https://selldocx.com/products
/test-bank-corporate-computer-and-network-security-5e-boyle

Corporate Computer Security, 5e **(Boyle/Panko)**
Chapter 2 Planning and Policy

1) Which of the following is FALSE about security management?
A) Management is abstract; technology is visible.
B) Security technology is far more important than security management.
C) There are fewer general principles in security management than technology.
D) It is generally a mistake to focus too heavily on security technology compared to security management.
Answer: B
Page Ref: 49
Learning Objective: 2.1 Justify the need for formal management processes
Difficulty: Difficult

2) *Comprehensive security* pertains to _____.
A) closing all routes of attack to their systems to attackers
B) closing all Internet-linked servers to attackers
C) lessening security issues in an entire company
D) decreasing the risk of all computer systems in a company
Answer: A
Page Ref: 49
Learning Objective: 2.1 Justify the need for formal management processes
Difficulty: Moderate

3) If a failure of a single element of a system will ruin security, this is called a(n) _____.
A) weakest-link failure
B) hybrid solution
C) internal audit
D) risk analysis
Answer: A
Page Ref: 49
Learning Objective: 2.1 Justify the need for formal management processes
Difficulty: Easy

4) *Process* pertains to _____.
A) the plan-protect-respond cycle
B) the systems life cycle
C) a planned series of actions
D) recovery according to plan
Answer: C
Page Ref: 50
Learning Objective: 2.1 Justify the need for formal management processes
Difficulty: Moderate

Copyright © 2021 Pearson Education, Inc.

5) Which of the following is NOT part of the highest-level security management process that most firms use today to protect against threats?
A) Plan
B) Process
C) Protect
D) Respond
Answer: B
Page Ref: 51
Learning Objective: 2.1 Justify the need for formal management processes
Difficulty: Moderate

6) The systems development life cycle is most connected to the _____ of the plan-protect-respond cycle of security management.
A) plan
B) process
C) protect
D) respond
Answer: C
Page Ref: 52
Learning Objective: 2.1 Justify the need for formal management processes
Difficulty: Moderate

7) *Response* is _____.
A) the second phase of the systems life cycle
B) the plan-based creation and operation of countermeasures
C) a planned series of actions
D) recovery according to plan
Answer: D
Page Ref: 53
Learning Objective: 2.1 Justify the need for formal management processes
Difficulty: Moderate

8) A firm's primary objective is to make a profit.
Answer: TRUE
Page Ref: 48
Learning Objective: 2.1 Justify the need for formal management processes
Difficulty: Easy

9) A firewall administrator should check the log file in a company each week.
Answer: FALSE
Page Ref: 49
Learning Objective: 2.1 Justify the need for formal management processes
Difficulty: Moderate

Copyright © 2021 Pearson Education, Inc.

10) One reason why security management is difficult is that companies need to protect a large number of resources.
Answer: TRUE
Page Ref: 50
Learning Objective: 2.1 Justify the need for formal management processes
Difficulty: Easy

11) Security is too complicated to be managed informally.
Answer: TRUE
Page Ref: 50
Learning Objective: 2.1 Justify the need for formal management processes
Difficulty: Easy

12) In the plan-protect-respond cycle, the three activities always take place in sequential order.
Answer: FALSE
Page Ref: 50
Learning Objective: 2.1 Justify the need for formal management processes
Difficulty: Easy

13) One key to making security an *enabler* is to get security involved near the end of most projects.
Answer: FALSE
Page Ref: 54
Learning Objective: 2.1 Justify the need for formal management processes
Difficulty: Easy

14) _____ are things that require a firm to change its security planning, protections, and response.
A) Responses
B) Protections
C) MSSPs
D) Driving forces
Answer: D
Page Ref: 58
Learning Objective: 2.2 Describe compliance laws and regulations
Difficulty: Moderate

15) Which of the following produced the greatest change in financial reporting requirement since the Great Depression?
A) The Sarbanes-Oxley Act
B) The General Data Protection Regulation
C) The Gramm-Leach-Bliley Act
D) The Health Insurance Portability and Accountability Act
Answer: A
Page Ref: 58
Learning Objective: 2.2 Describe compliance laws and regulations
Difficulty: Moderate

Copyright © 2021 Pearson Education, Inc.

