

-
- 1 In a review of a software acquisition process, the IS auditor will typically not review the following
- A. Whether the decision to acquire the software flows from the feasibility study
 - B. Whether the RFP (Request For Proposal) is adequately detailed for transaction volume, data base size, turn around time and response time requirements and vendor responsibilities are clearly specified in the RFP
 - C. Whether program change history exists
 - D. Whether sufficient documentation is available to justify the selection of the final vendor/ product
- 2 Which of the following device / technique is used in a data communications system to fully use the capacity of a high-speed data communication line?
- A. Multiplexing
 - B. Bridge
 - C. Coaxial cable
 - D. Star topology
-

-
- 3 Network Penetration Testing is also called as
- A. Ethical hacking
 - B. Handshaking
 - C. Cracking a user password
 - D. Social Engineering
- 4 For Information Security to be effective and complete
- A. Only Network security needs to be implemented
 - B. ISO/OSI reference model should be implemented
 - C. Security policy should be prepared and should not be shared with the users
 - D. Users of all types and all levels should be made adequately aware of their roles and responsibilities

-
- 5 Which of the following is FALSE with respect to Neural networks
- A. It is one of the Network Topology
 - B. These are computing systems modeled after the human brain
 - C. Such systems recognise patterns
 - D. Such systems get more and more refined with more and more data input.
- 6 A local area network (LAN) can be best described as
- A. Which connects computers of various types, terminals, printers and other devices within a limited proximity
 - B. Which allows users to meet and share ideas
 - C. Tape library containing backed up tapes
 - D. TCP-IP
- 7 Auditing around the computer is also called
- A. White Box approach
 - B. Black Box Approach
 - C. Yellow box approach
 - D. Red box approach
-

-
- 8 A Disaster can be defined as .
- A. A planned interruption of normal business process
 - B. Catastrophe
 - C. Local Incidence
 - D. An unplanned interruption of normal business process
- 9 Typically a post implementation review will not include
- A. Evaluation of projected cost benefits
 - B. System requirement and design
 - C. Review of application system's adequacy in meeting the user requirements and business objectives
 - D. Review of the controls in the application system
- 10 Input controls in Application systems are
- A. To prevent unauthorised access to application and application data
 - B. To prevent unauthorised physical access to the Data Centre
 - C. To ensure accuracy and completeness of data and instruction input into an application system
 - D. For User Acceptance Testing
-

-
- 11 A Digital Certificate verifies the
- A. Private Key of the subject
 - B. Public Key of the subject
 - C. Integrity of the message
 - D. Strength of the Encryption Algorithm
- 12 One of the following can be used for only sequential and not direct access
- A. CD-ROM
 - B. Magnetic disk
 - C. Floppy disks
 - D. Magnetic tape
- 13 Division of responsibilities is necessary to ensure that one person cannot singly commit a fraud, is known as?
- A. Access Control
 - B. Separation of duties
 - C. Need to know
 - D. Least privilege
-

-
- 14 A data warehouse is a
- A. Record room with excellent physical and environmental controls
 - B. A storage box to store huge data bases
 - C. A repository of information of heterogeneous databases
 - D. Data conversion
- 15 One of the following is not a physical access control technique
- A. Bolting door locks
 - B. Combination or cipher locks
 - C. Biometric door locks
 - D. Public Key Infrastructure

-
- 16 An audit review of physical and environmental security of a CRITICAL area, like data centre, will not cover the following
- A. Authorisation, authentication and access controls in the Operating systems and Application systems
 - B. Availability of identification sign boards for approach to the critical areas
 - C. Physical access controls to the critical areas
 - D. Environmental controls like Adequacy of Uninterrupted Power Supply system, Temperature and humidity controls, fire and smoke detection systems

17 The advantages of using fiber optic cables are that

I. The signal is attenuated. II. Larger data can be transmitted. III. Fiber optic cable is small. IV. They are less affected by electrical interference.

- A. I and II
- B. I and III
- C. I, II, and III
- D. II, III, and IV.

18 The main components of the central processing unit (CPU) of a computer are

- A. Semiconductors, printers, and memory.
- B. Arithmetic-logic unit, control unit, and primary memory.
- C. Random access memory, read only memory, and tape drive
- D. Primary storage, input-output devices, and hub

19 Which of the following statement regarding system testing is FALSE?

- A .System testing is a process in which a collection of programs is integrated into the overall product and tested
- B. It is done to check whether the Application system complies with the user interface requirements
- C. It involves two kinds of activities – integration testing and acceptance testing
- D. Individual units of software are tested in isolation

20 A packet filtering router

- A. Checks the header of each incoming packet to determine whether it matches any of the packet filtering rules
- B. Decrypts the data
- C. Is used as an application server
- D. A bastion host server

-
- 21 Which of the following is not an example of Data Input validation technique in Application software
- A. Range and limit check
 - B. Missing data check
 - C. Duplicate check
 - D. User-ID and Password
- 22 Which of the following is the MOST critical control in an application audit?
- A. Audit trails
 - B. Backup of application software
 - C. Access to application parameters
 - D. Authorisation of transactions
- 23 Cipher-text is
- A. Decrypted Text
 - B. Plain Text
 - C. Encrypted Text
 - D. Encryption Key
-

-
- 24 An audit review of a Business Continuity Plan will not cover the following
- A. Asset inventory and data classification
 - B. User Acceptance Testing process of New Application system
 - C. Backup and recovery procedures
 - D. Identification of threats and vulnerabilities
- 25 Application, Presentation and Session Layers in OSI Model are mapped to
- A. Application Layer in TCP/IP Model
 - B. Transport Layer in TCP/IP Model
 - C. Internet Layer in TCP/IP Model
 - D. Network Interface Layer in TCP/IP Model

