

1. Correct answer: B

The purpose of the steering committee is to bring the awareness of business issues and objectives to IT management

2. Correct answer: A

The incremental approach uses bottom-up modeling of the existing process. Overall gains tend to be small because this method focuses so hard on current processes

3. Correct answer: D

The Capability Maturity Model provides a baseline measurement of process maturity. The CMM begins with no process defined and progresses through five phases of documentation and controls. The fifth phase represents the highest level of maturity.

4. Correct answer: C

The steps are as follows: Visualize a need (envision); the sponsor sets BPR goals (initiate) document existing processes (diagnose); develop the new process (redesign); implement changes (reconstruct); provide post monitoring to improve the results (evaluate)

5. Correct answer: A

The business process re-engineering sequence is to plan for change, research possible implications, observe the current process, analyze potential opportunities for improvement and verify key performance indicators, adapt to the new/updated process, and work to improve the results.

6. Correct answer: C

The steering committee should be authorized by a formal charter. The lack of a steering committee indicates that IT is not governed by formal alignment to business objectives. The technology investment is not properly managed as an investment portfolio should be managed. The purpose of the steering committee is to convey business issues that IT should consider and objectives to fulfill. Membership of individuals on the steering committee should be formally designated.

7. Correct answer: D

The PMO provides governance to coordinate and oversee all projects across the organization This provides historical data for estimating, and success and failure criteria. PMO provides maturity to the process of managing projects.

8. Correct answer: C

The five levels of achievement in the Capability Maturity Model (CMM) are level 1—Initial level 2—Repeatable, level 3—Defined, level 4—Managed, and level 5—Optimized

9. Correct answer: A

A strategy provides answers to “what business” the organization wants to be in. This strategy is based on scenario planning and forecasting to alter the organization’s structure, priorities, locations, and staffing. It could result in the decision to buy, sell, or consolidate.

10. Correct answer: D

A government regulation is a mandatory control that forces compliance. Mandatory controls are the strongest type of control. Permission is explicit or it must be denied.

11. Correct answer: B

Nonworking processes, whether manual or automated, are usually the highest priority if their business value can be justified

12. Correct answer: C

The BSC is intended to provide a unifying approach on how the CEO expects the business process to interact across the organization. IT’s scorecard is a subset of the CEO’s overall enterprise scorecard. The BSC’s objective is to break down management barriers and convert department budgets into an entire cross-function work flow. The CEO or COO will control decisions to eliminate waste and prevent self-directed decisions by department managers.

13. Correct answer: D

The primary risks during the BPR design phase are improper scope, lack of necessary skills, political resistance, and a failure by management to support the project.

14. Correct answer: C

The steps are as follows: Visualize a need (envision); the sponsor sets BPR goals (initiate) document existing processes (diagnose); develop the new process (redesign); implement changes (reconstruct); provide post monitoring to improve the results (evaluate)

15. Correct answer: B

The capability maturity model (CMM) specifies five levels of control for software maturity levels. Answer A is incorrect because ISO 17799 is a comprehensive set of controls designed to gauge best practices in information security. Answer C is incorrect because COSO was designed to help prevent and detect fraud in financial reports. Answer D is incorrect because COBIT was designed to aid in the development of good IT process and policies.

16. Correct answer: C

A network administrator should not have programming responsibilities. Answers A, B, and D are all duties that an administrator can hold, but the network administrator might have end-user responsibilities, aid in the system administration, and help in the early phases of design

17. Correct answer: C

Key verification would provide the highest level of confidence. Answer A is incorrect because audit trails would provide details of the entered activities but would not improve accuracy. Answer B is incorrect because separating job roles would be an additional control but would not add any accuracy to the information that was entered incorrectly. Answer D is incorrect because supervisory review is a detective and compensating control, but is not the best answer.

18. Correct answer: C

Level 3 of the capability maturity model is considered the defined level. Level 3 is characterized by its capability to use qualitative measurements. Answers A, B, and D are incorrect because the levels do not feature qualitative measurement.

