# CHAPTER-1
# CONCEPTS OF GOVERNANCE AND MANAGEMENT OF INFORMATION SYSTEMS

**(1)** What Aspect to be covered in Key Governance Practices of GEIT?

a. Evaluate the governance system
b. Direct the governance system
c. Monitor the governance system
d. All of the Above

**(2)** What is not Covered under Internal control as per COSO?

a. Risk assessment
b. Control activities
c. Governance
d. Monitoring

**(3)** Which Clause of the listing agreements issued by SEBI in India is on similar lines of SOX regulation?

a. Clause 35 b. Clause 56 c. Clause 49 d. Clause 22

**(4)** From The following which is not the key function of IT steering committee?

a. Review status IS Budget
b. Implementation of IT security
c. Resolve conflicts
d. COSO

**(5)** Which is managerial activity in an enterprise in strategic planning?

a. Strategic planning
b. Management control
c. Operational control
d. All of the above

**(6)** Which is not a part of IT Strategic planning in an enterprise categories?

a. Enterprise Strategic Plan
b. Internal Control
c. Information Systems Requirements Plan
d. Information Systems Applications and Facilities Plan

**(7)** From following which is not part of Key Management Practices for Aligning IT Strategy with Enterprise Strategy?

a. Understand enterprise direction
b. Conduct a gap analysis
c. Communicate the IT strategy and direction
d. Communication and Information

**(8)** Based on the point of impact of risks, controls are classified as ?

a. Preventive b. Detective c. Corrective. d. All of the above

**(9)** From following which is common sources of Risk?

a. Economic Circumstances
b. Enterprise
c. Human Behaviors
d. A and C

**(10)** From the following which is not terminologies related to risk assessment?

a. Asset b. Standard c. Risk d. Vulnerability

**(11)** A threat is _____

a. Action b. event c. condition d. All of the above

**(12)** _____of the threat occurring means the estimation or the probability that the threat will succeed in achieving its undesirable event.

a. Risk b. Threat c. Likelihood d. Residual Risk

**(13)** Any risk still remaining after the counter measures are analysed and implemented is called_____

a. Residual Risk b. Countermeasure c. Asset d. Threat

**(14)** An action, technique or any other measures that reduces the vulnerability of a system is referred as _____

a. Countermeasure b. Risk c. Control d. Threat

**(15)** From the following which is not Risk Management Strategies?

a. Accept Risk b. Eliminate Risk c. Turn Back d. Alternative Action

**(16)** Which step is not a part of Key Management Practices of Risk Management?

a. Collect b. Risk profile c. Risk assessment d. Respond to Risk

**(17)** From following which is not a part of Components in COBIT?

a. Framework b. Monitor c. Control objectives

d. Process description

**(18)** We can Customizing COBIT 5 as per requirement, it can be applied to meet needs related to:

a. Information security b. Risk management

c. Governance and management of enterprise IT

d. All of the Above

**(19)** In COBIT 5 Process reference modelAPO stands for _____

a. Align, Plan, Organize b. Align, process ,order

c. Align , plan , occur d. Arrange, plan , Organize

**(20)** In Risk management, Risk Assessment consist of _____

a. Risk Identification b. Risk Analysis

c. Risk Prioritization d. All of The Above

**(21)** COBIT 5 provides key management practices for ensuring external compliances which are as follows: a)Optimize Response to External Requirements, b)Obtain Assurance of External Compliance, c)Identify External Compliance Requirements,d)Confirm External Compliance. Arrange this

a. C,A,D,B b. C,d,b,a c. C,A,B,D d. C,D,A,B

## Answers to MCQs:

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1. | (d) | 2. | (c) | 3. | (c) | 4. | (c) | 5. | (d) | 6. | (b) |
| 7. | () | 8. | (d) | 9. | (d) | 10. | (b) | 11. | (d) | 12. | (c) |
| 13. | (a) | 14. | () | 15. | () | 16. | (c) | 17. | (b) | 18. | (d) |
| 19. | () | 20. | (d) | 21. | (d) | | | | | | |

*---0---0---*

# CHAPTER-2

# INFORMATION SYSTEMS CONCEPTS

(1) From the following which is not Attributes of Information?

a. Reliability b. Availability c. Rate d. Important

(2) University system is As Example of_____-

a. Physical system b. Open System c. Manual system d. Deterministic system

(3) An information system comprise of _____

a. People b. hardware, software c. data d. All of the above

(4) From the Following which is not an Example of Major areas of CBIS?

a. Finance & Accounting b. Production or Manufacturing

c. Reports d. Inventory / Stores Management

(5) Which is not TPS Components?

a. Input b. Processing c. Feedback d. Storage

(6) Which systems are very useful in remote access of documents/internal communication?

a. Text processing system b. Electronic document management system

c. Teleconferencing and Videoconferencing d. Electronic message communication system

(7) Which is not Components of Message Communication Systems?

a. Email b. Video Conference c. Voice Mail d. Fax

(8) _____knowledge is that which can be formalized easily and as a consequence is easily available across the organization

a. Explicit b. Tacit c. Data d. Information

(9) _____ provide reports to management that can help in making effective, structured types as applicable to decisions of day-to-day operations

a. MIS b. TPS c. ESS d. DSS

(10) From following which is not Misconceptions about MIS?

a. Any reporting system is MIS. b. MIS is a management technique

c. MIS is a bunch of technologies. d. MIS is USED at Middle Level Management

(11) From the following which is Constraints in operating an MIS?

a. Staff co-operation Not available b. Unstructured decision

c. Quality d. Not tailor-made

(12) From the following which is not Components of DSS?

a. User b. Planning language c. Database d. Model base

(13) Examples of Decision Support Systems in Accounting:

a. Cost Accounting System b. Capital Budgeting System

c. Debtors management d. A & B

(14) Which is not characteristics of information used in executive decision-making?

a. Future orientation b. Informal Source

c. High degree of uncertainty d. Flexible

(15) Some of the properties that potential applications should possess to qualify for Expert System development:

a. Domain b. Structure c. Expertise d. All of the above

(16) To operate information systems (IS) effectively and efficiently, a business manager or business professional should have following knowledge :

a. Foundation Concepts b. Business Applications

c. Management Challenges d. All of the above

(17) _____designed to process and carry out routine transactions efficiently and accurately

a. TPS b. MIS c. ESS d. DSS

(18) _____These are systems that help in the enhancement of performance of or productivity of employees who are dealing with the data processing and information.