-
- 26 One of the following is not an advantage of expert systems
- A. The knowledge and experience of the expert is captured before he leaves the organisation
 - B. Development costs of expert systems are high
 - C. Helps ensure consistent and quality decisions
 - D. The codified knowledge in a central repository makes it easy to share it with the less experienced in the application area
- 27 One of the following is not an example of computer software
- A. Operating system
 - B. Word processing package
 - C. Application software
 - D. Modem.
-

-
- 28 Name the hardware that transforms the computer's digital information into signals that can be sent over ordinary telephone lines is called
- A. Router
 - B. IMAP
 - C. POP
 - D. Modem.
- 29 Three basic tenets of Information Security are
- *A. Encryption, authentication, Backups
 - B. Confidentiality, Integrity, Availability
 - C. Topology, addressing, DMZ
 - D. Access control lists, application controls, Network controls
- 30 In a data flow diagram, a "Data Stores" is represented by
- A. An arrow
 - B. A circle or rectangle with rounded edges
 - C. Parallel lines or open rectangle
 - D. A square
-

31 In a scenario where there is inadequate segregation of duties, which of the following is the greatest risk

- A. The data base administrator also is responsible for transaction entry and authorisation
- B. System analyst is responsible for taking backups
- C. System administrator is responsible for safe custody of the transaction records
- D. System analyst also does system software programming

32 UDP

- A. Is a unreliable connectionless protocol
- B. Is a reliable connectionless protocol
- C. Is used at Application Layer
- D. Does handshaking

-
- 33 Which of the following is NOT a Path of logical access
- A. Console
 - B. Terminal
 - C. Client/Server
 - D. User-ID and Password
- 34 Organizations are using microcomputers for data processing and presentation because use of microcomputer, compared to mainframe use, is more
- A. Controllable
 - B. Helpful for ensuring data integrity
 - C. Processing speed is faster
 - D. Cost effective.
- 35 In a flow chart, a rhombus means
- A. Start and stop
 - B. A processing step
 - C. A logical condition
 - D. Flow of information
-

-
- 36 Which of the following class of IP address can have least networks and highest hosts
- A. Class A
 - B. Class B
 - C. Class C
 - D. Class D
- 37 To delete a highly confidential file from a microcomputer one should use
- A. Secure Token card
 - B. Encryption
 - C. Disk utility
 - D. Multiplexer
- 38 ARP is
- A. Resolution Protocol
 - B. Media Access Control
 - C. Address Resolution Protocol
 - D. User Datagram Protocol
-

-
- 39 Following are the steps to be followed for prototyping
- A. Design, analysis, implementation, and maintenance
 - B. Design, implementation, analysis, and maintain
 - C. Requirements gathering, quick design, construction of prototype, customer evaluation of prototype and refinement of prototype
 - D. Feasibility Study, System Requirement Analysis, design, Program construction, Testing, implementation, and maintenance
- 40 One of the following is not likely to be the item in job description of a tape librarian
- A. Ensure that an adequate supply of tapes and cartridges are available
 - B. Tape storage and vaulting procedures, including off site storage of tapes
 - C. Maintaining logs of tape movement from and to the tape library
 - D. Carrying out user acceptance testing
-

41 Following is not one of the 10 domains of BS7799 standards

- A. Information security policy, Security Organisation
- B. Asset Classification and controls, personnel security, physical and environmental security
- C. Computer and network security, system access control, system development and maintenance
- D. Cryptography, PKI and Digital Signatures

42 An IP Address is divided into

- A. Network ID and Host ID
- B. Seven Layers
- C. Four Layers
- D. Sub net mask

-
- 43 Computer crimes are difficult to detect. Which of the following is not a reason for making computer crime detection difficult
- A. Difficult to trace the perpetrator's identity
 - B. Require only a logical access to the target computer system
 - C. Newer and easier methods of perpetrating crime
 - D. Logs and audit trails capture full particulars about the activities of users.
- 44 Asynchronous transmission happens when
- A. Two devices with dissimilar speeds communicate
 - B. Two devices with similar speeds communicate
 - C. OSI layers are used
 - D. BUS topology is used

-
- 45 In an audit of system development process, the auditor may not review
- A. Controls designed in the application
 - B. Data integrity is maintained
 - C. If ALL user requirements are completely met in the application
 - D. The system design meets important business requirements
- 46 When a set of complex conditions needs to be evaluated for selecting appropriate action, then the decision table is the preferred option. The decision table provides
- A. Conditions and actions in a tabular form
 - B. 4 GL
 - C. Unit testing
 - D. System testing
-

-
- 47 A vulnerability to an asset is
- A. A lack of access control
 - B. Confidentiality is not maintained
 - C. A security weakness associated with that asset
 - D. BCP is not defined
- 48 A ring topology can be best described as
- A. All computers connected to a central hub
 - B. Each computer is connected to its neighbor and each link passes communications through its neighbor to the destination computer
 - C. All computers are connected to a Backbone cable
 - D. All computers are connected to each other
- 49 The IS Security Procedures should not contain information about
- A. Data Classification
 - B. Application Controls
 - C. Description of weaknesses in the security architecture
 - D. Security awareness for end users
-

-
- 50 A Digital Certificate is issued by
- A. Registration Authority
 - B. Identifies the Public Key of the subject
 - C. INTERNIC
 - D. Certification Authority
- 51 To ensure that the application development would meet the desired business objectives
- A. User involvement in requirement specification and acceptance testing
 - B. PERT
 - C. CPM
 - D. Structured Programming

52 To evaluate the control procedures for preventing software licensing violations the system auditor need not

- A. Review the security policies and procedures
- B. Review the inventory of all standard and licensed software applications
- C. Carry out a sample or comprehensive checking of user PCs
- D. Review the backup procedures and backup controls

53 RAD (rapid application development) has following four stages

- A. Definition of scope, creation of a functional design, construction of application, deployment
- B. Design, analysis, implementation, and maintenance
- C. Design, implementation, analysis, and maintain
- D. Requirements gathering, quick design, construction of prototype, customer evaluation of prototype and refinement of prototype

-
- 54 In IP Address 122.35.0.56 which is the Network ID
- A. 122
 - B. 35
 - C. 35.0.56
 - D. 56
- 55 Which of the following statements about microcomputers, minicomputers, and mainframe computers is true?
- A. Microcomputers usually cost more than minicomputers but less than mainframes
 - B. Because of the increased use of microcomputers, mainframes will not be used in future
 - C. Minicomputers must be programmed directly in machine language while mainframes use higher-level language
 - D. The cost of per transaction to process has decreased in recent years on each type of computer.