19. Correct answer: D

Bottom-up policy development addresses the concerns of operational employees because it starts with their input and concerns, and examines risk. Answers A, B, and C are incorrect because all these items are tied to top-down policy development. A top-down approach aligns with company policy, is a slow process, and might not fully address the concerns of employees

20. Correct answer: C

A balanced score card is used to match the organization's information technology to the strategy of the organization. Answer A is incorrect because it is not used for benchmarking, answer B is incorrect because it is not used to measure effectiveness, and answer D is incorrect because it is not used to evaluate help-desk employees

21. Correct answer: A

Anytime an outsourcing provider will provide a time-sensitive process, such as ISP services, an SLA is one way to obtain a guarantee of the level of service the outsourcing partner is agreeing to provide. The SLA should specify the uptime, response time, and maximum outage time they are agreeing to. Answer B is incorrect because physical security is important, but it is not the most important, in this case. Answers C and D are incorrect because neither would serve as an adequate measure for an independent evaluation of the ISP's service capability

22. Correct answer: B

Custody is the access to cash, merchandise, or inventories. Answer A is incorrect because authorization describes verifying cash, approving purchases, and approving changes. Answer C is incorrect because recordkeeping deals with preparing receipts, maintaining records, and posting payments. Answer D is incorrect because reconciliation deals with comparing dollar amounts, counts, reports, and payroll summaries

23. Correct answer: D

Database administrator and systems analyst are two roles that ISACA believes can be combined. Answers A, B, and C are incorrect because none of these positions should be combined. The auditor should understand how the combination of certain roles increases risk. As an example, a system analyst should be discouraged from performing the duties of someone in a quality assurance role. If these roles are combined, quality-assurance levels could be compromised if strong compensating controls are not being used.

24. Correct answer: D

Before auditors can begin any technical duties, they must understand the environment in which they are working. The best way to do that is to review the business plan, which details the goals of the organization. Only after the business plan has been reviewed should the other items listed be reviewed. Therefore, answers A, B, and C are incorrect.

25. Correct answer: B

Discretionary control is usually the choice selected in business. Its weakness is that someone decides rather than uses a formal centralized authority. Auditors should investigate how decisions are made and who makes each decision. This is usually a good place to look for control failures.

26. Correct answer: A

Employee contracts provide evidence of the work relationship: that the employee is providing “work for hire” to the company. All of the employee’s discoveries and development become the intellectual property of the employer

27. Correct answer: C

The auditor needs to recognize that the sponsor may attempt to exceed their authority or fail to implement proper controls. Project scope should be controlled and verified to include separation of duties with preventative, detective, and corrective controls. It would be a failure in governance to allow a project to occur otherwise.

28. Correct answer: B

The major goal of using a BSC is to ensure that everyone under the CEO's COO's and CFO's management understands a primary unified direction. BSC is designed to kill empire building by division heads, vice presidents, and department-level directors. The number one deliverable is cutting waste by eliminating self-directed decisions below the C-level and returning control to the CEO or highest executive.

29. Correct answer: C

Shadow organizations indicate an integration failure caused by executive distrust or similar conflict. This creates additional conflict with inefficiencies of scale. Problems include conflicting strategies, and the sponsor violating separation of duties or exceeding their normal authority. Shadow organizations are known for duplication of effort, creating a high combined cost to the organization

30. Correct answer: A

Sponsor pays is notorious for problems of exceeding authority, violating separation of duties, and failing to implement all the governance controls. Sponsors tend to pay for only what they want. Exceptionally good sponsors consider everyone's needs ahead of their own agenda.

31. Correct answer: B

PERT analysis shows the critical path to illustrate the minimum specific tasks necessary to complete the project's objective. The CPM technique is a valuable tool for demonstrating what must be accomplished versus what was requested. High-dependency tasks get performed, while low-dependency tasks may be cancelled from the project

32. Correct answer: A

Qualitative measurement (opinion based) occurs at level 3, and quantitative measurement (counting based) is at level 4. Level 5 effectively converts the product into a commodity with the intent to squeeze out every last percentile of improvement. All workers are expected to just do what they are told and have no authority. At level 5, the company has the most control and may decide to outsource with lower-paid workers

33. Correct answer: D

Strategy defines the primary business we are in for the next three to five years. Using this information, the business can develop or adopt supporting standards and then create low-level procedures to accomplish the strategic objective.

34. Correct answer: A

Change control is a foundation of good governance. The purpose is to reduce question-able decisions. Benefits of change control include no longer wasting resources on low-profit tasks and preventing failure by reducing the risk (risk mitigation)

35. Correct answer: C

All of the available options except testing indicate that a control failure was present. The minimum effective control must include a preventative, detective, and corrective action

36. Correct answer: C

A dashboard provides a set of information to illustrate compliance of the processes, application and configurable elements and keeps the enterprise on course. A central document repository provides a great deal of data, but not necessarily the specific information that would be useful for monitoring and compliance. A knowledge management system provides valuable information but is generally not used by management for compliance purposes. Bench marking provides information to help management adapt the organization, in a timely manner, according to trends and environment

37. Correct answer: B

IS strategic plans must address the needs of the business and meet future business objectives, Hardware purchases may be outlined but not specific and neither budget targets nor development projects are relevant choices.

