

## **DOMAIN 02: GOVERNANCE AND MANAGEMENT OF IT**

- 1. What is the primary purpose of the IT steering committee?**
  - A. Make technical recommendations**
  - B. Identify business issues and objectives**
  - C. Review vendor contracts**
  - D. Specify the IT organizational structure**
  
- 2. Which of these strategies is used in business process re-engineering with an incremental approach?**
  - A. Bottom-up**
  - B. End-state**
  - C. Unconstrained**
  - D. Top-down**
  
- 3. The Software Engineering Institute's Capability Maturity Model (CMM) is best described by which of the following statements?**
  - A. Measurement of resources necessary to ensure a reduction in coding defects**
  - B. Documentation of accomplishments achieved during program development**
  - C. Relationship of application performance to the user's stated requirement**
  - D. Baseline of the current progress or regression**
  
- 4. What would be the area of greatest interest during an audit of a business process Re-engineering (BPR) project?**
  - A. The steering committee approves sufficient controls for fraud detection.**
  - B. Planning methods include Program Evaluation Review Technique (PERT).**
  - C. Risk management planning with alignment of the project to business objectives.**
  - D. Vendor participation including documentation, installation assistance, and training.**

**5. What is the correct sequence for benchmark processes in business process Re-engineering (BPR) projects?**

- A. Plan, research, observes, analyze, adapt and improve**
- B. Research, test, plan, adapt, analyze, improve**
- C. Plan, observes, analyze, improve, test**
- D. Observe, research, analyze, adapt, plan, implement**

**6. Which of the following statements is true concerning the steering committee?**

- A. Steering committee membership is composed of directors from each department.**
- B. The steering committee focuses the agenda on IT issues.**
- C. Absence of a formal charter indicates a lack of controls.**
- D. The steering committee conducts formal management oversight reviews.**

**7. Which of the following is not an advantage of a mature project management office (PMO)?**

- A. Advanced planning assistance**
- B. Master project register**
- C. Coordination of projects across departments**
- D. Independent projects**

**8. The Capability Maturity Model (CMM) contains five levels of achievement. Which of the following answers contains three of the levels in proper sequence?**

- A. Initial, Managed, Repeatable**
- B. Initial, Managed, Defined**
- C. Defined, Managed, Optimized**
- D. Managed, Defined, Repeatable**

**9. The organization's \_\_\_\_\_ is focused on exploiting trends forecast in the next three to five years.**

- A. Strategy**
- B. Long-term planning**

- C. Operational plan**
- D. Managerial plan**

**10. Which of the following is the best example of mandatory controls?**

- A. User account permissions**
- B. Corporate guidelines**
- C. Acceptable use policy**
- D. Government regulation**

**11. During the selection of a BPR project, which of the following is the ideal target with the highest return?**

- A. Marginal process**
- B. Nonworking process**
- C. Working process**
- D. Excluded process**

**12. Who sets the priorities and objectives of the IT balanced scorecard (BSC)?**

- A. Chief Information Officer (CIO)**
- B. Chief Financial Officer (CFO)**
- C. Chief Executive Officer (CEO)**
- D. IT steering committee**

**13. Which of the following business process reengineering (BPR) risks are likely to occur during the design phase?**

- A. Transition risk, skill risk, financial risk**
- B. Management risk, technical risk, HR risk**
- C. Technical risk, detection risk, audit risk**
- D. Scope risk, skill risk, political risk**

**14. Which of the following answers contains the steps for business process re-engineering (BPR) in proper sequence?**

- A. Diagnose, envision, redesign, reconstruct
- B. Evaluate, envision, redesign, reconstruct, review
- C. Envision, initiate, diagnose, redesign, reconstruct, evaluate
- D. Initiate, evaluate, diagnose, reconstruct, review

**15. Which of the following control documents describes a software-improvement process that is characterized by five levels, where each level describes a higher level of maturity?**

- A. ISO 17799
- B. CMM
- C. COSO
- D. COBIT

**16. A network administrator should not share the duties of which of the following roles?**

- A. Quality assurance
- B. Systems administrator
- C. Application programmer
- D. Systems analyst

