1. Which of the following BEST describes the purpose or character of an audit charter?
   A. An audit charter should be dynamic and change often to coincide with the changing nature of technology and the audit profession.
   B. An audit charter should clearly state audit's objectives for the delegation of authority for the maintenance and review of internal controls.
   C. An audit charter should document the audit procedures designed to achieve the planned audit objectives.
   D. An audit charter should outline the overall authority, scope and responsibilities of the audit function.
2. Which of the following would NOT be a reason why an IS auditor would prepare a formal audit program?
   A. To structure the IS auditor's own planning
   B. To guide assistants in performing planned procedures
   C. To provide audit documentation for review reference
   D. To assess the overall risk of operations within the organization
3. In a risk-based audit approach, an IS auditor is not only influenced by risk but also by:
   A. the availability of CAATs.
   B. management's representations.
   C. organizational structure and job responsibilities.
   D. the existence of internal and operational controls.
4. The MAJOR advantage of the risk assessment approach over the baseline approach to information security management is that it ensures that:
   A. information assets are over protected.
   B. a basic level of protection is applied regardless of asset value.
   C. appropriate levels of protection are applied to information assets.
   D. an equal proportion of resources are devoted to protecting all information assets.
5. Which of the following procedures would an IS auditor NOT perform during pre-audit planning to gain an understanding of the overall environment under review?
   A. Tour key organization activities
   B. Interview key members of management to understand business risks
   C. Perform compliance tests to determine if regulatory requirements are met
   D. Review prior audit reports
6. The use of risk assessment techniques will NOT help to determine the:
   A. areas or business functions to be audited.
   B. nature, extent and timing of audit procedures.
   C. likely audit findings, conclusions and recommendations.
   D. amount of time and resources to be allocated to an audit.
7. The primary purpose and existence of an audit charter is to:
   A. document the audit process used by the enterprise.
   B. formally document the audit department's plan of action.
   C. document a code of professional conduct for the auditor.
   D. describe the authority and responsibilities of the audit department.
8. Which of the following forms of evidence would be considered to be the MOST reliable when assisting an IS Auditor develop audit conclusions?
   A. A confirmation letter received from a third party for the verification of an account balance
   B. Assurance via a control self-assessment received from line management that an application is working as designed
   C. Trend data obtained from World Wide Web (Internet) sources
   D. Ratio analysis developed by the IS auditor from reports supplied by line management
9. Which of the following forms of evidence would be considered to be the MOST reliable?
   A. An oral statement from the auditee
   B. The results of a test performed by an IS auditor
   C. An internally generated computer accounting report
   D. A confirmation letter received from an outside source
10. Which of the following is the MOST likely reason why e-mail systems have become a useful source of evidence for litigation?
    A. Poor housekeeping leads to excessive cycles of backup files remaining available.
    B. Strong access controls establish accountability for activity on the e-mail system.
    C. Data classification is often used to regulate what information should be communicated via e-mail.
    D. Clear policy for using e-mail within the enterprise ensures that the right evidence is available.
11. Which of the following computer-based tools would assist an IS auditor when performing a statistical sampling of financial transactions maintained in a financial management information system?
    A. Spreadsheet auditor
    B. Parallel simulation
    C. Generalized audit software
    D. Regression testing
12. Which of the following would NOT be a use of generalized audit software programs?
    A. Verifying calculations and totals
    B. Performing intricate calculations
    C. Selecting data that an auditor defines as unusual
    D. Producing multiple reports and machine-readable output files
13. Which of the following BEST describes an integrated test facility?
    A. A technique that enables the IS auditor to enter test data into a live computer run for the purpose of verifying correct processing
    B. The utilization of hardware and/or software to review and test the functioning of a computer system

C. A method of using special programming options to permit printout of the path through a computer program taken to process a specific transaction
D. A procedure for tagging and extending transactions and master records that are used by an IS auditor for tests

14. Which of the following statements regarding test data techniques is TRUE?
A. It tests only preconceived situations.
B. It requires the use of a test data generator.
C. It requires a high degree of technical IS knowledge.
D. It requires limited computer time and clerical effort.

15. Which of the following statements regarding sampling is TRUE?
A. Sampling is generally applicable when the population relates to an intangible or undocumented control.
B. If an auditor knows internal controls are strong, the confidence coefficient may be lowered.
C. An example of attribute sampling would be to estimate the number of obsolete object code modules based upon a sample evaluation from the population of object code library.
D. Variable sampling is a technique to estimate the rate of occurrence of a given control or set of related controls.

16. Which of the following is NOT an advantage of using CAATs?
A. Reduces the level of audit risk
B. Provides broader and more consistent audit coverage
C. Saves time for source data input
D. Improves exception identification

17. An important distinction an IS auditor should make when evaluating and classifying controls as preventive, detective or corrective is:
A. the point when controls are exercised as data flows through the system.
B. only preventive and detective controls are relevant.
C. corrective controls can only be regarded as compensating.
D. classification allows an IS auditor to determine which controls are missing.

18. Which of the following statements regarding an IS auditor's use of a continuous audit approach is TRUE?
A. A continuous audit approach is desirable because it does not require an IS auditor to collect evidence on system reliability while processing is taking place, thus allowing more flexibility in approach.
B. When employing a continuous audit approach it is important that the IS auditor review and follow up immediately on all information collected.
C. The use of continuous auditing techniques can actually improve system security when used in time-sharing environments that process a large amount of transactions.
D. Since continuous audit techniques do not depend on the complexity of an organization's computer systems, they are often used to detect control problems in very complex systems.

19. An IS auditor's substantive test reveals evidence of fraud perpetrated from within a manager's account. The manager had written his password, allocated by the system administrator, inside his drawer, which was normally kept locked. The IS auditor concludes that the:
A. manager's assistant perpetrated the fraud.
B. perpetrator cannot be established beyond doubt.
C. fraud must have been perpetrated by the manager.
D. system administrator could have perpetrated the fraud

20. Which of the following statements pertaining to the determination of sample size is TRUE?
A. The larger the confidence level, the smaller the sample size "
B. The larger the standard deviation, the larger the sample size"
C. The smaller the precision amount, the smaller the sample size"
D. Sample size is not affected by the expected error rate in the population

21. Which of the following would NOT normally be performed using CAATs?
A. Footing totals
B. Selecting testing samples
C. Reconciling account posting
D. Testing aging of receivables

22. To gain a full understanding of a LAN environment, an IS auditor should document all of the following functions EXCEPT:
A. LAN topology and network design.
B. technical support/help desk functions.
C. duties and responsibilities of the LAN administrator.
D. the various computer applications used on the LAN.

23. During a review of a customer master file an IS auditor discovered numerous customer name duplications arising from variations in customer first names. In order to determine the extent of the duplication the IS auditor would use:
A. test data to validate data input.
B. test data to determine system sort capabilities.
C. generalized audit software to search for address field duplications.
D. generalized audit software to search for account field duplications.

24. A manufacturing company has implemented a new client/server system enterprise resource planning (ERP) system. Local branches transmit customer orders to a central manufacturing facility. Which of the following controls would BEST ensure that the orders are accurately entered and the corresponding products produced?
A. Verifying production to customer orders
B. Logging all customer orders in the ERP system

C. Using hash totals in the order transmitting process
D. Approving (production supervisor) orders prior to production

25. Which of the following would an IS auditor consider to be the BEST population to take a sample from when testing program changes?
A. Test library listings
B. Source program listings
C. Program change requests
D. Production library listings

26. Which of the following tests is an IS auditor performing when a sample of programs is selected to determine if the source and object versions are the same?
A. A substantive test of program library controls
B. A compliance test of program library controls
C. A compliance test of the program compiler controls
D. A substantive test of the program compiler controls

27. An integrated test facility is considered a useful audit tool because it:
A. is a cost efficient approach to auditing application controls.
B. enables the financial and IS auditors to integrate their audit tests.
C. compares processing output with independently calculated data.
D. provides the IS auditor with a tool to analyze a large range of information.

28. The primary reason for enabling software audit trails is to:
A. improve response time for users.
B. establish accountability and responsibility for processed transactions.
C. improve system efficiency since audit trails do not occupy disk-space.
D. provide useful information to auditors who may wish to track transactions.

29. When performing a procedure to identify the value of inventory that has been kept for more than eight weeks, an IS auditor would MOST likely use:
A. test data.
B. statistical sampling.
C. an integrated test facility.
D. generalized audit software.

30. Data flow diagrams are used by IS auditors to:
A. order data hierarchically.
B. highlight high-level data definitions.
C. graphically summarize data paths and storage.
D. portray step-by-step details of data generation.

31. A distinction that can be made between compliance testing and substantive testing is:
A. compliance testing tests details, while substantive testing tests procedures.
B. compliance testing tests controls, while substantive testing tests details.
C. compliance testing tests plans, while substantive testing tests procedures.
D. compliance testing tests for regulatory requirements, while substantive testing tests validations.

32. An IS auditors is expected to use due professional care when performing audits, which requires that the individual exercise skill or judgment:
A. commonly possessed by practitioners of that specialty.
B. which includes programming skills in the software under review.
C. relating to the selection of audit tests and evaluation of test results.
D. where an incorrect conclusion based on available facts will not be drawn.

33. An internal audit department, that organizationally reports exclusively to the chief financial officer (CFO) rather than to an audit committee, is MOST likely to:
A. have its audit independence questioned.
B. report more business-oriented and relevant findings.
C. enhance the implementation of the auditor's recommendations.
D. result in greater effective action being taken on the auditor's recommendations.

34. An IS auditor conducting a review of software usage and licensing discovers that numerous PCs contain unauthorized software. Which of the following actions should the IS auditor perform FIRST?
A. Personally delete all copies of the unauthorized software.
B. Inform auditee of the unauthorized software and follow-up to confirm deletion.
C. Report the use of the unauthorized software to auditee management and the need to prevent recurrence.
D. Take no action, as it is a commonly accepted practice and operations management is responsible for monitoring such use.

35. The risk that an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when, in fact, they do, is an example of:
A. inherent risk.
B.control risk.
C. detection risk.
D. audit risk.

36. A primary benefit derived from an organization employing control self assessment (CSA) techniques is that it:
A. can identify high-risk areas that might need a detailed review later.
B. allows IS auditors to independently assess risk.
C. can be used as a replacement for traditional audits.
D. allows management to relinquish responsibility for control.

37. An IS auditor's first step when implementing continuous monitoring systems is to identify:
A. reasonable target thresholds.
B. high-risk areas within the organization.
C. the location and format of output files.

D. applications that provide the highest potential payback.

38. Which of the following is an anti-virus detective control?
A. Route all links to external systems via a firewall.
B. Scan all diskettes and CDs brought in from outside the company before use.
C. Scan all files on all file server hard disks daily, moving suspect files to a safe area.
D. Use anti-virus software to update users' anti-virus configuration files every time they log in.

39. Which of the following represents the MOST significant exposure for an organization that leases personal computers?
A. Accounting for shared peripherals
B. Frequent reassignment of hardware
C. Obsolescence prior to lease termination
D.Software licensing issues on leased machines

40. When reviewing a system development project at the project initiation stage, an IS auditor finds that the project team is not proposing to strictly follow the organization's quality manual. To meet critical deadlines the project team proposes to fast track the validation and verification processes, commencing some elements before the previous deliverable is signed-off. Under these circumstances the IS auditor would MOST likely:
A.report this as a critical finding to senior management.
B. accept that different quality processes can be adopted for each project
C. report to IS management the team's failure to follow appropriate procedures.
D. report the risks associated with fast tracking to the project steering committee

41. During a review of the controls over the process of defining IT service levels an IS auditor would MOST likely interview the:
A. systems programmer.
B. legal staff.
C. business unit manager.
D. programmer.

42. Which of the following sampling methods is MOST useful when testing for compliance?
A. Attribute sampling
B. Variable sampling
C. Stratified mean per unit
D. Difference estimation

43. While performing an audit, an IS auditor used an application software mapping technique and discovered an error in system processing. In preparing the audit report the IS auditor should include:
A. a detailed (step-by-step) description of the mapping technique.
B. the detailed steps performed during the audit.
C. a listing of relevant parameters or source code of the system.
D. an overview of the application software mapping technique used.

44. Which of the following is a detective control?
A. Physical access controls
B. Segregation of duties
C. Back-up procedures
D. Audit trails

45. An IS auditor is assigned to perform a post implementation review of an application system. Which of the following situations may have impaired the independence of the IS auditor? The IS auditor:
A. implemented a specific control during the development of the application system.
B. designed an embedded audit module exclusively for auditing the application system.
C. participated as a member of the application system project team, but did not have operational responsibilities.
D. provided consulting advice concerning application system best practices.

46. Detection risk refers to a:
A. conclusion that material errors do not exist, due to an inadequate test procedure.
B. control that fails to detect an error.
C. control that detects a high-risk error.
D. control that detects an error but fails to report the same.

47. Information requirement definitions, feasibility studies, and user requirements are significant considerations when:
A. defining and managing service levels.
B. identifying IT solutions.
C. managing changes.
D. assessing internal IT control.

48. Which of the following steps would an IS auditor normally perform FIRST in a security review?
A. Evaluate physical access test results
B. Determine the risks/threats to the data center site
C. Review business continuity procedures
D. Test for evidence of physical access at suspect locations

49. Which of the following is the LEAST reliable audit evidence?
A. Results of data extractions
B. Results of test cases
C. Oral representations
D. Record of transactions

50. Which of the following types of information would an IS auditor find LEAST valuable when gaining an understanding of the IT process?
A. IT planning and deployment of documents with deliverables and performance results
B. Organization's policies and procedures relating to planning, managing, monitoring and reporting on performances"
C. Prior audit reports
D. Reports of IT functional activities

51. When an IS auditor obtains a listing of current users with access to the selected WAN/LAN and verifies that those listed are active associates, the IS auditor is performing a:
A. compliance test.
B. substantive test.
"C. statistical sample.
D. risk assessment.

52. Ensuring regular password change, assigning a new one-time password when a user forgets his/hers, and requiring users not to write down their passwords are all examples of:
A. audit objectives.
B. audit procedures.
C. controls objectives.
D. control procedures.

53. The FIRST task an IS auditor should complete when performing a new audit in an unfamiliar area is to:
A. design the audit programs for each system or function involved.
B. develop a set of compliance tests and substantive tests.
C. gather background information pertinent to the new audit.
D. assign human and economical resources.

54. Risk assessments performed by IS auditors is a critical factor for audit planning. An assessment of risk should be made to provide:
A. reasonable assurance that material items will be covered during the audit work.
B. sufficient assurance that material items will be covered during the audit work.
C. reasonable assurance that all items will be covered during the audit work.
D. sufficient assurance that all items will be covered during the audit work.

55. IS auditors must have a thorough understanding of the risk assessment process. Risk assessment is a(n):
A. subjective process.
B. objective process.
C. mathematical process.
D. statistical process.

56. The BEST time to perform a control self-assessment involving line management, line staff and the audit department would be during the:
A. compliance tests.
B. preliminary survey.
C. substantive tests.
D. preparation of the audit report.

57. While conducting a control self-assessment (CSA) program, an IS auditor facilitated workshops involving management and staff in judging and monitoring the effectiveness of existing controls. Which of the following is an objective of a CSA program?
A. to enhance audit responsibilities.
B. to identify problems.
C. to brainstorm solutions.
D. to complete the entire audit.

58. The responsibility, authority and accountability of the information systems audit functions is appropriately documented in an audit charter and MUST be:
A. approved by the highest level of management.
B. approved by audit department management.
C. approved by user department management.
D. changed every year before commencement of IS audits.

59. The IS auditor should be able to identify and evaluate various types of risks and their potential effects. Accordingly, which of the following risks is associated with trap doors?
A. Inherent risk.
B. Detection risk.
C. Audit risk.
D. Error risk.

60. IS auditors are MOST likely to perform tests of internal controls if, after their evaluation of such controls, they conclude that:
A. a substantive approach to the audit are more cost-effective.
B. the control environment is poor.
C. inherent risk is low.
D. control risks are within the acceptable limits.

61. An IS auditor performing an audit of the company's information system (IS) strategy would be LEAST likely to:
A. assess IS security procedures.
B. review both short and long-term IS strategies.
C. interview appropriate corporate management personnel.
D. ensure that the external environment has been considered.

62. Which of the following organizational goals would normally be mentioned in an organization's strategic plan?
A. Test a new accounting package.
B. Perform an evaluation of information technology needs.
C. Implement a new project planning system within the next 12 months.
D. Become the supplier of choice within a given time period for the product offered.

63. Which of the following conditions should exist in order for the local selection and purchase of IS products to be acceptable?
A. Local offices are independent and exchange data on an occasional basis.
B. Managers undertake a full cost-benefit analysis before deciding what to purchase.
C. The same type of data base management system is used throughout the organization.
D. Acquisitions are consistent with the organization's short- and long-term IS technology plans.

64. The initial step in establishing an information security program is the:
    A. development and implementation of an information security standards manual.
    B. performance of a comprehensive security control review by the IS auditor.
    C. adoption of a corporate information security policy statement.
    D. purchase of security access control software.
65. Which of the following documentation would an IS auditor place LEAST reliance on when determining management's effectiveness in communicating information systems policies to appropriate personnel?
    A. Interviews with user and IS personnel
    B. Minutes of the IS Steering Committee meetings
    C. User department systems and procedures manuals
    D. Information processing facilities operations and procedures manuals
66. An IS auditor who is reviewing application run manuals would expect them to contain:
    A. details of source documents.
    B. error codes and their recovery actions.
    C. program logic flowcharts and file definitions.
    D. change records for the application source code.
67. Which of the following statements pertaining to ISO 9000 is FALSE?
    A. The standard covers all aspects of an organization that may affect customer satisfaction.
    B. The standard covers both internal and external business processes.
    C. The standard defines a set of quality compliance requirements.
    D. The standard focuses heavily on documentation of activities.
68. Which of the following procedures would normally be performed last by an IS auditor who is auditing the outsourcing process?
    A. Assess the business needs of the organization.
    B. Perform a cost/benefit analysis including the assumptions behind it.
    C. Perform a control risk assessment.
    D. Review contracts with legal counsel.
69. A written security policy serves to heighten security awareness and should include all of the following key components EXCEPT:
    A. an index of computer hardware and software.
    B. management's approved support of the policy.
    C. authorization process for gaining access to computerized information.
    D. awareness philosophy to security procedures on a need-to-know basis.
70. The function of general ledger setup in an enterprise resource package (ERP) allows for the setting of accounting periods in the package. Access to this function has been permitted to users in finance, warehouse and order entry. The MOST likely reason for granting such broad access is the:
    A. need to change accounting periods on a regular basis.
    B. requirement to post entries for a closed accounting period.
    C. lack of proper policies and procedures for the segregation of duties.
    D. need to create/modify the chart of accounts and its allocations.
71. Which of the following procedures would MOST effectively detect employee loading of illegal software packages onto a network?
    A. The use of diskless workstations
    B. Periodic checking of hard drives
    C. The use of current anti-virus software
    D. Policies that result in instant dismissal if violated
72. Which of the following is LEAST likely to be associated with an incident response capability?
    A. Developing a database repository of past incidents and actions to facilitate future corrective actions.
    B. Declaring the incident, which not only helps to carry out corrective measures, but also to improve the awareness level.
    C. Developing a detailed operations plan that outlines specific actions to be taken to recover from an incident.
    D. Establishing multi-disciplinary teams consisting of executive management, security staff, information systems staff, legal counsel, public relations, etc. to carry out the response"
73. Which of the following should NOT be included in an organization's IS security policy?
    A. Access philosophy
    B. Access authorization
    C. Importance of security awareness
    D. Identity of sensitive security features
74. Which of the following should NOT be a role of the security administrator?
    A. Authorizing access rights
    B. Implementing security rule
    C. Allocating access rights
    D. Ensuring that security policies have been authorized by management
75. Which of the following is a role of an information systems steering committee?
    A.Initiate computer applications.
    B. Ensure efficient use of data processing resources.
    C. Prepare and monitor system implementation plans.
    D. Review the performance of the systems department.
76. Accountability for the maintenance of appropriate security measures over information assets resides with the:
    A. security administrator.
    B. systems administrator.
    C. data and systems owners.
    D. systems delivery/operations group.
77. An IS auditor performing a review of the MIS department discovers that formal project approval

procedures do not exist. In the absence of these procedures the MIS manager has been arbitrarily approving projects that can be completed in a short duration and referring other more complicated projects to higher levels of management for approval. The IS auditor should recommend FIRST that:
A. users participate in the review and approval process.
B. formal approval procedures be adopted and documented.
C. all projects are referred to appropriate levels of management for approval.
D. the MIS manager job description be changed to include approval authority.