-
- 56 User ID and Password as a technique of logical access control is
- A. What the user has
 - B. What the user knows
 - C. What the user is
 - D. Need to know
- 57 Following is the sequence of audit phases / steps
- A. Planning, preliminary review, compliance testing, substantive testing, reporting, Wrap-up, follow-up
 - B. Preliminary review, planning, substantive testing, reporting, compliance testing
 - C. Planning, follow-up, compliance testing, reporting,
 - D. Sampling, testing, reporting, follow-up

-
- 58 In IP Address 122.35.0.56 which is the host ID
- A. 122
 - B. 35
 - C. 35.0.56
 - D. 56
- 59 To avoid weaknesses associated with the login technique of using User ID and Password various controls need to be implemented. Following is not an effective control technique to address this concern
- A. Passwords of at least 8 characters should be enforced through system settings
 - B. Users should be forced to change the passwords at regular intervals through system settings
 - C. Users should be forced to select strong passwords through system settings
 - D. Users need not be forced to change their default passwords during their "first login" process
-

-
- 60 One of the following is not a password attack
- A. Password guessing
 - B. Brute force
 - C. Dictionary attack
 - D. Password encryption
- 61 Digital Signatures help in ensuring
- A. Authentication, maintaining integrity, non-repudiation
 - B. Access to internet
 - C. Routing
 - D. Application Security
- 62 Which of the following control will NOT normally be reviewed by an IS auditor in the review of a new application system?
- A. Documentation control
 - B. Programming controls
 - C. Operational controls
 - D. Unauthorised program Changes
-

63 Time Division Multiplexing is a technique where

- A. When numerous signals are assigned different sub-channels within the main channel
- B. Encryption is used
- C. A short time slot is allotted to each node who wish to use common channel
- D. Where access controls are used

64 The main advantage of using magnetic tapes as a storage medium is that it

- A. Permits random access
- B. Uses variable length records
- C. Is a low-cost medium
- D. Requires less labor-intensive intervention.

-
- 65 To exercise controls over physical access to facilities following technique is not used
- A. Identification badges
 - B. Manual logging
 - C. Security guards
 - D. Hardening of operating systems
- 66 When two devices communicate, they must decide about how data and control information is to be transmitted and interpreted. It is described by which of the following term?
- A. Router
 - B. Synchronous communication
 - C. Cable
 - D. Communication protocol.

-
- 67 One of the following statement about water based extinguishers is not true
- A. It can be safely used on computer equipment
 - B. Can be used on timber and paper based fires
 - C. Can be used on a localized fire
 - D. Can be used along with other extinguishers like carbon dioxide based extinguishers
- 68 Control Objective refers to
- A. Implementation of controls
 - B. Purpose to be achieved by implementing the controls
 - C. Using CAAT
 - D. UAT
- 69 The main purpose of a macro program in an spreadsheet application is
- A. Reduce keystrokes
 - B. Backup data
 - C. Delete redundant files
 - D. Rearrange data elements.
-

-
- 70 One of the main advantage of employing biometric access controls is
- A. It helps to restrict the access by authorized persons only
 - B. Sharing of password is restricted
 - C. Passwords can be encrypted
 - D. Audit trails can be enabled
- 71 Factors that degrade a signal are
- A. BUS topology
 - B. TCP-IP
 - C. Attenuation, Delay distortion, noise
 - D. Multiplexing
- 72 User ID and password is a
- A. Encryption control
 - B. Logical access control
 - C. Backup control
 - D. Environmental control

-
- 73 To identify the vulnerabilities in a telecommunication system, the auditor should first
- A. Review the open systems interconnect (OSI) network model
 - B. Identify the network operating costs
 - C. Determine the business purpose of the network
 - D. Make a list of the network software and hardware products into their respective layers.
- 74 The Critical Recovery Time Period / Recovery Time Objective is the length of time
- A. For which the company will process from the alternative site before returning to the main site
 - B. The company can run without the availability of Information System services before business gets significantly affected.
 - C. For carrying out DR tests and restoration drills
 - D. The Disaster Recovery Team will need to recover from a disaster
-

-
- 75 Which of the following hardware device is usually not used for "input"?
- A. Printer
 - B. Optical scanner
 - C. Cassette tape device
 - D. CRT Terminal
- 76 A microwave technique is a typical example of
- A. Line of sight transmission
 - B. Co-axial cables
 - C. TCP-IP
 - D. OSI Layer
- 77 One advantage of object-oriented programming in software design is that they help develop
- A. To maintain documentation
 - B. User friendly
 - C. Simple decision logic
 - D. Reusable code.
-

-
- 78 User ID and password is commonly used to login into the systems. In case of failure of a login the system should inform the user
- A. Whether the user ID was incorrect.
 - B. Whether the Password was incorrect
 - C. Display the password that should be used for the user ID
 - D. The system must not give any indication to the user whether the user ID or the password was incorrect
- 79 To protect a Local Area Network from external attacks?
- A. Passwords
 - B. Fiber optic cables
 - C. Ring Topology
 - D. Firewalls
-

80 In a closed access control philosophy

- A. Access to all information assets are initially
 - opened and then selectively closed
- B. Access to all information assets are initially closed and selectively opened
- C. Physical, logical, network, application and other types are controls are placed on the users
- D. Users are educated to follow the closed access philosophy