a. OAS b. TPS c. ESS d. DSS

(19) _____These are specifically designed to help management to make decisions in situations where there is uncertainty about the possible outcomes of those decisions.

a. OAS b. TPS c. ESS d. DSS

(20) _____is a reporting tool (software) that allows us to turn our organization's data into useful summarized reports

a. OAS b. TPS c. ESS d. DSS

(21) _____is process management software that allows an organization to use a system of integrated applications to manage the business and automate many back office functions related to technology, services and human resources.

a. OAS b. TPS c. ERP d. DSS

(22) some of the IT tools crucial for business growth.

a. Business Website b. Internet and Intranet

c. Business Intelligence d. All of the above

(23) Websites can be designed by using

a. HTML b. XML c. ASP.NET

d. All of the above

(24) From the following which is not as applications of DM?

a. text mining b. web analysis c. monitoring

d. finance planning and asset evaluation

## Answers to MCQs:

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1. | (d) | 2. | (a) | 3. | (d) | 4. | (c) | 5. | (c) | 6. | (b) |
| 7. | (b) | 8. | (a) | 9. | (a) | 10. | (d) | 11. | (a) | 12. | (b) |
| 13. | (d) | 14. | (d) | 15. | (d) | 16. | (d) | 17. | (a) | 18. | (a) |
| 19. | (d) | 20. | (c) | 21. | (c) | 22. | (d) | 23. | (d) | 24. | (c) |

*---0---0---*

# CHAPTER-3

# PROTECTION OF INFORMATION SYSTEMS

(1) The security objective comprises three universally accepted attributes, from the following list which is not applicable:

a. Confidentiality b. Integrity c. Availability d. Timeliness

(2) All the organizations know that _ _ _are crucial for the success of a company but fail to protect these plans, although it might have seen impossible for a company to completely prevent its act from being discovered.

a. Strategic plan b. Business information

c. Finance d. Operational

(3) _____is the statement of intent by the management about how to protect a company's information assets.

a. Standards b. Performance indicators

c. An information security policy d. Guidelines

(4) _____specify technologies and methodologies to be used to secure systems.

a. Standards b. Guidelines c. Procedures d. Policy

(5) _____help in smooth implementation of information security policy.

a. Standards b. Guidelines c. Procedures d. Policy

(6) _____are more detailed steps to be followed to accomplish particular security-related tasks.

a. Standards b. Guidelines c. Procedures d. Policy

(7) Security policy broadly comprises the following three groups of management. Who is not part of group

a. Management b. Technical group c. Legal expert d. User

(8) Which is not a part of Organisation Security Policy_____

a. Oganisational Information Security Policy b. Network & System Security Policy

c. Information Classification Policy d. Conditions for Connection

(9) From the following which is not a part of Impact of Technology on Internal Controls:

a. Segregation of Duties b. Authorization Procedures

c. Physical Control over Assets and Records d. BCP and DRP

(10) From the following list Objectives of Controls :

a. Preventive b. Detective c. Compensatory d. Physical Access

(11) "Authorisation of transaction" is an example of _____

a. Preventive b. Detective c. Compensatory d. Corrective

(12) "Hash totals" is an Example of _____

a. Preventive b. Detective c. Compensatory d. Corrective

(13) "Rerun procedures" is an Example of _____

a. Preventive b. Detective c. Compensatory d. Corrective

(14) A business continuity plan is significant_____.

a. Preventive b. Detective c. Compensatory d. Corrective

(15) organisation may not be able to implement appropriate controls and therefore there are adequate _____which may not be as efficient as the appropriate control but can reduce the probability of threats to the assets.

a. Preventive b. Detective c. Compensatory d. Corrective

(16) Security Guards is an example of _____

a. Physical access control b. Logical access control

c. Application control d. Managerial control

(17) The first entry door must close and lock, for the second door to open with only one person permitted to enter.

a. Dead man door b. Computer Terminal Locks

c. Controlled Single Entry Point d. Control of out of hours of employee

(18) In _____A responsible employee should escort all visitors

a. Controlled Visitor Access b. Security Guards

c. Alarm System d. Control of out of hours of employee-employees

(19) _____controls designate who is supposed to have access to a specific system resource and what type of transactions and functions are permitted on that system.

a. Physical access control b. Logical access control

c. Application control d. Managerial control

(20) Using_____a user can connect from one location's computer to another location's computer via a telecommunication media

a. Telecommunication Network b. Online Terminals

c. Dial-up Ports d. Operator Console

(21) This_____involves slicing of small amounts of money from a computerized transaction.

a. Salami b. Rounding down c. Data diddling d. Worms

(22) _____are malicious programs that are hidden under any authorized program.

a. Trojan horse b. Worms c. bomb d. Trap door

(23) _____changes the data before or as they are entered into the system. It occurs before computer security can protect data.

a. Salami b. Rounding down c. Data diddling d. Worms

(24) The_____is one of the crucial places whereany intruders can play havoc. Hence, access to this must berestricted.

a. Telecommunication Network b. Online Terminals

c. Dial-up Ports d. Operator Console

(25) _____ involves spying on information being transmitted overtelecommunication network

a. Piggybacking b. Data leakage c. Wire-tapping d. Subversive threats

(26) _____is the act of following an authorized person througha secured door or electronically attaching to an authorizedtelecommunication link that intercepts and alters transmission.

a. Piggybacking b. Data leakage c. Wire-tapping d. Subversive threats

(27) The_____requires the user to enter a password and thenthe system breaks the connection. If the caller is authorized, thecall back device dials the caller's number to establish a newconnection.

a. Firewall b. Call back devise

c. Enforce path d. Segregation of network

(28) _ _ _ _ is a system that enforces access controlbetween two networks. To accomplish this, all traffic betweenthe external network and the organization's Intranet must pass through this.

a. Firewall b. Call back devise

c. encryption d. Segregation of network

(29) If an intruder is able to bypass the network perimetersecurity controls, the operating system is the last barrier to beconquered for unlimited access to all the resources.

a. User access management b. Operating system access control

c. Application control d. Mobile computing

(30) Arrange the activities in Systems Development Management Controls.
a)Program Testing ,b)System Authorization Activities, c) Internal Auditor's Participation, d)User Specification Activities, e)User Test and Acceptance Procedure, f) Technical Design Activities,

a. b,d,f,c,a,e b. b,d,f,a,c,e c. b,d,f,e,c,a d. b,d,f,c,e,a

(31) The program development life cycle comprises six major phases –; a)Coding; b)Testing; c)Control; d)Planning,e)Operation and Maintenance, f)Design

a. A,b,c,d,e,f b. D,c,f,a,b,e c. D,c,f,a,e,b d. D,c,f,a,e,b

(32) _____which focuses on individual program modules.

