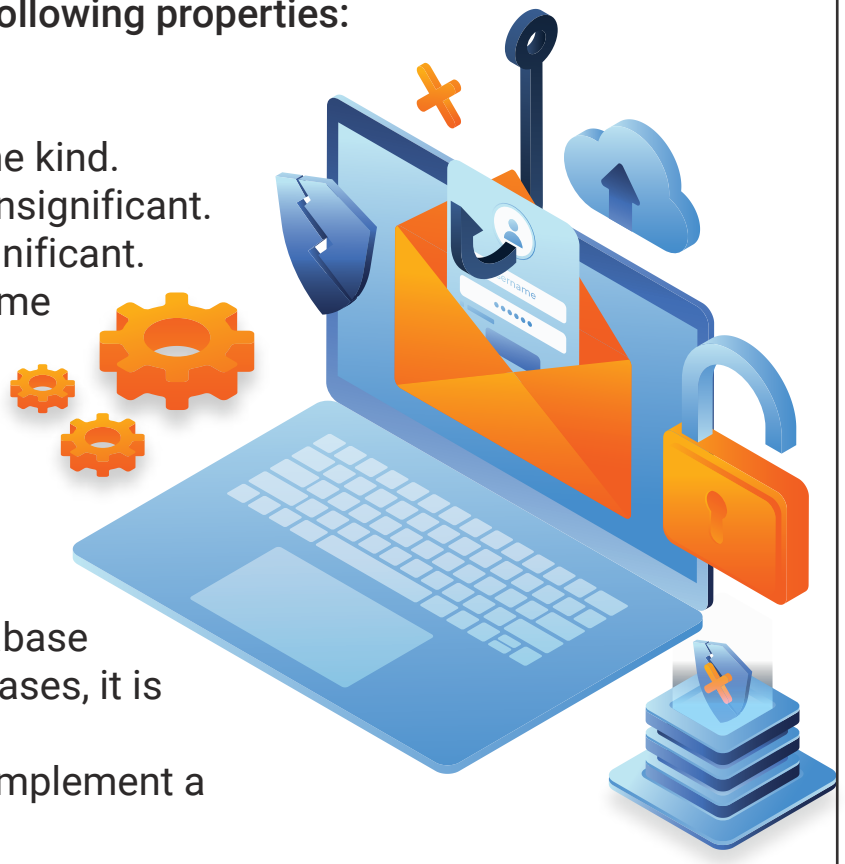
i. Hierarchical database model,
ii. Network database model, and
iii. Relational database model

- **Hierarchical database model:**
  - In this model there is a hierarchy of parent and child data segments. To create links between them, this model uses parent-child relationships.
  - These are 1:N (one-to-many) mappings between record types represented by logical trees

- **Network database model:**
  - In the network model, the basic data modeling construct is called a set.
  - A set is formed by an owner record type, a member record type & a name.
  - A member record type can have that role in more than one set, so a multiowner relationship is allowed.
  - An owner record type can also be a member or owner in another set. Usually, a set defines 1:N relationship, although one-to-one (1:1) is permitted
  - Disadvantages of Network database model:
    - Structures can be extremely complex and difficult to comprehend, modify or reconstruct in case of failure.
    - This model is rarely used in current environments.
    - The hierarchical and network models do not support high-level queries. The user programs have to navigate the data structures.

- **Relational database model**
- In Relational database model, the data and relationships among these data are organized in tables.
- A table is a collection of rows, also known as tuples, and each tuple in a table contains the same columns. Columns, called domains or attributes, correspond to fields.

- **Relational database has the following properties:**
  - Values are atomic.
  - Each row is unique.
  - Column values are of the same kind.
  - The sequence of columns is insignificant.
  - The sequence of rows is insignificant.
  - Each column has a unique name



- The relational model is independent from the physical implementation of the data structure, and has many advantages over the hierarchical and network database models. With relational databases, it is easier:
  - For users to understand and implement a physical database system
  - To convert from other database structures
  - To implement projection and join operations
  - To create new relations for applications
  - To implement access control over sensitive data
  - To modify the database

- A key feature of relational databases is the use of “normalization”
- **Normalization:**
  - a technique of organizing the data in the database
  - a systematic approach of decomposing tables to eliminate data redundancy(repetition) and undesirable characteristics like Insertion, Update & Deletion Anomalies

15. OSI Architecture:

- OSI model was developed by the International Organization for Standard ization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications

- OSI model is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.