78. Responsibility and reporting lines cannot always be established when auditing automated systems since:
A. diversified control makes ownership irrelevant.
B. staff traditionally change jobs with greater frequency.
C. ownership is difficult to establish where resources are shared.
D. duties change frequently in the rapid development of technology.

79. Which of the following criteria would an IS auditor consider to be the MOST important when evaluating the organization's IS strategy?
A. That it has been approved by line management
B. That it does not vary from the IS Department preliminary budget
C. That it complies with procurement procedures
D. That it supports the business objectives of the organization

80. Which of the following statements relating to separation of duties is TRUE?
A. Employee competence does not need to be considered when evaluating an organization's policy on separation of duties.
B. An organization chart provides an accurate definition of separation of employee duties.
C. A restrictive separation of duties policy can help improve an organization's efficiency and communication.
D.Policies on separation of duties in information systems must recognize the difference between logical and physical access to assets.

81. Which of the following tasks is normally performed by a clerk in the control group?
A. Maintenance of an error log
B. Authorization of transactions
C. Control of non-information systems assets
D. Origination of changes to master files

82. Which of the following is NOT a responsibility of a database administrator?
A. Designing database applications
B. Changing physical data definition to improve performance
C. Specifying physical data definition
D. Monitoring database usage

83. Which of the following is NOT a responsibility of computer operations?
A. Analyzing system schedules
B. Analyzing user specifications
C. Analyzing system degradation
D. Trouble-shooting teleprocessing problems

84. Which of the following functions should NOT be performed by scheduling and operations personnel in order to maintain proper segregation of duties?
A. Job submission
B. Resource management
C. Code correction
D. Output distribution

85. Which of the following functions is NOT performed by the IS control group?
A. Supervision of the distribution of output
B. Logging of input data
C. Scrutiny of error listings
D. Correction of errors

86. Which of the following exposures may result if an adequate separation of duties between computer operators and application programmers is NOT maintained?
A. Inadequate volume testing
B. Unauthorized program changes
C. Unintentional omissions of data
D. Data loss during program execution

87. Which of the following tasks would NOT normally be performed by a data security officer?
A. Developing the data classification methodology
B. Implementing security measures (e.g., password change procedures)"
C. Monitoring the effectiveness of security over data
D. Monitoring the completeness and accuracy of the data

88. An IS auditor has recently discovered that because of a shortage of skilled operations personnel, the security administrator has agreed to work one late night shift a month as the senior computer operator. The MOST appropriate course of action that the IS auditor should take is to:
A. advise senior management of the risk involved.
B. agree to work with the security officer on these shifts as a form of preventative control.
C. develop a computer-assisted audit technique to detect instances of abuses of this arrangement.
D. review the system log for each of the late-night shifts to determine whether any irregular actions occurred.

89. Many organizations require an employee to take a mandatory vacation of a week or more in order to:
A. ensure the employee maintains a quality of life, which will lead to greater productivity.
B. reduce the opportunity for an employee to commit an improper or illegal act.
C. provide proper cross training for another employee.
D. eliminate the potential disruption caused when an employee takes vacation one day at a time.

90. The quality assurance group is typically responsible for:
A.ensuring that the output received from system processing is complete.
B. monitoring the execution of computer processing tasks.
C. ensuring that programs and program changes and documentation adhere to established standards.
D. designing standards and procedures to protect data against accidental disclosure, modification, or destruction.

91. Which of the following would NOT be associated with well-written and concise job descriptions?
A. They are an important means of discouraging fraudulent acts.
B. They are often used as tools for use in performance evaluation.
C. They provide little indication of the degree of separation of duties.
D. They assist in defining the relationship between various job functions.

92. Which of the following BEST describes the role and responsibilities of a systems analyst?
A. Defines corporate databases
B. Determines user needs for application programming
C. Schedules computer resources
D. Tests and evaluates programmer and optimization tools

93. Which of the following functions, if combined, would provide the GREATEST risk to an organization?
A. Systems analyst and database administrator
B. Quality assurance and computer operator
C. Tape librarian and data entry clerk
D. Application programmer and tape librarian

94. Which of the following statements relating to application programmers is FALSE?
A. They are responsible for maintaining systems in production.
B. They should not move test versions into the production environment.
C. They are responsible for defining backup procedures.
D. They should not have access to system program libraries.

95. Which of the following is NOT an advantage of cross training employees?
A. It provides for succession planning.
B. It decreases dependence on one employee.
C. It provides back-up personnel in the event of absence.
D. It allows individuals to understand all parts of a system.

96. Responsibility for programmers and analysts who implement new systems and maintain existing systems is typically the role of the:
A. operations manager.
B. database administrator.
C. quality assurance manager.
D. systems development manager.

97. Which of the following is NOT an activity associated with information processing?
A. Systems analysis
B. Telecommunications
C. Computer operations
D. Systems programming

98. A local area network (LAN) administrator is restricted from:
A. having end-user responsibilities.
B. reporting to the end-user manager.
C. having programming responsibilities.
D. being responsible for LAN security administration.

99. Which of the following pairs of functions should not be combined to provide proper segregation of duties?
A. Tape librarian and computer operator
B. Application programming and data entry
C. Systems analyst and database administrator
D. Security administrator and quality assurance

100. An IS auditor is reviewing the data base administration function to ascertain whether adequate provision has been made for controlling data. The IS auditor should determine that the:
A. function reports to data processing operations.
B. responsibilities of the function are well defined.
C. database administrator is a competent systems programmer.
D. audit software has the capability of efficiently accessing the database.

101. A long-term IS employee with a strong technical background and broad managerial experience has applied for a vacant position in the IS audit department. Determining whether to hire this individual for this position should be based on the individual's vast experience and:
A. the length of service since this will help ensure technical competence.
B. the individual's age as training in audit techniques may be impractical.
C. IS knowledge since this will bring enhanced credibility to the audit function.
D. existing IS relationships where the ability to retain audit independence may be difficult.

102. An IS auditor reviewing the key roles and responsibilities of the database administrator (DBA) is LEAST likely to expect the job description of the DBA to include:
A. defining the conceptual schema.
B. defining security and integrity checks.
C. liaising with users in developing data model.
D. mapping data model with the internal schema.

103. Which of the following provisions in a contract for external information systems services would an IS auditor consider to be LEAST significant?
A. Ownership of program and files
B. Statement of due care and confidentiality
C. Continued service of outsourcer in the event of a disaster

D. Detailed description of computer hardware used by the vendor

104. Is it appropriate for an IS auditor from a company which is considering outsourcing its IS processing to request and review a copy of each vendor's business continuity plan?
A. Yes, because the IS auditor will evaluate the adequacy of the service bureau's plan and assist his/her company in implementing a complementary plan.
B. Yes, because, based on the plan, the IS auditor will evaluate the financial stability of the service bureau and its ability to fulfill the contract.
C. No, because backup to be provided should be adequately specified in the contract.
D. No, because the service bureau's business continuity plan is proprietary information to which users' IS auditors are not usually allowed access.

105. Which of the following indicators would LEAST likely indicate that complete or selected outsourcing of computer operators should be considered ?
A. The applications development backlog is greater than three years.
B. It takes one year to develop and implement a high-priority system.
C. More than 60 per cent of programming costs are spent on systems maintenance.
D. Duplicate information systems functions exist at two sites.

106. A probable advantage to an organization that has outsourced its data processing services is that:
A. greater IS expertise can be obtained from the outside.
B. more direct control can be exercised over computer operations.
C. processing priorities can be established and enforced internally.
D. greater user involvement is required to communicate user needs.

107. Service level agreements establish:
A. minimum service levels to be rendered by IS management.
B. minimum service levels to be achieved in the event of a disaster.
C. maximum service levels to be rendered by IS support services.
D.minimum levels of processing capabilities that can be affected by a disaster.

108. An organization has outsourced network and desktop support. Although the relationship has been reasonably successful, risks remain due to connectivity issues. Which of the following controls should FIRST be performed to assure the organization reasonably mitigates these possible risks?
A. Network defense program
B.Encryption/Authentication
C. Adequate reporting between organizations
D. Adequate definition in contractual relationship

109. An IS auditor reviewing an outsourcing contract of IT facilities would expect it to define:
A. hardware configuration.
B. access control software.
C. ownership of intellectual property.
D. application development methodology.

110. While conducting an audit of management's planning of IS, what would an IS auditor consider the MOST relevant to short-term planning for the IS department?
A. Allocating resources
B. Keeping current with technology advances
C. Conducting control self-assessment
D. Evaluating hardware needs

111. The data control department responsible for data entry should:
A. maintain access rules to data and other IT resources.
B. periodically review and evaluate the data security policy.
C. ensure proper safekeeping of source documents until processing is complete.
D. monitor security violations and take corrective action.

112. Which of the following IS functions may be performed by the same individual, without compromising on control or violating segregation of duties?
A. Job control analyst and applications programmer
B. Mainframe operator and system programmer
C. Change/problem and quality control administrator
D. Applications and system programmer

113. Which of the following is the MOST important function to be performed by IT management within an outsourced environment?.
A. Ensuring that invoices are paid to the provider
B. Participating in systems design with the provider
C. Renegotiating the provider's fees
D. Monitoring the outsourcing provider's performance

114. Which of the following key performance indicators would an IS manager be LEAST likely to systematically report to its board of directors?
A. Average response time to users requirements
B. Cost per transaction
C. IS costs per area
D. Disk storage space free

115. Employee termination practices should address all of the following EXCEPT:
A. arrangement for the final pay and removal of the employee from active payroll files.
B. notification to other staff and facilities security to increase awareness of the terminated employee's status.
C. employee bonding to protect against losses due to theft.
D. deletion of assigned logon-ID and passwords to prohibit system access.

116. Various standards have emerged to assist IS organizations in achieving an operational environment that is predictable, measurable and repeatable. The

standard that provides the definition of the characteristics and associated quality evaluation process to be used when specifying the requirements for and evaluating the quality of software products throughout their life cycle is:
A. ISO 9001.
B. ISO 9002.
C. ISO 9126.
D. ISO 9003.

117. Which of the following would provide the LEAST justification for an organization's investment in a security infrastructure?
A. Risk analysis of internal/external threats
B. A white paper report on Internet attacks, companies attacked, and damage inflicted"
C. A penetration test of the organization's network demonstrates that the threat from intruders is high
D. Reports generated internally from use of high-profile network tools

118. An IS auditor reviewing the organization IT strategic plan should FIRST review:
A. the existing information technology environment.
B. the business plan.
C. the present IT budget.
D. current technology trends.

119. Which of the following issues would be of LEAST concern when reviewing an outsourcing agreement in which the outsourcing vendor assumes responsibility of the information processing function?
A. The organization's right to audit vendor operations.
B. The loyalty of the third-party personnel.
C. The access control system that protects the outsourcing vendor's data.
D. The outsourcing vendor's software acquisition procedures.

120. A database administrator is responsible for:
A. maintaining the access security of data residing on the computers.
B. implementing database definition controls.
C. granting access rights to users.
D. defining system's data structure.

121. The security administrator is responsible for providing reasonable assurance over the confidentiality, integrity and availability of information system controls. Another duty that could be considered compatible, without causing a conflict of interest, would be:
A. quality assurance.
B. application programming.
C. systems programming.
D. data entry.

122. The development of an IS security policy is the responsibility of the:
A. IS department.
B. security committee.
C. security administrator.
D. board of directors.

123. A sound information security policy will MOST likely include a:
A. response program to handle suspected intrusions.
B. correction program to handle suspected intrusions.
C. detection program to handle suspected intrusions.
D. monitoring program to handle suspected intrusions.

124. Who of the following, who is responsible for network security operations?
A. Users, who periodically change their passwords.
B. Security administrators, who control services and computers.
C. Line managers, responsible for policies and procedures.
D. Security officers, who administer the security policy.

125. Which of the following would provide a mechanism whereby IS management can determine when, and if, the activities of the enterprise have deviated from planned, or expected levels?
A. Quality management
B. IS assessment methods
C. Management principles
D. Industry standards/benchmarking

126. Which of the following independent duties is performed by the data control group?
A. Access to data
B. Authorization tables
C. Custody of assets
D. Reconciliation

127. Which of the following situations would increase the likelihood of fraud?
A. Application programmers are implementing changes to production programs
B. Application programmers are implementing changes to test programs
C. Operations support staff are implementing changes to batch schedules
D. Data base administrators are implementing changes to data structures

128. Which of the following is the BEST way to handle obsolete magnetic tapes before disposing of them?
A. Overwriting the tapes
B. Initializing the tape labels
C. Degaussing the tapes
D. Erasing the tapes

129. An IS steering committee should:
A. include a mix of members from different departments and management levels.
B. ensure that IS security policies and procedures have been properly executed.
C. have formal terms of reference and maintain minutes of its' meetings.
D. be briefed about new trends and products at each meeting by a vendor.

130. Which of the following functions would represent a risk if combined with that of a system analyst, due to the lack of compensating controls?

A. Application programming
B. Data entry
C. Quality assurance
D. Data base administrator

131. Which of the following data entry controls provides the GREATEST assurance that data entered does not contain errors?
A. Key verification
B. Segregation of the data entry function from data entry verification
C. Maintaining a log/record detailing the time, date, employee's initials/user -id and progress of various data preparation and verification tasks"
D. Check digits

132. Which of the following would an IS auditor be MOST concerned with when evaluating the effectiveness and adequacy of a computer preventive maintenance program?
A. System downtime log
B. Vendors' reliability figures
C. A log of regularly scheduled maintenance
D. A written preventive maintenance schedule

133. Which of the following provides the MOST effective means of determining which controls are functioning properly in an operating system?
A. Consulting with the vendor
B. Reviewing the vendor installation guide
C. Consulting with the system programmer
D. Reviewing the system generation parameters

134. Which of the following is NOT a common database structure?
A. Network
B. Sequential
C. Hierarchical
D. Relational

135. Which of the following computer system risks would be increased by the installation of a database system?
A. Programming errors
B. Data entry errors
C. Improper file access
D. Loss of parity

136. The input/output control function is responsible for:
A. pulling and returning all tape files.
B. entering and key verifying data.
C. logging batches and reconciling hash totals.
D. executing both production and test jobs.

137. Utility programs that assemble software modules needed to execute a machine instruction application program version are:
A. text editors.
B. program library managers.
C. linkage editors and loaders.
D. debuggers and development aids.

138. Which of the following statements pertaining to a data communication system is FALSE?
A. It has multiple layers.
B. It interfaces with the operating system.
C. It operates on the content of the information.
D. It is concerned with the correct transmission between two points.

139. Which of the following is NOT an advantage of an object-oriented approach to data management systems?
A. A means to model complex relationships
B. The ability to restrict the variety of data types
C. The capacity to meet the demands of a changing environment
D. The ability to access only the information that is needed

140. Which of the following allow programmers to code and compile programs interactively with the computer from a terminal?
A. Firmware
B. Utility programs
C. Online programming facilities
D.Network management software

141. A data dictionary is an example of software that is used to:
A. describe application systems.
B. assist in fast program development.
C. improve operation efficiency.
D. test data quality.

142. Which of the following is NOT an advantage of image processing?
A. Verifies signatures
B. Improves service
C. Relatively inexpensive to use
D. Reduces deterioration due to handling

143. In a review of the operating system software selection and the acquisition process, an IS auditor would place more importance in finding evidence of:
A. competitive bids.
B. user-department approval.
C. hardware-configuration analysis.
D. purchasing department approval.

144. Which of the following line media would be MOST secure in a telecommunication network?
A. Broad band network digital transmission
B. Base band network
C. Dial up
D. Dedicated lines

145. What type of transmission requires modems in a network to be connected to terminals from the computer?
A. Encrypted
B. Digital
C. Analog
D. Modulated

146. Which of the following is NOT a telecommunications control?
A. Trailer record
B. Common carrier
C. Diagnostic routine

D. Echo check

147. An IS auditor needs to link his/her microcomputer to a mainframe system that uses binary synchronous data communications with block data transmission. However, the IS auditor's microcomputer, as presently configured, is capable of only asynchronous ASCII character data communications. Which of the following must be added to the IS auditor's computer to enable it to communicate with the mainframe system?
A. Protocol conversion and buffer capacity
B. Network controller and buffer capacity
C. Buffer capacity and parallel port
D. Parallel port and protocol conversion

148. Which of the following is a telecommunication device that translates data from digital form to analog form and back to digital?
A. Multiplexer
B. Modem
C. Protocol converter
D. Concentrator

149. Which of the following is a network architecture configuration that links each station directly to a main hub?
A. Bus
B. Ring
C. Star
D. Completed connected

150. Which of the following transmission media would NOT be affected by cross talk or interference?
A. Fiber optic systems
B. Twisted pair circuits
C. Microwave radio systems
D. Satellite radiolink systems

151. In Wide Area Networks (WANs):
A. data flow can be half duplex or full duplex.
B. communication lines must be dedicated.
C. circuit structure can be operated only over a fixed distance.
D. the selection of communication lines will affect reliability.

152. Which of the following Local Area Network (LAN) physical layouts are subject to vulnerability to failure if one device fails?
A. Star
B. Bus
C. Ring
D. Completely connected

153. Neural networks are effective in detecting fraud because they can:
A. discover new trends since they are inherently linear.
B. solve problems where large and general sets of training data are not obtainable.
C. attack problems that require consideration of a large number of input variables.
D. make assumptions about the shape of any curve relating variables to the output.