a. Unit test b. Integration test

c. Whole of program test d. Regression test

(33) Under this strategy, two complete copies of the databaseare maintained. The databases are concurrently updated.

a. Dual recording of data b. Periodic dumping of data

c. Logging input transactions d. Logging changes to the data

(34) These controls provide solutions, agreed-upon schedulesand strategies to overcome the data integrity problems that may arise when twoupdate processes access the same data item at the same time.

a. Access control b. Update control

c. Concurrent control d. Quality control

(35) From the following which is not Input controls

a. Source Document Control b. Data Coding Controls

c. Batch Controls d. Boundary control

(36) _____errors occur when two adjacent digits are reversed

a. Single transposition b. Multiple transposition

c. Truncation d. Addition

(37) _____is a control digit (or digits) added to the code when it is originally assigned thatallows the integrity of the code to be established during subsequent processing

a. Valid code b. Check digit c. Arithmetic Checks d. Cross check

(38) When programs or data are transmitted, additional controls areneeded. Transmission errors are controlled primarily by detecting errors orcorrecting codes.

a. Parity check b. Cross check c. Check digit d. Picture check

(39) "Twisted pair" is an example of _____

a. Guided media b. Unguided media

c. Communication lines d. Modem

(40) _____are needed because two nodes in a network can differ in terms of the rate at which they can send, received, and process data

a. Line error control b. Flow control

c. Link control d. Topological control

(41) The primary function is to perform protocol conversion to allow different types ofcommunication architectures to communicate with one another.

a. Lan b. Bridge c. Router d. Gateway

(42) An operating system might get stuck in an infinite loop. In theabsence of any control, the program will retain use of processor andprevent other programs from undertaking their work.

a. Error detection b. Multiple state execution

c. Timing control d. Component replication

(43) In _____Two or more fields can be compared and cross verified to ensure their correctness.

a. Reasonableness verification b. Edit check

c. Field Initialization d. Exception report

(44) Information would include accounting information, business plans, sensitive customer information of banks, solicitors and accountants etc are example of _____

a. Top Secret b. Highly Confidential

c. Proprietary d. Internal Use only

(45) Pending mergers or acquisitions;investment strategies; plans or designs; that could seriously damage the organization ifsuch information were lost or made public. This are example of _____

a. Top Secret b. Highly Confidential

c. Proprietary d. Internal Use only

(46) From the following which is not an example of data integrity policies:

a. Virus-Signature Updating b. Offsite Backup Storage

c. Disaster Recovery d. Insurance

(47) It is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masqueradingas a trustworthy entity in an electronic communication.

a. Phishing b. Spam c. Scavenging d. Eavesdropping

(48) It refers to an action or series of actions that preventsaccess to a software system by its intended/ authorized users; causes the delay of itstime-critical operations; or prevents any part of the system

from functioning.

a. Logic Time Bombs: b. Denial of Service (DoS) Attack

c. Masquerading or Impersonation d. Password Cracking:

(49) It refers to the unauthorized use of special system programs to bypassregular system controls and performs illegal acts.

a. Super Zapping b. Scavenging

c. Social Engineering Techniques d. Data Leakage

(50) In this case, perpetrator tricks an employee into givingout the information needed to get into the system.

a. Super Zapping b. Scavenging

c. Social Engineering Techniques d. Data Leakage

## Answers to MCQs:

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1. | (d) | 2. | (a) | 3. | (c) | 4. | (a) | 5. | (b) | 6. | (c) |
| 7. | (d) | 8. | (d) | 9. | (d) | 10. | () | 11. | (a) | 12. | (b) |
| 13. | (d) | 14. | (d) | 15. | (c) | 16. | (a) | 17. | (a) | 18. | (d) |
| 19. | (b) | 20. | (c) | 21. | (a) | 22. | (a) | 23. | (c) | 24. | (d) |
| 25. | (c) | 26. | (a) | 27. | (b) | 28. | (a) | 29. | (b) | 30. | (a) |
| 31. | (b) | 32. | (a) | 33. | (a) | 34. | (c) | 35. | (d) | 36. | (a) |
| 37. | (b) | 38. | (a) | 39. | (a) | 40. | (b) | 41. | (d) | 42. | (c) |
| 43. | (a) | 44. | (b) | 45. | (a) | 46. | (d) | 47. | (a) | 48. | (b) |
| 49. | (a) | 50. | (c) | | | | | | | | |

# CHAPTER-4

## BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING

**(1)** _ __ _ __ is an event which when materialised can disrupt the computer operations, thereby disrupting the business functions as well

a. Business Contingency
b. BCP Process
c. Business Continuity Planning (BCP)
d. BCP Manual

**(2)** _____ refers to the ability of enterprises to recover from a disaster and continue operations with least impact.

a. Business Contingency
b. BCP Process
c. Business Continuity Planning (BCP)
d. BCP Manual

**(3)** _____ is a documented description of actions to be taken, resources to be used and procedures to be followed before, during and after such disruptive event

a. Business Contingency
b. BCP Process
c. Business Continuity Planning (BCP)
d. BCP Manual

**(4)** The business continuity life cycle is broken down into four broad and sequential sections: a)determination of recovery alternatives; b)recovery plan validation. C) risk assessment; d)recovery plan implementation; Arrange it.

a. c,a,d,b
b. c,a,b,d
c. c,d,a,b
d. c,a,d,b

**(5)** Arrange phases of developing BCP :

a)Testing Program , b)Business Impact Analysis ,c) Plan Development ,d)Pre-Planning Activities ,e) Maintenance Program ,f)Initial Plan Testing and Plan Implementation, g)Detailed Definition of Requirements,h) Vulnerability Assessment and General Definition of Requirements,

a. d,h,b,g,c,a,e,f
b. d,a,c,b,e,g,f,h
c. d,h,b,g,a,c,e,f
d. d,h,b,e,a,f,g,h

**(6)** __ ____ _should be established which should undertake an overall responsibility for providing direction and guidance to the BCP team.

a. Management committee
b. Steering Committee
c. Project manager
d. Steering manager

**(7)** Security and control within an organisation should concentrate on reducing the possibility of disaster occurrence, rather than concentrating on minimising the impact of an actual disaster. Which phase do this.