- The OSI (Open Systems Inter-connection) is a proof-of-concept model composed of seven layers, each specifying particular specialized tasks or functions.

- The OSI model was defined in ISO/IEC 7498, which has the following parts:
  - ISO/IEC 7498-1 The Basic Model
  - ISO/IEC 7498-2 Security Architecture
  - ISO/IEC 7498-3 Naming and addressing
  - ISO/IEC 7498-4 Management framework

- Each layer is self-contained and relatively independent of the other layers in terms of its particular function

- There are seven OSI layers. Each layer has different functions. They are:

1. Physical Layer
2. Data-Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

Points to remember:

- The CISA candidate will not be tested on the specifics of this stan dard in the exam

- **The functions of each layer are as follows:**

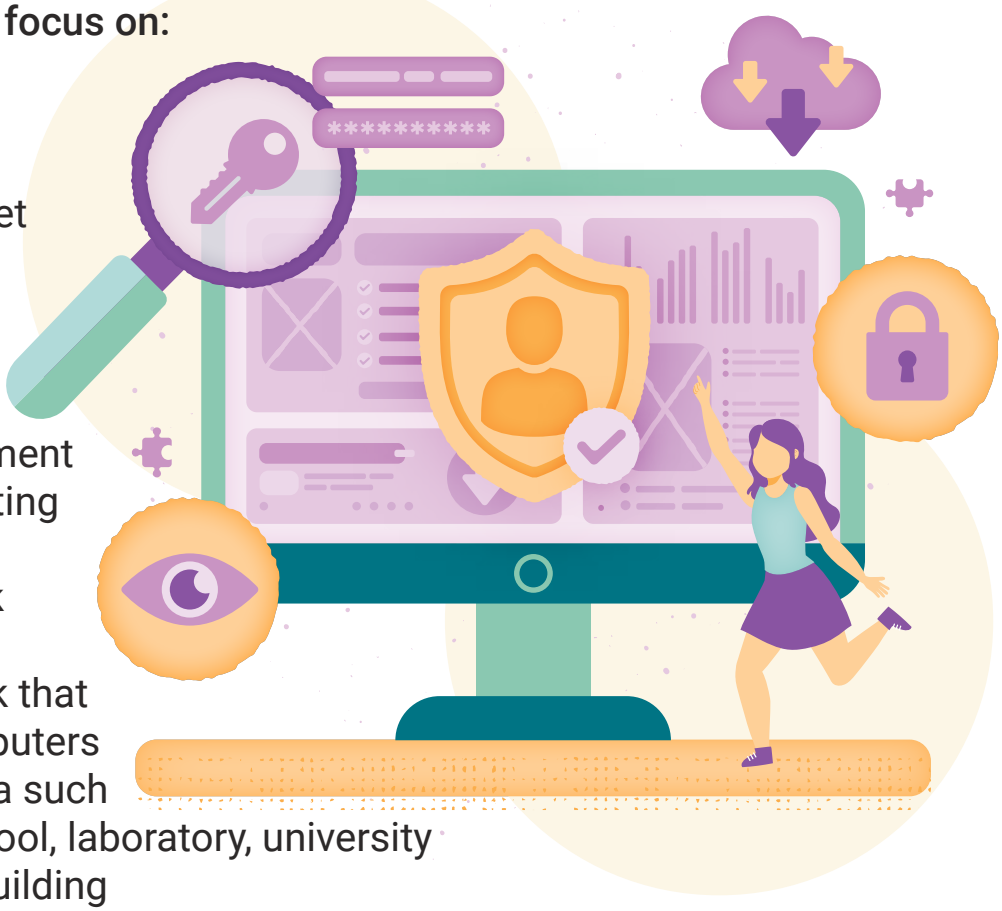
1. **Physical Layer** - The physical layer provides the hardware that transmits and receives the bit stream as electrical, optical or radio signals over an appropriate medium or carrier.
2. **Data-Link Layer** - The data link layer is used for the encoding, decoding & logical organization of data bits. Data packets are framed & addressed by this layer, which has two sublayers
3. **Network Layer -** This layer of the assigned the IP addresses & is responsi ble for routing & forwarding. This layer prepares the packets for the data link layer
4. **Transport Layer** - The transport layer provides reliable and transparent transfer of data between end points, end-to-end error recovery and flow control.
5. **Session Layer** -The session layer controls the dialogs (sessions) between computers. It establishes, manages & terminates the connections betwe- en the local and remote application layers
6. **Presentation Layer** - The presentation layer converts the outgoing data into a format acceptable by the network standard and then passes the data to the session layer (It is responsible for translation, compression & encryption)
7. **Application Layer** - provides a standard interface for applications that must communicate with devices on the network (e.g., print files on a net work-connected printer, send an email or store data on a file server)