**17. You are auditing a credit card payment system. Which of the following methods provides the best assurance that information is entered correctly?**

- A. Audit trails
- B. Separation of data entry and computer operator duties
- C. Key verification
- D. Supervisory review

**18. Which level of the CMM is characterized by its capability to measure results by Qualitative measures?**

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

**19. Which of the following is most closely associated with bottom-up policy development?**

- A. Aligns policy with strategy**
- B. Is a very slow process**
- C. Does not address concerns of employees**
- D. Involves risk assessment**

**20. Which of the following offers the best explanation of a balanced score card?**

- A. Used for benchmarking a preferred level of service**
- B. Used to measure the effectiveness of IT services by customers and clients**
- C. Verifies that the organization's strategy and IT services match**
- D. Measures the evaluation of help-desk employees**

**21. Your organization is considering using a new ISP now that the current contract is complete. From an audit perspective, which of the following would be the most important item to review?**

- A. The service level agreement**
- B. The physical securities of the ISP sit**
- C. References from other clients of the ISP**
- D. Background checks of the ISP's employees**

**22. Separation of duties is one way to limit fraud and misuse. Of the four Separation-of-duties controls, which most closely matches this explanation?**

**"This control allows employees access to cash or valuables"?**

- A. Authorization**
- B. Custody**
- C. Recordkeeping**
- D. Reconciliation**

**23. Which of the following job roles can be combined to create the least amount of**

risk or opportunity for malicious acts?

- A. Systems analyst and quality assurance
- B. Computer operator and systems programmer
- C. Security administrator and application programmer
- D. Database administrator and systems analysis

24. You have been asked to perform a new audit assignment. Your first task is to review the organization's strategic plan. Which of the following should be the first item reviewed?

- A. Documentation that details the existing infrastructure
- B. Previous and planned budgets
- C. Organizational charts
- D. The business plan

25. What is the name of the decentralized control method enabling someone to make a decision based on their own options?

- A. Executive
- B. Discretionary
- C. Detailed
- D. Mandatory

26. What is the primary purpose of employee contracts?

- A. Define the relationship as work for hire
- B. Prevent individuals from ever working for competitors
- C. Enforce the requirement to join a union
- D. Specify the terms of employee benefits

27. Which of the following is a governance problem that may occur when projects are funded under the "sponsor pays" method?

- A. Deliverables are determined by the sponsor.
- B. The definition of quality may be insufficient.
- C. The sponsor may not implement the proper controls.
- D. The sponsor may not have enough funding.

**28. Which of the following is not a reason cited in the text that balanced scorecard (BSC) implementations could fail?**

- A. Politics of losing the department budget**
- B. Top management provides full support**
- C. Lack of BSC training and awareness**
- D. Empire building by the department head**

**29. Shadow organization refers to two groups performing similar functions under different departments. What does the presence of a shadow organization indicate?**

- A. Twice the support coverage**
- B. A relationship of trust and proper delegation of authority**
- C. Executive distrust or failure to integrate**
- D. A sponsor who is cooperating as a team player with separation of duties**

**30. Which type of charge-back scheme is notorious for violating separation of duties or for attempting to exceed authority?**

- A. Sponsor pays**
- B. Actual usage billing**
- C. Charge-back**
- D. Budgeted cost**

**31. What is the advantage of using PERT analysis during projects for business process Re-engineering (BPR)?**

- A. It charts a detailed sequence of individual activities.**
- B. It is a critical path methodology.**
- C. It is used to perform root cause analysis.**
- D. It enables the use of decision tree reporting.**

**32. Which statement about the Capability Maturity Model is not true?**

- A. Level 3 provides quantitative measurement of the process output.**

- B. Level 3 processes have published objectives, measurements, and standards that are in effect across departmental boundaries.**
- C. Level 5 provides maximum control in outsourcing because the definition of requirements is very specific.**
- D. Level 5 maturity converts a product into a commodity and allows a company to pay less and demand unquestionable adherence to management's authority.**