81 Which of the following is a detective control?

- A. Security manager analyses and reviews the logs for violations of security procedures
- B. Users change their passwords at regular intervals
- C. Computer operators take backups as per schedule
- D. BCP is prepared

-
- 82 A CAAT is not likely to be used for
- A. Access and analysis of data
 - B. Different types of data structures and record formats
 - C. Audit report preparation
 - D. Checking of data classification and data ownership
- 83 Following is the not a technique for computer virus control
- A. User education
 - B. Anti virus software
 - C. Floppy Diskless nodes
 - D. Cleanliness of the data centre and office premises
- 84 A Digital Certificate does not contain
- A. Certificate Serial Number
 - B. Issuer's Name
 - C. Subject's Name
 - D. Private Key of the subject
-

-
- 85 Computer Aided Software Engineering (CASE) technology gives the following benefit
- A. UAT need not be performed
 - B. Users will readily accept and adopt the system.
 - C. All programs are automatically optimized for efficiency
 - D. Data integrity rules are consistently applied.
- 86 A biometrics authentication like finger print or voice recognition needs to be calibrated so that
- A. False positives and false negatives are low and the results are as accurate as possible
 - B. Encrypt the credentials
 - C. Create audit trails
 - D. Corrective control
-

-
- 87 In which of the following media the transmission loss is the Least
- A. Twisted pair
 - B. Coaxial cable
 - C. Fiber Optics
 - D. Star topology
- 88 Which of the following is a major difference between a floppy disk and a hard disk.
- A. Hard disk has a larger storage capacity than a floppy disk and access to information is much quicker
 - B. Hard disk is a sequential access medium whereas the floppy is a direct-access medium
 - C. Hard disk provides an audit trail, whereas a floppy disk does not
 - D. Hard disk is suitable for an online system, whereas a floppy disk is not.

-
- 89 In case of a parallel implementation of the Application software
- A. The old system is suspended on a specific day and the new system is tried out
 - B. Both the old and the new systems are run in parallel to verify if their outputs are same
 - C. The new system is first implemented in a small, non-critical unit and then moved to a larger unit
 - D. New system is put into production and the old system is put in test environment
- 90 Denial of Service is
- A. Penetration testing
 - B. Degrade, destruct and shutdown any or all of computer services
 - C. Routing of packets
 - D. Network Management System
-

91 In digital systems, following methods are used for error detection

- A. Parity checking, Cyclic Redundancy Checking, Checksum
- B. Cable, Ring Topology, Router
- C. Digital signature, PKI, MAC address
- D. Internet, Gateway, WAN.

92 One of the reasons for using RAID (Redundant Array of Inexpensive Disks) technology is

- A. If one drive fails, the data can still be reconstructed
- B. Reduces power consumption
- C. Taking backups is simpler
- D. Easy to implement

-
- 93 Which of the following is the most critical objective of segregation of duties?
- A. To avoid the possibility of an individual user carrying out all stages of a critical process singly
 - B. IT head is responsible for implementation of the controls relating to IT assets
 - C. Users are carrying out their jobs as described in the job descriptions
 - D. Senior management has done job descriptions
- 94 IP Address 122.35.0.56 is which class address
- A. Class A
 - B. Class B
 - C. Class C
 - D. Class D

-
- 95 UPS (Un-interruptible power supply) system is used in data centers to
- A. Implement access controls
 - B. Guard the computers against power fluctuations and power outages
 - C. Guard against errors in data transmission
 - D. Maintain the data centre room temperature
- 96 Unit testing is the process of testing individual units of software in isolation. One of the following is typically not performed by a programmer for Unit testing
- A. Functional tests to check whether programs do what they are supposed to do.
 - B. Performance tests to verify response time, the execution time, memory utilisation and traffic rates on data channels
 - C. Stress tests to overload a program in various ways
 - D. Integration testing
-

97 Following is not a threat

- A. Power loss, communication loss
- B. Accidental errors, computer virus, abuse of access,
- C. Natural disaster, theft of an asset, Fire
- D. Fire detection system, surveillance systems

98 The location of the Hot site should be

- A. The next building so that recovery can be quickly done
- B. About 5 Kms. away from the main site
- C. Should be sufficiently away from the main site to address the threats of earthquakes, nuclear zones, power grids, war zones etc.
- D. About 500 Kms away from the main site

-
- 99 Most of the surveys across the world have indicated that the highest percentage of threats emanate from
- A. Authorised users of systems
 - B. Hackers
 - C. Competitors
 - D. Terrorists
- 100 The process of attenuation can be resolved with the help of
- A. TCP-IP
 - B. Hub
 - C. Modem
 - D. Repeater
- 101 One of the following is not a type of BCP Test
- A. Checklist
 - B. Structured walk-through
 - C. Simulation
 - D. Taking good backups
-

102 Following people are involved in the SDLC methodology except

- A. Steering committee, project manager and project leader
- B. System analyst, module leader / team leader, programmers
- C. Database Administrator, Quality Assurance, Testers,
- D. Systems administrators, backup operators, physical security officer

103 Nimda is

- A. An operating system
- B. Name of a Hardware vendor
- C. An Encryption algorithm
- D. A powerful virus

104 Imaging systems convert a paper document into a digital image. One of the following is not the benefit of Imaging systems

- A. Imaging system consists of a computer with a good monitor, scanner and a printer
- B. Better service and productivity
- C. Better security
- D. Disaster preparedness

105 Information Security Policy is a top level management document. Which of the following statement about Information Security Policy is not correct, Information Security Policy

- A. Should comply with the requirements of Law of the Land
- B. Define the framework of accountability for security of information assets
- C. Does not need Top Management support
- D. Should outline security awareness and education of all members of the organisation.