Points to remember:

- The OSI layer that perform error detection and encryption – Data Link layer

16. Application of the OSI model in Network Architectures:

- The concepts of the OSI model are used in the design and development of organizations network architectures. This includes LAN, WAN, MAN and use of the public Transmission Control Protocol/Internet Protocol (TCP/IP)-based global Internet.
- **The discussion will focus on:**
  - LAN
  - WAN
  - Wireless networks
  - Public global internet infrastructure
  - Network administr-ation and control
  - Applications in a networked environment
  - On-demand computing



- **Local Area Network (LAN):**
  - a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building
  - **Media used in LAN:**
  - **Copper (twisted-pairs) circuit:**

- Twisted pairs are of two types:

(1) Shielded twisted pair - More attenuation, More cross talk and more interference

(2) unshielded twisted pair – More attenuation, More cross talk & more interference

-Two insulated wires are twisted around each other, with current flowing through them in opposite directions.

Advantages:

a. This reduces the opportunity for cross talk
b. Cheap
c. Readily available
d. Simple to modify

Disadvantages:

a. Easy to tap
b. Easy to splice
c. Interference and Noise

- **Fiber-optics systems:**
- It refers to the technology and medium used in the transmission of data as pulses of light through a strand or fiber medium made of glass or plas tic flashes of light.
- Fiber-optic systems have a low transmission loss as compared to twist ed-pair circuits.
- Optical fiber is smaller & lighter than metallic cable of the same capacity
- Fiber is the preferred choice for high-volume, longer-distance runs

- **Radio systems (wireless):**
- Data are communicated between devices using low-powered systems that broadcast (radiate) & receive electromagnetic signals representing data

Points to remember:

- The method of routing traffic through split-cable facilities or duplica-te-cable facilities is called “Diverse routing”
- The type of line media that provides the BEST security for a telecom munication network is “Dedicated lines”

17. LAN Topologies:

- Star topology
- Bus topology
- Ring topology

18. LAN components:

- **Repeaters** - physical layer devices that extend the range of a network or connect two separate network segments together
- **Hubs** - physical layer devices that serve as the center of a star-topology network or a network concentrator
- **Bridges** - data link layer devices that were developed to connect LANs or create two separate LAN or WAN network segments from a single segment to reduce collision domains
- **Switches** - data link level devices that can divide & interconnect network segments & help to reduce collision domains in Ethernet-based networks
- **Routers** - operate at the OSI network layer by examining network addresses (i.e., routing information encoded in an IP packet).
- **Gateways** - are devices that are protocol converters. Typically, they connect & convert between LANs & the mainframe, or between LANs & the Internet, at the application layer of the OSI reference model

19. WAN components:

- **WAN switches** - Data link layer devices used for implementing various WAN technologies such as ATM, point-to-point frame relay and ISDN
- **Routers** - devices that operate at the network layer of the OSI reference model & provide an interface between different network segments on an internal network or connects the internal network to an external network

- **Modems (modulator/demodulator)**
- Converts computer digital signals into analog data signals and analog data back to digital.
- A main task of the modems at both ends is to maintain their synchroniza tion so the receiving device knows when each byte starts and ends. Two methods can be used for this purpose:

- **Synchronous transmission** - a data transfer method in which a continuo- us stream of data signals is accompanied by timing signals (generated by an electronic clock) to ensure that the transmitter and the receiver are in step (synchronized) with one another. The data is sent in blocks (called frames or packets) spaced by fixed time intervals
- **Asynchronous transmission** - The term asynchronous is used to describe the process where transmitted data is encoded with start and stop bits, specifying the beginning & end of each character. Asynchronous trans mission works in spurts & must insert a start bit before each data charac ter & a stop bit at its termination to inform the receiver where it begins & ends.