154. E-cash is a form of electronic money that:
A. can be used over any computer network.
B. utilizes reusable e-cash coins to make payments.
C. does not require the use of an Internet digital bank.
D. contains unique serial numbering to track the identity of the buyer.

155. An organization is about to implement a computer network in a new office building. The company has 200 users located in the same physical area. No external network connections will be required. Which of the following network configurations would be the MOST expensive to install?
A. Bus
B. Ring
C. Star
D. Mesh

156. An organization is about to implement a computer network in a new office building. The company has 200 users located in the same physical area. No external network connections will be required. Which of the following network configurations would be the easiest for problem resolution?
A. Bus
B. Ring
C.Star
D. Mesh

157. Congestion control is BEST handled by which OSI layer?
A. Data link
B. Session layer
C. Transport layer
D. Network layer

158. Which of the following is NOT an element of a LAN environment?
A. Packet switching technology
B. Baseband (digital signaling)
C. Ring or short bus topology
D. Private circuit switching technology

159. Which of the following would an IS auditor NOT review when performing a general operational control review?
A. User manuals
B. Re-run reports
C. Maintenance logs
D. Backup procedures

160. Which of the following is NOT a function of an online tape management system?
A. Indicating which tapes should be cleaned
B. Maintaining an inventory listing of tapes
C. Allowing external tape labels to contain a serial number only
D. Controlling physical access to the tape library area

161. Which of the following is NOT related to file identification?
A. Periodic file inventory
B. External label standards
C. Retention period standards
D. High-level qualifier restrictions

162. An IS auditor has discovered that the organization's existing computer system is no longer adequate for the demands being placed on it by data processing, is not compatible with new models and cannot be expanded. As a result, a recommendation is made to use emulation. Emulation involves:
A. hardware which converts a new computer into an image of the old computer.
B. writing the programs in modules which simplify the transition to a new computer.
C. software which translates the old program into one readable by a new computer.
D. simulating a new computer on the old computer to produce machine independent code.

163. All of the following are properties of a relational database EXCEPT:
A. relational database technology separates data from applications
B. operational efficiencies are significantly increased with relational models
C. relational database models information in the structure of a table with columns and rows
D. in a relational model there is always a primary key for a tuple and there are no duplicate tuples

164. Which of the following is the operating systems mode in which all instructions can be executed?
A. Problem
B. Interrupt
C. Supervisor
D. Standard processing

165. During a review of a large data center an IS auditor observed computer operators acting as backup tape librarians and security administrators. Which of these situations would be MOST critical to report to senior management?
A. Computer operators acting as tape librarians
B. Computer operators acting as security administrators
C. Computer operators acting as a tape librarian and security administrator
D. It is not necessary to report any of these situations to senior management

166. Which of the following functions would be acceptable for the security administrator to perform in addition to his or her normal function?
A. Systems analyst
B. Quality assurance
C. Computer operator
D. Systems programmer

167. Which of the following is a hardware device that relieves the central computer from performing network control, format conversion and message handling tasks?
A. Spool
B. Cluster controller
C. Protocol converter
D. Front end processor

168. Which of the following tools for controlling input/output of data are used to verify output results and control totals by matching them against the input data and control totals?
A. Batch header forms
B. Batch balancing
C. Data conversion error corrections
D. Access controls over print spools

169. Which of the following tools is NOT used to monitor the efficiency and effectiveness of services provided by IS personnel?
A. Online monitors
B. Operator problem reports
C. Output distribution reports
D. Console logs

170. Which of the following would an IS auditor expect to find in a console log?
A. Names of system users
B. Shift supervisor identification
C. System errors
D. Data edit errors

171. Which of the following systems-based approaches would a financial processing company employ to monitor spending patterns in order to identify abnormal expenditures?
A. A neural network
B. Database management software
C. Management information systems
D. Computer assisted audit techniques

172. Which of the following is the BEST form of transaction validation?
A. Use of key field verification techniques in data entry
B. Use of programs to check the transaction against criteria set by management
C. Authorization of the transaction by supervisory personnel in an adjacent department
D. Authorization of the transaction by a department supervisor prior to the batch process

173. An IS auditor needs to link his/her microcomputer to a mainframe system that uses binary synchronous data communications with block data transmission. However, the IS auditor's microcomputer, as presently configured, is capable of only asynchronous ASCII character data communications. Which of the following must be added to the IS auditor's computer to enable it to communicate with the mainframe system?
A. Buffer capacity and parallel port
B. Network controller and buffer capacity
C. Parallel port and protocol conversion
D. Protocol conversion and buffer capability

174. Which of the following audit techniques would an IS auditor place the MOST reliance on when determining whether an employee practices good preventive and detective security measures?
A. Observation
B. Detail testing
C. Compliance testing
D. Risk assessment

175. Which of the following is NOT a way that executive information systems (EIS) are distinguished from other information systems?
A. EIS are much easier to use than other systems.
B. EIS normally include user friendly features.
C. EIS normally include other features such as e-mail and word processing abilities.
D. EIS focus on broad problems to a specific view.

176. An organization is considering installing a local area network (LAN) in a site under construction. If system availability is the main concern, which of the following topologies is MOST appropriate?
A. Ring
B. Line
C. Star
D. Bus

177. Capacity monitoring software is used to ensure:
A. maximum use of available capacity.
B. future acquisitions meet user functionality demands.
C. concurrent use by a large number of users.
D. continuity of efficient operation.

178. Receiving an electronic data interchange (EDI) transaction and passing it through the communications interface stage usually requires:
A. translating and unbundling transactions.
B. routing verification procedures.
C. passing data to the appropriate application system.
D. creating a point of receipt audit log.

179. Which one of the following types of firewalls would BEST protect a network from an Internet attack?
A. Screened sub-net firewall
B. Application filtering gateway
C. Packet filtering router
D. Circuit level gateway

180. A large manufacturing firm wants to automate its invoice and payment processing system with its suppliers. Requirements state that the system of high integrity will require considerably less time for review and authorization. The system should still be capable of quickly identifying errors that need follow up. Which approach below is BEST suited in meeting these requirements?
A. Establishing an inter-networked system of client servers with suppliers for increased efficiencies.
B. Outsourcing the function to a firm specializing in automated payments and accounts receivable/invoice processing.
C. Establishing an electronic data interchange (EDI) system of electronic business documents and transactions with key suppliers, computer to computer, in a standard format.
D. Reengineering existing processing and redesigning the existing system.

181. Which of the following is widely accepted as one of the critical components in networking management?
A. Configuration management
B. Topological mappings
C. Application of monitoring tools
D. Proxy server trouble shooting

182. An IS auditor consulting on a project to develop a network management system, would consider all of the following essential features EXCEPT:
A. the capacity to interact with the Internet for problem solving.
B. a graphical interface to map the topology.
C. a relational database to store the readings.
D. the ability to gather information from various network devices.

183. In protocols like HTTP, FTP, and SMTP, the implementation of the TCP/IP suite is arranged in the following manner:
A. TCP works at the transport layer and handles packets, while IP works at the network layer and handles addresses.
B. TCP works at the transport layer and handles addresses, while IP works at the network layer and handles packets.
C. TCP works at the presentation layer and handles proxies, while IP works at the data link layer and handles applets.
D. TCP works at any of the OSI layers and handles circuits, while IP also works at any of the OSI layers but handles messages.

184. Public-key infrastructure (PKI) integrates all of the following into an enterprise-wide network security architecture EXCEPT:
A. public-key cryptosystem.
B. digital certificates.
C. certificate authorities.
D. password key management.

185. All of the following are common problems with firewall implementations EXCEPT:
A. inadequately protecting the network and servers from virus attacks.
B. incorrectly configuring access lists.
C. logging of connections is either insufficient or not reviewed on a regular basis.
D. network services destined to internal hosts are passed through the firewall unscreened.

186. When auditing operating software development, acquisition or maintenance, the IS auditor would review system software maintenance activities to determine:
A. fallback or restoration procedures are in place in case of production failure.
B. impact of the product on processing reliability.
C. system software changes are scheduled when they least impact IS processing.
D. current versions of the software are supported by the vendor.

187. While evaluating a file/table design, an IS auditor should understand that a referential integrity constraint consists of:
A. ensuring the integrity of transaction processing.
B. ensuring that data are updated through triggers.

C. ensuring controlled user updates to database.
D. rules for designing tables and queries.

188. One of the responsibilities of the technical support function is:
A. ensuring job preparation, scheduling and operating instructions.
B. establishing, enhancing and maintaining a stable, controlled environment for the implementation of changes within the production software environment.
C. defining, establishing and maintaining a standard, consistent and well-defined testing methodology for computer systems.
D. obtaining detailed knowledge of the operating system and other systems software.

189. A universal serial bus (USB) port:
A. connects the network without a network card.
B. connects the network with an Ethernet adapter
C. replaces all existing connections.
D. connects the monitor.

190. How can an enterprise provide access to its intranet (i.e., extranet) across the Internet to its business partners?
A. Virtual private network
B. Client/server
C. Dial-in access
D. Network service provider

191. A hub is a device that connects:
A. two LANs using different protocols.
B. a LAN with a WAN.
C. a LAN with a MAN.
D. two segments of a single LAN.

192. Which of the following network configuration options, contains a direct link between any two host machines?
A. Bus
B. Ring
C. Star
D. Completely connected (mesh)

193. Which of the following can a local area network (LAN) administrator use to protect against exposure to illegal or unlicensed software usage by the network user?
A. Software metering
B. Virus detection software
C. Software encryption
D. Software inventory programs

194. Which of the following controls will MOST effectively detect the presence of bursts of errors in network transmissions?
A. Parity check
B. Echo check
C. Block sum check
D. Cyclic redundancy check

195. Which of the following types of firewalls provide the GREATEST degree and granularity of control?
A. Screening router
B. Packet-filter
C. Application-gateway
D. Circuit-gateway

196. Which of the ISO/OSI model layers provides service for how to route packets between nodes?
A. Data link
B. Network
C. Transport
D. Session

197. In a TCP/IP based network, an IP address specifies a:
A. network connection.
B. router/gateway.
C. computer in the network.
D. device on the network such as a gateway/router, host, server, etc.

198. Connection-oriented protocols in the TCP/IP suite are implemented in the:
A. transport layer.
B. application layer.
C. physical layer.
D. network layer.

199. The device to extend the network that must have storage capacity to store frames and act as a storage and forward device is a:
A. router.
B. bridge.
C. repeater.
D. gateway.

200. In a client/server architecture, a domain name service (DNS) is MOST important because it provides the:
A. address of the domain server.
B. resolution service for the name/address.
C. resolution on the Internet for the name/address.
D. domain name system.

201. In a web server, a common gateway interface (CGI) is MOST often used as a(n):
A. consistent way for data transfer to the application program and back to the user.
B. computer graphics imaging method for movie and TV.
C. graphic user interface for web design.
D. interface to access the private gateway domain.

202. Which of the following exposures associated with the spooling of sensitive reports for off-line printing would an IS auditor consider to be the MOST serious?
A. Sensitive data may be read by operators.
B. Data can be amended without authorization.
C. Unauthorized report copies might be printed.
D. Output would be lost in the event of system failure.

203. Applying a retention date on a file will ensure that:
A. data cannot be read until the date is set.
B. data will not be deleted before the date is set.
C. backup copies are not retained after that date.
D. datasets having the same name are differentiated.

204. Which of the following would NOT be considered a security threat to Internet web sites?
A. Hackers
B. Crackers
C. Virus writers

D. Asynchronous attacks

205. An IS auditor is assigned to help design the data security, data integrity and business continuity aspects of an application under development. Which of the following provides the MOST reasonable assurance that corporate assets are protected when the application is certified for production?
A. A certification review conducted by the internal auditor.
B. A certification review conducted by the assigned IS auditor.
C. Specifications by the user on the depth and content of the certification review.
D. An independent review conducted by another equally experienced IS auditor.

206. The MOST effective method of preventing unauthorized use of data files is:
A. automated file entry.
B. tape librarian.
C. access control software.
D. locked library.

207. Which of the following would NOT be considered a terminal access control?
A. Use of dial-up lines only in the event of an emergency
B. Disconnection of a terminal after it has been inactive for a period of time
C. Validation of passwords and transaction codes by the access control software
D. Logging of authorized and unauthorized attempts to access the computer systems

208. Which of the following factors is LEAST likely to allow a perpetrator to discover a valid password?
A. The number of characters in the password
B. The power of the computer used to break the password code
C. The number of incorrect access attempts allowed before disconnect
D. The content of the character set from which the password is composed

209. Which of the following would be MOST effective in establishing access control through the use of sign-on procedures?
A. Authorization and authentication of the user
B. Authentication and identification of the user
C. Authorization, authentication and location of the user"
D. Authorization, authentication, identification and location of the user"

210. Which of the following would BEST ensure the proper updating of critical fields in a master record?
A. Field checks
B. Control totals
C. Reasonableness checks
D. Before and after maintenance report

211. Which of the following controls is LEAST likely to discover changes made online to important master records?
A. Update access to master file is restricted to supervisor independent of data entry.
B. Clerks enter updates online, but these must be finalized by independent supervisor.
C. Edit listing of all updates are produced daily and reviewed by independent supervisor.
D. Update authorization form must be approved by independent supervisor before clerks enter updates.

212. Which of the following is the MOST effective control procedure for security of a stand-alone small business computer environment?
A. Supervision of computer usage
B. Daily management review of the trouble log
C. Storage of computer media in a locked cabinet
D. Independent review of an application system design

213. Which of the following logical access exposures involves changing data before, or as it is entered into the computer?
A. Data diddling
B. Trojan horse
C. Worm
D. Salami technique

214. When investigating a serious security access violation, the IS auditor should NOT:
A. refer the violation to the security administrator since he/she may be a party to the violation.
B. contact law enforcement to determine if violations have occurred elsewhere.
C. recommend corrective measures since this is the role of the Security Administrator.
D. perform a security access follow-up to determine if other violations have occurred.

215. Which of the following would be considered the BEST example of a proper password for use in system access?
A. XWA3
B. LARRY2
C. TWC2H
D. YRC45OPB

216. Data classification is important when identifying who should have access to:
A. test data and programs.
B. production data and programs.
C. production and test programs.
D. test and production data and programs.

217. Naming conventions for access controls are NOT:
A. setup by the owners of the data or application.
B. dependent on the importance and level of security that is needed.
C. established to promote the implementation of efficient access rules.
D. defined with the assistance of the database administrator.

218. Digital signatures provide data integrity since they require the:
A. signer to have a public key, and the receiver to have a private key.
B. signer to have a private key, and the receiver to have a public key.
C. signer and receiver to have a public key.
D. signer and receiver to have a private key.

219. Automated teller machines (ATMs) are a specialized form of a point of sale terminal which:
A. allow for cash withdrawal and financial deposits only.
B. are usually located in populous areas to deter theft or vandalism.
C. utilize protected telecommunication lines for data transmissions.
D. must provide high levels of logical and physical security.

220. Which of the following processes would be performed FIRST by the system when logging-on to an online system?
A. Initiation
B. Verification
C. Authorization
D. Authentication

221. Which of the following is a benefit of using callback devices?
A. Provide an audit trail
B. Can be used in a switchboard environment
C. Permit unlimited user mobility
D. Allow call forwarding

222. Having established an application's access control process, an IS auditor's next step is to ensure:
A. passwords are not shared.
B. password files are encrypted.
C. redundant logon-IDs are deleted.
D. allocation of logon-IDs is controlled.

223. In the ISO/OSI model, which of the following protocols is the FIRST to perform security over the user application?
A. Session layer.
B. Transport layer
C. Network layer
D. Presentation layer

224. A feature of a digital signature that ensures that the claimed sender cannot later deny generating and sending the message is:
A. data integrity.
B. authentication.
C. non-repudiation.
D. replay protection.

225. An IS auditor who intends to use penetration testing during an audit of Internet connections would:
A. evaluate configurations.
B. examine security settings.
C. ensure virus-scanning software is in use.
D. use tools and techniques that are available to a hacker.

226. Which of the following is NOT an employee security responsibility?
A. Keeping Logon-IDs and passwords secret
B. Helping other employees create passwords
C. Reading and understanding the security policy
D. Questioning unfamiliar people who enter a secured area

227. Naming conventions for system resources are an important prerequisite for access control because they ensure that:
A. resource names are not ambiguous.
B. users' access to resources is clearly and uniquely identified.
C. internationally recognized names are used to protect resources.
D. the number of rules required to adequately protect resources is reduced.

228. Passwords should be:
A. assigned by the security administrator.
B. changed every 30 days at the discretion of the user.
C. reused often to ensure the user does not forget the password.
D. displayed on the screen so that the user can ensure that it has been properly entered.

229. Logical access controls are used to protect:
A. operator consoles.
B. computer storage facilities.
C. data classification and ownership.
D. disks and tapes in the back-up library.

230. Which of the following is NOT a valid reason for using digital signatures to secure e-mail transmissions?
A. The signature is unforgeable.
B. Keys can be used indefinitely.
C. Signatures cannot be reused.
D. A signed document cannot be altered.

231. When performing an audit of access rights, an IS auditor should be suspicious of which of the following if allocated to a computer operator?
A. READ access to data
B. DELETE access to transaction data files
C. Logged READ/EXECUTE access to programs
D. UPDATE access to job control language/script files

232. An IS auditor who wishes to prevent unauthorized entry to the data maintained in a dial-up fast response system would recommend?
A. Online terminals be placed in restricted areas.
B. Online terminals be equipped with key locks.
C. ID cards be required to gain access to online terminals.
D. Online access be terminated after three unsuccessful attempts.

233. Which of the following controls would BEST serve to effectively detect intrusion?
A. User creation and user privileges are granted through authorized procedures.

B. Automatic logoff when a workstation is inactive for a particular period of time.
C. Automatic logoff of the system after a specified number of unsuccessful attempts.
D. Unsuccessful logon attempts are actively monitored by the security administrator.

234. Which of the following control weaknesses would an IS auditor performing an access controls review be LEAST concerned with?
A. Audit trails are not enabled.
B. Programmers have access to the live environment.
C. Group logons are being used for critical functions.
D. The same user can initiate transactions and also change related parameters.

235. Which of the following audit procedures would an IS auditor be LEAST likely to include in a security audit?
A. Review the effectiveness and utilization of assets.
B. Test to determine that access to assets is adequate.
C. Validate physical, environmental and logical access policies per job profiles.
D. Evaluate asset safeguards and procedures that prevent unauthorized access to the assets.

236. A firewall access control list may filter access based on each of the following parameters EXCEPT:
A. port.
B. service type.
C. network interface card (NIC).
D. internet protocol (IP) address.

237. Which of the following applet intrusion issues poses the GREATEST risk of disruption to an organization?
A. A program that deposits a virus on a client machine.
B. Applets recording keystrokes and, therefore, passwords.
C. Downloaded code that reads files on a client's hard drive.
D. Applets damaging machines on the network by opening connections from the client machine.