38. Correct answer: C

Long-range planning for the IT department should recognize organizational goals, technological advances and regulatory requirements. Typically, the IT department will have long-range and short range plans that are consistent and integrated with the organization's plans. These plans must be time and project-oriented and address the organization's broader plans towards attaining its goals.

39. Correct answer: A

A data security officer's prime responsibility is recommending and monitoring data security policies. Promoting security awareness within the organization is one of the responsibilities of a data security officer, but it is not as important as recommending and monitoring data security policies. The IT department, not the data security officer, is responsible for establishing procedures for IT security policies recommended by the data security officer and for the administration of physical and logical access controls

40. Correct answer: B

Commitment from senior management provides the basis to achieve success in implementing an information security program. An effective ERM framework is not a key success factor for an IS program. Although an effective IS budgeting process will contribute to success, senior management commitment is the key ingredient. Program planning is important, but will not be sufficient without senior management commitment

41. Correct answer: A

Evaluating the activities of boards and committees providing oversight is an important aspect of governance and should be measured

42. Correct answer: D

It is common for system development and maintenance to be undertaken by the same person. In both, the programmer requires access to the source code in the development environment, but should not be allowed access in the production environment

43. Correct answer: B

Segregation of duties will prevent combination of conflicting function. This is a preventive control and it is the most critical control *over* database administration

44. Correct answer: B

Authorization should be separated from all aspects of record keeping (origination, recording and correction). Such a separation enhances the ability to detect the recording of unauthorized transactions

45. Correct answer: C

This is the only practical one that has an impact. The IS auditor should recommend processes that detect changes to production source and object code, such as code comparisons, so the changes can be reviewed by a third party on a regular basis.

46. Correct answer: A

A digital signature is a cryptographic method that ensures data integrity, authentication of the message, and non-repudiation

47. Correct answer: C

A digital signature through the private cryptographic key authenticates a transmission from a sender through the private cryptographic key. It is a string of bits that uniquely represent another string of bits, a digital document. An electronic signature refers to the string of bits that digitally represents a handwritten signature captured by a computer system when a human applies it on an electronic pen pad, connected to the system.

48. Correct answer: C

A global enterprise product reengineering (EPR) software package can be applied to a business to replace, simplify and improve the quality of IS processing. Documentation is intended to help understand how, why and which solutions that have been selected and implemented, and therefore must be specific to the project. Documentation is also intended to support quality assurance and must be comprehensive



49. Correct answer: C

A policy statement reflects the intent and support provided by executive management for proper security and establishes a starting point for developing the security program.

50. Correct answer: B

A quality plan is an essential element of all projects. It is critical that the contracted supplier be required to produce such a plan. The quality plan for the proposed development contract should be comprehensive and encompass all phases of the development and include which business functions will be included and when. Acceptance is normally managed by the user area, since they must be satisfied that the new system will meet their requirements. If the system is large, a phased-in approach to implementing the application is a reasonable approach. Prototyping is a valid method of ensuring that the system will meet business requirements.

51. Correct answer: A

Audit responsibility enhancement is an objective of a control self-assessment (CSA) program

52. Correct answer: A

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. Think of it this way: If any reliance is placed on internal controls, that reliance must be validated through compliance testing. High control risk results in little reliance on internal controls, which results in additional substantive testing.

53. Correct answer: A

Bottom-up approach to the development of organizational policies is often driven by risk assessment

54. Correct answer: A

Data and systems owners are accountable for maintaining appropriate security measures over information assets

55. Correct answer: A

Proper segregation of duties prohibits a system analyst from performing quality-assurance functions

56. Correct answer: A

The board of directors is ultimately accountable for the development of an IS security policy

57. Correct answer: D

Above all else, an IS strategy must support the business objectives of the organization.



58. Correct answer: C

A company's implementation of IT will be less likely to succeed if senior management is not committed to strategic planning

59. Correct answer: A

End-user involvement is critical during the business impact assessment phase of business continuity planning

60. Correct answer: C

Criticality of assets is often influenced by the business criticality of the data to be protected and by the scope of the impact upon the organization as a whole. For example, the loss of a network backbone creates a much greater impact on the organization as a whole than the loss of data on a typical user's workstation.