a. Pre-Planning Activities (Business Continuity Plan Initiation)
b. Vulnerability Assessment and General Definition of Requirements
c. Business Impact Analysis
d. Detailed Definition of Requirements

**(8)** _____assesses the potential impacts of various events or incidents.

a. Pre-Planning Activities (Business Continuity Plan Initiation)
b. Vulnerability Assessment and General Definition of Requirements
c. Business Impact Analysis
d. Detailed Definition of Requirements

**(9)** _____enables the business continuity, capacity and capability to be established and maintained which are in accordance to the requirements of the enterprise.

a. BCM process
b. BCM information collection process
c. BCMDevelopment and Implementation Process
d. BCM strategy process

**(10)** Here_____prioritisation of an enterprise's products and services are done and the activities required to deliver them

a. BCM process
b. BCM information collection process
c. BCMDevelopment and Implementation Process
d. BCM strategy process

**(11)** Which is not parameters considered in deciding whether a service is Vital/Essential/Desirable are:

a. Loss of revenue
b. Loss of reputation;
c. Decrease in customer satisfaction
d. Loss of GOODWILL

**(12)** A risk that is almost certain to show-up during project execution. The occurrence of risk which can cause problems is more than 80% will fall under this category.

a. Definite b. Likely c. Unlikely d. Probable

**(13)** Risks that have 60-80% chances of occurrence can be grouped as likely.

a. Definite b. Likely c. Unlikely d. Probable

**(14)** Rare and exceptional risks which have a less than 10% chance of occurrence.

a. Definite b. Likely c. Unlikely d. Probable

**(15)** Risks that will cause a near negligible amount of damage to the overall progress of the project.

a. Trivial/Insignificant
b. Minor
c. Major
d. Catastrophic

**(16)** Risk which when materialize but does not result in significant damage falls under this category

a. Trivial/Insignificant b. Minor c. Major d. Catastrophic

**(17)** Risks with significantly large consequences which can lead to a great amount of loss are classified as critical.

a. Trivial/Insignificant
b. Minor
c. Major
d. Catastrophic

**(18)** These are the risks which can make the project completely unproductive and unfruitful, and must be a top priority during risk management.

a. Trivial/Insignificant b. Minor c. Major d. Catastrophic

**(19)** Like values_____can be categorized into Catastrophic.

a. 8 to 12 b. 4 to 6 c. 3 d. 1 and 2

**(20)** Which is not a part of Development of a BCM culture :

a. Leadership from senior personnel;
b. Assignment of responsibilities
c. Awareness
d. Interview

**(21)** The final component of a disaster recovery plan is a _____

a. Emergency plan b. Backup plan c. Recovery plan d. Test plan

**(22)** _____captures all files on the disk or within the folder selected for backup.

a. Full Backup
b. Incremental Back-up
c. Differential Back-up
d. Mirror back-up

**(23)** _____captures files that were created or changed since the last backup, regardless of backup type.

a. Full Backup
b. Incremental Back-up
c. Differential Back-up
d. Mirror back-up

**(24)** _____stores files that have changed since the last full backup.

a. Full Backup
b. Incremental Back-up
c. Differential Back-up
d. Mirror back-up

**(25)** _____should be used with caution because if a file is deleted by accident, sabotage or through a virus then the same file in mirror backup will also be deleted. Some do not consider a mirror to be a backup

a. Full Backup
b. Incremental Back-up
c. Differential Back-up
d. Mirror back-up

**(26)** _____is most frequently used to create an exact copy of the backup data.

a. Full Backup
b. Incremental Back-up
c. Differential Back-up
d. Mirror back-up

**(27)** If an organisation can tolerate some downtime (i.e., some downtime is available for recovery) then _____might be appropriate.

a. cold site back-up
b. Hot site backup
c. Warm site backup
d. Third party site backup

**(28)** If fast recovery is critical i.e., no downtime is permissible, an organisation might need _____

a. cold site back-up
b. Hot site backup
c. Warm site backup
d. Third party site backup

**(29)** _____has all cold site facilities plus hardware that might be difficult to obtain or install in an alternative location

a. cold site back-up
b. Hot site backup
c. Warm site backup
d. Third party site backup

**(30)** Two or more organisations might agree to provide back-up facilities to each other in the event of one facing a disaster

a. cold site back-up
b. Hot site backup
c. Warm site backup
d. Reciprocal agreement

## Answers to MCQs:

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1. | (a) | 2. | (c) | 3. | (d) | 4. | (a) | 5. | (a) | 6. | (b) |
| 7. | (b) | 8. | (c) | 9. | (a) | 10. | (b) | 11. | (d) | 12. | (a) |
| 13. | (b) | 14. | (c) | 15. | (a) | 16. | (b) | 17. | (c) | 18. | (d) |
| 19. | (a) | 20. | (d) | 21. | (d) | 22. | (a) | 23. | (b) | 24. | (c) |
| 25. | (d) | 26. | (d) | 27. | (a) | 28. | (b) | 29. | (c) | 30. | (c) |

*---0---0---*

# CHAPTER-5
# ACQUISITION, DEVELOPMENT AND IMPLEMENTATION OF INFORMATION SYSTEMS

(1) _____ is the process of gathering and interpreting facts, diagnosing problems, and using the information to recommend improvements to the system.

a. System analysis b. System design

c. System development d. System implementation

(2) An analysis on 'why organizations fail to achieve theirsystems development objectives' reveals bottlenecks. From the following list which is not user related Issue:

a. Resistance to Change b. Lack of Users' Participation

c. Inadequate Testing and User Training

d. Overworked or Under-Trained Development Staff

(3) In system development from following which cost is not included:

a. Development Costs b. Operating Costs:

c. Intangible Costs: d. Managerial remuneration

(4) _____approach is a traditional development approach in which each phase is carried insequence or linear fashion.When this approach is applied, an activity is undertaken only when the prior step is fully completed.

a. Waterfall b. Prototype c. Incremental d. Spiral

(5) _____ is ideal for supporting less experienced project teams and project managers orproject teams, whose composition fluctuates.

a. Waterfall b. Prototype c. Incremental d. Spiral

(6) Arrange the steps in prototype approach.a)Test and Revise b) Develop the Initial Prototype c) Obtain User Signoff of the Approved Prototype d)Identify Information System Requirements

a. d,b,a,c b. a,b,c,d c. d,b,c,a d. d,a,c,b

(7) The product is decomposed into a number of components, each of which are designed andbuilt separately (termed as builds). Each component is delivered to the client when it iscomplete.