238. Which of the following BEST describes the impact that effective firewall design and implementation strategies have as an enabler for improved information security?
A. A source of detailed information about network security.
B. A focal point for security auditing, both internal and external.
C. A chance to significantly reduce the threat of internal hacking.
D. A chance to root out undocumented connections and bring all remote access into line with written policy.

239. Which of the following information is LEAST likely to be contained in a digital certificate for the purposes of verification by a Trusted Third Party (TTP)/Certification Authority (CA)?
A. Name of the TTP/CA
B. Public key of the sender
C. Name of the public key holder
D. Time period for which the key is valid

240. Which of the following access control functions is LEAST likely to be performed by a database management system (DBMS) software package?
A. User access to field data
B. User sign-on at the network level
C. User authentication at the program level
D. User authentication at the transaction level

241. An IS auditor reviewing operating system access discovers that the system is not properly secured. In this situation the IS auditor is LEAST likely to be concerned that the user might:
A. create new users.
B. delete database and log files.
C. access the system utility tools.
D. access the system writeable directories.

242. An IS auditor conducting an access controls review in a client/server environment discovers that all printing options are accessible by all users. In this situation the IS auditor is MOST likely to conclude that:
A. exposure is greater since information is available to unauthorized users.
B. operating efficiency is enhanced since anyone can print any report, any time.
C. operating procedures are more effective since information is easily available.
D. user friendliness and flexibility is facilitated since there is a smooth flow of information among users.

243. An IS auditor discovers that programmers have update access to the live environment. In this situation the IS auditor is LEAST likely to be concerned that programmers can:
A. authorize transactions.
B. add transactions directly to the database.
C. make modifications to programs directly.
D. access data from live environment and provide faster maintenance.

244. An IS auditor performing a telecommunication access control review would focus the MOST attention on the:
A. maintenance of access logs of usage of various system resources.
B. authorization and authentication of the user prior to granting access to system resources.
C. adequate protection of stored data on servers by encryption or other means.
D. accountability system and the ability to properly identify any terminal accessing system resources.

245. An organization wants to introduce a new system to allow single-sign-on. Currently, there are five main application systems, and users must sign on to each one separately. It is proposed that under the single-sign-on system, users will only be required to enter one user-ID and password for access to all application systems. Under this type of single-sign-on system the risk of unauthorized access:
A. is less likely.
B. is more likely.
C. will have a greater impact.

D. will have a smaller impact.

246. Sign-on procedures include the creation of a unique user-ID and password. However, an IS auditor discovers that in many cases the user name and password are the same. The BEST control to mitigate this risk is to:
A. change the company's security policy.
B. educate users about the risk of weak passwords.
C. build in validations to prevent this during user creation and password change.
D. require a periodic review of matching of user-ID and passwords for detection and correction.

247. The PRIMARY objective of a logical access controls review assignment is to:
A. review access controls provided through software.
B. ensure access is granted per the organization's authorities.
C. walkthrough and assess access provided in the IT environment.
D. provide assurance that computer hardware is adequately protected against abuse.

248. The scope of a logical access controls review would include the evaluation of:
A. effectiveness and efficiency of IT security and related controls.
B. confidentiality, integrity and availability of information to authorized users.
C. access to systems software and application software to ensure compliance with the access policy.
D. access to user authorization levels, parameters and operational functions through application software.

249. Naming conventions for system resources are an important prerequisite for access control because they:
A. ensure that resource names are not ambiguous.
B. reduce the number of rules required to adequately protect resources.
C. ensure that user access to resources is clearly and uniquely identified.
D. ensure that internationally recognized names are used to protect resources.

250. When a PC that has been used for the storage of confidential data is sold on the open market, the:
A. hard disk should be demagnetized.
B. hard disk should be mid-level formatted.
C. data on the hard disk should be deleted.
D. data on the hard disk should be defragmented.

251. Which of the following exposures could be caused by a line-grabbing technique?
A. Unauthorized data access
B. Excessive CPU cycle usage
C. Lockout of terminal polling
D. Multiplexor control dysfunction

252. Which of the following is an advantage of using a local area network (LAN)?
A. LANs protect against virus infection.
B. LANs protect against improper disclosure of data.
C. LANs provide program integrity from unauthorized changes.
D. LANs provide central storage for a group of users.

253. Creation of an electronic signature:
A. encrypts the message.
B. verifies where the message came from.
C. cannot be compromised when using a private key.
D. cannot be used with e-mail systems.

254. Which of the following is a strength of a client/server security system?
A. Change control and change management procedures are inherently strong.
B. User can manipulate data without controlling resources on the mainframe.
C. Network components seldom become obsolete.
D. Access to confidential data or data manipulation is strongly controlled.

255. Which of the following automated reports measure telecommunication transmissions and determines whether transmissions are accurately completed?
A. Online monitors
B. Down time reports
C. Help desk reports
D. Response time reports

256. Which of the following statements pertaining to Internet security is TRUE?
A. Firewalls cannot stop hackers from gaining access to the corporate network.
B. Firewalls should sit in the most commonly used access point between a corporate network and the Internet.
C. Encrypted corporate data is secure as it transports across the Internet.
D. Not all corporate networks connected to the Internet are subject to attack.

257. An Internet secured gateway's domain name service:
A. prevents users outside a secure network from seeing addresses of secure hosts.
B. asks a user for the name of the host, and authenticates it before making contact.
C. offers a way to limit user access into or out of a secure network.
D. provides the ability to administer user names on a network.

258. Which of the following statements is TRUE relating to the use of public key encryption to secure data while it is being transmitted across a network?
A. Under public key encryption both the key used to encrypt and decrypt the data are made public.
B. Under public key encryption the key used to encrypt is kept private but the key used to decrypt the data is made public.
C. Under public key encryption the key used to encrypt is made public but the key used to decrypt the data is kept private.
D. Under public key encryption both the key used to encrypt and decrypt the data are kept private.

259. Which of the following would NOT protect a system from computer viruses?
A. Write-protect all diskettes, once they have been virus-checked.
B. Scan any new software before it is installed.
C. Boot only from diskettes that were initially checked for viruses.
D. Do not allow vendors to run demonstrations on company owned machines.

260. During the audit of a telecommunications system the IS auditor finds that the risk of data interception for communications with remote sites is very high. The MOST effective control that would reduce this exposure is:
A. encryption.
B. call-back modems.
C. message authentication.
D. dedicated leased lines.

261. An Internet-based attack on commercial systems using password sniffing can:
A. enable one party to act as if they are another party.
B. cause modification to the contents of certain transactions.
C. be used to gain access to systems containing proprietary information.
D. result in major problems with billing systems and transaction processing agreements.

262. Which of the following controls would be MOST comprehensive in a remote access network with multiple and diverse sub-systems?
A. Proxy server
B. Firewall installation
C. Network administrator
D. Password implementation and administration

263. Which of the following is NOT a principle applied in deriving the OSI layers?
A. Each layer should provide a well-defined function.
B. The integrity of data at each layer should be assured.
C. A layer should be created only when a different level of abstraction is needed.
D. The layer boundaries should be chosen to minimize the information flow across layer interfaces.

264. Which of the following is NOT a common function of application layer services?
A. Host to host data integrity
B. Application programming interfaces (APIs)
C. Global directory services to locate resources on a network
D. A uniform way of handling a variety of system monitors and devices

265. A decrease in amplitude as a signal propagates along a transmission medium is known as:
A. noise.
B. crosstalk.
C. attenuation.
D. delay distortion.

266. Use of data encryption is applicable to all of the following OSI layers EXCEPT:
A. physical layer.
B. data link layer.
C. application layer.
D. network and transport layer.

267. Which of the following is MOST affected by network performance monitoring tools?
A. Integrity
B. Availability
C. Completeness
D. Confidentiality

268. Java applets and ActiveX controls are distributed executable programs that execute in background of a web browser client. This is a reasonably controlled practice when:
A. a firewall exists.
B. a secure web connection is used.
C. the source of the executable is certain.
D. the host website is part of your organization.

269. Your organization has been an active Internet user for several years and your business plan now calls for initiating e-commerce via web-based transactions. You have decided to accept payment transactions by implementing agreements with the major credit card companies. They have suggested certain parameters for your firewall installation. Which of the following parameters will LEAST impact transactions in e-commerce?
A. Encryption is required
B. Timed authentication is required
C. Firewall architecture hides the internal network
D. Traffic is exchanged through the firewall at the application layer only

270. Which of the following encrypt/decrypt steps provides the GREATEST assurance in achieving confidentiality, message integrity and non-repudiation by either sender or recipient?
A. The recipient uses his/her private key to decrypt the secret key.
B. The encrypted pre-hash code and the message are encrypted using a secret key.
C. The encrypted pre-hash code is derived mathematically from the message to be sent.
D. The recipient uses the sender's public key, verified with a certificate authority, to decrypt the pre-hash code.

271. Which of the following controls would provide the GREATEST assurance over database integrity?
A. Audit log procedures
B. Table link/reference checks
C. Query/table access time checks
D. Roll-back and roll-forward database features

272. Use of asymmetric encryption over an Internet e-commerce site, where there is one private key for the hosting server and the public key is widely distributed to the customers, is MOST likely to provide comfort to the:

A. customer over the authenticity of the hosting organization.
B. hosting organization over the authenticity of the customer.
C. customer over the confidentiality of messages from the hosting organization.
D. hosting organization over the confidentiality of messages passed to the customer.

273. The database administrator (DBA) has recently informed you of his decision to disable certain normalization controls in the database management system (DBMS) software in order to provide users with increased query performance. This will MOST likely increase the risk of:
A. loss of audit trails.
B. redundancy of data.
C. loss of data integrity.
D. unauthorized access to data.

274. Which of the following techniques provides the BEST protection of e-mail message authenticity and confidentiality?
A. Signing the message using the sender's private key and encrypting the message using the receiver's public key.
B. Signing the message using the sender's public key and encrypting the message using the receiver's private key.
C. Signing the message using the receiver's private key and encrypting the message using the sender's public key.
D. Signing the message using the receiver's public key and encrypting the message using the sender's private key.

275. Which of the following is the MOST fundamental step in effectively preventing a virus attack?
A. Executing the updated anti-virus software in the background on a periodic basis.
B. Buying an effective standard anti-virus software, which is installed on all servers and workstations with hard disks.
C. Ensuring that all new software through all media is first checked for a virus in a separate PC before being loaded into the production environment.
D. Adopting a comprehensive anti-virus policy to protect the organization's computing facilities from virus attacks and communicating it to all users.

276. Confidential PC data is BEST protected by:
A. a password.
B. file encryption.
C. removable diskettes.
D. a key operated power source.

277. When auditing the security of a data center, an IS auditor would look for the presence of a voltage regulator to:
A. protect hardware against power surges.
B. maintain integrity if the main power is interrupted.
C. maintain immediate power if the main power is lost.
D. protect hardware against long-term power fluctuation.

278. Electromagnetic emissions from a terminal represent an exposure because they:
A. affect noise pollution.
B. disrupt processor functions.
C. produce dangerous levels of electric current.
D. can be detected and displayed.

279. Which of the following statements relating to power-off switches is FALSE?
A. They may need to immediately shut off power to the computer and peripheral devices.
B. Two emergency power switches should be installed inside the computer room adjacent to exits.
C. Emergency power-off switches should be clearly labeled.
D. Emergency power-off switches should be shielded against accidental activation.

280. Which of the following methods of suppressing a fire in a data center is the MOST effective and environmentally friendly?
A. Halon gas
B. Wet-pipe sprinklers
C. Dry-pipe sprinklers
D. Carbon dioxide gas

281. Which of the following environmental controls is appropriate to protect computer equipment against short-term reductions in electrical power?
A. Power line conditioners
B. A surge protective device
C. An alternative power supply
D. An interruptible power supply

282. Which of the following would be the LEAST important item in a business continuity plan?
A. Redundant facilities
B. Relocation procedures
C. Adequate insurance coverage
D. Current and available business continuity manual

283. Which of the following physical access controls would provide the highest degree of security over unauthorized access?
A. Bolting door lock
B. Cipher lock
C. Electronic door lock
D. Fingerprint scanner

284. Which of the following is LEAST likely to be classified as a physical access control?
A. Access to the work area is restricted through a swipe card.
B. All physical assets have an identification tag and are properly recorded.
C. Access to the premises is restricted and all visitors authorized for entry.
D. Visitors are issued a pass and escorted in and out by a concerned employee.

285. During the course of a physical verification of assets an IS auditor discovered discrepancies in properly identifying and recording assets which could be attributed to a lack of related procedures and policies. Which of the following would NOT be a resultant exposure caused by this situation?
A. Assets do not have an adequate identification tag.
B. Incorrect identification may affect warranty claims.
C. Incorrect identification may affect insurance claims.
D. Assets wrongly recorded may lead to misappropriation.

286. Which of the following procedures can a biometric system perform?
A. Measure airborne contamination.
B. Provide security over physical access.
C. Monitor temperature and humidity levels.
D. Detect hazardous electromagnetic fields in an area.

287. Which of the following concerns associated with the World Wide Web would be addressed by a firewall?
A. Unauthorized access from outside the organization
B. Unauthorized access from within the organization
C. Delay in Internet connectivity
D. Delay in downloading using file transfer protocol

288. A digital signature contains a message digest to:
A. show if the message has been altered after transmission.
B. define the encryption algorithm.
C. confirm the identity of the originator.
D. enable message transmission in a digital format.

289. Which of the following fire suppressant systems would an IS auditor expect to find when conducting an audit of an unmanned computer center?
A. Carbon dioxide
B. Halon
C. Dry-pipe sprinkler
D. Wet-pipe sprinkler

290. The use of web site certificates achieve all of the following objectives EXCEPT:
A. authenticate the user.
B. authenticate the web site.
C. warranty that the terms for transactions are properly revealed to the users.
D. ensure that the web site has effective controls to protect private users' information from entities that are not related to the business.

291. Which of the following types of transmission media provide the BEST security against unauthorized access?
A. Copper wire
B. Twisted pair
C. Fiber optic cables
D. Coaxial cables

292. Controls designed to ensure that unauthorized changes cannot be made to information once it resides in a file are known as:
A. data security controls.
B. implementation controls.
C. program security controls.
"D. computer operations controls.

293. Which of the following is the MOST effective technique for providing security during data transmission?
A. Communication log
B. Systems software log
C. Encryption
D. Standard protocol

294. Which of the following is the MOST effective control over visitor access to a data center?
A. Visitors are escorted
B. Visitor badges are required
C. Visitors sign in
D. Visitors are spot-checked by operators

295. Which of the following is a technique that could illegally capture network user passwords?
A. Encryption
B. Sniffing
C. Spoofing
D. Data destruction

296. All of the following are elements of a security infrastructure EXCEPT:
A. management commitment and support.
B. defined and documented security awareness training programs.
C. legal notice banners displayed on terminals with Internet connectivity.
D. defined and documented security policies and procedures.

297. Which of the following is the BEST audit procedure when examining if a firewall is configured in compliance with the organization's security policy?
A. Review the parameter settings
B. Interview the firewall administrator
C. Review the actual procedures
D. Review the device's log file for recent attacks

298. All of the following are significant Internet exposures EXCEPT:
A. loss of integrity.
"B. denial of service.
C. insufficient resources to improve and maintain integrity.
D. unauthorized access.

299. When an organization's network is connected with an external network in an Internet client/server model not under that organization's control, security becomes a concern. In providing adequate security in this environment, which of the following assurance levels is LEAST important?
A. Server and client authentication
B. Data integrity
C. Data recovery
D. Data confidentiality

300. Programs that can run independently and travel from machine to machine across network connections, which

may destroy data or utilize tremendous computer and communication resources, are referred to as:
A. trojan horses.
B. viruses.
C. worms.
D. logic bombs.

301. Which of the following would LEAST likely prevent an information security failure in a wide area network?
A. Conducting user training and awareness programs
B. Avoiding a single point of failure
C. Developing systems that are free from vulnerabilities
D. Regular and rigorous monitoring the systems logs

302. All of the following are common forms of Internet attacks EXCEPT:
A. exploitation of vulnerabilities in vendor programs.
B. denial of service attacks.
C. sending hostile code and attack programs as mail attachments.
D. systematic hacker foot-printing of an organization.

303. The management of an organization has encountered several security incidents recently and has decided to establish a security awareness program. Which of the following would be the LEAST effective in establishing a successful security awareness program?
A. Reward employees who report suspicious events
B. Provide training on a regular basis to new employees, support staff, users, and managers"
C. Stage mock incidents to see how well users and support staff respond
D. Utilize an intrusion detection system to report on incidents that occur

304. Password syntax rules should include all of the following EXCEPT:
A. be five to eight characters in length.
B. shadowed so they are not displayed.
C. allow for a combination of alphanumeric characters.
D. not be particularly identifiable with any user.

305. Information for detecting unauthorized input from a terminal would be BEST provided by the:
A. console log printout.
B. transaction journal.
C. automated suspense file listing.
D. user error report.

306. An IS auditor attempting to determine whether access to program documentation is restricted to authorized persons would MOST likely:
A. evaluate the record retention plans for off-premises storage.
B. interview programmers about the procedures currently being followed.
C. compare utilization records to operations schedules.
D. review data file access records to test the librarian function.

307. A systems analyst should have access to all of the following EXCEPT:
A. source code.
B. password identification tables.
C. user procedures.
D. edit criteria.

308. Authentication is the process by which the:
A. system verifies that the user is entitled to input the transaction requested.
B. system verifies the identity of the user.
C. user identifies himself to the system.
D. user indicates to the system that the transaction was processed correctly.

309. The IS auditor has determined that protection of computer files is inadequate. Which of the following is LEAST likely to have caused this problem?
A. Arrangements for compatible backup computer facilities
B. Procedures for release of files
C. Offsite storage procedures
D. Environmental controls

310. If inadequate, which of the following would MOST likely contribute to a denial of service attack?
A. Router configuration and rules
B. Design of the internal network
C. Updates to the router system software
D. Audit testing and review techniques

311. Which of the following is the MOST effective type of anti-virus software?
A. Scanners
B. Active monitors
C. Integrity checkers
D. Vaccines

312. The technique used to ensure security in virtual private networks (VPNs) is:
A. encapsulation.
B. wrapping.
C. transform.
D. encryption.

313. A critical function of a firewall is to act as a:
A. special router that connects the Internet to a LAN.
B. device for preventing authorized users from accessing the LAN.
C. server used to connect authorized users to private trusted network resources.
D. proxy server to increase the speed of access to authorized users.

314. During an audit of an enterprise that is dedicated to e-commerce in the modality of business-to-customer, the IS manager states that digital signatures are used in the establishment of its commercial relations. The auditor must prove that which of the following is used?
A. A biometric, digitalized and encrypted parameter with the customer's public key"
B. A hash of the data that is transmitted and encrypted with the customer's private key
C. A hash of the data that is transmitted and encrypted with the customer's public key

D. The customer's scanned signature, encrypted with the customer's public key"

315. Risk of hash compromise is BEST mitigated using:
A. digital signatures.
B. message encryption.
C. message authentication code.
D. cryptoanalysis.

