Questions

1. When planning an IS audit, which of the following factors is least likely to be relevant to the scope of the engagement?

A. The concerns of management for ensuring that controls are sufficient and working properly
B. The amount of controls currently in place
C. The type of business, management culture, and risk tolerance
D. The complexity of the technology used by the business in performing the business functions

2. Which of the following best describes how a CISA should treat guidance from the IS audit standards?

A. IS audit standards are to be treated as guidelines for building binding audit work when applicable.
B. A CISA should provide input to the audit process when defendable audit work is required.
C. IS audit standards are mandatory requirements, unless justification exists for deviating from the standards.
D. IS audit standards are necessary only when regulatory or legal requirements dictate that they must be applied.

3. Which of the following is not a guideline published for giving direction to IS auditors?

A. The IT auditors role in dealing with illegal acts and irregularities
B. Third-party service providers effect on IT controls
C. Auditing IT governance
D. Completion of the audits when your independence is Compromised

4. Which of the following is not part of the IS auditors code of ethics?

A. Serve the interest of the employers in a diligent loyal and honest manner.
B. Maintain the standards of conduct and the appearance of independence through the use of audit information for personal gain.
C. Maintain competency in the interrelated fields of audit and information systems.

D. Use due care to document factual client information on which to base conclusions and recommendations.

5. Due care can best be described as

A. A level of diligence that a prudent and competent person would exercise under a given set of circumstances
B. A level of best effort provided by applying professional judgment
C. A guarantee that no wrong conclusions are made during the course of the audit work
D. Someone with a lesser skill level that provides a similar level of detail or quality of work

6. In a risk-based audit approach, an IS auditor must consider the inherent risk and

A. How to eliminate the risk through an application of controls
B. Whether the risk is material, regardless of managements tolerance for risk
C. The balance of the loss potential and the cost to implement controls
D. Residual risk being higher than the insurance coverage purchased

7. Which of the following is not a definition of a risk type?

A. The susceptibility of a business to make an error that is material where no controls are in place
B. The risk that the controls will not prevent, detect, or correct a risk on a timely basis
C. The risk that the auditors who are testing procedures will not detect an error that could be material
D. The risk that the materiality of the finding will not affect the outcome of the audit report

8. What part of the audited businesses background is least likely to be relevant when assessing risk and planning an IS audit?

A. A mature technology set in place to perform the business processing functions
B. The management structure and culture and their relative depth and knowledge of the business processes
C. The type of business and the appropriate model of transaction processing typically used in this type of business

D. The companys reputation for customer satisfaction and the amount of booked business in the processing cue

9. Which statement best describes the difference between a detective control and a corrective control?

A. Neither control stops errors from occurring. One control type is applied sooner than the other.
B. One control is used to keep errors from resulting in loss, and the other is used to warn of danger.
C. One is used as a reasonableness check, and the other is used to make management aware that an error has occurred.
D. One control is used to identify that an error has occurred and the other fixes the problems before a loss occurs.

10. Which of the following controls is not an example of a pervasive general control?

A. IS security policy
B. Humidity controls in the data center
C. System-wide change control procedures
D. IS strategic direction, mission, and vision statements

11. One of the most important reasons for having the audit organization report to the audit committee of the board is because

A. Their budgets are more easily managed separate from the other budgets of the organization
B. The departments resources cannot easily be redirected and used for other projects
C. The internal audit function is to assist all parts of the organization and no one reporting manager should get priority on this help and support
D. The audit organization must be independent from influence from reporting structures that do not enable them to communicate directly with the audit committee

12. Which of the following is not a method to identify risks?

A. Identify the risks, then determine the likelihood of occurrence and cost of a loss.
B. Identify the threats, their associated vulnerabilities, and the cost of losses.

C. Identify the vulnerabilities and effort to correct, based on the industrys best practices.
D. Seek managements risk tolerance and determine what threats exist that exceed that tolerance.

13. What is the correct formula for annual loss expectancy?

A. Total actual direct losses divided by the number of years it has been experienced
B. Indirect and direct potential loss cost times the number of times it might possibly occur
C. Direct and indirect loss cost estimates times the number of times the loss may occur in a year
D. The overall value of the risk exposure times the probability for all assets divided by the number of years the asset is held

14. When an audit finding is considered material, it means that
A. In terms of all possible risk and management risk tolerance, this finding is significant.
B. It has actual substance in terms of hard assets.

C. It is important to the audit in terms of the audit objectives and findings related to them.
D. Management cares about this kind of finding so it needs to be reported regardless of the risk.

15. Which of the following is not considered an irregularity or illegal act?

A. Recording transactions that did not happen
B. Misusing assets
C. Omitting the effects of fraudulent transactions
D. None of the above

16. When identifying the potential for irregularities, the auditor should Consider

A. If a vacation policy exists that requires fixed periods of vacation to be mandatory
B. How much money is devoted to the payroll
C. Whether the best practices are deployed in the IS environment
D. What kind of firewall is installed at the Internet

17. Some audit managements choose to use the element of surprise to

A. Scare the auditees and to see if there are procedures that can be used as a backup
B. Ensure that staffing is sufficient to manage an audit and daily processing simultaneously
C. Ensure that supervision is appropriate during surprise inspections
D. Ensure that policies and procedures coincide with the actual practices in place

18. Which of the following is not a reason to be concerned about auditor independence?

A. The auditor starts dating the change control librarian.
B. The auditor invests in the business spin-off of the company.
C. The auditor used to manage the same business process at a different company.
D. The auditor is working as consultant for the implementation portion of the project being audited.

19. Control objectives are defined in an audit program to

A. Give the auditor a view of the big picture of what the key control issue are based on the risk and management input
B. Enable the auditor to scope the audit to only those issues identified in the control objective
C. Keep the management from changing the scope of the audit
D. Define what testing steps need to be performed in the program

20. An audit charter serves the following primary purpose:

A. To describe the audit process used by the auditors
B. To document the mission and business plan of the audit department
C. To explain the code of ethics used by the auditor
D. To provide a clear mandate to perform the audit function in terms of authority and responsibilities

21. In order to meet the requirements of audit, evidence sampling must Be

A. Of a 95 percent or higher confidence level, based on repeated pulls of similar sample sizes
B. Sufficient, reliable, relevant, and useful, and supported by the

appropriate analysis
C. Within two standard deviations of the mean for the entire population of the data
D. A random selection of the population in which every item has an equal chance of being selected

22. Audit evidence can take many forms. When determining the types required for an audit, the auditor must consider

A. CAATs, flowcharts, and narratives
B. Interviews, observations, and reperformance testing
C. The best evidence available that is consistent with the importance of the audit objectives
D. Inspection, confirmation, and substantive testing

23. The primary thing to consider when planning for the use of CAATs in an audit program is

A. Whether the sampling error will be at an unacceptable level
B. Whether you can trust the programmer who developed the tools of the CAATs
C. Whether the source and object codes of the programs of the CAATs match
D. The extent of the invasive access necessary to the production environment

24. The most important aspect of drawing conclusions in an audit report is to

A. Prove your initial assumptions were correct.
B. Identify control weakness based on test work performed.
C. Obtain the goals of the audit objectives and to form an opinion on the sufficiency of the control environment.
D. Determine why the client is at risk at the end of each step.