a. Waterfall b. Prototype c. Incremental d. Spiral

(8) _ _ _ _ ofdevelopment also helps to ease the traumatic effect of introducing completely new system allat once.

a. Waterfall b. Prototype c. Incremental d. Spiral

(9) _____combines the features of the prototyping model and the waterfall model. OR _ is intended for large, expensive and complicated projects. OR Gamedevelopment is a main area where _____is used and needed.

a. Waterfall b. Prototype c. Incremental d. Spiral

(10) _____model comprises feature such as time boxes, joint application development etc

a. Waterfall b. Prototype c. Incremental d. RAD

(11) This is an organized set of software development methodologies based on the iterative andincremental development, where requirements and solutions evolve through collaborationbetween self-organizing, cross-functional teams.

a. Waterfall b. Prototype c. Incremental d. Agile

(12) From the following which is not dimension of scope in preliminary investigation:

a. Functionality Requirements b. Control Requirements

c. Performance Requirements d. Conducting Interviews

(13) From the following which is not feasibility study?

a. Technical b. Schedule/Time c. Behavioral d. Interview

(14) _____ includes an evaluation of all the incremental costs and benefitsexpected if the proposed system is implemented

a. Technical b. Schedule/Time c. Financial d. Economic

(15) Implementing sophisticatedsoftware solutions becomes difficult at specific locations because of the reluctance ofskilled personnel to move to such locations.

a. Technical b. Schedule/Time c. Resources d. Economic

(16) _____is concerned with ascertaining the views of workers,employees, customers and suppliers about the use of computer facility

a. Technical b. Operational c. Resources d. Economic

(17) From the following list which is not Fact finding Technics :

a. Documents b. Observation c. Techniacal d. interview

(18) _ _____is a pictorial representation technique that can be used by analysts to represent the inputs, outputs and processes of a business process.

a. Flowchart b. Data flow diagram

c. System component matrix d. Decision table

(19) A Data Flow Diagram uses few simple symbols to illustrate theflow of data among external entities (such as people or organizations, etc.), processing activities and data storage elements.

a. Flowchart b. Data flow diagram

c. System component matrix d. Decision table

(20) This shape indicate _____

a. Data source and data destination b. Data flow

c. Transformation process d. Data store

(21) A data dictionary contains descriptive information about the data itemsin the files of a business information system. It is computer file about data.

a. Flowchart b. Data flow diagram

c. System component matrix d. Data dictionary

(22) Whenever a project team has to develop an application in a fieldthat's new to them, they take the help of a

a. domain specialist
b. IS auditor
c. Steering committee
d. System analyst

(23) From the following which is not a Major Activities in Database Designing?

a. Design of Data/Information flow
b. Conceptual modeling
c. Data modeling
d. Physical Layout Design

(24) From the following which is not The considerations are valid for both acquisition of hardware and software:

a. Vendor Selection
b. Geographical Location of Vendor
c. Evaluation of Users Feedback
d. Benchmark

(25) _____relatedto vendors' proposals are accomplished by sample programs that represent at least apart of the buyer's primary work load and include considerations and can be currentapplications that have been designed to represent planned processing needs

a. Testing Problems
b. Benchmarking problems
c. Public Evaluation Reports
d. Checklists

(26) _____should be designed to verify the response time,the execution time, the throughput, primary and secondary memory utilization and the traffic rates on data channels and communication links.

a. Functional test
b. Performance test
c. Stress test
d. Parallel test

(27) _____is a form of testing that is used to determine the stability of a given system or entity. It involves testing beyond normal operational capacity, often toa breaking point, in order to observe the results

a. Functional test
b. Performance test
c. Stress test
d. Parallel test

(28) _____Testing takes an external perspective of the testobject, to derive test cases. These tests can be functional or non-functional, thoughusually functional.

a. Desk check
b. Black box
c. White box
d. Code inspection

(29) It uses an internal perspective of the system to design testcases based on internal structure. It requires programming skills to identify all pathsthrough the software.

a. Desk check
b. Black box
c. White box
d. Code inspection

(30) Each time a new module is added or any modification made in the software, it changes. New data flow paths are established, new I/O may occur and new controllogic is invoked. These changes may cause problems with functions that previously workedflawlessly

a. Static testing
b. Dynamic testing
c. Integration testing
d. Regression testing

(31) In user acceptance testing_____will be performed by user of the organization

a. Alpha test
b. Beta test
c. Recovery test
d. Security test

(32) This is achieved through an abrupttakeover – an all or no approach. With this strategy, the changeover is done in one operation, completely replacing the old system in one go.

a. Direct Implementation / Abrupt Change-Over
b. Phased Changeover
c. Pilot Changeover
d. Parallel Changeover

(33) With this strategy, implementation can be staged withconversion to the new system taking place gradually.

a. Direct Implementation / Abrupt Change-Over
b. Phased Changeover
c. Pilot Changeover
d. Parallel Changeover

(34) With this strategy, the new system replaces the old one in one operation but only on a small scale. Any errors can be rectified or further beneficialchanges can be introduced and replicated throughout the whole system in goodtime with the least disruption

a. Direct Implementation / Abrupt Change-Over
b. Phased Changeover
c. Pilot Changeover
d. Parallel Changeover

(35) _____tried out in one branch of the company or in one location. If successful then the it is extended until it eventually replaces the old system completely.

a. Direct Implementation / Abrupt Change-Over
b. Phased Changeover
c. Pilot Changeover
d. Parallel Changeover

(36) The old system remainsfully operational while the new systems come online. With this strategy, the old andthe new system are both used alongside each other, both being able to operateindependently.

a. Direct Implementation / Abrupt Change-Over
b. Phased Changeover
c. Pilot Changeover
d. Parallel Changeover

(37) _____ is anticipated and can be planned foroperational continuity and avoidance of anticipated risk.

a. Schedule maintenance
b. Preventive maintenance
c. Rescue maintenance
d. Corrective maintenance

(38) _____refers to previously undetectedmalfunctions that were not anticipated but require immediate troubleshooting solution.

a. Schedule maintenance
b. Preventive maintenance
c. Rescue maintenance
d. Corrective maintenance

(39) _____concerns with the activities aimed atincreasing the system's maintainability, such as updating documentation, addingcomments, and improving the modular structure of the system.

a. Schedule maintenance
b. Preventive maintenance
c. Rescue maintenance
d. Corrective maintenance