**33. Which of the following statements has the best correlation to the definition of strategy?**

- A. Defines the techniques to be used in support of the business objective**
- B. Defines the necessary procedures to accomplish the goal**
- C. Defines guidelines to follow in a recipe for success**
- D. Defines what business we are in for the next three years**

**34. Why is change control considered a governance issue?**

- A. It forces separation of duties to ensure that at least two people agree with the decision.**
- B. Change control increases the number of people employed and therefore provides a valuable economic advantage.**
- C. It allows management to hire less-skilled personnel and still get the same results.**
- D. Proper implementation of governance saves money by reducing the need for change control.**

**35. Which of the following is not considered a control failure?**

- A. Using a policy that lacks a detective mechanism to identify violations**
- B. Modifying an ineffective procedure outside of change control**
- C. Testing to discover how many policy violations have occurred**
- D. Implementing a policy or standard without consequences of failure**

**36. In order for management to effectively monitor the compliance of processes and applications, which of the following would be the MOST ideal?**

- A. A central document repository**
- B. A knowledge management system**
- C. A dashboard**
- D. Benchmarking**



**37. Which of the following would be included in an IS strategic plan?**

- A. Specifications for planned hardware purchases**
- B. Analysis of future business objectives**
- C. Target dates for development projects**
- D. Annual budgetary targets for the IS department**

**38. Which Of the following BEST describes an IT department's strategic planning process?**

- A. The IT department will have either short-range or long range plans depending on the organization's border plans and objectives.**
- B. The IT department's strategic plan must be time- and project oriented, but not so detailed as to address and help determine priorities to meet business needs.**
- C. Long-range planning for the IT department should recognize organizational goals, technological advances and regulatory requirements.**
- D. Short range planning for the IT department does not need to be integrated into the short- range plans of the organization since technological advances will drive the IT department plans much quicker than organizational plans.**

**39. The MOST important responsibility of data security officer in an organization is:**

- A. Recommending and monitoring data security policies.**
- B. Promoting security awareness within the organization.**
- C. Establishing procedures for IT security policies.**
- D. Administering physical and logical access controls.**

**40. What is considered the MOST critical element for the successful implementation of an information security (IS) program?**

- A. An effective enterprise risk management (ERM) framework**
- B. Senior management commitment**
- C. An adequate budgeting process**
- D. Meticulous program planning**

**41. An IS auditor should ensure that IT governance performance measures:**

- A. Evaluate the activities of IT oversight committees.**
- B. Provide strategic IT drivers.**
- C. Adhere to regulatory reporting standards and definitions.**
- D. Evaluate the IT department.**

**42. Which of the following tasks may be performed by the same person in well-controlled information processing computer center?**

- A. Security administration and change management**
- B. Computer operations and system development**
- C. System development and change management**
- D. System development and systems maintenance**

**43. Which of the following is the MOST critical control over database administration?**

- A. Approval of DBA activities**
- B. Segregation of duties**
- C. Review of access logs and activities**
- D. Review of the use of database tools.**

**44. When a complete segregation of duties cannot be achieved in an online system environment, which of the following functions should be separated from the others?**

- A. Origination**
- B. Authorization**
- C. Recording**
- D. Correction**

**45. In a small organization where segregation of duties is not practical, an employee performs the function of computer operator and application programmer. Which of the following controls should the IS auditor recommend?**

- A. Automated logging of changes to development libraries**
- B. Additional staff to provide segregation of duties**
- C. Procedures that verify that only approved program changes are implemented**
- D. Access controls to prevent the operator from making program modifications**

**46. To affix a digital signature to a message, the sender must first create a message digest by applying a cryptographic hashing algorithm against:**

- A. The entire message and thereafter enciphering the message digest using the sender's private key.**
- B. Any arbitrary part of the message and thereafter enciphering the message digest using the sender's private key.**
- C. The entire message and thereafter enciphering the message using the sender's private key.**
- D. The entire message and thereafter enciphering the message along with the message digest using the sender's private key.**