16) The Sarbanes-Oxley Act was passed in _____.
A) 2000
B) 2002
C) 2010
D) 2012
Answer: B
Page Ref: 58
Learning Objective: 2.2 Describe compliance laws and regulations
Difficulty: Moderate

17) Which of the following is an EU privacy law?
A) The Sarbanes-Oxley Act
B) The General Data Protection Regulation
C) The Gramm-Leach-Bliley Act
D) The Health Insurance Portability and Accountability Act
Answer: B
Page Ref: 60
Learning Objective: 2.2 Describe compliance laws and regulations
Difficulty: Moderate

18) Which of the following is also known as the Financial Services Modernization Act?
A) GDPR
B) GLBA
C) HIPAA
D) SB 1386
Answer: B
Page Ref: 60
Learning Objective: 2.2 Describe compliance laws and regulations
Difficulty: Moderate

19) Which of the following was the first data breach notification law in the U.S.?
A) GDPR
B) GLBA
C) HIPAA
D) SB 1386
Answer: D
Page Ref: 60
Learning Objective: 2.2 Describe compliance laws and regulations
Difficulty: Moderate

Copyright © 2021 Pearson Education, Inc.

20) _____ was the last state to implement a data breach notification law in _____.
A) Georgia; 2000
B) Alabama; 2018
C) North Dakota; 2016
D) California; 2018
Answer: B
Page Ref: 60
Learning Objective: 2.2 Describe compliance laws and regulations
Difficulty: Moderate

21) One of the first data breach notification laws in the U.S. was created in _____.
A) California
B) New York
C) Illinois
D) Texas
Answer: A
Page Ref: 60
Learning Objective: 2.2 Describe compliance laws and regulations
Difficulty: Moderate

22) Who has the power to prosecute companies that fail to take reasonable precautions to protect private information?
A) HIPAA
B) FTC
C) GDPR
D) GLBA
Answer: B
Page Ref: 61
Learning Objective: 2.2 Describe compliance laws and regulations
Difficulty: Moderate

23) _____ has set the standards for companies that accept credit cards as a form of payment.
A) FISMA
B) FTC
C) PCI-DSS
D) HIPAA
Answer: C
Page Ref: 61
Learning Objective: 2.2 Describe compliance laws and regulations
Difficulty: Moderate

Copyright © 2021 Pearson Education, Inc.

24) Why was FISMA enacted?
A) To set standards for companies that accept credit card payments
B) To set accreditation standards for members of a particular industry
C) To prosecute firms that fail to take reasonable precautions to protect customers' private information
D) To bolster computer and network security within the federal government
Answer: D
Page Ref: 61
Learning Objective: 2.2 Describe compliance laws and regulations
Difficulty: Difficult

25) Compliance laws create requirements to which corporate security must respond.
Answer: TRUE
Page Ref: 58
Learning Objective: 2.2 Describe compliance laws and regulations
Difficulty: Easy

26) The Sarbanes-Oxley Act was passed in 2012.
Answer: FALSE
Page Ref: 60
Learning Objective: 2.2 Describe compliance laws and regulations
Difficulty: Easy

27) Given the importance of Sarbanes-Oxley compliance for companies, most firms were forced to increase their security efforts.
Answer: TRUE
Page Ref: 60
Learning Objective: 2.2 Describe compliance laws and regulations
Difficulty: Easy

28) The GLBA is considered the most important EU privacy rule ever created.
Answer: FALSE
Page Ref: 60
Learning Objective: 2.2 Describe compliance laws and regulations
Difficulty: Easy

29) There are strong federal laws requiring companies to provide notice of a data breach.
Answer: FALSE
Page Ref: 60
Learning Objective: 2.2 Describe compliance laws and regulations
Difficulty: Moderate

30) HIPAA has the power to require firms to pay to be audited annually by an external firm.
Answer: FALSE
Page Ref: 61
Learning Objective: 2.2 Describe compliance laws and regulations
Difficulty: Easy

Copyright © 2021 Pearson Education, Inc.

31) The first stage of FISMA is a certification of a system by an organization.
Answer: TRUE
Page Ref: 62
Learning Objective: 2.2 Describe compliance laws and regulations
Difficulty: Easy

32) Which of the following is considered the first step for a corporation in managing security?
A) To decide where the security function will sit on a firm's organization chart
B) To determine what devices need secured and which software to use to do that
C) To determine the size of the security staff and the budget that will support that staff
D) To decide the objectives of the security function
Answer: A
Page Ref: 62
Learning Objective: 2.3 Describe organizational security issues
Difficulty: Moderate

33) Which of the following is considered a fundamental problem with making IT security a staff department outside IT?
A) Separation reduces accountability.
B) IT security would report to a firm's CIO.
C) Security changes that would need to be made would be easier.
D) Security and IT could share many of the same technological skill set.
Answer: A
Page Ref: 64
Learning Objective: 2.3 Describe organizational security issues
Difficulty: Moderate

34) Which of the following is NOT one of the three auditing departments that are part of most corporations?
A) Financial auditing
B) Internal auditing
C) Outside auditing
D) IT auditing
Answer: C
Page Ref: 65
Learning Objective: 2.3 Describe organizational security issues
Difficulty: Easy

Copyright © 2021 Pearson Education, Inc.