(40) From the following which is not characteristic of A good coded application and programs:

a. Reliability b. Robustness c. Readability d. Standard

(41) Which characteristic of A good coded application and programs indicate 'what program is supposed to do', but should also takecare of 'what it should not do'.

a. Reliability b. Robustness c. Readability d. Accuracy

(42) Which characteristic of A good coded application and programs indicateIt refers to the applications' strength to uphold its operations in adversesituations by taking into account all possible inputs and outputs of a program in case of least likely situations.

a. Reliability b. Robustness c. Readability d. Accuracy

(43) _____ is normally responsible for more than one projectand liaisonsing with the client or the affected functions.

a. Project manager b. Project leader

c. Module leader d. System analyst

(44) From the following which is not a part of SRS :

a. Information Description b. Behavioral Description

c. Appendices d. Data dictionary

(45) The data flow diagram and system flow charts that users review arecommonly generated by systems developers using the on-screen drawing modules found in_____.

a. CASE b. CAAT

c. Data dictionary d. System component matrix

## Answers to MCQs:

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1. | (a) | 2. | (d) | 3. | (d) | 4. | (a) | 5. | (a) | 6. | (a) |
| 7. | (c) | 8. | (c) | 9. | (d) | 10. | (d) | 11. | (d) | 12. | (d) |
| 13. | (d) | 14. | (d) | 15. | (c) | 16. | (b) | 17. | (c) | 18. | (a) |
| 19. | (b) | 20. | () | 21. | (d) | 22. | (a) | 23. | (a) | 24. | (d) |
| 25. | (b) | 26. | (b) | 27. | (c) | 28. | (b) | 29. | (c) | 30. | (d) |
| 31. | (a) | 32. | (a) | 33. | (b) | 34. | (c) | 35. | (c) | 36. | (c) |
| 37. | (a) | 38. | (c) | 39. | (b) | 40. | (d) | 41. | (d) | 42. | (b) |
| 43. | (a) | 44. | (d) | 45. | (a) | | | | | | |

*---0---0---*

# CHAPTER-6
# AUDITING OF INFORMATION SYSTEMS

**(1)** From Following which is not an objective of IS audit

a. data Integrity Objectives
b. asset Safeguarding standard
c. system Efficiency Objectives
d. system Availability Objectives

**(2)** The use of computers to carry out trading activities is also increasing through internet. This can create problems with contracts.

a. Lack of visible audit trail
b. Legal issues
c. Audit evidence
d. Data retention & storage

**(3)** Data may be entered into the computer directly without the presence of supporting documentation resulting in less paperwork being available for audit examination.

a. Lack of visible audit trail
b. Legal issues
c. Audit evidence
d. Absence of input document

**(4)** Financial systems may have the ability to approve and record financial transactions (i.e., transactions are generated automatically).

a. System generated transactions
b. Systematic error
c. Lack of visible audit trail
d. Audit evidence

**(5)** From the following which are not IT audits categories :

a. Systems Development
b. Telecommunications, Intranets, and Extranets
c. Information Processing Facilities
d. IT-related frauds

**(6)** Steps in Information Technology Audit :
a)Closure, b) Fieldwork , c)Planning and preparation, d)Reporting,e) Analysis,f)Pre-audit survey Arrange IT.

a. F,c,b,e,d,a
b. F,c,e,a,d,b
c. F,c,b,e,a,d
d. F,c,b,d,a,e

**(7)** _____defines how to organise information security in any kind of Organisation and herefore different security should be prioritised to ensure overall effectiveness.

a. ISO 27001
b. ISO 27002
c. ISO 27003
d. ISO 27004

**(8)** _____provides management of organisation about information technology management, control, and security and IS auditors with guidance on different information technology associated risks and recommended practices.

a. GTAG
b. ISO 27001
c. IIA
d. ITIL

**(9)** Risks that affect a system and taken into consideration at the time of assessment can be categorised as

a. inherent risks
b. control risks
c. detection risks.
d. All of the above

**(10)** _____is a measure of the auditor's assessment of the likelihood that the risk may exceed a tolerable level which could be material either individually or in combination with other errors and will not be prevented or detected by the client's internal control system.

a. inherent risks
b. control risks
c. detection risks.
d. All of the above

**(11)** _____ is the risk that the IT auditor's substantive procedures will not detect an error which could be material either individually or in combination with other errors.

a. inherent risks b. control risks

c. detection risks. d. All of the above

**(12)** _____ is built into the system at those points where important processing occurs and takes images of the flow of transactions as it moves through the application

a. Snapshot b. ITF c. SCARF d. CIS

**(13)** _____involves the creation of a dummy entity in the application system files and does audit or test data against this entity to verify processing authenticity, accuracy, and completeness.

a. Snapshot b. ITF c. SCARF d. CIS

**(14)** _____technique involves embedding (i.e., fixing) audit software modules within a system to provide continuous monitoring of the system's transactions

a. Snapshot b. ITF c. SCARF d. CIS

**(15)** _____ is a variation of a SCARF continuous audit technique. This technique can be used to trap exceptions whenever the application system uses a database management system

a. Snapshot b. ITF c. SCARF d. CIS

**(16)** Inter auditor devised a system of_____which tags records of a change in name or address. The internal audit department will investigate these tagged records for detecting any fraud.

a. audit hooks b. ITF c. SCARF d. CIS

**(17)** _____controls attempt to ensure that a chronological record of all events that have occurred in a system is maintained.

a. Audit trail b. audit hooks c. ITF d. SCARF

**(18)** _____detection is to protect the system from outsiders who are attempting to breach system controls and also to report changes in system performance due to virus or worm.

a. real-time b. After the fact c. Tag d. CIS

**(19)** Which is not a part of audits may be conducted during system development process.

a. Concurrent Audit b. Post - implementation Audit

c. General Audit d. Internal audit

**(20)** _____Establishes interface between the user of the system and the system itself.

a. Boundary Controls b. Input Controls

c. Communication Controls d. Processing Controls

**(21)** _____Responsible for for computing, sorting, classifying and summarizing data

a. Boundary Controls b. Input Controls

c. Communication Controls d. Processing Controls

**(22)** _____ provide functions that determine the data content available to users, data format, timeliness of data and how data is prepared and routed to users.

a. Boundary Controls b. Output Controls

c. Communication Controls d. Processing Controls

**(23)** _____Responsible to provide functions to define, create, modify, delete and read data in an information system

a. Boundary Controls b. Output Controls

c. Database Controls d. Processing Controls

**(24)** _____maintains the chronology of events that occur when a user attempts to gain access to and employ systems resources.