25. Some things to consider when determining what reportable findings should be are

A. How many findings there are and how long the report would be if all findings were included
B. The materiality of the findings in relevance to the audit objectives and managements tolerance for risk
C. How the recommendations will affect the process and future audit work
D. Whether the test samples were sufficient to support the conclusions

26. The primary objective of performing a root cause analysis is to
A. Ask why three times.
B. Perform an analysis that justifies the recommendations.
C. Determine the costs and benefits of the proposed recommendations.
D. Ensure that you are not trying to address symptoms rather than the real problem that needs to be solved.

27. The primary reason for reviewing audit work is to

A. Ensure that the conclusions, testing, and results were performed with due professional care.
B. Ensure that the findings are sufficient to warrant the final report rating.
C. Ensure that all of the work is completed and checked by a supervisor.
D. Ensure that all of the audits are consistent in style and technique.

28. Which criteria would an IS auditor consider to be the most important aspect of an organization IS strategy?

A. It includes a mission statement.
B. It identifies a mechanism for charging for its services.
C. It includes a Web-based e-commerce strategy.
D. It supports the business objectives.

29. From a segregation of duties standpoint, which of the following job functions should be performed by change control personnel?

I. Verifying that the source and object code match before moving code into production
II. Scheduling jobs to run in the production environment
III.Making changes to production code and data when programs fail
IV. Applying operating system patches
A. I only
B. I, II, and III
C. II and IV only
D. I and IV only

30. In a database management environment, which of the following functions should not be performed by the database administrator?

A. Sizing table space and memory allocations

B. Testing queries and consulting on table join limitations
C. Reviewing logs for fraudulent activity or access errors
D. Performing back ups and recovery procedures

31. Many organizations require employees to take a mandatory one to two full weeks of contiguous vacation each year because

A. The organization wants to ensure that their employees quality of life provides for happy employees in the workplace.
B. The organizations wants to ensure that potential errors in process or irregularities in processing are identified by forcing a person into the job function as a replacement periodically.
C. The organization wants to ensure that the benefits provided by the company are fully used to enable full employment of replacement staff as much as possible.
D. The organization wants to ensure that their employees are fully cross-trained and able to take over other functions in case of a major disruption or disaster.

32. Which of the following would be most important in evaluating an IS organizations structure?

I. Human Resource policies that adequately describe job functions and duties sufficiently
II. Organization charts that identify clear reporting and authority lines
III.System configurations that are well documented in the system architecture
IV. Training requirements and provisions for cross training that are documented along with roles and responsibilities
A. I and II only
B. I, II, III, and IV
C. I, II, and IV only
D. II and III only

33. In a review of Human Resource policies in an IS organization, an IS auditor would be most concerned with the absence of

A. Requirements for job rotation on a periodic basis
B. A process for exit interviews to understand the employees perception of management
C. The requirement for employees to sign a form signifying that they have read policies
D. The existence of a termination checklist requiring that keys and company property are obtained and all access permissions are to be revoked upon termination

34. A System Development Life Cycle can be best described as

A. A process used by programmers to document SOP 98-1 compliance
B. A methodology used to guide the process of software creation project management
C. A system design methodology that includes all the steps in problem definition, solution identification, testing, implementation, and maintenance of the solution
D. A process used to manage change control and approval cycles in a development environment

35. What is the primary difference between policies and standards?

A. Policies provide a high-level framework and standards are more dynamic and specific.
B. Policies take longer to write and are harder to implement than standards.
C. Standards require interpretation and must have associated procedures.
D. Policies describe how to do things and standards provide best practices guidance.

36. Which of the following is not a standard?

A. Approved access control methodologies
B. How to request a new account
C. Minimum security baseline for hardening a UNIX server
D. Description of acceptable back up and recovery methods for production data

37. Which of the following are not key considerations when reviewing third-party services agreements?

A. Provisions exist to retain ownership of intellectual property and assets.
B. The lowest price possible is obtained for the service rendered.
C. Business continuity planning and processes are part of the signed agreement.
D. Security and regulatory concerns are identified as risks during negotiations.

38. When evaluating project management, which of the following would you be least concerned in seeing evidenced?

A. Well-defined project scope and objectives
B. Costs identified with the resources allocated to the project
C. Timelines with achievable milestones
D. Sponsorship and approval by business process management

39. When evaluating a change control process, the IS auditor would be most concerned if he or she observed the following:

A. Change control personnel permitting systems programmers to patch operating systems
B. Computer operators running jobs that edit production data
C. Application programmers correcting data errors in production
D. Change control personnel copying code from the production for testing purposes.

40. During the review of a problem management system, it is determined that several problems have been outstanding and unresolved for an excessively long period. Which of the following reasons is most questionable to the IS auditor reviewing the management controls of this process?

A. The problem has been sent to the vendor who will send a fix with the next software release.
B. The problem has been determined to be a user error and has been referred to the business unit for correction and additional training.
C. The problem is intermittent and after researching, remains outstanding until reoccurrence.
D. The problem is seen as a low risk issue and is therefore low on the priority list to be addressed.

41. During the problem analysis and solution design phases of an SDLC methodology, which of the following steps would you be most concerned with finding?

A. Current state analysis and documentation processes
B. Entity relationship diagramming and process flow definitions
C. Pilot testing of planned solutions
D. Gathering of functional requirements from business sponsors

42. What is the primary concern that an IS auditor should consider when reviewing Executive Information Systems (EIS)?

A. Ensure that senior management actually uses the system to monitor the IS organization.
B. Ensure that the information being provided is accurate and timely.
C. Ensure that the information provided fairly summarizes the actual performance of the IS organization so that indicators will be representative of the detailed tracking and monitoring systems.
D. Ensure that MTBFs are kept to a minimum and within acceptable boundaries.

43. SOP 98-1 is an accounting position that needs to be considered by the IS auditor primarily because

A. The AICPA requires all auditors to be aware and comment on this statement of position.
B. Management may be capitalizing software development tasks that should be expensed.
C. Keeping track of development efforts from a capital and expense perspective is indicative of good management of IS organizations.
D. SOP 98-1 tracking systems are required to be interfaced directly to accounting systems and may introduce opportunities for fraudulent accounting.

44. When reviewing the management processes for overseeing budgeting and spending, the IS auditor should be least concerned with which of the following items?

A. Ensuring that all spending is reconciled to a budgeted line item and the variances to budget are explained
B. Ensuring that all of the budgeted money is spent in a budget year

C. Ensuring that expenditures are recorded and reported on budgets to IS organizational management
D. Ensuring that SOP 98-1 provisions are adequately documented and appropriately allocated

45. When evaluating information security management, which of the following are not items the IS auditor would consider commenting on as a potential control weakness?
A. A security program had not been developed using a risk-based approach.
B. The information security officer does not accept responsibility for security decisions in the organization.
C. The use of intrusion detection technologies has not been considered for use in the security program.
D. Account administration processes do not require agreement to acceptable behavior guidelines from all persons requesting accounts.

46. In evaluating business continuity management, what three factors are considered important aspects of the overall management of the program by the IS auditor?