**47. 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.**

**48. Which of the following BEST describes the necessary documentation for an enterprise product Re-engineering (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**

**49. 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.**

**50. Company.com has contracted with 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.**

**51. What is the primary objective of a control self-assessment (CSA) program?**

- A. Enhancement of the audit responsibility**
- B. Elimination of the audit responsibility**
- C. Replacement of the audit responsibility**
- D. Integrity of the audit responsibility**

**52. IS auditors are MOST likely to perform compliance tests of internal controls if, after their initial evaluation of the controls, they conclude that control risks are within the acceptable limits. Is it true or false?**

- A. True**
- B. False**

**53. What type of approach to the development of organizational policies is often driven by risk assessment?**

- A. Bottom-up**
- B. Top-down**

- C. Comprehensive**
- D. Integrated**

**54. Who is accountable for maintaining appropriate security measures over information assets?**

- A. data and systems owners**
- B. data and systems users**
- C. data and systems custodians**
- D. data and systems auditors**

**55. Proper segregation of duties prohibits a system analyst from performing quality-assurance functions. Is it true or false?**

- A. True**
- B. False**

**56. Who is ultimately accountable for the development of an IS security policy?**

- A. The board of directors**
- B. Middle management**
- C. Security administrators**
- D. Network administrators**

**57. A core tenant of an IS strategy is that it must:**

- A. Be inexpensive**
- B. Be protected as sensitive confidential information**
- C. Protect information confidentiality, integrity, and availability**
- D. Support the business objectives of the organization**

**58. If senior management is not committed to strategic planning, how likely is it that a company's implementation of IT will be successful?**

- A. IT cannot be implemented if senior management is not committed to strategic planning.**

- B. More likely.**
- C. Less likely.**
- D. Strategic planning does not affect the success of a company's implementation of IT.**

**59. Which of the following is MOST critical during the business impact assessment phase of business continuity planning?**

- A. End-user involvement**
- B. Senior management involvement**
- C. Security administration involvement**
- D. IS auditing involvement**

**60. What influences decisions regarding criticality of assets?**

- A. The business criticality of the data to be protected**
- B. Internal corporate politics**
- C. The business criticality of the data to be protected, and the scope of the impact upon the organization as a whole**
- D. The business impact analysis**

**61. Any changes in systems assets, such as replacement of hardware, should be immediately recorded within the assets inventory of which of the following? Choose the BEST answer.**

- A. IT strategic plan**
- B. Business continuity plan**
- C. Business impact analysis**
- D. Incident response plan**

**62. Whenever an application is modified, what should be tested to determine the full impact of the change? Choose the BEST answer.**

- A. Interface systems with other applications or systems**
- B. The entire program, including any interface systems with other applications or systems**
- C. All programs, including interface systems with other applications or systems**
- D. Mission-critical functions and any interface systems with other applications or systems**

**63. Function Point Analysis (FPA) provides an estimate of the size of an information system based only on the number and complexity of a system's inputs and outputs. Is it true or false?**

- A. True**
- B. False**

**64. Who assumes ownership of a systems-development project and the resulting system?**

- A. User management**
- B. Project steering committee**
- C. IT management**
- D. Systems developers**

**65. \_\_\_\_\_ (fill in the blank) is/are ultimately accountable for the functionality, reliability, and security within IT governance. Choose the BEST answer.**

- A. data custodians**
- B. The board of directors and executive officers**
- C. IT security administration**
- D. Business unit managers**

**66. What must an IS auditor understand before performing an application audit? Choose the BEST answer.**

- A. The potential business impact of application risks.**
- B. Application risks must first be identified.**
- C. Relative business processes.**
- D. Relevant application risks.**

**67. When are benchmarking partners identified within the benchmarking process?**

- A. In the design stage**
- B. In the testing stage**
- C. In the research stage**
- D. In the development stage**

**68. If an IS auditor finds evidence of risk involved in not implementing proper segregation of duties, such as having the security administrator perform an operations function, what is the auditor's primary responsibility?**