a. Boundary Controls
b. Input Controls
c. Communication Controls
d. Processing Controls

**(25)** _____ maintains a chronology of the events from the time a sender dispatches a message to the time a receiver obtains the message.

a. Boundary Controls
b. Input Controls
c. Communication Controls
d. Processing Controls

**(26)** Application security audit should be based on layered approach. Which is not a part of this layers :

a. Operational Layer
b. Tactical Layer
c. Strategic Layer
d. Knowledge layer

**(27)** The operational layer audit issues not include:

a. User Accounts and Access Rights
b. Password Controls:
c. Segregation of Duties
d. Biometric

**(28)** At this layer, the top management takes action for drawing security policy, security training and security guideline:

a. Operational Layer
b. Tactical Layer
c. Strategic Layer
d. Knowledge layer

**(29)** _____layer, which includes supporting functions in the form of such as security administration, IT risk management, etc.

a. Operational Layer
b. Tactical Layer
c. Strategic Layer
d. Knowledge layer

**(30)** _____ is a basic internal control that prevents or detects errors and irregularities by assigning recording of transaction or custody of assets to separate individuals

a. User Accounts and Access Rights
b. Password Controls:
c. Segregation of Duties
d. Biometric

## Answers to MCQs:

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1. | (d) | 2. | (b) | 3. | (d) | 4. | (a) | 5. | (d) | 6. | (a) |
| 7. | (a) | 8. | (a) | 9. | (d) | 10. | (b) | 11. | (c) | 12. | (a) |
| 13. | (b) | 14. | (c) | 15. | (d) | 16. | (a) | 17. | (a) | 18. | (a) |
| 19. | (d) | 20. | (a) | 21. | (d) | 22. | (b) | 23. | (c) | 24. | (a) |
| 25. | (c) | 26. | (d) | 27. | (d) | 28. | (c) | 29. | (a) | 30. | (c) |

# CHAPTER-7

# INFORMATION TECHNOLOGYREGULATORY ISSUES

(1) Which is not the key issues of electronic information impacting enterprises and auditors :

a. Authenticity b. Reliability c. Accessibility d. Confidentiality

(2) Section_____provides the conditions subject to which an electronic record may be authenticated by means of affixing digital signature:

a. Sec 3 b. Sec 3A c. Sec 4 d. Sec 5

(3) First the electronic record is converted into a message digest byusing a mathematical function known as _____which digitally freezes the electronicrecord thus ensuring the integrity of the content of the intended communication contained inthe electronic record:

a. hash function b. Digital library c. Database d. DBMS

(4) Any person by the use of a_____of the subscriber can verify the electronic record.

a. public key b. private key c. Digital signature d. hash function

(5) _____may prescribe the procedure for the purpose of ascertainingwhether electronic signature is that of the person by whom it is purported to have beenaffixed or authenticated.

a. State Government b. Appropriate Government

c. Central Government d. All of the above

(6) _____ provides that where any law requires that any information or matter should be in the typewritten or printed form, then such requirement shall be deemed to be satisfied if it is in an electronic form.

a. Sec 4 b. Sec 5 c. Sec 6 d. Sec 7

(7) _____may prescribe the manner and format in which such electronic records shall be filed, created or issued.

a. State Government b. Appropriate Government

c. Central Government d. All of the above

(8) _____provides that the documents, records or information which is to be retained for any specified period shall be deemed to have been retained if the same is retained in the electronic form.

a. Sec 4 b. Sec 5 c. Sec 6 d. Sec 7

(9) When a contract is made then the communication, acceptance and the revocation of proposals, as the case may be are expressed in electronic form or by means of an electronic record.

a. Sec 10 b. Sec 10A c. Sec 14 d. Sec 7

(10) Whoever knowingly or intentionally tampers with the computer code source documents, then _____provides for punishment up to three years or with a fine which may extend to Rs. 2 lakhs or with both.

a. Sec 66 b. Sec 65 c. Sec 69 d. Sec 70

(11) Whoever intentionally or knowingly captures; publishes or transmits the image of a private area of any person without his or her consent:

a. Sec 66B b. Sec 66C c. Sec 66D d. Sec 66E

(12) introducing any computer contaminant which is likely to cause death or injuries to persons or damage or destruction of property or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70.

a. Sec 66B b. Sec 66C c. Sec 66D d. Sec 66F

(13) Intermediary shall preserve and retain such information as specified for such duration and in such manner as the Central Government may prescribe.

a. Sec 66 b. Sec 67 c. Sec 67A d. Sec 67 C

(14) Power to issue directions for blocking for public access of any information through any computer resource:

a. Sec 68 b. Sec 69 c. Sec 69A d. Sec 69B

(15) ___ __ _ may, by notification in the Official Gazette, declare any computer resource to be a protected system Under sec 70.

a. State Government b. Appropriate Government

c. Central Government d. All of the above

(16) _____shall prescribe the information security practices and procedures for such protected system under sec 70.

a. State Government b. Appropriate Government

c. Central Government d. All of the above

(17) Whoever makes any misrepresentation or suppresses any material fact from the Controller or the Certifying Authority for obtaining any License or Electronic Signature Certificate:

a. Sec 70 b. Sec 71 c. Sec 72 d. Sec 72A

(18) Any person including an intermediary who while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned.

a. Sec 70 b. Sec 71 c. Sec 72 d. Sec 72A

(19) _____is the apex body overseeing the insurance business in India.

a. IRDA b. RBI c. SEBI d. ROC

(20) All insurers shall have their systems and process audited at least once in__years by a CA firm a.