I. Impact to the businesses has been studied and agreed to from the business management as a basis from which to understand the continuity needs.
II. Interactions of all affected processes have been identified so that priorities for recovery can be determined.
III.Recovery tests have been successful and determined to fully meet the needs of the business.
IV. Contracts have been negotiated with hot site vendors, enabling for the immediate declarations of disaster to result in quicker recovery times.
V. The procedures required to manage the business processes without the information systems have been well documented and moved off-site to provide for interim recovery processing.
A. I, II, and III
B. I, III, and IV
C. II, IV, and V
D. I, II, and V

47. Which of the following sets of documentation would an IS auditor expect to find at the off-site facility for business continuity and recovery processes?
I. User manuals and training documentation

II. Current systems configurations
III.Current systems and application code
IV. Operational procedures and required forms and supplies for processing
A. II, III, and IV only
B. I, II, and III only
C. I, III, and IV only
D. All of the above

48. The best way to understand the security configuration of an operating system is to

A. Consult the vendors installation manuals
B. Review the security plan for the system
C. Interview the systems programmer who installed the software
D. Review the system-generated configuration parameters

49. What three things are the most important security controls that should be present when reviewing an operating systems security?

I. The code comes from a trusted source.
II. Audit logging is turned on.
III.Unnecessary services are turned off.
IV. The default passwords are changed.
V. Systems administrators do not have any more access than they need to in order to perform their job.
A. I, II, and III
B. III, IV, and V
C. I, III, and IV
D. I, II, and IV

50. Databases are complex to evaluate from a risk perspective because

A. Access controls for application views, query permissions, field level table access, as well as access to reports and query results must be reviewed to assess the security of data.
B. They can have complex data structures that may be joined through several keys.
C. Data definitions must be maintained in order to understand the data classifications.
D. Data flows and data normalization processes make both table sizing and transaction mapping difficult.

51. In a two-phase commit database transaction, the roll back process is

Initiated

A. When the client and server cannot agree on a communication protocol
B. In multi-tier architectures that need to reject a proxy request
C. When a committed transaction cannot be completed by all participating servers and clients involved
D. When ownership of the session cannot be assured and committed to.

52. Which of the following is not a design consideration to investigate when reviewing security packages?

A. What kind of changes and compromises must occur to existing processes
B. How well the security updates and patches are maintained on the security package
C. What weaknesses and deficiencies cause a security package to be considered
D. What kind of support effort will be required to maintain the product adequately

53. Which of the following is not normally a concern when reviewing the implementation of an operation console system?

A. Whether the expertise to implement the system is being provided by the vendor to backfill existing functions, enabling the existing staff to learn the new systems
B. Whether the scope and goals of the implementation plan are being met in a cost effective and timely manner
C. Whether the KPIs used to manage the business will be improved by the implementation process
D. Understanding how well the console will interface with other operations components and what compatibility issues exist.

54. Which of the following will not be information that you would expect to find documented when evaluating a computer hardware installation project?

A. Procedures for defining the requirements and submitting the requests for proposals and bids
D. How the hardware installation has improved the process throughputs

C. Functional requirements for the hardware based on the business plans and needs
D. Placement and location decisions for equipment installations

55. Which of the following is the most effective method of assessing the controls over the hardware maintenance process?

A. Look at the hardware and assess whether the maintenance is current and that the equipment is well kept.
B. Following the recommended maintenance tasks and maintenance schedules, determine that the procedures are carried out and evidenced as completed by logging and dating the actual maintenance efforts.
C. Identify the required maintenance procedures from the vendors information and ensure that these processes are addressed by the IS organizations procedures.
D. Look at the problem logs and validate whether maintenance processes are determining the mean time between failures when compared to the industry averages.

56. When reviewing voice systems maintenance processes, which of the following is the least critical to the audit objective of ensuring customer satisfaction?

A. Ensuring that as-built drawing modifications are made to the copy of the drawings kept in the office
B. Ensuring that the support staff is knowledgeable and available to perform the necessary maintenance tasks
C. Ensuring that the physical security of the PBX devices is managed properly
D. Ensuring that planning and configurations provide for flexibility with minimal impact to the user base

57. Which of the following should an IS auditor review when performing an assessment of a PBX?
I. Ensure that the dial-in numbers enabling toll-free outbound access are turned off.
II. Ensure that voicemail systems do not enable access to phone lines through hijacking.
III.Ensure that the access codes for the maintenance ports have been changed from the default.
IV. Ensure that outbound toll numbers, such as 900 numbers, are restricted.
V. Ensure that excessive phone usage is flagged and investigated for

fraud.
A. I, II, III, and IV only
B. II, III, and IV only
C. II, III, IV, and V only
D. I, II, III, IV, and V

58. Which of the following would you not expect to find in an Internet DMZ?

A. DNS servers that advertise addresses to the Internet
B. Mail relay servers that receive incoming mail and push outgoing mail
C. Web servers containing content and business logic
D. Proxy servers that authenticate access requests to internal content

59. When reviewing data network architecture, which of the following is not a primary review criteria for the IS auditor?

A. All router access is controlled by secure authentication methods.
B. Network routing enables the efficient flow of the businesses critical traffic.
C. Protocols that are not needed for the business and administration of the network are disabled.
D. VLANs using layer 2 switching techniques are employed to secure the traffic of critical data.

60. In a well-segregated operational environment, which of the following scenarios would you expect to see?

A. Computer operators responding to systems messages and initiating problem tickets for failed jobs
B. Change control librarians making modifications to code only when notified of errors by the application programmers
C. Tape librarians managing print queues and reloading paper for printers as well as loading off-site storage containers with back up tapes
D. Operators assisting system programmers with troubleshooting the operating system by adjusting parameters while the programmers observed the results

61. What are the most important criteria to assess when reviewing job descriptions?

A. The job functions are all defined for the work that needs done,

and training is required
B. Clear authority is established and everyone knows who holds what roles in the organization
C. Vacations are mandated and job rotation is provided for
D. Performance is monitored and raises are based on goals that are defined jointly

62. The primary purpose of key performance indicators are to

A. Give management the ability to make sure that the staff is doing their work
B. Monitor the capacity of the systems equipment and process performance metrics
C. Provide management with a tool to gauge the overall health of the process and to point to potential trouble spots
D. Enable operators to know when things are going wrong and whether the SLA is being met

63. In a media management system review, the IS auditor does not need to concern themselves with
A. Whether the systems catalog accurately reflects the physical library's location of the media
B. Whether the media is accessed by only those individuals with a need to know
C. Whether the media is accurately identified for movement off site for back up purposes
D. Whether the system adequately retires media and provides for its recycling in a secure manner

64. What is the most important aspect of a change control system?

A. All changes are documented and approved.
B. Changes are managed through automated tools, preventing access from people.
C. Copies of production are maintained in case the change fails.
D. Quality is ensured through testing and approval.

65. When emergency changes are identified during a change control review, what should the IS auditor also expect to find?

A. A control weakness, because these actions should not be allowed to occur and it should be reported
B. That the changes were applied as necessary and the related problems tickets were logged

C. Disciplinary actions related to enabling the changes to occur without approval by the system owner
D. A process for notifying the system owner of the changes and all associated actions taken with explanation

66. Which characteristics of a problem management system are important to the IS auditors review?

I. All problems are tracked through to conclusion.
II. All problems are initiated automatically, thus ensuring that the correct data is captured.
III.Escalation processes ensure that problems do not sit unresolved.
IV. All relative IS operation areas have access to the system to review and address the problems.
V. Statistics can be gathered from the system to facilitate the analysis of the IS problems.
A. I, II, III, IV, and V
B. I, III, IV, and V only
C. II, III, IV, and V only
D. I, III, and V only

67. Critical aspects of an SLA review include all of these items except

A. An annual review and revalidation of the business needs
B. Ensuring that the expected services are clearly defined
C. Ensuring that monitoring and escalation procedures are in place
D. Ensuring that the service provider is supplying service to all customers equitably.