106 EDI Architecture has following layers

- A. Physical, Data link, Network, Transport, Session, Presentation, Application
- B. Application, Transport, Internet, Network Interface
- C. Semantic, Standard, Transport, Physical
- D. Vector, replicator and payload

107 Static routing means

- A. Routing tables are automatically updated by routers using special packets.
- B. Routing tables are configured and managed by the Network Administrator
- C. Only one way communication is possible
- D. Line-to-Line encryption

108 The basic components of a client/server system are

- A. LAN, WAN, Router
- B. Firewall, Access Control Lists
- C. Client, Server, A robust and good communication system, A GUI based Operating System, Open-database connectivity drivers and application programming interfaces
- D. IP Address, OSI Layers, TCP-IP

109 A reciprocal backup agreement for recovery is an arrangement wherein

- A. Two companies having spare processing time and compatible hardware capabilities agree formally or informally to backup each other's critical applications.
- B. Organization uses a service bureau's site for recovery
- C. Cold site arrangement
- D. Warm Site arrangements

110 In Salami Technique

- A. The perpetrator rounds down the amounts in transactions
- B. Input data is modified
- C. The perpetrator slices off the values from the nearest desired decimal place
- D. Data awaiting transmission is attacked

111 A computer program which helps in carrying out a business operation (e.g. Inventory management, Accounting, banking operations etc.) is called

- A. Operating system
- B. Application program
- C. Scanner
- D. Utility program.

112 BCP loses its utility very quickly due to several reasons. Which of the following is not a reason for BCP to lose its utility?

- A. Technological changes
- B. Vendor changes
- C. Staff changes
- D. Backup restoration drills

113 The main function of Network Layer (in OSI Layers) is

- A. Segmentation and re-assembly
- B. Routing
- C. Providing user interface
- D. Session management

114 Residual Risk means

- A. Risk which remains after risk treatment
- B. Risk which is covered with insurance
- C. Threat
- D. Risk treatment

-
- 115 A Video Surveillance System (VSS) is a
- A. Preventive control
 - B. Detective control
 - C. Corrective control
 - D. Substitution for a physical guard
- 116 Distributed computing does not provide following advantage
- A. Telecommunications costs are usually lower
 - B. Computers in other locations may be used in case of a disaster
 - C. Implementation and maintenance of security is very easy
 - D. Hardware cost for each site is less than the cost of having a central site.
- 117 An ATM (Automated Teller Machine) is a
- A. Specialized point of sale terminal
 - B. Specialized machine for Electronic Fund Transfer
 - C. Specialized machine for Electronic Data Interchange
 - D. Specialized machine for doing e-commerce
-

-
- 118 Digital Signatures are based on the
- A. Symmetric keys
 - B. Asymmetric but mathematically complementary keys
 - C. Signing paper documents
 - D. Ensuring availability of data.
- 119 Program that checks the source code for syntax errors and translates it into an object program is called
- A. Interpreter
 - B. Compiler
 - C. Debugger
 - D. Encrypter.
- 120 Following control will best prevent the threat of theft of data
- A. Access Control Lists
 - B. Access privileges are established on the principle of "need to know, need to do" basis
 - C. Biometric controls
 - D. Audit trails
-

121 Typically the job of a Data Base Administrator will not include the following

- A. Plan the structure of the data base
- B. Document the data base controls
- C. Ensure that the data is subject to strict accountability and auditing procedures
- D. Tune the operating system for better performance

122 If a workstation contains a processor, monitor, storage, and communication capabilities, it is said to be

- A. Dumb Terminal
- B. Desktop publishing workstation
- C. Intelligent workstation
- D. Router

123 To ensure that any business application is maintainable in future

- A. Development activity should be monitored.
- B. End-user computing efforts are not permitted.
- C. Documentation standards should exist and strictly followed.
- D. Software source code should be properly backed up.

124 Computer Forensics

- A. Deals with techniques of committing frauds
- B. Is a technique used for hacking
- C. Is a Penetration Testing Technique
- D. Deals with the employment of set of predefined procedures to thoroughly examine a computer system using software and tools to extract and preserve evidence of criminal activity

125 Backup is a primary technique employed for recovering from a Disaster. Which of the following describes a technique differential backup?

- A. Every day full disk is backed up
- B. All transactions done after full back up, are backed up
- C. All transactions done after the last backup of transactions, are backed up
- D. Using tape library

126 Hashing technique helps in ensuring

- A. Confidentiality
- B. Integrity
- C. Availability
- D. Network Controls

127 In an IS audit process the auditor is not expected to perform one of the following

- A. Obtaining and documenting evidence that the audit area is adequately controlled and the operations are effective and efficient by using appropriate audit technique.
- B. Evaluating the strengths and weaknesses of audit areas and reporting on their efficiency, effectiveness and state of control by analysing the audit evidence
- C. Implement the recommendations of the audit report
- D. Adhering to the norms of ethics and professional standards to ensure quality and consistency of audit work

128 Which of the following is the least cost method of DR Plan testing?

- A. Parallel simulation
- B. Unit / department wise testing
- C. Full interruption test
- D. Checklist test

129 Which of the following is not true of an efficient security policy implementation?

- A. It should support the mission and business of the organisation
- B. Be cost effective
- C. Have a comprehensive and organisation wide approach
- D. Implement security on Operating System, RDBMS, Applications and Networks

130 The clerk keyed in a date as "13 -13 - 2003", which was accepted by the application software. Which of the control is missing in the application

- A. Range check
- B. Existence check
- C. Completeness check
- D. Sequence check

131 In a symmetric encryption technology

- A. Encryption key is not used
- B. Same key is used for encryption as well decryption
- C. For encryption and decryption different keys are used
- D. RSA is an example of synchronous encryption technique

132 The correct sequence of activities in the systems development life cycle is

- A. Design, analysis, implementation, and maintenance
- B. Design, implementation, analysis, and maintain
- C. Feasibility Study, System Requirement Analysis, design, Program construction, Testing, implementation, and maintenance
- D. Programming, analysis, implementation, and operation

133 Any structured methodology of software development should consist of several steps. Which of the following is not a step in software development