35) _____ in regard to outside IT security means checking out closely the IT security implications of a potential partnership before beginning the relationship.
A) A hybrid solution
B) Internal auditing
C) Risk analysis
D) Due diligence
Answer: D
Page Ref: 66
Learning Objective: 2.3 Describe organizational security issues
Difficulty: Moderate

36) The most common type of IT security outsourcing is done for _____.
A) laptops
B) e-mail
C) all hardware
D) all software
Answer: B
Page Ref: 66
Learning Objective: 2.3 Describe organizational security issues
Difficulty: Easy

37) An advantage to using an MSSP is _____.
A) cost
B) control of employees
C) constant internal control
D) independence
Answer: D
Page Ref: 66
Learning Objective: 2.3 Describe organizational security issues
Difficulty: Moderate

38) The usual title for a company's security department head is chief security officer.
Answer: TRUE
Page Ref: 62
Learning Objective: 2.3 Describe organizational security issues
Difficulty: Easy

39) Most analysts recommend placing security outside IT.
Answer: TRUE
Page Ref: 64
Learning Objective: 2.3 Describe organizational security issues
Difficulty: Moderate

Copyright © 2021 Pearson Education, Inc.

40) Most firms have a CSO report direct to the company's CEO.
Answer: FALSE
Page Ref: 64
Learning Objective: 2.3 Describe organizational security issues
Difficulty: Easy

41) The financial auditing department examines organizational units for efficiency, effectiveness, and adequate controls.
Answer: FALSE
Page Ref: 64
Learning Objective: 2.3 Describe organizational security issues
Difficulty: Moderate

42) IT security is almost always mistrusted by other departments because of security's potential to make life harder.
Answer: TRUE
Page Ref: 64
Learning Objective: 2.3 Describe organizational security issues
Difficulty: Easy

43) Which of the following compares probable losses with the costs of security protections?
A) Weakest-link failure
B) Reasonable risk
C) Internal audits
D) Risk analysis
Answer: D
Page Ref: 68
Learning Objective: 2.4 Describe risk analysis
Difficulty: Easy

44) The _____ of the classic risk analysis calculation is the percentage of an asset's value that would be lost in a breach.
A) single loss expectancy
B) annualized loss expectancy
C) exposure factor
D) countermeasure impact
Answer: C
Page Ref: 69
Learning Objective: 2.4 Describe risk analysis
Difficulty: Moderate

Copyright © 2021 Pearson Education, Inc.

45) What does a central logging server of an MSSP on a network do?
A) It calculates the amount of processing ability needed for a system.
B) It uploads a firm's event log data.
C) It uploads the number of times that employees have logged into—or attempted to log into—questionable sites.
D) It automatically creates a firewall when questionable activity is detected.
Answer: B
Page Ref: 67
Learning Objective: 2.4 Describe risk analysis
Difficulty: Moderate

46) Which of the following is an outsourcing alternative?
A) PCI-DSS
B) FISMA
C) MSSP
D) ISO 27000
Answer: B
Page Ref: 67
Learning Objective: 2.4 Describe risk analysis
Difficulty: Moderate

47) In the classic risk analysis calculation, once you know how much damage an incident may cause from a single breach, the next issue is how frequently breaches will occur. This is normally done on a(n) _____ basis.
A) annualized
B) weekly
C) daily
D) bi-annual
Answer: A
Page Ref: 69
Learning Objective: 2.4 Describe risk analysis
Difficulty: Moderate

48) In the classic risk analysis calculation, the countermeasure impact assesses the _____.
A) drawbacks of a countermeasure
B) benefits of a countermeasure
C) costs of a countermeasure
D) number of incidents of all possible countermeasures
Answer: B
Page Ref: 70
Learning Objective: 2.4 Describe risk analysis
Difficulty: Moderate

Copyright © 2021 Pearson Education, Inc.