68. What is the most important aspect of performing an evaluation of information security controls on a process or system?

A. Ensuring that the best practice control techniques are being utilized properly
B. Understanding the businesses functional requirements of the process to ensure that they can be accomplished
C. Ensuring that the deployed controls work as part of the overall security architecture program
D. Making sure that access is strictly controlled based on a need to know

69. The concept of data integrity implies that

A. Access has not been given to those who do not have a need to

know
B. Data can be accessed by processes when necesssary to support the business function
C. Data has not been altered or modified outside of the expected and approved processing steps
D. Data has not been made available to processes for which the data classification has not been accredited

70. When reviewing security and business risks, it is most important to keep in mind that

A. Business risks are not as important as the security exposures to potential hackers.
B. The customers expectation of privacy should take precedent over the businesses risk tolerance when considering security controls.
C. Data classification should determine the security controls requirements.
D. Some compromise of the security controls to accommodate the businesses risk tolerance is a necessary part of doing business.

71. When evaluating the role of the information security officer, you should be most concerned to find that

A. The security officers role was not well documented as part of the job description.
B. The security officers role is defined as a key decision maker on a new product review committee.
C. Part of the defined role was the accountability for ensuring that the security controls kept any security breaches from occurring.
D. The authority for carrying out the role of a security officer was not explicitly tied to the organizations policy.

72. When reviewing an information system to assess its privacy risks, an IS auditor would consider all of the following except

A. Ensuring that the appropriate consent has been obtained from the customer before the release of sensitive data
B. The business needs for the client data within the processes
C. Proper disclosures to the customer of what the data is used for and how it will be protected
D. The laws and regulations relevant to the industry for privacy controls on customer data

73. While reviewing an information security program, the IS auditor determines that the best practices have not been followed as guidelines for developing the program. Which of the following would be the least important factor to consider when determining the recommendation related to changes for the program?

A. Whether a risk assessment was part of the determination of what the program elements should be
B. Whether the security officer had documented polices and procedures to direct the program
C. Whether the architectural design of the security deployed an indepth state-of-the-art defense
D. Whether any inventory of the existing controls for managing security threats has been done

74. Policy for information security is a primary requirement for establishing control in an IS organization. Which of the following is not a reason why this is the case?

A. A policy establishes the steps required to put security in place.
B. A policy establishes the authority and accountability to get the security job done.
C. A policy sets the expectations for the employees behavior as it relates to security.
D. The policy provides the mandate for putting the security program elements in place.

75. During an IS audit, the IS auditor determines that there is a control weakness due to the lack of available standards. When developing the findings and recommendation for the audit report, which of the following items should not be considered for inclusion as reasons for improving standards in the organization?

A. Standards provide common ground that will increase the efficiency of the operations
B. Standards creation is an industry best practice
C. Standards ensure that individual policy interpretation will not result in the establishment of weaker security overall by lowering the minimum security level
D. Standards provide simplified solutions to problems, enabling leverage of fewer solutions and economies of scale

76. During your review of an information security risk assessment, which of the following elements would you be least concerned with

if no evidence was available to substantiate it?
A. The exercise of risk assessment is reperformed periodically.
B. The threats and vulnerabilities have been determined.
C. The existing controls have been inventoried and assessed for their effectiveness.
D. The risk assessment included a tactical as well as a strategic initiatives assessment.

77. When making a recommendation to establish a product review process that includes the security officer as part of the approval team, what should your strongest argument in the recommendation be?

A. Security that is built into a process as part of the initial design can be seven times cheaper than the cost of implementing it after the product is in production.
B. Plans should be documented and defended to upper management before they are used to implement a new program.
C. The return on investment for products should be assessed prior to starting development so that these returns can be compared to actual gains after the product has been implemented.
D. Plans should be evaluated to ensure that they follow the SDLC methodology standard in the organization and that the methodology has input from information security.

78. When reviewing the identification process used to establish user accounts, what is the most important aspect of the process?

A. All of the relevant information is gathered about the person establishing the identity.
B. Proof is provided to strongly tie the individual presenting themselves as the person for whom the ID is being established.
C. Authorization is obtained for all accounts provided for the individual who is requesting access.
D. The individual is given the opportunity to change their password immediately upon first log in.

79. The security concept of need to know implies all of the following except

A. All access allowed within a permission set or role that is approved on a need to know basis can be viewed, copied, or modified because of the permissions granted.
B. Access is required to perform the assigned functions supporting

the business process.
C. Data owners and their stewards have explicitly determined that the access by this role or person is acceptable.
D. The least amount of privilege necessary to perform the function has been granted to the role or person receiving this permission.

80. An IS auditor would expect to see a defense in-depth approach to security or would recommend that one be adopted for all of the following reasons except

A. It provides several different security mechanisms that increase the difficulty for hackers and intruders due to the increased knowledge required for compromise.
B. More complex security solutions can lead to higher requirements for training and related support costs including audit requirements.
C. Security solutions never completely solve a problem and a defense in-depth approach provides opportunities to address residual risk from one solution with another solution.
D. Costs can be reduced by multiple iterations of solving most of a problem at a minimal cost and then applying another economic solution to address most of the remaining exposure rather than the extensive and expensive application of one solution set.

82. When reviewing role-based access, which of the following parameters should the IS auditor be least concerned with?

A. Business functions and job descriptions provide the input to determine that the accesses defined are sufficient to performing the required tasks.
B. The defined role is applicable to a job function or set of job functions that provides a categorization of need that defines a role.
C. The access permissions of a particular role are reconciled to the actual functions performed on a periodic basis.
D. The establishment of new roles is reviewed and approved by the data owner or steward.

83. During an evaluation of an account administration process, what should an IS auditor be most concerned about finding?

A. Employee terminations that did not result in the closing of computer accounts in a timely fashion
B. Time-of-day restrictions that were not used to limit access to systems
C. Password aging that was not forced on accounts providing access

to the network
D. Accounts, which were supposed to have been suspended from disuse, were not followed up on and deleted

84. When evaluating a single sign on implementation, what single factor adds the most risk and provides concern for the IS auditor in their review?

A. The fact that password resets must be effectively propagated across all systems in some way for single sign on to work properly
B. The issue of systems administrators making changes to a system managed by the single sign on solution, thus putting the accounts out of synchronization
C. The concern that single sign on cannot be effectively achieved unless roles and access needs are defined for all systems on which the user may need to perform their functions
D. The concern that, if compromised, the single sign on access provides a wide range of access where access had been more limited previously

85. When reviewing application design processes for information security controls, which of the following is least likely to be of concern to an IS auditor?

A. The SDLC methodology does not require that security is considered as part of the design criteria.
B. The testing of the application coding does not consider the security requirements identified in the design phase of the systems development process.
C. The sample data used for testing and design is not adequately segregated from the production version of the data.
D. Access permissions of testing and design personnel permits data modification in the test environment.