61. Correct answer: B

Any changes in systems assets, such as replacement of hardware, should be immediately recorded within the assets inventory of a business continuity plan

62. Correct answer: B

Whenever an application is modified, the entire program, including any interface systems with other applications or systems, should be tested to determine the full impact of the change

63. Correct answer: B

Function point analysis (FPA) provides an estimate of the size of an information system based on the number and complexity of a system's inputs, outputs, and files.

64. Correct answer: A

User management assumes ownership of a systems-development project and the resulting system

65. Correct answer: B

The board of directors and executive officers are ultimately accountable for the functionality, reliability, and security within IT governance

66. Correct answer: C

An IS auditor must first understand relative business processes before performing an application audit

67. Correct answer: C

Benchmarking partners are identified in the research stage of the benchmarking process

68. Correct answer: A

An IS auditor's primary responsibility is to advise senior management of the risk involved in not implementing proper segregation of duties, such as having the security administrator perform an operations function

69. Correct answer: B

Business unit management is responsible for implementing cost-effective controls in an automated system

70. Correct answer: A

Ensuring that security and control policies support business and IT objectives is a primary objective of an IT security policies audit

71. Correct answer: D

When auditing third-party service providers, an auditor should be concerned with 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. Correct answer: A

Proper segregation of duties prevents a computer operator (user) from performing security administration duties.

73. Correct answer: A

Adopting and communicating a comprehensive antivirus policy is the most fundamental step in preventing virus attacks. All other antivirus prevention efforts rely upon decisions established and communicated via policy.

74. Correct answer: B

The project steering committee is responsible for the overall direction, costs, and timetables for Systems development projects.

75. Correct answer: B

Threats exploit vulnerabilities to cause loss or damage to the organization and its assets

76. Correct answer: A

Choice A takes into consideration the likelihood and magnitude of the impact and provides the best measure of the risk to an asset

77. Correct answer: C

Monitoring the time (choice A) and audit programs (choice D), as well as adequate training (choice B), will improve the IS audit staff's productivity (efficiency and performance), but that

which delivers value to the organization are the resources and efforts being dedicated to, and focused on, the higher-risk areas.

78. Correct answer: B

Generalized audit software features include mathematical computations, stratification, statistical analysis, sequence checking, duplicate checking and re-computations. An IS auditor, using generalized audit software, could design appropriate tests to re-compute the payroll, thereby determining if there were overpayments and to whom they were made

79. Correct answer: D

One of the main objectives of an audit is to identify potential risks; therefore, the most proactive approach would be to identify and evaluate the existing security practices being followed by the organization

80. Correct answer: D

It is important for an IS auditor to identify and evaluate the existing controls and security once the potential threats and possible impacts are identified. Upon completion of an audit an IS auditor should describe and discuss with management the threats and potential impacts on the assets.

81. Correct answer: A

An IS auditor should focus on when controls are exercised as data flow through a computer system

82. Correct answer: C

By observing the IS staff performing their tasks, an IS auditor can identify whether they are performing any incompatible operations, and by interviewing the IS staff, the auditor can get an overview of the tasks performed. Based on the observations and interviews the auditor can evaluate the segregation of duties

83. Correct answer: B

If the answers provided to an IS auditor's questions are not confirmed by documented procedures or job descriptions, the IS auditor should expand the scope of testing the controls and include additional substantive tests

84. Correct answer: A

A point-of-sale system is a critical online system that when inoperable will jeopardize the ability of Company.com to generate revenue and track inventory properly

85. Correct answer: B

Including the finding in the final report is a generally accepted audit practice. If an action is taken after the audit started and before it ended, the audit report should identify the finding and describe the corrective action taken

86. Correct answer: A

Including the finding in the final report is a generally accepted audit practice. If an action is taken after the audit started and before it ended, the audit report should identify the finding and describe the corrective action taken.

87. Correct answer: C

A steering committee should exist to ensure that the IT strategies support the organization's goals. The absence of an information technology committee or a committee not composed of senior managers would be an indication of a lack of top-level management commitment. This condition would increase the risk that IT would not be aligned with the organization's strategy.