- A. To advise senior management.**
- B. To reassign job functions to eliminate potential fraud.**
- C. To implement compensator controls.**
- D. Segregation of duties is an administrative control not considered by an IS auditor.**

**69. Who is responsible for implementing cost-effective controls in an automated system?**

- A. Security policy administrators**
- B. Business unit management**
- C. Senior management**
- D. Board of directors**

**70. Ensuring that security and control policies support business and IT objectives is a primary objective of:**

- A. An IT security policies audit**
- B. A processing audit**
- C. A software audit**
- D. A vulnerability assessment**

**71. When auditing third-party service providers, an IS auditor should be concerned with which of the following? Choose the BEST answer.**

- A. Ownership of the programs and files**
- B. A statement of due care and confidentiality, and the capability for continued service of the service provider in the event of a disaster**
- C. A statement of due care**
- D. Ownership of programs and files, a statement of due care and confidentiality, and the capability for continued service of the service provider in the event of a disaster**



**72. Proper segregation of duties prevents a computer operator (user) from performing security administration duties. Is it true or false?**

- A. True**
- B. False**

**73. Which of the following is the most fundamental step in preventing virus attacks?**

- A. Adopting and communicating a comprehensive antivirus policy**
- B. Implementing antivirus protection software on users' desktop computers**
- C. Implementing antivirus content checking at all network-to-Internet gateways**
- D. Inoculating systems with antivirus code**

**74. Who is responsible for the overall direction, costs, and timetables for systems-development projects?**

- A. The project sponsor**
- B. The project steering committee**
- C. Senior management**
- D. The project team leader**

**75. Which of the following exploit vulnerabilities to cause loss or damage to the organization and its assets?**

- A. Exposures**
- B. Threats**
- C. Hazards**
- D. Insufficient controls**

**76. Overall business risk for a particular threat can be expressed as:**

- A. A product of the probability and magnitude of the impact if a threat successfully exploits vulnerability.**
- B. The magnitude of the impact should a threat source successfully exploit the vulnerability.**
- C. The likelihood of a given threat source exploiting a given vulnerability.**
- D. The collective judgment of the risk assessment team.**

**77. To ensure that audit resources deliver the best value to the organization, the FIRST step would be to:**

- A. Schedule the audits and monitor the time spent on each audit.**
- B. Train the IS audit staff on current technology used in the company.**
- C. Develop the audit plan on the basis of a detailed risk assessment.**
- D. Monitor progress of audits and initiate cost control measures.**

**78. The vice president of human resources has requested an audit to identify payroll overpayments for the previous year. Which would be the BEST audit technique to use in this situation?**

- A. Test data**
- B. Generalized audit software**
- C. Integrated test facility**
- D. Embedded audit module**

**79. During a security audit of IT processes, an IS auditor found that there were no documented security procedures. The IS auditor should:**

- A. Create the procedures document.**
- B. Terminate the audit.**
- C. Conduct compliance testing.**
- D. Identify and evaluate existing practices.**

**80. In the course of performing a risk analysis, an IS auditor has identified threats and potential impacts. Next, the IS auditor should:**

- A. Identify and assess the risk assessment process used by management.**
- B. Identify information assets and the underlying systems.**
- C. Disclose the threats and impacts to management.**
- D. Identify and evaluate the existing controls.**

**81. When evaluating the collective effect of preventive, detective or corrective controls within a process, an IS auditor should be aware of which of the following?**

- A. The point at which controls are exercised as data flow 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

**82. Which audit technique provides the BEST evidence of the segregation of duties in an IS department?**

- A. Discussion with management
- B. Review of the organization chart
- C. Observation and interviews
- D. Testing of user access rights

**83. An IS auditor interviewing a payroll clerk finds that the answers do not support job descriptions and documented procedures. Under these circumstances, the IS auditor should:**

- A. Conclude that the controls are inadequate.
- B. Expand the scope to include substantive testing.
- C. Place greater reliance on previous audits.
- D. Suspend the audit.