86. Which of the following are data classification controls?

I. Labeling the removable media containing classified data with the highest level of data sensitivity contained on the media
II. Publishing a policy that defines what data classifications are and how these classifications are to be applied
III.Encrypting data when it is being transmitted across the Internet
IV. Treating all forms of a given data classification as equal in terms of protection requirements
V. Regulatory requirements to protect customer data from disclosure

without prior consent

A. I, II, and IV only
B. I, II, III, and IV only
C. I, II, III, IV, and V
D. I, II, IV, and V only

87. Which of the following is not a password control?

A. Requiring that a password have a minimum length and complexity
B. Encrypting passwords when in transit and at rest
C. Limiting the reuse of passwords through the use of a history file
D. Limiting the number of unique sessions an account can initiate

88. When evaluating strong authentication usage, what should an IS auditor be most concerned with?

A. Ensuring that the two factors are maintained in separate databases to ensure segregation
B. Determining the identification process for each factor and ensuring they are synchronized
C. Reviewing the biometric aspects of strong authentication or acceptable type I and type II error rates
D. Reviewing the physical controls related to the storage of the physical tokens or card stock supplies

89. During a review of a PKI, the IS auditor determines that nonrepudiation cannot be assured for a set of transactions. This most likely means that

A. The certificate authority will not stand behind the validation of the certificate used at the time when the transaction occurred.
B. The users certificate was compromised or was expired when the time the transaction occurred.
C. In reviewing the transaction flow and the security related to the use of the certification, it cannot be conclusively proven that no other person could have possibly been responsible for the transaction that had occurred.
D. The transaction did not go through as anticipated, causing a roll back of the request and negating the signed transaction.

90. Which of the following would an IS auditor expect to see as part of an information security architecture?

I. Evidence of the application of a defense in-depth strategy
II. A risk-based approach to the application and location of the security controls
III.A plan that takes into consideration the business needs and processes
IV. The inclusion of the management and operational controls as well as technical controls
A. I, II, and IV only
B. I, II, III, and IV
C. II and IV only
D. I, II, and III only

91. When performing a review of the host-based security controls, the risk factors that need to be considered are

I. The value of the data contained on the server being secured
II. The functions and tasks required of the server
III.The services that are not needed in the configuration of the server
IV. The operating system type and its vulnerabilities
V. Requirements for encryption related to the services provided by the server
A. I, II, III, IV, and V
B. I, II, and IV only
C. II, III, and V only
D. III, IV, and V only

92. Minimum security baselines (MSBs) and host-based intrusion detection relate to each other in what important aspect?

A. They both are security controls that apply to a device (server) as opposed to network-based controls.
B. Host-based intrusion detection cannot be successfully implemented unless MSBs are adequately maintained on the same device

C.Host-based intrusion detection controls can be used in place of applying MSBs on the same device.
D. They should both be implemented on all servers as part of a robust security architecture.

93. During a network security review, the IS auditor determines that the firewall rule set is incorrectly built to protect the organization from

the risks that are unacceptable to the business. The IS auditor should

A. Immediately notify the IS organization management so corrections can be made to prevent further vulnerability.
B. Discuss the issue with audit management and prepare the findings and a recommendation for their report.
C. Point out the deficiency to the firewall support staff, but note the state the controls were found in at the time of the review.
D. Look at the rest of the controls to ensure that the risk has not been mitigated by some other method before doing anything.

94. What is the primary purpose of a DMZ in network architecture?

A. To provide a place where authentication can occur before enabling access to sensitive data
B. To separate business logic from classified data
C. To provide a neutral zone where transaction requests can be made and honored without affecting the security of either adjacent zone
D. To provide a location for proxy servers and drop off servers to reside without reducing the security of the more secure adjacent network zone

95. When evaluating the encryption used to protect a data transmission over the Internet, which of the following is not a relevant security control?

A. Virtual private network
B. Message digest
C. Digital certificate technologies
D. Secure sockets layer technologies

96. Network intrusion detection and incident response are important parts of any security program. What aspects of an audit review must be included when evaluating these programs?

I. Proper staff levels and training of the staff to react and respond to issues as they present themselves
II. Establishment of a need for using either of these techniques based on the possibility of them actually being required
III.The response time requirements and the ability of the program in place to meet those needs
IV. Managements commitment to the programs and their support for enabling them to function when necessary

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

97. While evaluating third-party connections in an organization, an IS auditor discovers PCAnywhere software resident on a financial workers desktop workstation. Which of the following controls would be seen as the strongest risk mitigate to unauthorized network access in this situation?

A. The software is used only for the remote control of the workstation and access must be authenticated by dial up server controls first.
B. The software may be correctly configured to use network authentication prior to enabling connection through a modem to it.
C. The modem is unplugged and only connected when needed.
D. The software is configured to use dial back and only enables outgoing connections made to known numbers.

98. In an evaluation of virus protection processes, which three controls cover the most risk out of those listed here?

A. Virus protection deployed on every workstation, the blocking of dangerous attachments in all email at the mail servers, and a strong user education program about email viruses
B. Virus protection active on all mail servers, the blocking of dangerous attachments in all email at the mail servers, and a strong user education program about email viruses

C. A strong user education program about email viruses and virus protection that is actively enforced on all workstations, and the blocking of dangerous attachments in all emails at the mail servers
D. Virus protection on all mail servers, the blocking of dangerous attachments in all emails at the mail servers, and virus protection that is actively enforced on all workstations

99. Which of the following is not a control to address the risks associated with social engineering attempts?

A. Asking for a name of person to call back, documenting all of the requests, and validating the person by some means before granting access

B. Adding the physical security responsibilities to the systems support people because they know who needs access to the operations center best
C. Following the rules for access and permissions at all times to avoid opportunities for allowing your guard to be down
D. Developing a healthy suspicion and learn to Òthink like an attacker.

100. What is the most important control concern associated with the logging and monitoring of system or network activity?

A. Ensuring that the information is time synchronized so forensic analysis can be accurately performed
B. The placement of the sensors and protection of the logs from the systems administrators access
C. Developing exception-based reporting and log correlation processes to reduce the amount of log review required
D. Having the staff support available to read through the logs and take action on the results found

101. When evaluating personnel safety controls in an IS operation, what is the best method to use for evaluating its sufficiency?

A. Obtaining copies of the safety and emergency evacuation manual to evidence compliance with the requirement for procedures and documentation
B. Reviewing the records of testing of personal safety devices and their maintenance histories

C. Spot interviewing a few passing IS staff personnel and asking them about their knowledge of the safety measures and procedures
D. Looking for posted evacuation signs and personal safety equipment stored in easily accessible locations to the users

102. What is the most challenging aspect of evaluating physical security controls in an IS organization?

A. Assessing all of the numerous controls and ensuring that each one is managed properly
B. Determining how to assess flexible situations such as security movement and the belongings of VIPs and visitors
C. Being able to obtain proof of the physical security controls effectiveness in preventing or deterring unauthorized acts
D. Touring the physical site and inspecting the controls to ensure

that they are functioning properly

103. In a review of the environmental controls, all of the following are factors that need to be considered except

A. The need for power continuity and the deployment of UPS, batteries, and generators as applicable
B. The maintenance and testing schedule recorded for the fire suppression systems that protect the information systems
C. Personnel evacuation plans and emergency exit routes posted in the operations center
D. Moisture and temperature monitoring and tracking over time

104. An IS auditor is reviewing an organizations contingency planning and recoverability. What is the most important factor to consider for the success of the recovery plan?

A. The plan has identified all of the critical applications required to be covered for the business to survive.
B. The plan is stored off-site.
C. The process is supported by senior management and funded adequately.
D. Back ups are made and moved off-site regularly.

105. When reviewing business impacts of possible disruption scenarios, which of the following criteria should be considered?