316. Secure socket layer (SSL) protocol addresses the confidentiality of a message through:
A. symmetric encryption.
B. message authentication code.
C. hash function.
D. digital signature certificates.

317. An organization is considering connecting a critical PC-based system to the Internet. Which of the following would provide the BEST protection against hacking?
A. Application level gateway
B. Remote access server
C. Proxy server
D. Port scanning

318. A “dry-pipe” fire extinguisher system is a system that uses:
A. water, but in which water does not enter the pipes until a fire has been detected.
B. water, but in which the pipes are coated with special watertight sealants.
C. carbon dioxide instead of water.
D. halon instead of water.

319. An enterprise is implementing a business-to-business (B-to-B) network infrastructure to ensure efficient and effective communication and supply chain management with all international customers and suppliers. The enterprise would like to utilize the network infrastructure for secure communication, paperless negotiations and agreements and to ensure appropriate evidence for all transactions. The MOST appropriate solution is:
A. asymmetric encryption and digital signatures.
B. symmetric encryption and digital signatures.
C. public key infrastructure (PKI).
D. message authentication code and digital signatures.

320. Electronic signatures can prevent messages from being:
A. suppressed.
B. repudiated.
C. disclosed.
D. copied.

321. Confidential data stored on a laptop is BEST protected by:
A. storage on optical disks.
B. log-on ID and password.
C. data encryption.
D. physical locks.

322. Security administration procedures require read-only access to:
A. access control tables.
B. security log files.
C. logging options.
D. user profiles.

323. Which of the following would an IS auditor consider a MAJOR risk of using single sign-on?
A. It enables access to single multiple applications
B. It represents a single point of failure
C. It causes an administrative bottleneck
D. It leads to a lockout of valid users

324. Naming convention for access controls are usually set by:
A. data owners with the help of the security officer.
B. programmers with the help of the security officer.
C. system analysts with the help of the security officer.
D. librarian with the help of the security officer.

325. Which of the following is the MOST secure way to connect a private network over the Internet in a small-to medium-sized organization?
A. Virtual private network
B. Dedicated line
C. Leased line
D. Integrated services digital network

326. The potential for unauthorized system access, by way of terminals or workstations within the organization's facility, is increased when:
A. connecting points are available in the facility to connect laptops to the network.
B. users do not write their system passwords on, or near, their work areas.
C. terminals with password protection are located in unsecured locations.
D. terminals are located within the facility in small clusters of a few terminals, each under direct charge and supervision of an administrator.

327. The BEST defense against eavesdropping into computer networks is:
A. encryption.
B. moving the defense perimeter outward.
C. reducing the amplitude of the communication signal.
D. masking the signal with noise.

328. A virtual private network (VPN) performs which of the following functions?
A. Hides information from sniffers on the net
B. Enforces security policies
C. Detects misuse or mistakes
D. Regulates access

329. Within an e-Commerce transaction through the Internet, the process of applying a digital signature to the data that travels in the network, provides which of the following?
A. Confidentiality and integrity
B. Security and nonrepudiation
C. Integrity and nonrepudiation
D. Confidentiality and nonrepudiation

330. Which of the following would an IS auditor consider a weakness when performing an audit of an organization that uses a public key infrastructure with digital

certificates for its business-to-consumer transactions via the Internet?
A. Customers are widely dispersed geographically, but not the certificate authorities (CA).
B. Customers can make their transactions from any computer or mobile device.
C. The certificate authority has several data processing subcenters to administrate certificates.
D. The organization is the owner of the CA.

331. Which of the following implementation modes would provide the GREATEST amount of security to outbound data connecting to the Internet?
A. Transport mode with authentication header (AH) plus encapsulating security payload (ESP)
B. SSL mode
C. Tunnel mode with AH plus ESP
D. Triple-DES encryption mode

332. Which of the following is the MOST reliable sender authentication method?
A. Digital signatures
B. Asymmetric cryptography
C. Digital certificates
D. Message authentication code

333. In the Internet encryption process, which of the following steps provides the GREATEST assurance in achieving authenticity of a message?
A. The pre-hash code is derived mathematically from the message being sent.
B. The pre-hash code is encrypted using the sender's private key.
C. Encryption of the pre-hash code and the message using the secret key.
D. Sender attains the recipient's public key and verifies the authenticity of its digital certificate with a certificate authority.

334. An Internet security threat that could compromise integrity is:
A. theft of data from the client.
B. exposure of network configuration information.
C. a trojan horse browser.
D. eavesdropping on the net.

335. An IS auditor performing a review of the implemented security infrastructure of an organization that provides business-to-business activities, observes that PKI services are being used. The auditor's conclusion would be that they use:
A. personal key information.
B. private key infrastructure.
C. public key infrastructure.
D. practical kerberos implementation.

336. In a public key infrastructure (PKI), the authority which is responsible for the identification and authentication of an applicant for a digital certificate (i.e., certificate subjects) is the:
A. registration authority (RA).
B. issuing certification authority.
C. subject certification authority.
D. policy management authority.

337. Which of the following is used to create Web pages on the Internet?
A. HTTP
B. HTML
C. TCP/IP
D. FTP

338. Which of the following is a simple networking device that interconnects two or more local area networks (LANs)?
A. Router
B. Bridge
C. Gateway
D. Brouter

339. Controls over electronic distribution of software would not include
A. Checksum
B. Digital signatures
C. Virus scanners
D. Intrusion detectors

340. Analyzing data protection requirements for installing a LAN does not include:
A. Uninterruptible power supply
B. Back ups
C. Fault tolerance
D. Operating systems

341. The most desirable metrics for system reliability, availability and responsiveness include (MTBF is mean time between failures, MTTR is mean time to repair, EMRT is emergency response time, and MTTF is mean time to failure):
A. High MTBF, low MTTR, low EMRT and high MTTF"
B. Low MTBF, high MTTR, low EMRT and low MTTF"
C. Low MTBF, low MTTR, high EMRT and high MTTF"
D. High MTBF, high MTTR, high EMRT and low MTTF"

342. A videoconferencing product where individuals work jointly on an electronic document is called a:
A. Workflow application
B. Multipoint application
C. Spreadsheet application
D. Whiteboard application

343. In which of the following situations would a checkpoint/restart procedure NOT enable recovery?
A. Experiencing temporary failure of the hardware
B. Loading tapes out of sequence in a multi-volume file
C. Completing the run of an incorrect version of the program
D. Suffering temporary power loss to the Data Center during the run

344. If a database is restored using before image dumps, where should the process be restarted following an interruption?
A. Before the last transaction
B. After the last transaction
C. The first transaction after the latest checkpoint
D. The last transaction before the latest checkpoint

345. Which of the following is an important consideration in providing backup for online systems?
A. Maintaining system software parameters
B. Ensuring periodic dumps of transaction logs
C. Ensuring grandfather-father-son file backups
D. Maintaining important data at an off-site location

346. As updates to an online order entry system are processed, the updates are recorded on a transaction tape and a hard copy transaction log. At the end of the day, the order entry files are backed up onto tape. During the backup procedure, the disk drive malfunctions and the order entry files are lost. Which of the following are necessary to restore these files?
A. The previous day's backup file and the current transaction tape
B. The previous day's transaction file and the current transaction tape
C. The current transaction tape and the current hardcopy transaction log
D. The current hardcopy transaction log and the previous day's transaction file

347. Which of the following business recovery strategies would require the least expenditure of funds?
A. Warm site facility
B. Empty shell facility
C. Hot site subscription
D. Reciprocal agreement

348. Which of the following alternative business recovery strategies would be LEAST appropriate in a large database and online communications network environment where the critical business continuity period is 10 days?
A. Hot site
B. Cold site
C. Reciprocal agreement
D. Dual information processing facilities

349. For which of the following applications would rapid recovery be MOST crucial?
A. Point-of-sale
B. Corporate planning
C. Regulatory reporting
D. Departmental chargeback

350. An organization's disaster recovery plan should address early recovery of:
A. all information systems processes.
B. all financial processing applications.
C. only those applications designated by the IS Manager.
D. processing in priority order, as defined by business management.

351. An off-site information processing facility:
A. should have the same amount of physical access restrictions as the primary processing site.
B. should be easily identified from the outside so that in the event of an emergency it can be easily found.
C. should be located in proximity to the originating site so that it can quickly be made operational.
D. need not have the same level of environmental monitoring as the originating site since this would be cost prohibitive.

352. An advantage of the use of hot sites as a backup alternative is:
A. the costs associated with hot sites are low.
B. that hot sites can be used for an extended amount of time.
C. that hot sites can be made ready for operation within a short period of time.
D. that hot sites do not require that equipment and systems software be compatible with the primary installation being backed up.

353. An IS auditor reviewing back-up procedures for software need only determine that:
A. object code libraries are backed up.
B. source code libraries are backed up.
C. both object and source codes libraries are backed up.
D. program patches are maintained at the originating site.

354. Which of the following control concepts should be included in a comprehensive test of disaster recovery procedures?
A. Invite client participation.
B. Involve all technical staff.
C. Rotate recovery managers.
D. Install locally stored backup.

355. Which of the following tests would NOT apply to a review of the data center disaster recovery plan?
A. Setting up alternative processing facilities
B. Testing full functionality of restored applications
C. Installing key files from those stored in the Media Library
D. Executing application programs from off site backup copies

356. Which of the following is the business continuity planning and reconstruction team that is responsible for updating the applications database working from terminals at the user recovery site during a reconstruction?
A. Applications team
B. Network recovery team
C. Emergency operations team
D. Data preparation and records team

357. Which of the following procedures would an IS auditor perform to BEST determine whether adequate recovery/restart procedures exist?
A. Reviewing program code
B. Reviewing operations documentation
C. Turning off the UPS, then the power"
D. Reviewing program documentation

358. A company performs full back-up of data and programs on a regular basis. The primary purpose of this practice is to:
A. maintain data integrity in the applications.
B. restore application processing after a disruption.

C. prevent unauthorized changes to programs and data.
D. ensure recovery of data processing in case of a disaster.

359. An IS auditor conducting a review of disaster recovery planning at a financial processing organization has discovered the following:

? The existing disaster recovery plan was compiled two years ago by a systems analyst in the organization's IT department using transaction flow projections from the operations department.

? The plan was presented to the deputy CEO for approval and formal issue, but it is still awaiting his attention.

? The plan has never been updated, tested or circulated to key management and staff, though interviews show that each would know what action to take for their area in the event of a disruptive incident.

The IS auditor's report should recommend that:
A. the deputy CEO be censured for his failure to approve the plan.
B. a board of senior managers be set up to review the existing plan.
C. the existing plan be approved and circulated to all key management and staff.
D. an experienced manager coordinate the creation of a new plan or revised plan within a defined time limit.

360. An IS auditor conducting a review of disaster recovery planning at a financial processing organization has discovered the following:
? The existing disaster recovery plan was compiled two years ago by a systems analyst in the organization's IT department using transaction flow projections from the operations department.
? The plan was presented to the deputy CEO for approval and formal issue, but it is still awaiting his attention.
? The plan has never been updated, tested or circulated to key management and staff, though interviews show that each would know what action to take for their area in the event of a disruptive incident.
The basis of the organization's disaster recovery plan is to re-establish live processing at an alternative site where a similar, but not identical hardware configuration is already established.
The IS auditor should:
A. take no action as the lack of a current plan is the only significant finding.
B. recommend that the hardware configuration at each site should be identical.
C. perform a review to verify that the second configuration can support live processing.
D. report that the financial expenditure on the alternative site is wasted without an effective plan.

361. Disaster recovery planning for a company's computer system usually focuses on:
A. operations turnover procedures.
B. strategic long-range planning.
C. the probability that a disaster will occur.
D. alternative procedures to process transactions.

362. The MAIN purpose for periodically testing off-site hardware back-up facilities is to:
A. ensure the integrity of the data in the database.
B. eliminate the need to develop detailed contingency plans.
C. ensure the continued compatibility of the contingency facilities.
D. ensure that program and system documentation remains current.

363. During a business continuity planning review, the IS auditor discovered that software back-up is being kept only by the IT department and that senior management is not aware of where back-ups are being kept. Which of the following recommendations is an IS auditor LEAST likely to make?
A. Validations in the application software should be made to prevent unauthorized access to data.
B. Off-site security and environmental protection systems should be similar to the production environment.
C. There should be off-site storage of software company data, work product or deliverables in a protected vault for such period as specified.
D. A comprehensive business continuity plan should be formulated to meet the business needs and provide required capabilities in the event of any failure of IT systems.

364. A large chain of shops with electronic funds transfer (EFT) at point-of-sale devices has a central communications processor for connecting with the banking network. Which of the following is the BEST disaster recovery plan for the communications processor?
A. Off-site storage of daily back-ups
B. Alternative standby processor onsite
C. Installation of duplex communication links
D. Alternative standby processor at another network node

365. The following table lists the estimate of the probability of a computer system being destroyed in a natural disaster and the corresponding overall business loss. Which system has the greatest exposure to loss?

Likelihood :: Losses (in $)
A. 10% :: 6 million
B. 15% :: 5 million
C. 20% :: 2.5 million
D. 25% :: 4 million

366. Which of the following would an IS auditor consider to be the MOST important to review when conducting a business continuity audit?
A. A hot site is contracted for and available as needed.
B. A business continuity manual is available and current.
C. Insurance coverage is adequate and premiums are current.

D. Media backups are performed on a timely basis and stored off-site.

367. Which of the following methods of providing telecommunication continuity involves routing traffic through split or duplicate cable facilities?
A. Diverse routing
B. Alternative routing
C. Redundancy
D. Long haul network diversity

368. Which of the following is NOT a feature of an uninterruptible power supply (UPS)?
A. A UPS provides electrical power to a computer in the event of a power failure.
B. A UPS system is an external piece of equipment or can be built into the computer itself.
C. A UPS should function to permit an orderly computer shutdown.
D. A UPS uses a greater wattage into the computer to ensure enough power is available.

369. Most business continuity tests should:
A. be conducted at the same time as normal business operations.
B. address all system components.
C. evaluate the performance of personnel.
D. be monitored by the IS auditor.

370. Which of the following would BEST ensure continuity of a wide area network (WAN) across the organization?
A. Built-in alternative routing
B. Full system back-up taken daily
C. A repair contract with a service provider
D. A duplicate machine alongside each server

371. The MOST significant level of business continuity planning program development effort is generally required during the:
A. testing stage.
B. evaluation stage.
C. Maintenance stage.
D. early stages of planning.

372. An IS auditor reviewing an organization's information systems disaster recovery plan should verify that it is:
A. tested every 6 months.
B. regularly reviewed and updated.
C. approved by the chief executive officer (CEO).
D. communicated to every departmental head in the organization.

373. Which of the following implementations of digital encryption standard is the simplest implementation?
A. Electronic code block (ECB)
B. Cipher block chaining (CBC)
C. Cipher feedback (CFB)
D. Output feedback (OFB)

374. Which of the following manages the certificate life cycle of public key pairs to ensure adequate security and controls exist in e-commerce applications?
A. Registration authority
B. Certificate authority
C. Certification relocation list
D. Certification practice statement

375. An IS auditor performing a review of the back-up processing facilities would be MOST concerned that:
A. adequate fire insurance exists.
B. regular hardware maintenance is performed.
C. offsite storage of transaction and master files exists.
D. backup processing facilities are fully tested.

376. Which of the following findings would an IS auditor be MOST concerned about when performing an audit of backup and recovery and the offsite storage vault?
A. There are three individuals with a key to enter the area
B. Paper documents are also stored in the offsite vault
C. Data files, which are stored in the vault, are synchronized"
D. The offsite vault is located in a separate facility

377. Which of the following represents the GREATEST risk created by a reciprocal agreement for disaster recovery made between two companies?
A. Developments may result in hardware and software incompatibility
B. Resources may not be available when needed
C. The recovery plan cannot be tested
D. The security infrastructures in each company may be different

378. All of the following are security andcontrol concerns associated with disaster recovery procedures EXCEPT:
A. loss of audit trail.
B. insufficient documentation of procedures.
C. inability to restart under control.
D. inability to resolve system deadlock.

379. Losses can be minimized MOST effectively by using outside storage facilities to do which of the following?
A. Include current, critical information in backup files"
B. Ensure that current documentation is maintained at the backup facility
C. Test backup hardware
D. Train personnel in backup procedures

380. Which of the following BEST describes the difference between a disaster recovery plan and a business continuity plan?
A. The disaster recovery plan works for natural disasters whereas the business continuity plan works for non-planned operating incidents such as technical failures.
B. The disaster recovery plan works for business process recovery and information systems whereas the business continuity plan works only for information systems.
C. The disaster recovery plan defines all needed actions to restore to normal operation after an un-planned incident whereas the business continuity plan only deals with critical operations needed to continue working after an un-planned incident.
D. The disaster recovery plan is the awareness process for employees whereas the business continuity plan

contains the procedures themselves to recover the operation.

381. Which of the following would warranty a quick continuity of operations when the recovery time window is short?
A. A duplicated back-up in an alternate site
B. Duplicated data in a remote site
C. Transfer of data the moment a contingency occurs
D. A manual contingency procedure

382. Which of the following is MOST important to have in a disaster recovery plan?
A. Backup of compiled object programs
B. Reciprocal processing agreement
C. Phone contact list
D. Supply of special forms

383. At the end of a simulation of an operational contingency test, the IS auditor performed a review of the recovery process. The IS auditor concluded that the recovery was more than the critical time frame that was necessary. Which of the following actions would the auditor recommend?
A. Widen the physical capacity to accomplish better mobility in a shorter time.
B. Shorten the distance to reach the hot site.
C. Perform an integral review of the recovery tasks.
D. Increase the number of human resources involved in the recovery process.

384. An IS auditor inspects an organization's offsite storage and plans to sample the system and program documentation. The IS auditor is MOST likely interested in reviewing:
A. error conditions and user manuals.
B. application run books.
C. job stream control instructions.
D. exception processing instructions.

385. While reviewing the business continuity plan of an organization, the IS auditor observed that the organization's data and software files are backedup on a periodic basis. Which characteristic of an effective plan does this demonstrate?
A. Deterrence
B. Mitigation
C. Recovery
D. Response

386. Which of the following disaster recovery/continuity plan components provides the GREATEST assurance for recovery after a disaster?
A. The requirement that the alternate facility be available until the original information processing facility is restored.
B. User management involvement in the identification of critical systems and their associated critical recovery times and the specification of needed procedures.
C. Copies of the plan kept at the homes of key decision making personnel.
D. Adequate feedback to management to assure that the business continuity plans are indeed workable and that the procedures are current.

387. Which of the following principles must exist to ensure the viability of a duplicate information processing facility?
A. The site is near the primary site to ensure quick and efficient recovery is achieved.
B. The site contains the most advanced hardware available from the chosen vendor.
C. The workload of the primary site is monitored to ensure adequate backup is complete.
D. The hardware is tested when it is established to ensure it is working properly.

388. There are several methods of providing telecommunications continuity. The method of routing traffic through split cable or duplicate cable facilities is:
A. alternative routing.
B. diverse routing.
C. long haul network diversity.
D. last mile circuit protection.