**84. For which of the following applications would rapid recovery be MOST crucial?**

- A. Point-of-sale system
- B. Corporate planning
- C. Regulatory reporting
- D. Departmental charge back

**85. During a change control audit of a production system, an IS auditor finds that the change management process is not formally documented and that some migration procedures failed.**

**What should the IS auditor do next?**

- A. Recommend redesigning the change management process.
- B. Gain more assurance on the findings through root cause analysis.
- C. Recommend that program migration be stopped until the change process is documented.
- D. Document the finding and present it to management.

**86. Corrective action has been taken by an auditee immediately after the identification of a reportable finding. The auditor should:**

- A. Include the finding in the final report, because the IS auditor is responsible for an accurate report of all findings.**
- B. Not include the finding in the final report, because the audit report should include only unresolved findings.**
- C. Not include the finding in the final report, because corrective action can be verified by the IS auditor during the audit.**
- D. Include the finding in the closing meeting for discussion purposes only.**

**87. The MOST likely effect of the lack of senior management commitment to IT strategic planning is:**

- A. A lack of investment in technology.**
- B. A lack of a methodology for systems development.**
- C. Technology not aligning with the organization's objectives.**
- D. An absence of control over technology contracts.**

**88. Which of the following is a function of an IS steering committee?**

- A. Monitoring vendor-controlled change control and testing**
- B. Ensuring a separation of duties within the information's processing environment**
- C. Approving and monitoring major projects, the status of IS plans and budgets**
- D. Liaising between the IS department and the end users**

**89. Involvement of senior management is MOST important in the development of:**

- A. Strategic plans.**
- B. IS policies.**
- C. IS procedures.**
- D. Standards and guidelines.**

**90. Effective IT governance will ensure that the IT plan is consistent with the organizations :**

- A. Business plan.**
- B. Audit plan.**
- C. Security plan.**
- D. Investment plan.**

**91. Establishing the level of acceptable risk is the responsibility of:**

- A. Quality assurance management.**
- B. Senior business management.**
- C. The chief information officer.**
- D. The chief security officer.**

**92. IT governance is PRIMARILY the responsibility of the:**

- A. Chief Executive Officer.**
- B. Board of directors.**
- C. IT steering committee.**
- D. Audit committee.**

**93. As an outcome of information security governance, strategic alignment provides:**

- A. Security requirements driven by enterprise requirements.**
- B. Baseline security following best practices.**
- C. Institutionalized and commoditized solutions.**
- D. An understanding of risk exposure.**

**94. Which of the following IT governance best practices improves strategic alignment?**

- A. Supplier and partner risks are managed.**
- B. Knowledge base on customers, products, markets and processes is in place.**
- C. A structure is provided that facilitates the creation and sharing of business information.**
- D. Top management mediates between the imperatives of business and technology.**

**95. Effective IT governance requires organizational structures and processes to ensure that:**

- A. The organization's strategies and objectives extend the IT strategy.**
- B. The business strategy is derived from an IT strategy.**
- C. IT governance is separate and distinct from the overall governance.**
- D. The IT strategy extends the organization's strategies and objectives.**

**96. Which of the following is the MOST important element for the successful implementation of IT governance?**

- A. Implementing an IT scorecard**
- B. Identifying organizational strategies**
- C. Performing a risk assessment**
- D. Creating a formal security policy**

**97. The MAJOR consideration for an IS auditor reviewing an organization's IT project portfolio is the:**

- A. IT budget.**
- B. Existing IT environment.**
- C. Business plan.**
- D. Investment plan.**

**98. When implementing an IT governance framework in an organization the MOST important objective is:**

- A. IT alignment with the business.**
- B. Accountability.**
- C. Value realization with IT.**
- D. Enhancing the return on IT investments.**

**99. The ultimate purpose of IT governance is to:**

- A. Encourage optimal use of IT.**
- B. Reduce IT costs.**
- C. Decentralize IT resources across the organization.**
- D. Centralize control of IT.**