I. The likelihood customers will take their business somewhere else and return
II. The potential losses in terms of buildings and equipment
III.The costs associated with redeploying a process to replace the one that is lost
IV. The time it would take to fully recover and return to processing
V. The losses of current business from not meeting existing commitments
A. I, II, and III only
B. I, II, III, IV, and V
C. I, II, III, and V only
D. II, III, IV, and V only

106. An IS auditor determines that external consulting was used to create a recovery plan. Which of the following actions would be most appropriate for the IS auditor to take?

A. Review the costs and contract deliverables for the consulting engagement and assess the adequacy of the contract.
B. Review the methodology used by the firm and assess its appropriateness for the engaged organization.
C. Ensure that the decisions made by the consultant seemed reasonable for the given business and organizational structure.
D. Review the resultant plan and ensure that the business and IS staff were involved in inputting to the final product.

107. When reviewing a business and systems recovery plan, which of the following will be most important to find within the contents of the plan?

A. Simple checklists depicting the steps that need to be taken to affect a recovery
B. Change control information related to what has changed since the last plan update
C. Call trees depicting the recovery teams and their contact information
D. Inventories of hardware and equipment used on-site

108. When reviewing the rationale for recovery options and decisions, which of the following best describes the correct approach for determining the appropriate direction for recovery planning?

A. Planning for a recovery scenario that will not be costly to implement a solution for while still meeting the requirement for a recovery plan
B. Looking at all options for the worst case disaster scenario and picking the solution that is cheapest while still meeting the needs of the business
C. Determining the downtime associated with each recovery option and deciding on the one that will recover the business most quickly
D. Determining the most likely disaster situation and picking the solution that most closely represents the existing processing configuration

109. A business continuity plan should address the recovery of

A. All mission critical computer applications
B. Only those applications related to generating revenue for the business
C. All applications needing recovery within the first 24 hours after a

disruption
D. Applications and processes determined by management to be high priority to management

110. Which of the following application attributes are not relevant when determining the priority order for recovery?

A. The dependency of the critical applications on the output of this particular application
B. The need for the critical applications to be recovered in order to supply input to this application
C. The importance of this application to the business processing needs
D. How much downtime is acceptable to the users of this the application

111. To be effective for disaster recovery, back up copies of computer information should be

A. Stored on-site in the production environment in a fireproof and watertight container
B. A series of incremental back ups labeled and stored properly in the media library
C. Moved off-site as quickly as possible
D. Labeled and cataloged, corresponding to the recovery plans, and sent to the location specified in the plan

112. When evaluating recovery plan documentation, an IS auditor determines that the plans execution will result in the exposure of sensitive data to team members that do not have a need to know for this data. The auditor should

A. Notify management of a material weakness in their final audit report.
B. Recommend that stronger controls be applied to the data management during the recovery process.

C. Focus their efforts on the recoverability of the business processes and note the control weakness for follow-up after the recovery is complete.
D. Review the procedures for compensating controls or manual processes to control access during recovery.

113. Incorporating systems and process changes into a recovery plan is an important part of keeping it relevant and viable for the recovery

of the business process. Which of the following approaches would best meet the needs of the business for ensuring that the changes are appropriately incorporated into the recovery plan documentation?

A. Testing the plan and making changes only as necessary to support the recovery plan process requirements
B. Sending all IS operational changes to the recovery site for inclusion into the recovery documentation
C. Updating the documentation during the periodic review of the plan and incorporating only the relevant changes
D. Making the business unit recovery teams accountable for their respective portions of the recovery plans and related updates

114. When reviewing a systems disaster recovery plan, an IS auditor should look for operations procedures that

A. Have been approved by senior management
B. Follow the procedures used by the IS organization in normal production
C. Describe how to perform the successful operation of the recovered subset of operations
D. Describe all aspects of the current process in detail

115. The declaration of a disaster that invokes a recovery plan process should be

A. Made by the IS organizational manager as soon as the need is identified
B. Documented as a process requiring formal approval and an audit trail to provide evidence of the decision
C. Only done after a repair and restore has been tried and has failed
D. A decision of the business senior management after considering all alternatives, risks, and costs.

116. When reviewing the information recovery procedures, an IS auditor would be least concerned with finding procedures that

A. Lay down the last complete back up and then all of the subsequent incremental back ups that are available
B. Recover all available information from the available back up tapes and move forward with the available information
C. Use hard copy transaction records to return the transactions processing history to the time of disaster from the last available back up

D. Use the best information available and reconcile the inventories to understand the transactions that may have been lost during the disaster or disruption

117. The most important aspect of a recovery plan in the initial hours of a recovery process will be that

A. Call lists and rosters are included for contacting the recovery teams.
B. People have been trained what to do and where to meet to gather and begin recovery without the documented plan.
C. A disaster is declared by management and the EOC is activated as a control center.
D. Testing results have been included to show current recoverability.

118. When reviewing a recovery plan, an IS auditor will be least concerned with plans for managing the press and media by

A. Providing a location away from the immediate action where the media and press can be briefed periodically by the designated spokesperson, and allowed the opportunity to ask questions
B. Providing space for the press and media inside the Emergency Operations Center (EOC) with immediate access to recovery teams
C. Using a policy to tell the media and press as little as possible and denying all rumors with a no comment reply
D. Using a policy that encourages the media to talk to the workers and ask questions as they come in and out of the recovery area as a way to communicate without interfering with management and the recovery process.

119. What is the primary advantage of a hot site over a cold site for recovery planning?

A. There is less work to do at the time of disaster because the site management will prepare it for you.
B. Communications have already been tested, thus providing for a higher probability of success.
C. Testing has occurred at this location in the past, so recovery teams are more familiar with the facilities and how to go about affecting a recovery.
D. Downtime is minimized because equipment does not have to be configured and installed.

120. When reviewing the plans for business operation recovery, an IS auditor would be most concerned to find which of the following unaddressed by the plan?

A. That there is adequate space for accommodating the business staff in an alternate site
B. That computer workstations are available with the latest technology on them with which to perform the business processes
C. That a desktop appropriate for the processing of the recovered business can be made available
D. That connectivity to the EOC is provided for the business desktops for communication

121. When observing the testing of recovery in a dual-site, operational, recovery plan configurations, what should an IS auditor expect to see?

A. Business continues as it normally would with no downtime or disruption
B. Additional equipment being quickly turned on and added to the configuration at the surviving site to accommodate full processing with minimal disruption
C. Two identical sets of processing equipment set up for hot fail over from one site to the other with no impact on the users
D. A procedure that sheds some testing, reporting, and lesser essential functions, allowing for the concentration of the surviving site on the critical business processing to be performed.

122. When reviewing the recovery testing reports to management, an IS auditor will be most concerned if the following is not part of the report:

A. An assessment of the time it takes to recover compared to the management expectations for recovery and a gap analysis of the potential impact that any shortfall may have on managements risk or loss expectations
B. A comprehensive list of all of the problems and the resultant assigned action items
C. A description of the process used to test the recovery, depicting the assumptions made about the recovery situation that was being tested
D. A list of planned goals or milestones with an analysis of the ones that were achieved and those that were not successfully tested.

123. When reviewing a systems development project, what would the most important objective be for an IS auditor?

A. Ensuring that the data security controls are adequate to protect the data.
B. Ensuring that the standards and regulatory commitments are met.
C. Ensuring that the business requirements are satisfied by the project.
D. Ensuring that the quality controls and development methodologies are adhered to.

124. When participating in an application development project, which of the following would not be appropriate activities for an IS auditor?