2 b. 3 c. 4 d. 5

(21) Stock Exchange authorities shall appoint the Auditors based on the Selection Norms. However, auditors can perform a maximum of _ successive audits.

a. 2 b. 3 c. 4 d. 5

(22) The Auditor must have experience in/direct access to experienced resources in theareas covered under TOR. It is recommended that resources employed shall haverelevant industry recognized certifications

a. CISA b. CISM c. CISSP d. Any one of the above

(23) In ISO 27001:2013 Annex A has been revised and restructured; there are now_____controls under 14categories rather than the previous 133 controls under 11 categories:

a. 114 b. 124 c. 110 d. 103

(24) In ISO 27001:2013 Annex A has been revised and restructured; there are now 114 controls under 14categories rather than the previous_____controls under 11 categories.

a. 133 b. 143 c. 155 d. 165

(25) From the following Which is not part if Service Strategy, ITIL

a. IT Service Generation
b. Financial Management
c. Business Relationship Management
d. Accounting and Finance

## Answers to MCQs:

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1. | (d) | 2. | (b) | 3. | (a) | 4. | (a) | 5. | (c) | 6. | (a) |
| 7. | (b) | 8. | (d) | 9. | (b) | 10. | (b) | 11. | (d) | 12. | (d) |
| 13. | (d) | 14. | (c) | 15. | (b) | 16. | (c) | 17. | (b) | 18. | (d) |
| 19. | (a) | 20. | (b) | 21. | (b) | 22. | (d) | 23. | (a) | 24. | (a) |
| 25. | (d) | | | | | | | | | | |

# CHAPTER-8

# EMERGING TECHNOLOGIES

(1) The idea of _____ is to make use of such non utilized computing power by the needy organizations, and thereby increasing the Return On Investment (ROI) on computing investments.

a. Grid computing b. Cloud computing

c. Virtualization d. E-commerce

(2) _____simply means the use of computing resources as a service through networks, typically the Internet.

a. Grid computing b. Cloud computing

c. Virtualization d. Mobile computing

(3) _ _ __ cloud computing environment resides within the boundaries of an organization and is used exclusively for the organization's benefits. These are also called Internal Clouds or Corporate Clouds

a. Private cloud b. Public cloud

c. Hybrid cloud d. Community cloud

(4) Which cloud is known as Internal Clouds or Corporate Clouds

a. Private cloud b. Public cloud

c. Hybrid cloud d. Community cloud

(5) _____ is provisioned for open use by the general public. They are administrated by third parties over the Internet.

a. Private cloud b. Public cloud

c. Hybrid cloud d. Community cloud

(6) From the following which is not Characteristics of Public Cloud are as follows?

a. highly Scalable b. Affordable

c. stringent SLAs d. Partially Secure

(7) _____infrastructure is provisioned for exclusive use by a specific group of consumers from organizations that have shared same issues.

a. Private cloud b. Public cloud

c. Hybrid cloud d. Community cloud

(8) ___ is a hardware-level service which provides computing resources for cloud users to run their application on-demand. This allows users to maximize the utilization of computing capacities without having to own and manage their own resources.

a. IAAS b. PAAS c. SAAS d. CAAS

(9) _____provides users with extra data communication capacity needed to accommodate increase in data traffic during data-intensive activities such as video conferencing or large file downloads

a. IAAS b. PAAS c. SAAS d. NAAS

(10) _____ _ provides the users the ability to develop and deploy an application on the development platform provided by the service provider

a. IAAS b. PAAS c. SAAS d. NAAS

(11) _____provides ability to the end users to access an application over the Internet that is hosted and managed by the service provider.

a. IAAS b. PAAS c. SAAS d. NAAS

(12) From the following which is Characteristics of Cloud Computing:

a. multi-Sharing b. high Availability and reliability

c. services in Pay-per-use mode d. All of the above

(13) Which is advantage of Cloud computing :

a. almost Unlimited storage b. highly Scalable

c. Affordable d. stringent SLAs

(14) _____refers to the technology that allows transmission of data via a computer without being connected to a fixed physical link.

a. Grid computing b. Cloud computing

c. Virtualization d. Mobile computing

(15) From which is not the Limitations of Mobile Computing?

a. Human interface with device b. Revising the technical architecture

c. Transmission / signals d. Security Standards

(16) _____ or Green IT is a practice of using computers and IT resources in a more efficient, environmentally friendly and responsible way.

a. Grid computing b. Cloud computing

c. Virtualization d. Green computing

(17)___Refers to business policy that allows employees to use their preferred computing devices, like smartphones and laptops for business purposes which has made work atmosphere more flexible and also empowering employees to work beyond their required hours.

a. Mobile computing b. Cloud computing

c. BYOD d. Green computing

18) While discussing Risk of BYOD, _____It is normally in the form of 'Lack of Device Visibility'.

a. Network Risk b. Device Risk

c. Implementation Risk d. Application Risk

(19) While discussing Risk of BYOD,_____It is normally in the form of 'Application Viruses and Malware.

a. Network Risk b. Device Risk

c. Implementation Risk d. Application Risk

(20) While discussing Risk of BYOD,_____It is normally in the form of 'Weak BYOD Policy.

a. Network Risk b. Device Risk

c. Implementation Risk d. Application Risk

21) _____basically refers to the transition from static HTML Web pages to a more dynamic Web which is more organized and is based on serving Web applications to users.

a. Web 2.0 b. Web 3.0 c. Social media d. Byod

22) _____are specifically designed for core field workers like chartered accountants, doctors, engineers or members of the corporate industries. A very good example is LinkedIn; Caclubindia

a. Social Contact Networks
b. Study Circles
c. Social Networks for Specialist Groups
d. Police and Military Networks

23) The present world (e-commerce world) has triggered people to invest in social networks, which will try to analyze the social behavior and will send this information to respective marts and stores.

a. Social Contact Networks
b. Study Circles
c. Social Networks for Specialist Groups
d. Shopping and Utility Service Networks

(24) _____give freedom to the users of a Social Network to express their thoughts in a free manner and helps in discussion of topics through their personal website which is updated frequently by user.

a. Communities b. Blogging c. Folksonomy d. Mashups

(25) _____is a set of co-related pages on a particular subject and allow users to share content :

a. Communities b. Blogging c. Wikis d. Mashups

(26) The term _____also known as the Semantic Web, describes sites wherein the computers will be generating raw data on their own without direct user interaction.

a. Web 2.0 b. Web 3.0 c. Social media d. Byod

(27) Web 3.0 technology uses the_____Technology, which features the data that are publishable and reusable on the web through query- able formats.

a. Data Web
b. Semantic Web
c. Web Services
d. artificial intelligence

## Answers to MCQs:

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1. | (a) | 2. | (b) | 3. | (a) | 4. | (a) | 5. | (b) | 6. | (d) |
| 7. | (d) | 8. | (a) | 9. | (d) | 10. | (b) | 11. | (c) | 12. | (d) |
| 13. | (a) | 14. | (d) | 15. | (b) | 16. | (d) | 17. | (c) | 18. | (a) |
| 19. | (d) | 20. | (c) | 21. | (a) | 22. | (c) | 23. | (d) | 24. | (b) |
| 25. | (c) | 26. | (b) | 27. | (a) | | | | | | |

*---0---0---*