- A. Problem analysis
- B. Design and construction of solution
- C. Verification of appropriateness of the solution
- D. Access controls

134 •To effectively reduce the concern of physical piggybacking following control is used

- A. Biometric door locks
- B. Electronic door locks
- C. Dead man doors
- D. Compound walls and perimeter fencing

135 Which of the following is not an advantage of SDLC framework

- A. Better control by project managers
- B. Cost and time overruns
- C. Compliance to prescribed standards ensuring better quality
- D. Documentation that SDLC stresses on is an important measure of communication and control

136 A Bastion Host

- A. Is a secure and tamper proof implementation of an Operating System
- B. Router
- C. Internet
- D. OSI Layers

137 File naming conventions donot help in achieving one of the following

- A. Finding a file quickly'
- B. Implementing Access Control
- C. Taking backups
- D. Encryption of information

138 When a set of complex conditions need to be evaluated for selecting appropriate action, then one of the following is used

- A. Decision table
- B. Flow chart
- C. Data flow diagram
- D. Decision tree

139 RAID stands for

- A. Redundant array of inexpensive disks
- B. Redundant array of intermediate disks
- C. Redundant array of expensive disks
- D. Redundant array of inefficient disks

140 At the end of the system requirement analysis phase, the systems analyst prepares a document, which is reviewed by the user/customer.

- A. Test report
- B. Systems requirement specification
- C. Source code
- D. Application manuals

141 An auditor should check for the following general controls in audit of a firewall

- A. Physical Security, OS Security, Change Control procedures, documentation controls, recording and analysis of Logs
- B. System specification, designing, logic controls, programming disciplines
- C. Topology, cables, environmental controls
- D. Operating system installation procedures, Application system installation procedures, Data Centre procedures, backup restoration procedures.

142 Which of the following is not true of access control

- A. Identify users including programs and resources
- B. Determine whether the user (including programs) has rights of access to the computer resource
- C. Restrict the action of users to permitted resources and abilities thereof
- D. Is acceptance testing

143 UNIT testing is the process of

- A. Testing individual units of software in isolation
- B. A collection of programs is integrated into the overall product and tested
- C. Integration testing
- D. Prototype testing

144 The Header of a TCP-IP packet contains information about the

- A. MAC addresses
- B. Source Port, Destination Port, Sequence Number
- C. Topology
- D. PKI

145 In case of a Pilot implementation

- A. The new system is first implemented in a small non-critical unit and then moved to larger units
- B. Both the old and new systems are run in parallel to verify if their output is the same
- C. The old system is suspended on a specific date and the new system is tried out
- D. Testing of new system in parts

146 Audit trails do not help in

- A. Establishing accountability
- B. Maintain a record of all actions on resources by users and computer programs and processes
- C. Performance monitoring
- D. Preventing errors

147 In CMM level - 1

- A. SW process is characterised as ad-hoc and occasionally even chaotic and indicates that the organisation is operating without well-defined processes in place.
- B. Basic project management principles are established to track cost, schedule, and check functionality.
- C. The SW process for both management and engineering activities is documented, standardised and integrated into a standard SW process for the organisation.
- D. Detailed measures of the SW process and product quality are established and performed. Both the SW process and products are quantitatively understood and controlled.

148 Following is not a result of poor / inadequate SDLC methodology

- A. Exceed budgeted time
- B. Exceed financial budget
- C. Incompatibility with existing systems
- D. Meets user requirements

149 Which of the following is not a risk in EDI

- A. Improper transaction authorisation
- B. Possibility of loss or duplication of data of EDI documents
- C. Confidentiality may be lost as EDI documents are transmitted
- D. For the success of EDI implementation, BPR needs to be done

150 Which of the following statement about firewall is true?

A firewall cannot

- A. Filter packets based on the defined rule
- B. Provide defense against external attacks
- C. Provide for control over access to sensitive services
- D. Protect against ALL types of threats posed by users within the organisation.

151 Biometric access mechanism offers a high level of authentication based on

- A. What the user has
- B. What the user is
- C. What the user knows
- D. User-ID and password

152 PERT (Program Evaluation Review Technique)

- A. Represents activities in a project as a network indicating the sequential and parallel relationship between activities
- B. Is a programming language
- C. Is a networking topology
- D. Defines the critical path which has the highest duration of time

153 Which of the following is not a control requirement in EDI

- A. Encryption of the messages
- B. Use of sequence numbers
- C. Controls to ensure that all inbound EDI transactions are accurately received and processed only once.
- D. Use of imaging systems for converting paper documents (like purchase orders, invoices, shipping documents etc.) into electronic form

154 Attack on the data awaiting transmission is called

- A. Spoofing
- B. Synchronous attack
- C. Asynchronous attack
- D. Buffer Overflow

155 Frequency indicates

- A. The number of cycles a signal completes in one second
- B. Multiplexing
- C. MAC address
- D. Repeater

156 One of the following is not a feature of a 4GL (forth-generation language)

- A. They have a user-friendly syntax
- B. They can produce graphical outputs
- C. They have powerful querying capabilities
- D. They are written in machine code

-
- 157 Crypt analysis is a technique which is a method of
- A. Encryption
 - B. Recovering the plain text from cipher text without using the key
 - C. Using Asymmetric keys
 - D. Generating hash
- 158 Software programs which are installed permanently by the computer vendors (as part of its main memory) to provide protection from erasure or loss against electrical power interruptions is known as
- A. Application Software
 - B. Software control
 - C. Firmware
 - D. Random access memory (RAM).
- 159 In a wet pipe system of fire extinguishing
- A. Water is not present in the pipes
 - B. Water is present in the pipes
 - C. Dry power is used
 - D. Carbon dioxide is used
-

160 TCP

- A. Is a Connection oriented and reliable protocol
- B. Is a Connectionless and unreliable protocol
- C. Resolves IP address with MAC address
- D. Works at Application Layer