88. Correct answer: C

The IS steering committee typically serves as a general review board for major IS projects and should not become involved in routine operations; therefore, one of its functions is to approve and monitor major projects, the status of IS plans and budgets

89. Correct answer: A

Strategic plans provide the basis for ensuring that the enterprise meets its goals and objectives. Involvement of senior management is critical to ensuring that the plan adequately addresses the established goals and objectives

90. Correct answer: A

To govern IT effectively, IT and business should be moving in the same direction, requiring that the IT plans are aligned with an organization's business plans

91. Correct answer: B

Senior management should establish the acceptable risk level, since they have the ultimate or final responsibility for the effective and efficient operation of the organization

92. Correct answer: B

The chief executive officer is instrumental in implementing IT governance per the directions of the board of directors

93. Correct answer: A

Information security governance, when properly implemented, should provide four basic outcomes: strategic alignment, value delivery, risk management and performance measurement. Strategic alignment provides input for security requirements driven by enterprise requirements

94. Correct answer: D

Top management mediating between the imperatives of business and technology is an IT strategic alignment best practice. Supplier and partner risks being managed is a risk management best practice. A knowledge base on customers, products, markets and processes being in place is an IT value delivery best practice. An infrastructure being provided to facilitate the creation and sharing of business information is an IT value delivery and risk management best practice

95. Correct answer: D

Effective IT governance requires that board and executive management extend governance to IT and provide the leadership, organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives, and that the strategy is aligned with business strategy

96. Correct answer: B

The key objective of an IT governance program is to support the business, thus the identification of organizational strategies is necessary to ensure alignment between IT and corporate governance. Without identification of organizational strategies, the remaining choices-even if implemented-would be ineffective

97. Correct answer: C

One of the most important reasons for which projects get funded is how well a project meets an organization's strategic objectives. Portfolio management takes a holistic view of a company's overall IT strategy. IT strategy should be aligned with the business strategy and, hence, reviewing the business plan should be the major consideration

98. Correct answer: A

The goals of IT governance are to improve IT performance, to deliver optimum business value and to ensure regulatory compliance. The key practice in support of these goals is the strategic alignment of IT with the business {choice A}. To achieve alignment, all other choices need to be tied to business practices and strategies

99. Correct answer: A

IT governance is intended to specify the combination of decision rights and accountability that is best for the enterprise. It is different for every enterprise

100. Correct answer: B

Defined (level 3) is the lowest level at which an IT balanced scorecard is defined

101. Correct answer: D

Governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly

102. Correct answer: B

This choice directly addresses the problem. An organization wide approach is needed to achieve effective management of data assets. This includes enforcing standard definitions of data elements, which is part of a data governance initiative. The other choices, while sound development practices, do not address the root cause of the problem described

103. Correct answer: D

There is a probability that a terminated employee may misuse access rights; therefore, disabling the terminated employee's logical access is the most important action to be taken.

104. Correct answer: B

Required vacations/holidays of a week or more in duration in which someone other than the regular employee performs the job function is often mandatory for sensitive positions, as this reduces the opportunity to commit improper or illegal acts. During this time it may be possible to discover any fraudulent activity that was taking place

105. Correct answer: D

Compensating controls are internal controls that are intended to reduce the risk of an existing or potential control weakness that may arise when duties cannot be appropriately segregated

106. Correct answer: B

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

107. Correct answer: D

Strategic planning sets corporate or departmental objectives into motion. Comprehensive planning helps ensure an effective and efficient organization. Choice D represents a business objective that is intended to focus the overall direction of the business and would thus be a part of the organization's strategic plan. The other choices are project-oriented and do not address business objectives.

108. Correct answer: D

Strategic planning sets corporate or department objectives into motion. Both long-term and short term strategic plans should be consistent with the organization's broader plans and business objectives for attaining these goals

109. Correct answer: B

The IT strategic plan exists to support the organization's business plan. To evaluate the IT strategic plan, an IS auditor would first need to familiarize themselves with the business plan

110. Correct answer: B

Boards of directors and executive management can use the information security governance. When the responsibilities for IT security in an organization are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed, it is said to be 'managed and measurable maturity model to establish rankings for security in their organizations.

111. Correct answer: C

An IT balanced scorecard (BSC) provides the bridge between IT objectives and business objectives by supplementing the traditional financial evaluation with measures to evaluate customer satisfaction, internal processes and the ability to innovate

112. Correct answer: C

The IT strategic plan must include a clear articulation of the IT mission and vision. The plan need not address the technology, operational controls or project management practices.

113. Correct answer: B

A bottom-up approach begins by defining operational-level requirements and policies, which are derived and implemented as the result of risk assessments. Enterprise-level policies are subsequently developed based on a synthesis of existing operational policies

114. Correct answer: B

Change requires that good change management processes be implemented and enforced

115. Correct answer: A

Deriving lower level policies from corporate policies (a top-down approach) aids in ensuring consistency across the organization and consistency with other policies

116. Correct answer: C

Privacy laws prohibiting the cross-border flow of personally identifiable information would make it impossible to locate a data warehouse containing customer information in another country