A. Testing the performance and behavior of the system controls to ensure that they are working properly
B. Attending design and development meetings to monitor progress and provide input on control design options
C. Reviewing reports of progress to management and contributing to their content based on fieldwork and opinions forms from reviewing documentation provided
D. Assisting in the development of controls for application modules and user interfaces

125. When reviewing an application development project that uses a prototyping development methodology, with which of the following would the IS auditor be most concerned?

A. The users are testing the systems before the designs are completely documented.
B. The functional requirements were not documented and agreed to before the prototyping processes began.
C. The documentation of the coding processes and testing criteria were not complete and well referenced.
D. The systems specifications were not signed off on before the development processes were started.

126. In a systems development life cycle, the following process steps occur:

I. Systems Design
II. Feasibility Analysis
III.Systems Testing and Acceptance
IV. Systems Specification Documentation
V. Functional Requirements Definition

VI.Systems Development
What is the natural order of the processes in an SDLC methodology?
A. V, IV, II, I, VI, III
B. V, II, IV, I, VI, III
C. II, IV, V, VI, I, III
D. II, V, I, VI, III, IV

127. Where would be the ideal place for an IS auditor to find the first consideration of security controls?

A. During the design phase of the system development process
B. When determining what the systems specification will need to be
C. When reviewing the functional requirements for the system
D. When testing the system for overall compliance to regulatory, privacy, and security requirements

128. The main difference between a functional requirement and a systems specification is:

A. A functional requirement is a business process need, and a systems specification defines what the system must do to meet that need.
B. Functional requirements address the details of the need form a data perspective, and systems specifications define them from an operational systems perspective.
C. Functional requirements define more of what needs to happen, and systems specifications define how something will happen.
D. Functional requirements define all aspects of the process flow from a business process perspective while systems specifications are more hardware and operating system-specific.

129. Which of the following is not a criterion for an effective feasibility analysis report?

A. An assessment of the proposed solution approach and its viability in the existing business process
B. An assessment of the impact of the new application on the business processes and workflows
C. An analysis of the costs and projected benefits of the application, determining overall benefit or detraction from the business prospects of the overall business strategy
D. An assessment of the systems development methodology proposed for the design of the application

130. If there was a most important place for the quality assurance teams to be involved in the development project, where would that place be?

A. During the testing and code migration from test environments to production-ready code
B. At the beginning of the project to ensure that quality standards are established and understood by all of the development team members
C. During the code development to ensure that processes are followed according to standards and are well documented
D. In the final phases to ensure that all of the quality processes and requirements were met prior to signing off on final acceptance

131. What aspect of the systems development testing process needs to be addressed during the systems design process?

A. The use cases are documented to show how the product is supposed to work when completed.
B. The detailed work plans and process steps are defined so that they can be checked for completeness during testing of the development process.
C. The expectations and outcomes of the development process are defined formally for testing criteria.
D. The project design is checked against the functional requirements.

132. When reviewing a systems design, an IS auditor would be least concerned
to find that which of the following was not considered?

A. The provisions for adequate internal controls and the addressing of regulatory requirements
B. Increased costs and delays in the project deadlines
C. The observance of quality assurance standards and processes
D. The failure to consider environmental and facility needs as part of the design

132. When reviewing a systems development project, an IS auditor observes that the decision has been made to use a purchased vendor package to address the business requirements. The IS auditors should:

A. Discuss the contract and costs with the vendor to ensure that the best deal has been obtained for the organization
B. Review the ROI assumptions and decide whether they are still valid
C. Review the contract for a right to audit clause in the agreement
D. Review the build versus buy recommendation and determine that the costs and benefits are fairly stated in the recommendations made

133. The most important issue with change control during the development of large scale systems is:

A. Managing the versions of code in development to ensure that testing will result in a workable system
B. Ensuring that testing and backout procedures have been provided for each change
C. Ensuring that maintenance and disaster recovery procedures have been documented for each change promoted through the process
D. Tracking which module has been tested with other modules to understand the development progress

134. When reviewing a development effort where third-party programming staff are used, the IS auditor would be most concerned with?

A. Ensuring that they are qualified and knowledgeable about the tools and techniques being used
B. Ensuring that the code is reviewed independently from the third-party staff and ensuring that the ownership rights are maintained within the organization
C. Ensuring that background checks are made for individual third-party staff members to protect the organization from undesirable persons participating in the effort
D. The impact to the cost and timeline estimates originally presented and approved by management

135. An independent quality assurance function should perform all of the following roles except:

A. Ensuring that the development methods and standards are adhered to throughout the process
B. Ensuring that the testing assumptions and approved modules of developed code are aligned to give a final product that meets

the design criteria
C. Reviewing the code to ensure that proper documentation and practices were followed
D. Correcting development deficiencies and resubmitting corrected code through the testing process

136. Which of the following are not considered communication controls?

A. Network traffic monitoring and alert systems
B. Encryption techniques to limit accessibility to traffic in transit
C. Access control devices that limit network access
D. Bandwidth management tools to shift data based on traffic volumes

137. Review of documentation in a systems development review is very important for all of the following reasons except:

A. Training and maintenance efforts require that good documentation be made available for their processes to work effectively
B. Allowing the IS auditor to review the process without actually having to perform code-level reviews of programming efforts
C. Disaster recovery and support processes depend on the quality of the systems and user documentation
D. User effectiveness and production processing depends on the users ability to read and understand the manuals and procedures associated with the application development process

138. In reviewing a vendor solution bidding process during a systems development review, an IS auditor would be most concerned to find that:

A. A vendor solution had been chosen prior to documenting the vendor criteria.
B. The chosen vendors cost was not the lowest of the providers of an acceptable solution.
C. Some of the vendors received more information about the bid request than the others did.
D. Some of the bidders on the vendor list were not capable of responding effectively to the bid based on their business model and the product being requested.

139. Which of the following is not a risk associated with the decision to use a vendor software solution?

A. The risk that the vendor might discontinue support of a product that is mission critical to the business
B. The risk that the costs and contract provisions might adversely impact the business model in the long term
C. The risk that in-house support expertise might be insufficient to adequately address ongoing support and maintenances need of the product
D. The risk that business needs for enhancements and corrections might not be addressed in a timely manner

140. During go-live, security and change management controls are often relaxed to facilitate the implementation. What actions are most appropriate for the IS auditor during this process?

A. Raising concerns about the control deficiencies to business management and suggesting additional controls
B. Waiting until the implementation process is completed and running audit and analysis tools on all transactions during the implementation period
C. Recommending that the risks of reduced controls be accepted and encouraging the process to move into a more controlled phase as quickly as possible
D. Observing the implementation process to understand the extent of control risk that is residual to the process and recommending prudent, additional steps to regain assurance of data integrity

141. During the user testing of the application under development, the IS auditor would be most concerned if he or she found that:

A. Users were accessing the test system from their normal workstations to test the system
B. Production data was being used for testing the system
C. Users were not all trained to the same level of competency for the testing process
D. Interfaces were simulated to provide input to testing and were not actually being represented by live input feeds

142. Corporate governance can best be described as

A. A formal process of implementing controls across the system
B. A process that ensures that all risks have controls associated with them
C. The guiding principles and policies of the organization

D. The process for ensuring that all risks and accountabilities are managed within a business

143. When reviewing a corporate governance system, an IS auditor would be most concerned to find which of the following deficiencies in the process?