161 According to Ron Weber a disaster recovery plan comprises of the following four parts

- A. Hot site, warm site, cold site, mobile vans
- B. DR Team Leader, DR Team members, testing, auditing
- C. The emergency plan, the backup plan, the recovery plan and the test plan
- D. Evacuation Drills, Restoration Drills, Parallel testing, Full interruption testing

-
- 162 One of the following is not a benefit associated with CASE (Computer Assisted Software Engineering)
- A. CASE can help achieve standardisation of application processes
 - B. Use of CASE tools requires extensive training
 - C. CASE tools generate inputs of each stage from the outputs of previous stage and consistency of application quality can be ensured
 - D. Tasks such as diagramming which are monotonous need not be done by the programmer, and can be left to the CASE tools
- 163 In day to day operations the access controls could be administered by the administrators of various components like operating system administrators, data base administrators, network administrators etc. However the responsibility of authorizing access to production data rests with
- A. Data owner
 - B. Operating systems administrator
 - C. Data base administrator
 - D. System developer
-

-
- 164 Reverse engineering is a technique of
- A. Drawing design specification from the actual product by studying the source code.
 - B. Program restructuring
 - C. Data restructuring
 - D. Compiling the source code into machine executable code
- 165 To avoid the concerns associated with multiple logons and multiple passwords for a user, following technology can be used
- A. Brute force
 - B. Password encryption
 - C. Single sign on
 - D. Token based authentication
- 166 Risk management is the process of
- A. Assessing risk, reducing risk to an acceptable level and maintaining the level of risk
 - B. Implementing Physical and Environmental controls
 - C. Implementing Logical Access controls
 - D. Preparing, testing and maintaining a BCP
-

167 In an Asymmetric encryption technique

- A. Encryption key is not used
- B. Same key is used for encryption as well decryption
- C. For encryption and decryption different keys are used
- D. RSA is an example of synchronous encryption technique

168 Object Oriented Systems development (OOSD) uses the object-oriented methodology. Which of the following is not an advantage of OOSD?

- A. Ability to manage a variety of data types
- B. Guarantees that application will meet ALL user demands
- C. Ability to manage complex relationships
- D. Capacity to meet demands of a changing environment and reusability of logical elements

169 In a business process, the master file on computer is updated once in a day for the day's transactions. This method of updating the master file is known as

- A. Parallel processing
- B. Online processing
- C. Real-time processing
- D. Batch processing

170 In SDLC Data Flow Diagrams are used in which of the phase?

- A. Feasibility study
- B. Design
- C. Implementation
- D. Requirements

171 In the OSI Layers - network Layer is at number

- A. 1
- B. 2
- C. 3
- D. 4

172 The systems auditor is least likely to participate in which of the SDLC phase?

- A. Feasibility study
- B. Program construction
- C. Testing
- D. User requirements

173 The PRIMARY OBJECTIVE of a audit / review of logical access control is to

- A. Ensure that the logical access controls are as per the organisation's Information security policy
- B. Ensure that the logical access controls are as per requirements and recommendation of the users of technology
- C. Ensure that the logical access controls are easy
 - for the users to follow
- D. Helps in disaster recovery

-
- 174 The correct order (Layer 1 to Layer 7) of OSI Layers is
- A. Physical, Data link, Network, Transport, Session, Presentation, Application
 - B. Application, Presentation, Session, Transport, Network, Data link, Physical.
 - C. Data link, Network, Transport, Session, Physical, Presentation, Application
 - D. Physical, Network, Transport, Application
- 175 Which of the following device enables an immediate update of inventory in a retail environment?
- A. Console
 - B. Printer
 - C. Video display terminal
 - D. Point-of-sale terminal.

176 When planning the purchase of new hardware or software a Request For Proposal is prepared. It should not include

- A. System requirements such as transaction volume, size of data proposed to be held on line, response time and turn around time requirements
- B. Technology specification, if any, e.g. the choice of a database software might restrict the choice of hardware and vice-versa
- C. Data entry screen designs
- D. Vendor responsibilities - apart from supply of hardware / software, the vendor is expected to deliver other things such as training, documentation and delivery dates

177 One of the following is not an environmental control technique

- A. Fireproof walls, floors, and ceilings
- B. Security Guard
- C. Electrical surge protectors and UPS
- D. Concealed protective wiring

178 Following are the common debugging tools

- A. Memory dumps, Trace, Logic path monitors, output analysers
- B. PERT
- C. CPM
- D. SDLC

179 In the initiation phase of the BCP following activities are performed

- A. Establish a business continuity plan work group and develop a high-level business continuity planning strategy.
- B. Perform a risk assessment
- C. Develop and document contingency test plans
- D. Conducts test

180 The objective of Boundary controls in Applications is

- A. To prevent unauthorised access to application and application data
- B. To prevent unauthorised physical access to the Data Centre
- C. To ensure accuracy and completeness of data and instruction input into an application system
- D. For User Acceptance Testing

181 For communication (data, voice, images etc.), very small organizations are more likely to use

- A. Public switched telephone lines
- B. Fast-packet switches
- C. E-mail systems
- D. Hubs.

182 One of the following rule is not applicable in structured programming

- A. Every program should have only one entry and one exit
- B. Integration testing need not be done
- C. The GOTO syntax is best avoided in structured programming
- D. Programs should be developed either top-down or bottom-up

183 For processing of cheques, Banks require a reliable, yet economical form of input. The technique mostly used by banks is

- A. Magnetic tape
- B. Optical Character Recognition
- C. Bar coding
- D. Magnetic ink character recognition.