389. Which of the following offsite information processing facility conditions would cause an IS auditor the GREATEST concern?
A. The facility is clearly identified on the outside with the company name.
B. The facility is located more than an hour driving distance from the originating site.
C. The facility does not have any windows to let in natural sunlight.
D. The facility entrance is located in the back of the building rather than the front.

390. Which of the following is a continuity plan test that uses actual resources to simulate a system crash to cost-effectively obtain evidence about the plan's effectiveness?
A. Paper test
B. Post test
C. Preparedness test
D. Walkthrough

391. An offsite backup facility having electrical writing, air conditioning, flooring, etc., but no computer or communications equipment, intended to operate an information processing facility is better known as a:
A. cold site.
B. warm site.
C. dial up site.
D. duplicate processing facility.

392. Which of the following methods of results analysis, during the testing of the business continuity plan (BCP), provides the BEST assurance that the plan is workable?
A. Quantitatively measuring the results of the test
B. Measurement of accuracy
C. Elapsed time for completion of prescribed tasks
D. Evaluation of the observed test results

393. A large organization with numerous applications running on its mainframe system is experiencing a growing backlog of undeveloped applications. As part of a master plan to eliminate this backlog, end-user computing with prototyping is being introduced, supported by the acquisition of an interactive application generator system. Which of the following areas is MOST critical to the ultimate success of this venture?
A. Data control
B. Systems analysis
C. Systems programming
D. Application programming

394. Which of the following general control items would NOT normally be found in an audit of user programming procedures in an end-user computing environment?
A. Console log procedures
B. Change control procedures
C. Back-up and recovery procedures
D. Documentation standards and procedures

395. Which of the following represents a typical prototype of an interactive application?
A. Screens and process programs
B. Screens, interactive edits and sample reports"
C. Interactive edits process programs and sample reports
D. Screens, interactive edits, process programs and sample reports"

396. Which of the following statements relating to the use of spreadsheets is FALSE?
A. An essential control feature is the performance of adequate testing.
B. It is important to develop complete and appropriate documentation.
C. In the designing process, it is important that data be limited to one spreadsheet.
D. The reference area should include the file name, the version number, and the creation date and time.

397. Which of the following tasks would NOT be performed by an IS auditor when reviewing systems development controls in a specific application?
A. Attend project progress meetings.
B. Review milestone documents for appropriate sign-off.
C. Compare development budgets with actual time and dollars spent.
D. Design and execute testing procedures for use during acceptance testing.

398. Which of the following represents the MOST pervasive control over application development?
A. IS auditors
B. Standard development methodologies
C. Extensive acceptance testing
D. Quality assurance groups

399. A computerized information system frequently fails to meet the needs of users because:
A. user needs are constantly changing.
B. the growth of user requirements was inaccurately forecast.
C. the hardware system limits the number of concurrent users.
D. user participation in defining the system's requirements is inadequate.

400. Which of the following are objectives of using a system development life cycle methodology?
A. Ensuring that appropriate staffing is complete and providing a method of controlling costs and schedules.
B. Providing a method of controlling costs and schedules and ensuring communication among users, IS auditors, management and IS personnel.
C. Providing a method of controlling costs and schedules and an effective means of auditing project development.
D. Ensuring communication among users, IS auditors, management and personnel and ensuring that appropriate staffing is complete.

401. A primary reason for an IS auditor's involvement in the development of a new application system is to determine that:
A. adequate controls are built into the system.
B. user requirements are satisfied by the system.
C. sufficient hardware is available to process the system.
D. data are being developed for pre-implementation testing of the system.

402. In which of the following phases of the system development life cycle of a new application system is it the MOST important for the IS auditor to participate?
A. Design
B. Testing
C. Programming
D. Implementation

403. During a detailed system design, the IS auditor would be LEAST concerned with:
A. adequacy of audit trails.
B. handling of rejected transactions.
C. adequacy of hardware to handle the system.
D. procedures to ensure that all transactions are received.

404. Which of the following groups/individuals assume ownership of systems development life cycle projects and the resulting system?
A. User management
B. Senior management
C. Project steering committee
D. Systems development management

405. Which of the following statements regarding the function of a systems development life cycle steering committee is FALSE?
A. Review project progress regularly.
B. Report only to senior management on project status.
C. Serve as a coordinator and advisor to answer questions about system and program design.

D. Take corrective action regarding personnel changes on the project team.

406. The responsibility of assuring that the systems development life cycle design adheres to corporate security policies and tests system security prior to implementation is that of the:
A. security officer.
B. project manager.
C. quality assurance.
D. project steering committee.

407. An IS auditor who is participating in a systems development life cycle project should:
A. recommend appropriate control mechanisms regardless of cost.
B. obtain and read project team meeting minutes to determine the status of the project.
C. ensure that adequate and complete documentation exists for all project phases.
D. not worry about his/her own ability to produce key deliverables by the promised dates since work will progress regardless.

408. The phases and deliverables of a systems development life cycle project should be determined:
A. during the early planning stages of the project.
B. after early planning has been completed, but before work has begun.
C. during the work stages as deliverables are determined based on risks and exposures.
D. only after all risks and exposures have been identified and the IS auditor has recommended appropriate controls.

409. Where a systems development life cycle methodology is inadequate, the MOST serious immediate risk is that the new system will:
A. be completed late.
B. exceed the cost estimates.
C. not meet business and user needs.
D. be incompatible with existing systems.

410. Which of the following is a management technique that enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality?
A. Function point analysis
B. Critical path methodology
C. Rapid application development
D. Program evaluation review technique

411. Which of the following is NOT an advantage of using structured analysis (SA)?
A. SA supports CASE tools.
B. SA addresses users concerns quickly.
C. SA is more applicable to problem-oriented analysis than design.
D. SA addresses the issue of structuring systems into concurrent tasks.

412. Which of the following is an advantage of prototyping?
A. The finished system normally has strong internal controls.
B. Prototype systems can provide significant time and cost savings.
C. Change control is often less complicated with prototype systems.
D. It ensures that functions or extras are not added to the intended system.

413. The use of fourth generation languages (4GLs) should be weighed carefully against using traditional languages because 4GLs:
A. can lack lower level detail commands necessary to perform data intensive operations.
B. cannot be implemented on both the mainframe processors and microcomputers.
C. generally contain complex language subsets which must be used by skilled users.
D. cannot access database records and produce complex Online outputs.

414. Which of the following is NOT a feature of structured programming for defining applications?
A. Programs are written using a bottom-up approach.
B. Programs are easy to develop and maintain.
C. Design modules are independent of each other.
D. Design is accomplished through a series of diagrams, showing relationships.

415. Which of the following computer aided software engineering (CASE) products is used for developing detailed designs, such as screen and report layouts?
A. Super CASE
B. Upper CASE
C. Middle CASE
D. Lower CASE

416. Which of the following is a characteristic of a decision support system (DSS)?
A. DSS is aimed at solving highly structured problems.
B. DSS combines the use of models with non-traditional data access and retrieval functions.
C. DSS emphasizes flexibility in the decision making approach of users.
D. DSS supports only structured decision-making tasks.

417. Which of the following statements pertaining to data warehouses is FALSE?
A. A data warehouse is designed specifically for decision support.
B. The quality of the data in a data warehouse must be very high.
C. Data warehouses are made up of existing databases, files and external information.
D. A data warehouse is used by senior management only because of the sensitivity of the data.

418. The primary role of an IS auditor in the system design phase of an application development project is to:
A. advise on specific and detailed control procedures.
B. ensure the design accurately reflects the requirement.
C. ensure all necessary controls are included in the initial design.

D. advise the development manager on adherence to the schedule.

419. Which of the following would be considered to be the MOST serious disadvantage of prototyping systems development?
A. The prototyping software is expensive.
B. Prototyping demands excessive computer usage.
C. Users may perceive that the development is complete.
D. The users' needs may not have been correctly assessed.

420. An advantage of using sanitized live transactions in test data is that:
A. all transaction types will be included.
B. every error condition is likely to be tested.
C. no special routines are required to assess the results.
D. test transactions are representative of live processing.

421. An IS auditor's primary concern when application developers wish to use a copy of yesterday's transaction file from the production process to show that the development can cope accurately with the required volume is that:
A. users may prefer to use contrived data for testing.
B. unauthorized access to sensitive data may result.
C. error handling and credibility checks may not be fully proven.
D. full functionality of the new process is not necessarily tested.

422. Many IT projects experience problems because the development time and/or resource requirements are underestimated. Which of the following techniques would improve the estimation of the resources required in system construction after the development of the requirements specification?
A. PERT chart
B. Recalibration
C. Cost-benefit analysis
D. Function point estimation

423. Which of the following is the MOST important reason for the IS auditor to be involved in the system development life cycle process?
A. Evaluate the efficiency of resource utilization.
B. Develop audit programs for subsequent audits of the system.
C. Evaluate the selection of hardware to be used by the system.
D. Ensure that adequate controls are built into the system during development.

424. Which of the following is a primary purpose for conducting parallel testing?
A. To determine if the system is more cost-effective.
B. To enable comprehensive unit and system testing.
C. To highlight errors in the program interfaces with files.
D. To ensure the new system meets all user requirements.

425. Unit testing is different from system testing because:
A. unit testing is more comprehensive.
B. programmers are not involved in system testing.
C. system testing relates to interfaces between programs.
D. system testing proves user requirements are adequate.

426. Which of the following audit procedures would an IS auditor normally perform FIRST when auditing the current documented systems development life cycle?
A. Determine procedural adequacy.
B. Analyze procedural effectiveness.
C. Evaluate level of compliance with procedures.
D. Compare established standards to observed procedures.

427. An IS auditor who has participated in the development of an application system might have their independence impaired if they:
A. perform an application development review.
B. recommend control and other system enhancements.
C. perform an independent evaluation of the application after its implementation.
D. are actively involved in the design and implementation of the application system.

428. Which of the following tools would NOT be used in program debugging during system development?
A. Compiler
B. Memory dump
C. Output analyzer
D. Logic path monitor

429. Which of the following statements relating to structured query language (SQL) is TRUE?
A. SQL is harder to use than a programming language.
B. A user must know where the information is located to gain access.
C. A user must know how the information is structured to gain access.
D. SQL serves as an interface between the client, computer, and server.

430. A significant problem in planning and controlling a software development project is determining:
A. project slack times.
B. a project's critical path.
C. time and resource requirements for individual tasks.
D. precedent relationships which preclude the start of certain activities until others are complete.

431. Which of the following is NOT a role of a project sponsor who is involved in a systems development project?
A. Provides funding for the project
B. Responsible for data and application ownership
C. Monitors and controls costs and project timetable
D. Works with the project manager to define success parameters

432. Large scale systems development life cycle (SDLC) efforts:
A. are not affected by the use of prototyping tools.
B. can be carried out independent of other organizational practices.

C. require that business requirements be defined before the project begins.
D. require that project phases and deliverables be defined during the duration of the project.

433. Which of the following is a reason to involve an IS auditor in systems design activities?
A. Post-application reviews do not need to be performed.
B. Total budgeted system development costs can be reduced.
C. It is extremely costly to institute controls after a system becomes operational.
D. The extent of user involvement in design activities is significantly reduced.

434. Which of the following would NOT normally be part of a feasibility study?
A. Identifying the cost savings of a new system.
B. Defining the major requirements of the new system.
C. Determining the productivity gains of implementing a new system.
D. Estimating a pay-back schedule for cost incurred in implementing the system.

435. Detailed systems specifications do NOT normally include:
A. overviews of each program in the system.
B. program, operations and user documentation.
C. a systems flowchart showing the system logic, data files and reports of the system.
D. a systems narrative depicting the systems objectives, the major functions to be performed and the relationships of the major functions.

436. The purpose of the system development life cycle program and procedure development phase is to:
A. prepare, test and document all computer programs and manual procedures.
B. document a business or system problem to a level at which management can select a system solution.
C. prepare a high-level design of a proposed system solution and present reasons for adopting a solution.
D. expand the general design of an approved system solution so that programming and procedure writing can begin.

437. The knowledge base of an expert system that uses questionnaires to lead the user through a series of choices before a conclusion is reached is known as:
A. rules.
B. decision trees.
C. semantic nets.
D. data flow diagrams.

438. Structured programming is BEST described as a technique that:
A. provides knowledge of program functions to other programmers via peer reviews.
B. reduces the maintenance time of programs by the user of small-scale program modules.
C. makes the readable coding reflect as closely as possible the dynamic execution of the program.
D. controls the coding and testing of the high-level functions of the program in the development process.

439. Peer reviews that detect software errors during each program development cycle resulting in faster implementation, better documentation, easier maintenance and higher programmer morale are called:
A. emulation techniques.
B. structured walkthroughs.
C. modular program techniques.
D. top-down program construction.

440. An IS auditor who plans on testing the connection of two or more system components that pass information from one area to another would use:
A. pilot testing.
B. parallel testing
C. interface testing.
D. regression testing.

441. An advantage in using a bottom-up versus a top-down approach to software testing is that:
A. interface errors are detected earlier.
B. confidence in the system is achieved earlier.
C. errors in critical modules are detected earlier.
D. major functions and processing are tested earlier.

442. During which phase of a system development process would an IS auditor first consider application controls?
A. Construction
B. System design
C. Acceptance testing
D. Functional specification

443. Which of the following quality mechanisms is MOST likely to occur when a system development project is in the middle of the construction stage?
A. Unit tests
B. Stress tests
C. Regression testing
D. Acceptance testing

444. An IS auditor reviewing a system development project would be MOST concerned whether:
A. business objectives are achieved.
B. security and control procedures are adequate.
C. the system utilized the strategic technical infrastructure.
D. development will comply with the approved quality management processes.

445. A large number of system failures are occurring when corrections to previously detected faults are resubmitted for acceptance testing. This would indicate that the development team is probably not adequately performing which of the following types of testing?
A. Unit testing
B. Integration testing
C. Design walkthroughs
D. Configuration management

446. An organization is developing a new business system. Which of the following will provide the MOST assurance that the system provides the required functionality?

A. Unit testing
B. Regression testing
C. Acceptance testing
D. Integration testing

447. Which of the following techniques would provide the BEST assurance that the estimate of program development effort is reliable?
A. Function point analysis
B. Estimates by business area
C. Computer based project schedule
D. Estimate by experienced programmer

448. An IS auditor reviewing an organization's test strategy discovers that it is proposed that the test database be refreshed weekly from a section of the production database. Which of the following would MOST likely be affected by this approach?
A. Completeness of testing
B. Test processing efficiency
C. Documentation of test results
D. Integrity of the production data

449. Which of the following would be a major DISADVANTAGE of using prototyping as a systems development methodology?
A. User expectations of project timescales may be over-optimistic.
B. Effective change control and management is impossible to implement.
C. User participation in day-to-day project management may be too extensive.
D. Users are not usually sufficiently knowledgeable to assist in system development.

450. An IS auditor involved as a team member in the detailed system design phase of a system under development would be MOST concerned with:
A. internal control procedures.
B. user acceptance test schedules.
C. adequacy of the user training program.
D. clerical processes for resubmission of rejected items.

451. The PRIMARY reason for separating the test and development environments would be to:
A. restrict access to systems under test.
B. segregate user and development staff.
C. control the stability of the test environment.
D. secure access to systems under development.

452. The use of coding standards is encouraged by IS auditors because they:
A. define access control tables.
B. detail program documentation.
C. standardize dataflow diagram methodology.
D. ensure compliance with field naming conventions.

453. During which of the following phases in systems development would user acceptance test plans normally be prepared?
A. Feasibility study
B. Requirements definition
C. Implementation planning
D. Post-implementation review

454. In the development of an important application affecting the entire organization, which of the following would be the MOST appropriate project sponsor?
A. The information systems manager
B. A member of executive management
C. An independent management consultant
D. The manager of the key user department

455. Which of the following is LEAST likely to be included in the feasibility study?
A. Statutory requirements
B. Operating system implications
C. Control and audit specifications
D. Hardware capacity considerations

456. Which of the following development methods uses a prototype that can continually be updated to meet changing user or business requirements?
A. Data oriented development (DOD)
B. Object oriented development (OOD)
C. Business process reengineering (BPR)
D. Rapid application development (RAD)

457. Which of the following should be included in a feasibility study for a project to install electronic data interchange (EDI)?
A. The encryption algorithm format
B. The detailed internal control procedures
C. The necessary communication protocols
D. The proposed trusted third-party agreement

458. When reviewing the quality of an IS department's development process, the IS auditor finds that they do not use any formal, documented methodology and standards. The IS auditor's MOST appropriate action would be to:
A. complete the audit and report the finding.
B. investigate and recommend appropriate formal standards.
C. document the informal standards and test for compliance.
D. withdraw and recommend a further audit when standards are implemented.

459. Which of the following testing methods is MOST effective during the initial phases of prototyping?
A. System testing
B. Parallel testing
C. Volume testing
D. Top-down testing

460. IS management has decided to rewrite a legacy customer relations system using fourth generation languages (4GLs). Which of the following risks is MOST often associated with system development using 4GLs?
A. Inadequate screen/report design facilities
B. Complex programming language subsets
C. Lack of portability across operating systems
D. Inability to perform data intensive operations

461. Which of the following audit procedures would MOST likely be used in an audit of a systems development project?
A. Develop test transactions
B. Use code comparison utilities
C. Develop audit software programs
D. Review functional requirements documentation

462. When a new system is to be implemented within a short timeframe, it is MOST important to:
A. finish writing user manuals.
B. perform user acceptance testing.
C. add last-minute enhancements to functionalities.
D. ensure that code has been documented and reviewed.

463. Which of the following should NOT be criteria related to the decision to acquire system software?
A. Hard and soft costs
B. Integration with the existing environment
C. Similarity of the acquired system software to that currently in use
D. Appropriateness of the proposed software to the desired computer environment

464. Which of the following is NOT considered an advantage of packaged software?
A. Reduced development cost
B. Reduced risk of logic error
C. Increased processing efficiencies
D. Increased flexibility due to optional features

465. Which of the following would NOT be a reason for IS Audit involvement in information systems contractual negotiations?
A. Often hardware does not interface in an acceptable manner.
B. Many information systems projects incur additional costs over the contract cost.
C. Vendors may go out of business and discontinue service support on their products.
D. Only the IS auditor can determine whether the controls in the system are adequate.

466. If the decision has been made to acquire software rather than develop it internally, this decision is normally made during the:
A. requirements definition phase of the project.
B. feasibility study phase of the project.
C. detailed design phase of the project.
D. programming phase of the project.

467. Which of the following is NOT an advantage of concurrent software licensing?
A. The license is based on the number of users that can access the software at one time.
B. Network administrators can identify the need to purchase software based on need and use.
C. It is a method that can be used to prevent illegal duplication of software.
D. Users must wait for access, if all concurrent access sessions are in use.