A. Gaps in the handing down of the authority necessary to carry out the responsibilities given to unit management
B. Lack of an enforcement and disciplinary process for ensuring that governance and direction is in effect
C. Unit level goals that do not tie directly to the overall mission of the business
D. Incomplete measurement processes for ensuring that the governance direction is carried out

144. What is the most important thing to keep in mind when reviewing a business process for best practice design?

A. The state of the art solutions that are available in the market to perform these business functions
B. The current business model and its overall performance metrics
C. The requirements, business goals, and core competencies defined by the business model
D. What the competition is doing

145. What is the primary role that Key Performance Indicators (KPIs) have in supporting the business process effectiveness?

A. KPIs show when controls may not be working properly.
B. KPIs are used to show that the service levels and business requirements are being met.
C. KPIs show the percentage of a systems uptime and measure the output volumes and speeds.
D. KPIs can be used to draw conclusions about the overall performance of the processes and target variances for follow-up analysis.

146. Management controls are intended to do all of the following except

A. Enable for individual units to establish policies to meet their particular needs.
B. Provide baseline guidance and direction for the entire business culture and style.

C. Set rules for the business processes that are followed by all units and departments.
D. Establish a framework for corporate governance and compliance.

147. When evaluating a business process reengineering project, an IS auditor would be least concerned to find that

A. The staff that actually performs the current processes is not involved with the design of the redesign of the process
B. Management commitment and support is not clearly stated in writing
C. External facilitators are not involved in the analysis and streamlining of the existing processes
D. The scope of the project has not been documented to include all of the existing facets of the business process being examined

148. All of the following are valid ways of measuring customer satisfaction except

A. Sending out questionnaires with the product and asking for feedback on service and performance
B. Using internally generated KPIs to see whether the performance levels are being met or exceeded

C. Measuring repeat business and customer base growth from internal sales and shipping information
D. Measuring the percentage of overall market share this particular business has in the market and its relative growth over time

149. Which of the following are valid reasons for considering an e-business solution in support of the business process?

I. The customer base is widely scattered and remote to the physical business location.
II. The costs of doing business over the Web have been shown to be more efficient for the business than other mechanisms.
III.Everybody is doing it.
IV. The sales department believes that adding functionality to the Web presence will move customers from a browse to a buy online model by making this business option available to them.
V. Real time and immediate support of the business transactions can be best supported by an online transaction model.
A. I, II, and III only

B. I, II, III, and IV only
C. I and II only
D. I, II, and V only

150. When reviewing the design and implementation of risk controls, it will be most important for the IS auditor to determine that

A. All risks are being completely mitigated through the proper application of control mechanisms.
B. Controls prevent risks situations from occurring wherever possible.
C. As many risks as possible are addressed by the control that is being considered for implementation.
D. There is a proper balance between the gravity of the risk and the control measure implemented.

151. Preventive controls are primarily used to
A. Stop a process and notify the operations that an error has occurred
B. Keep an error situation from occurring by recognizing the condition and denying its occurrence

C. Monitor and check error conditions that cannot be easily managed in other ways
D. Address complex ranges of error conditions that can all be addressed by unique prevention condition statements

152. When evaluating the effectiveness of detective controls that are applied to business systems, an IS auditor should consider the following:

I. Whether preventive controls would be more appropriate for the risk type and possible loss scenario
II. The error rate and accuracy of the control in identifying out of bounds conditions
III.The reporting mechanism used to notify management of an error condition
IV. The cost of the control compared to the potential loss to the system
V. Whether the risk is significant enough to warrant any controls at all
A. I, II, and IV only
B. II, III, and IV only
C. IV, V, and II only
D. I, II, III, IV, and V

153. What is the primary difference between a corrective control and a detective control where business processes are concerned?

A. Business processes cannot be corrected in midtransaction, thus making corrective controls less applicable.
B. Best practices typically indicate preventive controls over either of these other two control choices.
C. Corrective controls include detection as part of the way these controls operate and then fix the problem as well.
D. Corrective controls can only fix a small range of errors, while detective controls can detect a far greater scope of possible error conditions.

154. What is the primary difference to keep in mind when evaluating automated and manual controls?

A. Automated controls can operate in an unattended fashion, which requires less testing and monitoring.
B. Manual controls require human interaction to be successfully deployed and must consider human fallibility as part of the accuracy assessment.
C. Potential losses are more difficult to measure with manual controls because the error rates are more difficult to measure.
D. Training and documentation are required for manual controls while automated control do not require such documentation.

155. A risk assessment has determined that the losses that could be potentially incurred with the delivery system of a business may cost up to $10,000 per month. Preventive controls have been recommended that will save the company $7,000 per month, but this control will take three months to implement at a cost of $100,000 and at an ongoing cost of $1,000 per month. The business process has a life span of five years and has been in production for one year. Is the control justified?

A. Yes, the savings over the remaining life of the process would be $315,000, thus justifying the expense.
B. No, the $3,000 per month that will be missed over the life of the process ($144,000) exceeds the cost of the control.
C. Yes, the total cost of the control over the remaining process life is $145,000, while the potential loss without the control would be $480,000.
D. Maybe, if the potential savings over the remaining life of the

process ($315,000) minus the total cost of the control ($145,000) represents a material risk to the companys management ($170,000), management may consider implementing the control and avoiding the risk.

156. The Annual Loss Expectancy (ALE) of a risk without controls is expected to be $35,000 to a business process you are evaluating. You are recommending a control that will save 80 percent of that loss at an annual cost of $20,000 over the life of the process. Is the control justifiable?

A. No, the savings is insignificant and relative to the cost.
B. Yes, 80 percent of the loss amounts to $28,000 per year, which exceeds the annual cost by $8,000 per year.
C. No, ALE is a subjective number and cannot be depended on to make this decision.
D. Maybe, it depends on the managements appetite for risk and loss.

157. What is the most important aspect of risk analysis to keep in mind when reviewing a business process?

A. Senior management must be held accountable for all risks to the business.
B. All risks do not need to be eliminated for a business to be profitable.
C. Risks must be identified and documented in order to perform proper analysis on them.
D. Line management should be involved in the risk analysis because management sees risks daily that others would not recognize.

158. Before making a recommendation to management for the further mitigation of residual risk during a gap analysis in a risk assessment, the following considerations should be decided upon:

I. Managements risk tolerance
II. The best type of control for the risk scenario and the process
III.The gap between the acceptable risk and the residual risk
IV. The state of the art, best practice for the process being reviewed
V. Additional risk mitigation that the proposed control would address for the process under review
A. I, II, III, and V only
B. II, III, and V only
C. II, III, IV, and V only

D. I, II, III, IV, and V

159. What is the primary reason for independent assurance as a requirement for relying on control assessment and evaluation?

A. The review of controls by independent reviewers transfers some amount of the risk to the reviewing body or organization.
B. IS auditors are more knowledgeable about risks and controls and are better suited to review them and determine their effectiveness.
C. Unless the controls are reviewed by an independent and objective review process, the quality of the controls cannot be assured.
D. Management needs to have independent assurance that the risks are managed effectively as part of their corporate governance requirement.

160. What are examples of additional risk to a business that a third party may add to the overall risks of the business?

A. None, a business will actually take on some of the risk and reduce the overall risks to the business.
B. A business will take on the risk that they do not have proper processes in place to perform inefficiently.
C. A business will take on the risks that the contractual commitments do not adequately compensate for poor performance of the third-party vendor.
D. A business will take on the risk that the customers are impacted by missed service level commitments or the misuse of customer information.