184 The system design is converted into a working program. A good program should have the following characteristics except

- A. Accuracy - that the program should not only do what it is supposed to do, but also should not do what it is not supposed to do.
- B. Reliability - that the program keeps doing the same consistently over a period
- C. Robustness - that the program takes into consideration all possible inputs and outcomes of a program and is able to work under extraordinary circumstances
- D. Should not adhere to the secure programming practices

185 The best approach to avoid terrorist attacks on critical installations like Data Centre is to

- A. Take good backups and keep them at the offsite location
- B. Maintain a low a profile about the location of the critical installations
- C. Ensure that environmental controls like wiring, cabling, extinguishers, alarm systems etc. are implemented and working
- D. Monitor activities of terrorists.

186 The main function of Transport Layer (in OSI Layers) is

- A. Segmentation and Reassembly
- B. Routing
- C. Transmitting voltage signals
- D. Converting the data into signals

187 Which of the following statement about check digit in Application is incorrect

- A. A check digit is a redundant digit that helps verify the accuracy of other characters in the field / record being checked
- B. Check digits may be prefixed or suffixed to the actual data
- C. The program recalculates the check digit and compares it with the check digit in the record
- D. Check digits are used for encryption of records

188 The steps involved in the feasibility study phase does not include

- A. Identification of the problem
- B. Identification of objectives
- C. User acceptance testing
- D. Delineation of scope

189 When a paper form / document (e.g. a return) is filled in by hand (with block style letters and numbers, in designated areas on the form), the technique that will most likely be used to translate the details into machine-readable form is known as

- A. Terminal
- B. MICR (magnetic Ink Character Recognition)
- C. OCR (Optical Character Recognition)
- D. POS (Point of Sale)

-
- 190 In a full-duplex mode of data transmission
- A. Data is always transmitted in one direction, only
 - B. Data is transmitted in both direction but in only one direction at a time
 - C. Data is transmitted in both directions simultaneously.
 - D. Pager is an example of full-duplex
- 191 A recovery site which has all the facilities except the hardware is called a
- A. Hot site
 - B. Warm Site
 - C. Cold site
 - D. Electronic vaulting
- 192 Halon based fire extinguishers are banned because
- A. They cause damage to the computer equipment
 - B. They cannot be used on electrical fires
 - C. They deplete Ozone and hence are not environment friendly
 - D. They lead to suffocation of human being
-

193 Substantive testing means

- A. Tests of controls
- B. Testing of BCP
- C. Detailed transactions testing if the compliance testing reveals insufficient application controls or general controls
- D. Testing of physical and logical controls

194 One of the following is not a "preventive" control measure to prevent violations relating to the software licensing

- A. Audit trails for software usage
- B. Floppy drives and writable CD drives should be removed from the user PCs
- C. User education program for Information Security Procedures
- D. Install metered software on the LAN and ensure that all PCs access applications only through the metered software

195 Which of the following is the BEST way to protect confidentiality of E-mail?

- A. Take a printout and send it through courier
- B. Encrypt the message so that only the recipient can decrypt it
- C. Request a read receipt confirmation from the receiver
- D. Call up and confirm that only the receiver has viewed the message

196 Specialized programs like sort and data comparison are called.

- A. Utility programs
- B. Software programs
- C. Source programs
- D. Object programs

-
- 197 For transmission of critical information over a WAN, which of the following techniques gives better security?
- A. Leased lines
 - B. Routers
 - C. Bus topology
 - D. End-to-end data encryption.
- 198 Which of the following is not a characteristic of an Audit Mission statement?
- A. It defines the primary purpose of the audit function.
 - B. It also outlines the value addition that will be provided.
 - C. It provides an overview of the focus, priorities, values and principles that will measure audit decisions.
 - D. It gives detailed guidelines for the delegation of authority and empowers auditors to discharge their responsibilities effectively.

199 To effectively address the concerns of social engineering attacks, one of the following is an effective measure

- A. Removing the help desk function
- B. User Awareness
- C. Logging
- D. Physical access controls

200 The IS auditor is not expected to

- A. Review and report on the effectiveness of control systems
- B. Take a final decision and implement recommended controls
- C. Review logs for access violations
- D. Carry out compliance and substantive testing

1	C	18	B	35	C	52	A
2	A	19	D	36	A	53	A
3	A	20	A	37	C	54	A
4	D	21	D	38	C	55	D
5	A	22	C	39	C	56	B
6	A	23	C	40	D	57	A
7	B	24	B	41	D	58	C
8	D	25	A	42	A	59	D
9	B	26	B	43	D	60	D
10	C	27	D	44	A	61	A
11	B	28	D	45	C	62	D
12	D	29	B	46	A	63	C
13	B	30	C	47	C	64	C
14	C	31	A	48	B	65	D
15	D	32	A	49	C	66	D
16	A	33	D	50	D	67	A
17	D	34	D	51	A	68	B

69	A	86	A	103	D	120	B
70	A	87	C	104	A	121	D
71	C	88	A	105	C	122	C
72	B	89	B	106	C	123	C
73	C	90	B	107	B	124	D
74	B	91	A	108	C	125	C
75	A	92	A	109	A	126	B
76	A	93	A	110	C	127	C
77	D	94	A	111	B	128	C
78	D	95	B	112	D	129	D
79	D	96	D	113	B	130	A
80	B	97	D	114	A	131	B
81	A	98	C	115	B	132	D
82	D	99	A	116	C	133	D
83	D	100	D	117	A	134	C
84	D	101	D	118	B	135	B
85	D	102	D	119	B	136	A

137	D	154	C	171	C	188	C
138	A	155	A	172	B	189	C
139	A	156	D	173	A	190	C
140	B	157	B	174	D	191	C
141	A	158	C	175	A	192	C
142	D	159	B	176	C	193	C
143	A	160	A	177	B	194	A
144	B	161	C	178	A	195	B
145	A	162	B	179	A	196	A
146	A	163	A	180	A	197	D
147	D	164	A	181	A	198	D
148	D	165	C	182	B	199	B
149	D	166	A	183	D	200	B
150	D	167	C	184	D		
151	B	168	B	185	B		
152	A	169	D	186	A		
153	D	170	D	187	D		