20. WAN technologies:

- **Point to point protocol** - (PPP) is a data link layer communications proto col used to establish a direct connection between two nodes. PPP is a widely available remote access solution that supports asynchronous and synchronous links, and operates over a wide range of media.
- **X.25** - is a standard suite of protocols used for packet-switched communi cations over a wide area network
- **Frame Relay** - Frame relay is a packet-switching telecommunication ser vice designed for cost-efficient data transmission for intermittent traffic between LAN and between endpoints in WAN
- **Integrated services digital network (ISDN)** – It is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network
- **Asynchronous transfer mode** – ATM is a dedicated-connection switching technology that organizes digital data into 53-byte cell units & transmits them over a physical medium using digital signal technology
- **Multiprotocol label switching** - Multiprotocol label switching (MPLS) is a mechanism used within computer network infrastructures to speed up the time it takes a data packet to flow from one node to another. It enables computer networks to be faster and easier to manage by using short path labels instead of long network addresses for routing network packets.
- **Digital subscriber lines** - Digital subscriber line (DSL) is a technology that transports high-bandwidth data over simple telephone line that is directly connected to a modem. This allows for file-sharing, and the transmission of pictures and graphics, multimedia data, audio and video conferencing and much more

- **Virtual Private Network (VPN):**

- extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Application running on an end system (PC, smartphone etc.) across a VPN may therefore benefit from the functionality, security, and management of the private network
- VPN technology was developed to allow remote users & branch offices to access corporate applications and resources. To ensure security, the private network connection is established using an encrypted layered tunneling protocol, and VPN users use authentication methods, including passwords or certificates, to gain access to the VPN.

- **There are three types of VPNs:**

1. **Remote-access VPN** - Used to connect telecommuters and mobile users to the enterprise WAN in a secure manner; it lowers the barrier to telecommuting by ensuring that information is reasonably protected on the open Internet.
2. **Intranet VPN** - Used to connect branch offices within an enterprise WAN
3. **Extranet VPN** - Used to give business partners limited access to each other's corporate network; and example is an automotive manufacturer with its suppliers

21. Network Performance Metrics:

- **Latency:** The delay that a message or packet will experience on its way from source to destination. A very easy way to measure latency in a TCP/IP network is to use the ping command.
- **Throughput:** The quantity of useful work made by the system per unit of time. In telecommunications, it is the number of bytes per second that are passing through a channel.

Points to remember:

- Ping command is used to measure the latency

22. Network Management Issues:

A WAN needs to be monitored and managed similarly to a LAN. ISO, as part of its communications modeling effort (ISO/IEC 10040), has defined five basic tasks related to network management:

- **Fault management** - Detects the devices that present some kind of tech nical fault
- **Configuration management** - Allows users to know, define and change, remotely, the configuration of any device
- **Accounting resources** - Holds the records of the resource usage in the WAN (who uses what)
- **Performance management** - Monitors usage levels and sets alarms when a threshold has been surpassed
- **Security management** - Detects suspicious traffic or users, & generates alarms accordingly

23. Network Management tools:

- **Response Time** - Identify the time necessary for a command entered by users at a terminal to be answered by the host system.
- **Downtime Reports** - Track the availability of telecommunications line & circuits. Interruptions due to power line failure, traffic, overload, operator error or other anomalous conditions are identified in a downtime reports
- **Online Monitors** - Check data transmissions accuracy & errors. Monitoring can be performed be echo checking & status checking all transmissions, ensuring that messages are not lost or transmitted more than one.
- **Network Monitors** - Real time display of network nodes and status.
- **Protocol Analyzers** – It is a diagnostic tool used for monitoring packets flowing within the network.
- **Simple Network Management Protocol (SNMP)** - It is a TCP/IP-based protocol that monitors and controls different variables throughout the network, manages configurations, & collects statistics on performance and security
- **Help desk reports** - It is prepared by the help desk, which is staffed or supported by IT technicians trained to handle problems occurring during normal IS usage.

24. Disaster Recovery Planning (DRP):

- DRP is an element of an internal control system established to manage availability and restore critical processes/IT services in the event of interruption.

- The purpose of this continuous planning process is
  - to ensure that cost-effective controls to prevent possible IT disruptions and
  - to recover the IT capacity of the organization in the event of a disruption are in place

- DRP is a continuous process. Once the criticality of business processes & supporting IT service, system & data are defined, they are periodically reviewed and revisited

- The ultimate goal of the DRP process is
  - to respond to incidents that may impact people and
  - the ability of operations to deliver goods & services to the marketplace and to comply with regulatory requirements

- The difference between BCP and DRP is as follows:
  - BCP is focused on keeping the business operations running, perhaps in a different location or by using different tools or processes, after the disas ter has happened. DRP is focused on restoring business operations after the disaster has taken place.
  - BCP often includes Non-IT aspects of the business. DRP often focuses on IT systems