468. Which of the following BEST describes the necessary documentation of an enterprise product reengineering (EPR) software installation?
A. Specific developments only
B. Business requirements only
C. All phases of the installation must be documented
D. No need to develop a customer specific documentation

469. When auditing the requirements phase of a software acquisition, an IS auditor would:
A. assess the adequacy of audit trails.
B. identify and determine the criticality of the need.
C. verify cost justifications and anticipated benefits.
D. ensure that control specifications have been defined.

470. A company has contracted an external consulting firm to implement a commercial financial system to replace its existing in-house developed system. In reviewing the proposed development approach, which of the following would be of GREATEST concern?
A. Acceptance testing is to be managed by users.
B. A quality plan is not part of the contracted deliverables.
C. Not all business functions will be available on initial implementation.
D. Prototyping is being used to confirm that the system meets business requirements.

471. Which of the following should be in place to protect the purchaser of an application package in the event that the vendor ceases to trade?
A. Source code held in escrow.
B. Object code held by a trusted third party.
C. Contractual obligation for software maintenance.
D. Adequate training for internal programming staff.

472. Change management procedures are established by IS management to:
A. control the movement of applications from the test environment to the production environment.
B. control the interruption of business operations from lack of attention to unresolved problems.
C. ensure the uninterrupted operation of the business in the event of a disaster.
D. verify that system changes are properly documented.

473. Which of the following system software elements enables complex system maintenance?
A. System exits
B. Special system logon-IDs
C. Network change controls
D. Bypass label processing

474. Which of the following program change controls is NOT the responsibility of the user department?
A. Updating documentation to reflect all changes
B. Initiating requests within its scope of authority
C. Approving changes before implementation, based on the results of testing"
D. Approving changes before implementation, based on review of changes to manual procedures"

475. Which of the following is MOST effective in controlling application maintenance?
A. Informing users of the status of changes
B. Establishing priorities on program changes
C. Obtaining user approval of program changes
D. Requiring documented user specifications for changes

476. Which of the following should be tested if an application program is modified in an authorized maintenance procedure?
A. The integrity of the database
B. The segment of the program which has been amended
C. The access controls for the applications programmer
D. The complete program, including any interface systems"

477. A post-implementation review of a new or extensively modified system is usually performed by:
A. end-users and IS auditor
B. IS auditor and project development team.
C. project steering committee and project development team.
D. project development team and end-users.

478. In regard to moving an application program from the test environment to the production environment, the BEST control would be provided by having the:
A. application programmer copy the source program and compiled object module to the production libraries.
B. application programmer copy the source program to the production libraries and then have the production control group compile the program.
C. production control group copy the source program and compile the object module to the production libraries.
D. production control group copy the source program to the production libraries and then compile the program.

479. Utilizing audit software to provide code comparisons of production programs is an audit technique used to test program:
A. logic.
B. changes.
C. efficiency.
D. computations.

480. Which of the following BEST describes the process used to solve a year or date problem in a current operating system?
A. Development of a requirements definition document and performance of a feasibility study for all critical business functions
B. Definition of detailed design specifications for applications based on the general design and user specifications
C. Testing, verification, and validation of converted or replaced platforms, applications, databases, and utilities"
D. Authoring of user procedure manuals and training developed during the time that coding begins

481. Which of the following would NOT represent a strong test approach for an organization attempting to solve a year or date problem in a current operating system?
A. A phased approach for testing and validation that includes unit, integration, systems, and acceptance testing.
B. Use of a program logic analyzer to assess and identify key data paths of critical applications in prioritizing conversion and testing efforts.
C. A robust test facility separate from the production environment to avoid contamination or interference with the operation of the productions systems.
D. Use of integrated power tools that support testing of critical application prototypes and establishment of a central repository for requirements coming out of this process.

482. An advantage to setting a stop or freezing point on the design of a new project is to:
A. prevent further changes to a project in process.
B. indicate the point when the design is to be completed.
C. require changes after that point be reviewed and evaluated for cost-effectiveness.
D. provide the project management team with more control over the project design.

483. All of the following system maintenance controls are the responsibility of the user department EXCEPT:
A. initiating requests within its scope of authority.
B. updating systems documentation to reflect all changes.
C. approving changes before implementation, based on the results of testing.
D. approving changes before implementation, based on review of changes to manual procedures.

484. If an application program is modified and proper system maintenance procedures are in place, which of the following should be tested?
A. The integrity of the database.
B. The access controls for the applications programmer
C. The complete program, including any interface systems"
D. The segment of the program containing the revised code

485. An IS auditor performing an application maintenance audit would review a manually prepared log of program changes to determine the:
A. number of authorized program changes.
B. creation date of a current object module.
C. number of program changes actually made.
D. creation date of a current source program.

486. Ideally, stress testing should only be carried out in a:
A. test environment using test data.
B. production environment using live workloads.
C. test environment using live workloads.
D. production environment using test data.

487. When auditing the proposed acquisition of a new computer system, the IS auditor should FIRST establish that:
A. a clear business case has been approved by management.
B. corporate security standards will be met.
C. users will be involved in the implementation plan.
D. the new system will meet all required user functionality.

488. Which of the following is an object-oriented technology characteristic that permits an enhanced degree of security over data?
A. Inheritance
B. Dynamic warehousing
C. Encapsulation
D. Polymorphism

489. The objective of software test designs is to provide the highest likelihood of finding most errors with a minimum of time and effort. Which of the following methods is LEAST likely to meet the design objective?
A. Black box tests which are used to determine that software functions are operational.
B. White box testing predicated on a close examination of procedural detail of all software logical paths.
C. Regression testing in conducting previous tests to ensure that new errors have not been introduced.
D. Software test design that provides for unit, integration, systems, and acceptance testing.

490. All of the following are used as cost estimating techniques during the project planning stage EXCEPT:
A. PERT charts.
B. function points.
C. delphi technique.
D. expert judgment.

491. Which of the following is a dynamic analysis tool for the purpose of testing of software modules?
A. Black box test
B. Desk checking
C. Structured walk-through
D. Design and code

492. The primary purpose of a system test is to:
A. test the generation of the designed control totals.
B. determine that the documentation of the system is accurate.
C. evaluate the system functionally.
D. ensure that the system operators get familiar with the new system.

493. When implementing an application software package, which of the following presents the GREATEST risk?
A. Multiple software versions are not controlled
B. Source programs are not synchronized with object code
C. Parameters are not set correctly
D. Programming errors

494. For the design and programming of an information system, which is the typical sequence in which participation of these individuals should occur?
A. Technical analyst, functional analyst, programmer"
B. Technical analyst, programmer, computer operator"
C. Functional analyst, technical analyst, programmer"
D. Technical analyst, technical support, programmer"

495. In the design of an application system, the IS auditor:
A. should participate to ensure appropriate controls are included in the system.
B. should not get involved because it would affect his/her objectivity.
C. should be able to code some of the control routines that should be included in the programs.
D. defines all the controls that need to be included in the system.

496. Which of the following controls would be MOST effective in ensuring that production source code and object code are synchronized?
A. Release-to-release source and object comparison reports
B. Library control software restricting changes to source code
C. Restricted access to source code and object code
D. Date and time-stamp reviews of source and object code

497. Following the development of an application system, it is determined that several design objectives have not been achieved. This is MOST likely to have been caused by:
A. insufficient user involvement.
B. early dismissal of the project manager.
C. inadequate quality assurance (QA) tools.
D. non-compliance with defined approval points.

498. During a post-implementation review of an enterprise resource management system an IS auditor would MOST likely:
A. review access control configuration.
B. evaluate interface testing.
C. review detailed design documentation.
D. evaluate system testing.

499. An executable module is about to be migrated from the test environment to the production environment. Which of the following controls would MOST likely detect an unauthorized modification to the module?
A. Object code comparison
B. Source code comparison
C. Timestamps
D. Manual inspection

500. The use of object-oriented design and development techniques would MOST likely:
A. facilitate the ability to reuse modules.
B. improve system performance.
C. enhance control effectiveness.
D. speed up the system development life cycle.

501. Once an application's access control process has been established, an IS auditor should verify that:

A. passwords are not shared.
B. files and passwords are encrypted.
C. profile assignments are controlled by the IS manager.
D. there are no functions overlapping in the database administration.

502. Which of the following is a measure of the size of an information system based on the number and complexity of a system's inputs, outputs and files?
A. Program evaluation review technique (PERT)
B. Rapid application development (RAD)
C. Function point analysis (FPA)
D. Critical path method (CPM)

503. The purpose for requiring source code escrow in a contractual agreement is to:
A. ensure the source code is available if the vendor ceases to exist.
B. permit customization of the software to meet specified business requirements.
C. review the source code for adequacy of controls.
D. ensure vendor complies with legal requirements.

504. Which of the following should be performed FIRST when acquiring software?
A. Identify data processing requirements
B. Compare delivery schedules to requirements
C. Negotiate price
D. Establish business needs

505. An IS auditor participating in new software development projects will provide an increased contribution and the organization will experience increased efficiency if:
A. procedures to identify and document needs and requirements of the users are established.
B. procedures to store the developed software are defined in the systems development life cycle phases.
C. development, test and production environments are defined separately from each other.
D. procedures and formal guidelines are established that identify each system development life cycle phase.

506. The purpose of debugging programs is to:
A. generate random data that can be used to test programs before implementing them.
B. protect valid changes from being overwritten by other changes during the programming.
C. define the program development and maintenance costs to be include in the feasibility study.
D. ensure that abnormal terminations and coding flaws are detected and corrected.

507. The difference between white-box testing and black-box testing is that white-box testing:
A. involves the IS auditor.
B. Is performed by an independent programmer team.
C. examines the program internal logical structure.
D. uses the bottom-up approach.

508. Which of the following is the BEST way to achieve good quality software?
A. The primary means is through thorough testing.
B. It is most beneficial to find and quickly correct programming errors.
C. The amount of checking should be dictated by available time and budget.
D. Well-defined processes and structured reviews should be applied throughout the project.

509. Which of the following groups/individuals assume overall direction and responsibility for costs and timetables of systems development life cycle projects?
A. User management
B. Project steering committee
C. Senior management
D. Systems development management

510. Failure to adequately define or manage the requirements for a system can result in a number of risks. The GREATEST risk is:
A. inadequate user involvement.
B. inadequate allocation of resources.
C. requirement change during development.
D. inadequate estimation of the critical path.

511. Which of the following methodologies is appropriate for planning and control activities and resources in a system project?
A. Critical path methodology (CPM)
B. Program evaluation review technique (PERT)
C. Gantt charts
D. Function point analysis

512. One of fourth generation language's (4GL) distinguishing features is portability which means?
A. Environmental independence
B. Workbench concepts (temporary storage, text editing, etc.)"
C. Ability to design screen formats and develop graphical outputs
D. Ability to execute online operations

513. An organization has contracted with a vendor for a turnkey solution for their electronic toll collection system (ETCS). The vendor has provided its proprietary application software as part of the solution. The vendor contract should have a clause for:
A. a backup server to be available to run all ETCS operations with up-to-date data in the event of failure of the original ETCS server.
B. a backup server of a similar configuration as the ETCS server and be loaded with all the relevant software and data.
C. systems staff of the organization to be trained to handle any eventualities.
D. source code of ETCS application software to be kept under an escrow agreement.

514. An IS auditor reviewing systems development in Internet determines that the BEST reason why the system developer is using applets is because:
A. it is sent over the network from the web server.
B. the server does not run the program and the output is not sent over the network.

C. they improve the performance of both the web server and network.
D. it is a JAVA program downloaded through the web browser run on the client machine from the web server.

515. An enterprise has established a steering committee to oversee its e-business program. The steering committee would MOST likely be involved in the:
A. documentation of software requirements.
B. escalation of project issues.
C. design of interface controls between systems.
D. specification of management reports.

516. Which of the following is a control to detect an unauthorized change in a production environment?
A. Deny programmer access to production data.
B. Require change requests to include information about dates, descriptions, cost analysis and anticipated effects.
C. Run a source comparison program between control and current source periodically.
D. Establish procedures for emergency changes.

517. An IS auditor reviewing the design phase of the program development life cycle would seek to determine that:
A. program documentation provides little evidence about the quality of the design approach used during software development.
B. programmers specify the structure and operations of a program that will satisfy a requirement's specification.
C. an object-oriented approach to design is employed when low-level programming languages are used to develop programs.
D. a formal approach to design is not followed when high-level languages are used to develop programs.

518. Which of the following statements pertaining to business process reengineering (BPR) is TRUE?
A. BPR projects cause concern since they often lead to an increased number of people using technology.
B. Significant cost savings are achieved through reduced complexity and volatility in information technology.
C. BPR leads to weaker organizational structures and less accountability.
D. Information protection (IP) is a greater risk as it is more likely to be in conflict with BPR.

519. Which of the following is the FIRST point at which control totals should be implemented in order to prevent the loss of data during the processing cycle?
A. During data preparation
B. In transit to the computer
C. Between related computer runs
D. During the return of the data to the user department

520. Electronic data interchange (EDI) is an application system:
A. that performs based on business needs and activities.
B. that provides utility programs for a limited number of application systems.
C. where applications, transactions and trading partners supported remain static over time.
D. that transmits transactions using sophisticated formats and file definitions.

521. An IS auditor evaluates the test results of a major modification to a production system module that deals with payments computation. The IS auditor finds that 50% of the calculations do not match predetermined totals. Which of the following would MOST likely be the next step in the audit?
A. Designing further tests of the calculations that are in error
B. Identifying other variables that may render the test results inaccurate
C. Examining some of the cases with incorrect calculations to confirm the results
D. Documenting the results and preparing a report of findings, conclusions, and recommendations"

522. The use of expert systems:
A. facilitates consistent and efficient quality decisions.
B. captures the knowledge and experience of industry experts.
C. cannot be used by IS auditors since they deal with system specific controls.
D. improves system efficiency and effectiveness, not personal productivity and performance.

523. A strength of an implemented quality system based on ISO 9001 is that it:
A. guarantees quality solutions to business problems.
B. enhances improvements in software life cycle activities.
C. provides clear answers to questions concerning cost-effectiveness.
D. does not depend on the maturity of the implemented quality system.

524. As a business process reengineering project takes hold it is expected that:
A. business priorities will remain stable.
B. information technologies will not change.
C. the process will improve product, service and profitability.
D. input from clients and customers will no longer be necessary.

525. Functionality is a characteristic associated with evaluating the quality of software products throughout their lifecycle, and is BEST described as the set of attributes that bear on the:
A. existence of a set of functions and their specified properties.
B. ability of the software to be transferred from one environment to another.
C. capability of software to maintain its level of performance under stated conditions.
D. relationship between the level of performance of the software and the amount of resources used.

526. Which of the following statements relating to business process reengineering (BPR) is FALSE?

A. A key factor in a successful BPR is to define the areas to be reviewed and to develop a project plan.
B. An IS auditor is concerned with the key controls that exist in the new business process and not those that once existed.
C. Management is responsible for implementing and monitoring the new process.
D. Advantages of BPR are usually realized when the reengineering process appropriately suits the business and risk.

527. Compensating controls are intended to:
A. reduce the risk of an existing or potential control weakness.
B. predict potential problems before they occur.
C. remedy problems discovered by detective controls.
D. report errors or omissions.

528. Anti-virus software should be used as a:
A. detective control.
B. preventive control.
C. corrective control.
D. compensating control.

529. Which of the following types of data validation and editing are used to determine if a field contains data, and not zeros or blanks?
A. Check digit
B. Existence check
C. Completeness check
D. Reasonableness check

530. Edit controls are considered to be:
A. preventive controls.
B. detective controls.
C. corrective controls.
D. compensating controls.

531. Which of the following provides the ability to verify data values through the stages of application processing?
A. Programmed controls
B. Run-to-run totals
C. Limit checks on calculated amounts
D. Exception reports

532. Which of the following is intended to reduce the amount of lost or duplicated input?
A. Hash totals
B. Check digits
C. Echo checks
D. Transaction codes

533. Software that maintains audit trails for an application system may pose control concerns if:
A. user-IDs are recorded in the audit trail.
B. the details cannot be amended by the security administrator.
C. date time stamps are recorded indicating when actions occurred.
D. users can amend audit trail records when correcting system errors.

534. Which of the following would NOT be used as a completeness check?
A. Parity bits
B. Check digits
C. Batch headers
D. Trailer records

535. Which of the following would an IS auditor do FIRST after the discovery of a Trojan Horse program in the computer system?
A. Investigate the author.
B. Remove any underlying threats.
C. Establish compensating controls.
D. Have the offending code removed.

536. Which of the following database administrator activities is unlikely to be recorded on detective control logs?
A. Deletion of a record
B. Change of a password
C. Disclosure of a password
D. Changes to access rights

537. The editing/validation of data entered from a remote site would be MOST effectively performed at the:
A. central processing site after application program processing.
B. central processing site during application program processing.
C. remote processing site after transmission to the central processing site.
D. remote processing site prior to transmission to the central processing site.

538. Application controls are NOT designed to control the:
A. error log.
B. user.
C. transmittal control.
D. data processing environment.

539. A basic control in a real-time application system is a(n):
A. audit log.
B. console log.
C. terminal log.
D. transaction log.

540. A system user wrote a routine into a payroll application that searched his own payroll number. As a result, if this payroll number should ever fail to appear during the payroll application run, a special routine would generate random numbers that would be placed onto every paycheck. This routine is known as:
A. scavenging.
B. data leakage.
C. piggybacking.
D. a Trojan Horse.

541. Which of the following is NOT an objective of application controls?
A. Detection of the cause of exposure
B. Analysis of the cause of exposure
C. Correction of the cause of exposure
D. Prevention of the cause of exposure

542. In order to prevent the loss of data during the processing cycle, the FIRST point at which control totals should be implemented would be:

A. during data preparation.
B. in transit to the computer.
C. between related computer runs.
D. during the return of the data to the user department.

543. A user connected to a LAN has introduced a newly released virus to the network while copying files from a floppy disk. Which of the following would be the MOST effective control in detecting the existence of the virus?
A. Scan of all floppy disks before use
B. Virus monitor on the network file server
C. Scheduled daily scan of all network drives.
D. Virus monitor on user's personal computer

544. When installing new anti-virus software it is NOT necessary to:
A. periodically update the software.
B. uninstall older versions of the software.
C. install the new software on subsequently purchased machines.
D. install the new software on every machine in the same configuration.

545. Functional acknowledgements are used:
A. as an audit trail for EDI transactions.
B. to functionally describe the IS department.
C. to document user roles and responsibilities.
D. as a functional description of application software.

546. An IS auditor who has discovered unauthorized transactions and fraud during a review of EDI transactions is likely to recommend improving:
A. EDI trading partner agreements.
B. environmental controls and a tested business continuity plan.
C. authentication techniques over sending and receiving messages.
D. general program change, operations and systems support controls.

547. Which of the following is NOT an application control likely to be found in an EDI interface?
A. Hash totals
B. Echo checks
C. Record counts
D. Validity checks

548. Which of the following statements regarding the impact of EDI on internal controls is FALSE?
A. Security will be increasingly important.
B. Errors must be identified and followed up more quickly.
C. Fewer opportunities for review and authorization will exist.
D. IPF management will have increased responsibilities over data center controls.