**100. What is the lowest level of the IT governance maturity model where an IT balanced scorecard exists?**

- A. Repeatable but Intuitive**
- B. Defined**
- C. Managed and Measurable**
- D. Optimized**

**101. Responsibility for the governance of IT should rest with the:**

- A. IT strategy committee.**
- B. Chief Information Officer (CIO).**
- C. Audit committee.**
- D. Board of directors.**

**102. An IS auditor identifies that reports on product profitability produced by an organization's finance and marketing departments give different results. Further investigation reveals that the product definition being used by the two departments is different. What should the IS auditor recommend?**

- A. User acceptance testing (UAT) occur for all reports before release into production**
- B. Organizational data governance practices be put in place**
- C. Standard software tools be used for report development**
- D. Management sign-off on requirements for new reports**

**103. When an employee is terminated from service, the MOST important action is to:**

- A. Hand over all of the employee's files to another designated employee.**
- B. Complete a backup of the employee's work.**
- C. Notify other employees of the termination.**
- D. Disable the employee's logical access.**

**104. Many organizations require an employee to take a mandatory vacation (holiday) of a week or more to:**

- A. Ensure the employee maintains a good 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.**

**105. Which of the following controls would an IS auditor look for in an environment where duties cannot be appropriately segregated?**

- A. Overlapping controls**
- B. Boundary controls**
- C. Access controls**
- D. Compensating controls**

**106. To gain an understanding of the effectiveness of an organization's planning and management of investments in IT assets, an IS auditor should review the:**

- A. Enterprise data model.**
- B. IT balanced scorecard (BSC).**
- C. IT organizational structure.**
- D. Historical financial statements.**

**107. Which of the following goals would you expect to find 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 for the product offered.**

**108. Which of the following would an IS auditor consider to be the MOST important when evaluating an organization's IS strategy? That it:**



- A. Has been approved by line management.**
- B. Does not vary from the IS department's preliminary budget.**
- C. Complies with procurement procedures.**
- D. Supports the business objectives of the organization.**

**109. An IS auditor reviewing an organization's IT strategic plan should FIRST review:**

- A. The existing IT environment.**
- B. The business plan.**
- C. The present IT budget.**
- D. Current technology trends.**

**110. In an organization, the responsibilities for IT security are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed. This represents which level of ranking in the information security governance maturity model?**

- A. Optimized**
- B. Managed**
- C. Defined**
- D. Repeatable**

**111. To aid management in achieving IT and business alignment, an IS auditor should recommend the use of:**

- A. Control self-assessments.**
- B. A business impact analysis.**
- C. An IT balanced scorecard.**
- D. Business process re-engineering.**

**112. When reviewing the IT strategic planning process, an IS auditor should ensure that the plan:**

- A. Incorporates state of the art technology.**
- B. Addresses the required operational controls.**
- C. Articulates the IT mission and vision.**
- D. Specifies project management practices.**

**113. The advantage of a bottom-up approach to the development of organizational policies is that the policies:**

- A. Are developed for the organization as a whole.**
- B. Are more likely to be derived as a result of a risk assessment.**
- C. Will not conflict with overall corporate policy.**
- D. Ensure consistency across the organization.**

**114. The rate of change in technology increases the importance of:**

- A. Outsourcing the IS function.**
- B. Implementing and enforcing good processes.**
- C. Hiring personnel willing to make a career within the organization.**
- D. Meeting user requirements.**

**115. A top-down approach to the development of operational policies will help ensure that:**

- A. They are consistent across the organization.**
- B. They are implemented as a part of risk assessment.**
- C. Compliance with all policies.**
- D. They are reviewed periodically.**

**116. Which of the following would MOST likely indicate that a customer data warehouse should remain in-house rather than be outsourced to an offshore operation?**

- A. Time zone differences could impede communications between IT teams.**
- B. Telecommunications cost could be much higher in the first year.**
- C. Privacy laws could prevent cross-border flow of information.**
- D. Software development may require more detailed specifications.**