Points to remember:

- The prerequisite for developing a disaster recovery planning is – to have a management commitment.
- The PRIMARY GOAL of Disaster Recovery planning and Business continuity planning should always be – Safety of Personnel (Human safety first)
- Occupant Emergency Plan (OEP) provides the response procedures for occupants of a facility in the event a situation poses a threat to the heal and safety of personnel
- The critical first step in disaster recovery & contingency planning is – to complete a business impact analysis
- The term "Disaster Recovery" refers to recovery of technological environment
- The BCP is ultimate responsibility of Board of Directors
- Minimizing single points of failure or vulnerabilities of a common disaster is mitigated by geographically dispersing resources.
- Disaster Recovery planning addresses the technological aspect of business continuity planning
- A disaster recovery plan for an organization should focus on reducing the length of recovery time and the cost of recovery.
- The results of tests and drills are the BEST evidence of an organization's disaster recovery readiness.
- Fault-tolerant hardware is the only technology that provides continuous & uninterrupted support in the event of a disaster or disruption

25. Recovery Point Objective (RPO) and Recovery Time Objective (RTO):

Points to remember:

- The CISA candidate should be familiar with which recovery strate gies would be best with different RTO and RPO parameters.

- **Recovery Point objective:**

- RPO is determined based on the acceptable data loss in case of disrup- tion of operations.

- RPO indicates the earliest point in time in which it is acceptable to recov er the data. For example, if the process can afford to lose the data up to four hours before disaster, then the latest backup available should be up to four hours before disaster or interruption and the transactions that occurred during the RPO period and interruption need to be entered after recovery (known as catch-up data)

- RPO effectively quantifies the permissible amount of data loss in case of disruption.

- **Recovery Time Objective:**
- The RTO is determined based on the acceptable downtime in case of a disruption of operations.
- It indicates the earliest point in time at which the business operations (and supporting IT systems) must resume after disaster

- Both of these concepts are based on time parameters.
- The nearer the time requirements are to the center (0-1 hours), the higher the cost of the recovery strategies.
- If the RPO is in minutes (lowest possible acceptable data loss), then data mirroring or real-time replication should be implemented as the recovery strategy.
- If the RTO is in minutes (lowest acceptable time down), then a hot site, dedicated spare servers (and other equipment) and clustering must be used.

- The below table represents the relationship between RPO and RTO:

Disruption hours	Recovery Time Objective	Recovery Point objective
0 to 1 hour	Active-Active clustering	Mirroring (Real-time replication)
1 to 4 hours	Active-passive clustering (Hot Standby)	Disk-based back-ups, snapshots, delayed replication, log shipping
4 – 24 hours	Cold Standby	Tape backups, log shipping

Points to remember:

- Recovery Point Objective (RPO) will be deemed critical if it is small
- If the Recovery point objective (RPO) is close to zero, then it means that the activity is critical & hence the cost of maintaining the environment would be higher
- The LOWEST expenditure in terms of recovery arrangement can be through Reciprocal agreement
- A hot site is maintained and data mirroring is implemented, where Recovery Point Objective (RPO) is low
- The BEST option to support 24/7 availability is – Data Mirroring
- The metric that describes how long it will take to recover a failed system is – Mean time to Repair (MTTR)

26. Additional parameters in defining recovery strategy:

- **Interruption window** - The maximum period of time the organization can wait from the point of failure to the critical services/applications restoration. After this time, the progressive losses caused by the interruption are unaffordable.

- **Service delivery objective (SDO)** - Level of services to be reached during the alternate process mode until the normal situation is restored. This is directly related to the business needs.

- **Maximum tolerable outages** - Maximum time the organization can support processing in alternate mode. After this point, different problems may arise, especially if the alternate SDO is lower than the usual SDO, and the information pending to be updated can become unmanageable.