549. A company disposing of personal computers that once were used to store confidential data should first:
A. demagnetize the hard disk.
B. low level format the hard disk.
C. delete all data contained on the hard disk.
D. defragment the data contained on the hard disk.

550. Procedures for controls over processing include:
A. hash totals.
B. reasonableness checks.
C. online access controls.
D. before and after image reporting.

551. A tax calculation program maintains several hundred tax rates. The BEST control to ensure that tax rates entered into the program are accurate is:
A. independent review of the transaction listing.
B. programmed edit check to prevent entry of invalid data.
C. programmed reasonableness checks with 20% data entry range.
D. visual verification of data entered by the processing department.

552. During an audit of the tape management system at a data center an IS auditor discovered that some parameters are set to bypass or ignore the labels written on tape header records. However, the IS auditor did note that there were effective staging and job set-up procedures. In this situation the IS auditor would conclude that the:
A. tape header should be manually logged and checked by the operators.
B. staging and job set-up procedures are not appropriate compensating controls.
C. staging and job set-up procedures compensate for the tape label control weakness.
D. tape management system is putting processing at risk and that the parameters must be set correctly.

553. An IS auditor reviewing database controls discovered that normal processing changes to the database were handled through a standard set of procedures. However, changes made after normal hours required only an abbreviated number of steps. In this situation what would be considered an adequate set of compensating controls?
A. Use of DBA user account to make the change.
B. Use of normal user account with access to make changes to the database.
C. Use of DBA user account to make changes, logging of changes, as well as before and after image with the changes being reviewed the following day.
D. Use of normal user account to make changes, logging of change, as well as before and after image changes being reviewed the following day.

554. During a review of the accounts payable (A/P) department the IS auditor discovered that user departments failed to review all invoices prior to submitting them for processing. This occurred because user departments were required to submit invoices to A/P within three business days in order to take advantage of vendor discounts. Given this fact, which of the following control reviews should the IS auditor recommend to ensure that invoices were entered correctly and that discounts were correctly taken?
A. Ensure that invoices were reviewed by A/P.

B. Ensure invoice copies are reviewed after they had been submitted to A/P.
C. Ensure that invoice copies were compared to edit reports that show invoice detail and discount information.
D. Ensure that invoice copies were compared to edit reports that show invoice detail and discount information prior to releasing the payment.

555. IS management has recently informed the IS auditor of its decision to disable certain referential integrity controls in the payroll system to provide users with a faster report generator. This will MOST likely increase the risk of:
A. data entry by unauthorized users.
B. a non-existent employee being paid.
C. an employee receiving an illegal raise.
D. duplicate data entry by authorized users.

556. Which of the following message services provides the strongest protection that a specific action has occurred?
A. Proof of delivery
B. Non-repudiation
C. Proof of submission
D. Message origin authentication

557. The primary reason for replacing checks (cheques) with electronic funds transfer (EFT) systems in the accounts payable area is to:
A. make the payment process more efficient.
B. comply with international EFT banking standards.
C. decrease the number of paper-based payment forms.
D. reduce the risk of unauthorized changes to payment transactions.

558. An IS auditor recommends that an initial validation control should be programmed into a credit card transaction capture application. The initial validation process would MOST likely:
A. check that the type of transaction is valid for that card type.
B. verify the format of the number entered then locate it on the database.
C. ensure that the transaction entered is within the cardholder's credit limit.
D. confirm that the card was not shown as lost or stolen on the master file.

559. A proposed transaction processing application is highly complex with many sources of data capture and many different routes for output, in both paper and electronic form. To ensure that transactions are not lost during processing, the IS auditor is MOST likely to recommend the inclusion of:
A. validation controls.
B. internal credibility checks.
C. clerical control procedures.
D. automated systems balancing.

560. A programmer managed to gain access to the production library, modified a program that was then used to update a sensitive table in the payroll database and restored the original program. Which of the following methods is MOST effective to detect these unauthorized changes?
A. Source code comparison
B. Executable code comparison
C. Integrated Test Facilities (ITF)
D. Periodic review of transaction log files

561. Following a recent reorganization of the company's legacy database, it was discovered that certain records were accidentally deleted. Which of the following controls would have MOST effectively detected this occurrence?
A. Range check
B. Table look-ups
C. Run-to-run totals
D. One-for-one checking

562. A company has recently upgraded its legacy purchase system, enabling EDI transmissions. Which of the following controls should be implemented in the EDI interface in order to provide for efficient data mapping?
A. Key verification
B. One-for-one checking
C. Manual recalculations
D. Functional acknowledgements

563. Which of the following would NOT be a specific control aspect in an ongoing applications review of an enterprise resource planning (ERP) package?
A. Authorization of change management procedures
B. ERP functional authorizations match user organizational tasks and responsibilities
C. Risks associated to the implemented authorizations from an internal control point of view
D. Appropriate mapping of the organization's business process controls with the ERP package

564. Sales orders are automatically numbered sequentially at each of a retailer's multiple outlets. Small orders are processed directly at the outlets, with large orders sent to a central production facility. The MOST appropriate control to ensure that all orders transmitted to production are received accurately would be to:
A. send and reconcile transaction counts and totals.
B. have data transmitted back to the local site for comparison.
C. compare data communications protocols with parity checking.
D. track and account for the numerical sequence of sales orders at the production facility.

565. Which of the following is a compensating control to a programmer having access to accounts payable production data?
A. Processing controls such as range checks and logic edits
B. Reviewing accounts payable output reports by data entry
C. Reviewing system-produced reports for checks (cheques) over a stated amount
D. Having the accounts payable supervisor match all checks (cheques) to approved invoices

566. Which of the following was NOT a critical or complete step used to solve an organization's Year 2000 (Y2k) problem?
A. The Y2k problem must have been brought to the attention and addressed by executive management.
B. Y2k solutions should have solved internal problems that would have occurred if software supporting major business applications were not corrected.
C. Testing to determine which applications would have been affected and the changes that were needed were critical to solving the Y2k problem.
D. The IS auditor should have taken an aggressive approach to reviewing management's Y2k strategic goals and planning to ensure the problem has been addressed.

567. The use of a GANTT chart can:
A. assist in project control.
B. highlight project checkpoints.
C. ensure documentation standards.
D. direct the post-implementation review.

568. Which of the following tests performed by an IS auditor would be the MOST effective in determining compliance with an organization's change control procedures?
A. Review software migration records and verify approvals.
B. Identify changes that have occurred and verify approvals.
C. Review change control documentation and verify approvals.
D. Ensure that only appropriate staff can migrate changes into production.

569. Which of the following statements pertaining to program evaluation review technique (PERT) is FALSE?
A. The initial step in designing a PERT network is to define project activities and their relative sequence.
B. An analyst may prepare many diagrams before the PERT network is complete.
C. PERT assumes a perfect knowledge of the times of individual activities.
D. PERT assumes that activities can be started and stopped independently.

570. Given the typical risk ratings below, an IS auditor performing an independent risk rating of critical systems would rate a situation where functions could be performed manually, at a tolerable cost, for an extended period of time as:
A. critical.
B. vital.
C. sensitive.
D. non-critical.

571. A retail company recently installed data warehousing client software in multiple, geographically diverse sites. Due to time zone differences between the sites, updates to the warehouse are not synchronized. This will affect which of the following the MOST?
A. Data availability
B. Data incompleteness
C. Data redundancy
D. Data inaccuracy

572. Which of the following information valuation methods is LEAST likely to be used during a security review?
A. Processing cost
B. Replacement cost
C. Unavailability cost
D. Disclosure cost.

573. A sequence of bits appended to a digital document that is used to secure an e-mail sent through the Internet is called a:
A. digest signature.
B. electronic signature.
C. digital signature.
D. hash signature.

574. Application controls ensure that when inaccurate data is entered into the system, the data is:
A. accepted and processed.
B. accepted and not processed.
C. not accepted and not processed.
D. not accepted and processed.

575. The BEST method of proving the accuracy of an electronically produced tax calculation is by:
A. detailed visual review and analysis of the source code of the calculation programs.
B. recreating program logic using generalized audit software to calculate monthly totals.
C. preparing simulated transactions for processing and comparing to predetermined results.
D. automatic flowcharting and analysis of the source code of the calculation programs.

576. An IS auditor performing a review of application controls would evaluate the:
A. efficiency of the application in meeting the business processes.
B. impact of any control weakness discovered.
C. business processes served by the application.
D. optimization in the use of the applications.

577. In integrated systems, input/output controls must be reviewed in:
A. systems receiving output from other systems.
B. systems sending output to other systems.
C. systems sending and receiving data.
D. interfaces between the two systems.

578. During a business process reengineering (BPR) of a financial institution's teller transaction activities an IS auditor should evaluate:
A. the impact of removed controls.
B. the cost of new controls.
C. BPR project plans.
D. continuous improvement and monitoring plans.

579. Data quality in a data warehouse is achieved by:
A. cleansing.
B. restructuring.
C. ensuring the credibility of source data.
D. transformation.

580. A characteristic of a data warehouse is:
A. object orientation.
B. subject orientation.
C. departmental specific.
D. volatile databases.

581. Which of the following is an implementation risk within the process of decision support systems?
A. Management control
B. Semi-structured dimensions
C. Inability to specify purpose and usage patterns
D. Changes in decision processes

582. Once an organization has finished the business process reengineering (BPR) of all its critical operations, the IS auditor would MOST likely focus on a review of:
A. pre-BPR process flowcharts.
B. post-BPR process flowcharts.
C. BPR project plans.
D. continuous improvement and monitoring plans.

583. All of the following are input controls EXCEPT:
A. batch totals.
B. monetary totals.
C. run-to-run totals.
D. hash totals.

584. An IS auditor performing a review of the electronic funds transfer (EFT) operations of a retailing company would verify that the customers credit limit is verified before funds are transferred by reviewing the EFT:
A. system's interface.
B. switch facility.
C. personal identification number generating procedure.
D. operation back-up procedures.

585. A manufacturer has been purchasing materials and supplies for its business through an e-commerce application. Which of the following should this manufacturer rely on to prove that the transactions were actually made?
A. Reputation
B. Authentication
C. Encryption
D. Non-Repudiation

586. A company uses a bank to process its weekly payroll. Time sheets and payroll adjustment forms (e.g., hourly rate changes, terminations) are filled in and delivered to the bank, which prepares checks (cheques) and reports for distribution. To BEST ensure payroll data accuracy:
A. payroll reports should be compared to input forms.
B. gross payroll should be recalculated manually.
C. checks (cheques) should be compared to input forms.
D. checks (cheques) should be reconciled with output reports.

587. Prices are charged on the basis of a standard master file rate that changes as volume increases. Any exceptions must be manually approved. What is the MOST effective automated control to help ensure that all price exceptions are approved?
A. All amounts are displayed back to the data entry clerk, who must verify them visually.
B. Prices outside the normal range should be entered twice to verify data entry accuracy.
C. The system 'beeps' when price exceptions are entered and prints such occurrences on a report.
D. A second-level password must be entered before a price exception can be processed.

588. A general hardware control that helps to detect data errors when data are communicated from one computer to another is known as a:
A. duplicate check.
B. table look up.
C. validity check.
D. parity check.

589. An independent software program that connects two otherwise separate applications to share computing resources across heterogeneous technologies is known as:
A. middleware.
B. firmware.
C. software.
D. embedded systems.

590. Using test data as part of a comprehensive test of program controls in a continuous online manner is called:
A. test data/deck.
B. base case system evaluation.
C. integrated test facility (ITF).
D. parallel simulation.

591. Which of the following ensures completeness and accuracy of accumulated data?
A. Processing control procedures
B. Data file control procedures
C. Output controls
D. Application controls

592. Access rules and logic are normally included in which of the following documents?
A. Technical reference documentation
B. User manuals
C. Functional design specifications
D. System development methodology documents

593. Which of the following represents the GREATEST potential risk in an EDI environment?
A. Transaction authorization
B. Loss or duplication of EDI transmissions
C. Transmission delay
D. Deletion or manipulation of transactions prior to or after establishment of application controls

594. The need for the modification of validation and editing routines to improve efficiency is normally indicated by:
A. excess overrides.
B. an override activity report.
C. error control and correction.
D. separation of duties.

595. Which of the following application controls indicate failures in input or processing controls?
A. Process control procedures
B. Data file control procedures
C. Output control procedures
D. Data integrity tests

596. Which of the following translates e-mail formats from one network to another so that the message can travel through all the networks?
A. Gateway
B. Protocol converter
C. Front-end communication processor
D. Concentrator/multiplexor

597. In an EDI process, the device which transmits and receives electronic documents is the:
A. communications handler.
B. EDI translator.
C. application interface.
D. EDI interface.

598. A control that detects transmission errors by appending calculated bits onto the end of each segment of data is known as a:
A. reasonableness check.
B. parity check.
C. redundancy check.
D. check digits.

599. Which of the following substantive tests examine the accuracy, completeness, consistency and authorization of data?
A. Data integrity test
B. Relational integrity test
C. Domain integrity test
D. Referential integrity test

600. Which of the following data validation edits is effective in detecting transposition and transcription errors?
A. Range check
B. Check digit
C. Validity check
D. Duplicate check

Answers

1 D	56 B	111 C	166 B	221 A	276 B	331 C	386 A	441 C	496 D	551 A
2 D	57 A	112 C	167 D	222 B	277 A	332 C	387 C	442 D	497 A	552 C
3 D	58 A	113 D	168 B	223 A	278 D	333 B	388 B	443 A	498 A	553 C
4 C	59 A	114 D	169 A	224 C	279 B	334 C	389 A	444 A	499 A	554 D
5 C	60 D	115 C	170 C	225 D	280 C	335 C	390 C	445 B	500 A	555 B
6 C	61 A	116 C	171 A	226 B	281 A	336 A	391 A	446 C	501 B	556 B
7 D	62 D	117 B	172 B	227 D	282 C	337 B	392 A	447 A	502 C	557 A
8 A	63 D	118 B	173 D	228 A	283 D	338 B	393 B	448 B	503 A	558 B
9 D	64 C	119 D	174 A	229 C	284 B	339 D	394 A	449 A	504 A	559 D
10 A	65 B	120 B	175 D	230 B	285 A	340 D	395 B	450 A	505 D	560 D
11 C	66 B	121 A	176 A	231 B	286 B	341 A	396 C	451 C	506 D	561 C
12 B	67 B	122 D	177 D	232 D	287 A	342 D	397 D	452 D	507 C	562 D
13 A	68 C	123 A	178 B	233 D	288 A	343 C	398 B	453 B	508 D	563 D
14 A	69 A	124 B	179 A	234 A	289 A	344 A	399 D	454 B	509 B	564 A
15 B	70 C	125 B	180 C	235 A	290 A	345 B	400 B	455 C	510 C	565 D
16 C	71 B	126 D	181 A	236 C	291 C	346 A	401 A	456 D	511 B	566 B
17 A	72 A	127 A	182 A	237 D	292 A	347 D	402 A	457 C	512 A	567 A
18 C	73 D	128 C	183 A	238 C	293 C	348 C	403 C	458 C	513 D	568 B
19 B	74 A	129 C	184 D	239 C	294 A	349 A	404 A	459 D	514 C	569 C
20 B	75 B	130 C	185 A	240 B	295 B	350 D	405 B	460 D	515 B	570 C
21 C	76 C	131 A	186 D	241 A	296 C	351 A	406 A	461 D	516 C	571 B
22 B	77 B	132 A	187 B	242 A	297 A	352 C	407 C	462 B	517 B	572 A
23 C	78 C	133 D	188 D	243 A	298 C	353 C	408 A	463 C	518 A	573 C
24 A	79 D	134 B	189 B	244 B	299 C	354 C	409 C	464 C	519 A	574 C
25 D	80 D	135 C	190 A	245 C	300 C	355 C	410 C	465 D	520 A	575 C
26 B	81 A	136 C	191 D	246 C	301 C	356 D	411 D	466 B	521 C	576 B
27 C	82 A	137 C	192 D	247 B	302 D	357 B	412 B	467 D	522 A	577 C
28 B	83 B	138 C	193 D	248 C	303 D	358 B	413 A	468 C	523 B	578 A
29 D	84 C	139 B	194 D	249 B	304 B	359 D	414 A	469 D	524 C	579 C
30 C	85 D	140 C	195 C	250 A	305 B	360 C	415 C	470 B	525 A	580 B
31 B	86 B	141 A	196 B	251 A	306 B	361 D	416 C	471 A	526 B	581 C
32 A	87 D	142 C	197 A	252 D	307 B	362 C	417 D	472 A	527 A	582 A
33 A	88 A	143 C	198 A	253 B	308 B	363 A	418 C	473 A	528 B	583 C
34 C	89 B	144 D	199 B	254 B	309 A	364 D	419 C	474 A	529 C	584 A
35 C	90 C	145 C	200 C	255 A	310 A	365 D	420 D	475 C	530 A	585 D
36 A	91 C	146 B	201 A	256 C	311 C	366 D	421 B	476 D	531 B	586 A
37 B	92 B	147 A	202 C	257 A	312 A	367 A	422 D	477 D	532 A	587 D
38 C	93 D	148 B	203 B	258 C	313 C	368 D	423 D	478 D	533 D	588 D
39 B	94 C	149 C	204 D	259 C	314 C	369 C	424 D	479 B	534 B	589 A
40 D	95 D	150 A	205 D	260 A	315 A	370 A	425 C	480 C	535 D	590 B
41 C	96 D	151 D	206 C	261 C	316 A	371 D	426 D	481 D	536 C	591 A
42 A	97 A	152 C	207 A	262 D	317 A	372 B	427 D	482 C	537 D	592 A
43 D	98 C	153 C	208 B	263 B	318 A	373 A	428 A	483 B	538 D	593 A
44 D	99 B	154 A	209 D	264 A	319 A	374 A	429 D	484 C	539 D	594 A
45 A	100 B	155 D	210 D	265 C	320 B	375 C	430 C	485 A	540 D	595 D
46 A	101 D	156 C	211 D	266 A	321 C	376 C	431 C	486 C	541 B	596 A
47 B	102 D	157 C	212 A	267 B	322 B	377 A	432 C	487 A	542 A	597 A
48 B	103 D	158 D	213 A	268 C	323 A	378 D	433 C	488 C	543 C	598 C
49 C	104 A	159 A	214 B	269 C	324 A	379 A	434 B	489 B	544 B	599 A
50 C	105 B	160 D	215 C	270 D	325 A	380 C	435 B	490 A	545 A	600 B
51 A	106 A	161 C	216 D	271 B	326 A	381 D	436 A	491 A	546 C	
52 D	107 B	162 C	217 D	272 A	327 A	382 A	437 B	492 C	547 B	
53 C	108 D	163 B	218 B	273 B	328 A	383 C	438 B	493 C	548 D	
54 A	109 C	164 C	219 D	274 A	329 C	384 A	439 B	494 C	549 A	
55 A	110 A	165 B	220 D	275 D	330 D	385 B	440 C	495 A	550 B	