27. Recovery strategies:

- A recovery strategy identifies the best way to recover a system (one or many) in case of interruption, including disaster, and provides guidance based on which detailed recovery procedures can be developed

- **The selection of a recovery strategy would depend on:**
  - The criticality of the business process and the applications supporting the processes
  - Cost
  - Time required to recover
  - Security

- Recovery strategies based on the risk level identified for recovery are as follows:
  - **Hot sites** - facilities with space and basic infrastructure and all of the IT & communications equipment required to support the critical applications, along with office furniture and equipment for use by the staff.
  - **Warm sites** - are complete infrastructures but are partially configured in terms of IT, usually with network connections and essential peripheral equipment such as disk drives, tape drives and controllers.
  - **Cold sites** - are facilities with the space and basic infrastructure adequate to support resumption of operations, but lacking any IT or communications equipment, programs, data or office support.
  - Duplicate information processing facilities
  - **Mobile sites** - are packaged, modular processing facilities mounted on transportable vehicles & kept ready to be delivered and set up at a location that may be specified upon activation
  - **Reciprocal agreements** - are agreements between separate, but similar, companies to temporarily share their IT facilities in the event that one company loses processing capability. Reciprocal agreements are not considered a viable option due to the constraining burden of maintaining hardware & software compatibility between the companies, the complications of maintaining security and privacy compliance during shared operations, & the difficulty of enforcing the agreements should a disagreement arise at the time the plan is activated.

- **Reciprocal arrangements with other organisations** - are agreements between two or more organizations with unique equipment or applications. Under the typical agreement, participants promise to provide assistance to each other when an emergency arises.

Points to remember:

- The CISA candidate should know these recovery strategies & when to use them
- An offsite information processing facility having electrical wiring, air conditioning and flooring, but no computer or communications equipment is a Cold site
- The type of offsite information processing facility is often an acceptable solution for preparing for recovery of non-critical systems and data is a cold site
- Data mirroring and parallel processing are both used to provide near-immediate recoverability for time-sensitive systems & transcation processing
- Organizations should use off-site storage facilities to maintain redundancy of current and critical information within backup files.
- An off-site processing facility should not be easily identifiable externally because easy identification would create an additional vulnerability for sabotage
- The GREATEST concern when an organization's backup facility is at a warm site is – Timely availability of hardware.
- The GREATEST risk created by a reciprocal agreement for disaster recovery made between two companies is – Developments may result in hardware and software incompatibility.

28. Different Recovery/continuity/response teams and their responsibilities:

- Incident response team
- Emergency action team
- Information security team
- Damage assessment team
- Offsite storage team
- Software team
- Applications team
- Administrative support team
- Salvage team
- Emergency operations team
- Network recovery team
- Communications team
- Transportation team
- User hardware team
- Relocation team
- Legal affairs team
- Recovery test team
- Training team

Points to remember:

- The responsibility of disaster recovery relocation team is to co-or dinate the process of moving from hot site to a new location or to the restored original location.
- The responsibility of offsite storage team is to obtain, pack and ship media and records to the recovery facilities, as well as estab lishing and overseeing an offsite storage schedule.
- The responsibility of transportation team is to locate a recovery site, if one has not been predetermined, and coordinating the trans port of company employees to the recovery site.
- The responsibility of salvage team is managing the relocation proj ect and conducting a more detailed assessment of the damage to the facilities and equipment.

29. Back-up and restoration:

- **Back-up schemes:**
  There are three main schemes for backup:

  - **Full back-up** - This type of backup scheme copies all files & folders to the backup media, creating one backup set (with one or more media, depending on media capacity)
  - **Incremental back-up** - An incremental backup copy the files and folders that changed or are new since the last incremental or full backup
  - **Differential back-up** - A differential backup will copy all files & folders that have been added or changed since a full backup was performed. This type of backup is faster & requires less media capacity than a full backup & requires only the last full and differential backup sets to make a full restoration

Points to remember:

- The BEST backup strategy for a large database with data support ing online sales is – Weekly full back-up with daily incremental back-up

30. Disaster Recovery testing methods:

- **Checklist review -** This is a preliminary step to a real test. Recovery check lists are distributed to all members of a recovery team to review & ensure that the checklist is current.
- **Structured walk-through** - Team members physically implement the plans on paper & review each step to assess its effectiveness, identify enhancements, constraints and deficiencies.
- **Simulation test** -The recovery team role plays a prepared disaster scenario without activating processing at the recovery site.
- **Parallel test** - The recovery site is brought to a state of operational readiness, but operations at the primary site continue normally.
- **Full interruption test** - Operations are shut down at the primary site and shifted to the recovery site in accordance with the recovery plan; this is the most rigorous form of testing but is expensive and potentially disruptive.

Points to remember:

- A continuity plan test that uses actual resources to simulate a system crash to cost-effectively obtain evidence about the plan's effectiveness is preparedness test
- The most effective test of DRP for organisations having number of offices across a wide geographical area is preparedness test
- The type of BCP test that requires only representatives from each operational area to meet to review the plan is Walk-through test