49) The _____ of the classic risk analysis calculation is the value of the thing to be protected.
A) asset value
B) annualized loss expectancy
C) exposure factor
D) countermeasure impact
Answer: A
Page Ref: 69
Learning Objective: 2.4 Describe risk analysis
Difficulty: Easy

50) Discounted cash flow analysis is also called _____.
A) IRR
B) TCI
C) NPV
D) ROI
Answer: D
Page Ref: 70
Learning Objective: 2.4 Describe risk analysis
Difficulty: Moderate

51) Which of the following is NOT a logical possible response to risk by a company?
A) Risk reduction
B) Risk acceptance
C) Risk transference
D) Risk analysis
Answer: D
Page Ref: 73
Learning Objective: 2.4 Describe risk analysis
Difficulty: Moderate

52) Installing firewalls in a company is an example of _____.
A) risk reduction
B) risk acceptance
C) risk transference
D) risk avoidance
Answer: A
Page Ref: 73
Learning Objective: 2.4 Describe risk analysis
Difficulty: Moderate

Copyright © 2021 Pearson Education, Inc.

53) The most common example of risk transference is _____.
A) insurance
B) no countermeasures
C) installing firewalls
D) IT security measures
Answer: A
Page Ref: 73
Learning Objective: 2.4 Describe risk analysis
Difficulty: Easy

54) Implementing no countermeasures to security challenges and absorbing any damages that may occur is known as _____.
A) risk reduction
B) risk acceptance
C) risk transference
D) risk avoidance
Answer: B
Page Ref: 73
Learning Objective: 2.4 Describe risk analysis
Difficulty: Easy

55) Return on investment analysis requires the computation of either the net present value or the _____.
A) risk transference
B) risk avoidance
C) internal rate of return
D) total cost of incident
Answer: C
Page Ref: 70
Learning Objective: 2.4 Describe risk analysis
Difficulty: Moderate

56) IT security planning always focuses on risk.
Answer: TRUE
Page Ref: 68
Learning Objective: 2.4 Describe risk analysis
Difficulty: Easy

57) The annualized loss expectancy of the classic risk analysis calculation is the yearly average loss expected from a compromise for the asset.
Answer: TRUE
Page Ref: 69
Learning Objective: 2.4 Describe risk analysis
Difficulty: Moderate

Copyright © 2021 Pearson Education, Inc.

58) Although IT security can reduce the risk of attacks for companies, security also has some negative side effects.
Answer: TRUE
Page Ref: 69
Learning Objective: 2.4 Describe risk analysis
Difficulty: Moderate

59) The classic risk analysis calculation is difficult or impossible to use in actual practice.
Answer: TRUE
Page Ref: 70
Learning Objective: 2.4 Describe risk analysis
Difficulty: Easy

60) The worst problem with classic risk analysis is that it is rarely possible to estimate the annualized rate of occurrence for threats.
Answer: TRUE
Page Ref: 71
Learning Objective: 2.4 Describe risk analysis
Difficulty: Moderate

61) ROI is typically quite easy to measure for security investments.
Answer: FALSE
Page Ref: 72
Learning Objective: 2.4 Describe risk analysis
Difficulty: Moderate

62) A positive of classic risk analysis is that it imposes general discipline for thinking about risks and countermeasures.
Answer: TRUE
Page Ref: 73
Learning Objective: 2.4 Describe risk analysis
Difficulty: Moderate

63) _____ includes all of a firm's technical countermeasures and how they are organized into a complete system of protection.
A) Technical security architecture
B) Risk avoidance
C) Corporate security policy
D) Implementation guidance
Answer: A
Page Ref: 74
Learning Objective: 2.5 Describe technical security infrastructure
Difficulty: Moderate

Copyright © 2021 Pearson Education, Inc.

64) Technologies that a company has implemented in the past but that now are somewhat ineffective are known as _____.
A) central security management consoles
B) legacy security technologies
C) technical security architecture
D) defense in depth
Answer: B
Page Ref: 75
Learning Objective: 2.5 Describe technical security infrastructure
Difficulty: Moderate

65) When an attacker has to break through multiple countermeasures to succeed, it's known as _____.
A) defense in depth
B) single point of vulnerability
C) weakest link
D) technical security architecture
Answer: A
Page Ref: 75
Learning Objective: 2.5 Describe technical security infrastructure
Difficulty: Moderate

66) Which of the following defines the opposite of defense in depth?
A) Weakest link
B) Defense in depth
C) Single point of vulnerability
D) Technical security architecture
Answer: C
Page Ref: 75
Learning Objective: 2.5 Describe technical security infrastructure
Difficulty: Moderate

67) _____ refers to the intention to minimize lost productivity and attempt to not slow innovation.
A) Minimizing security burdens
B) Defining the weakest link
C) A single point of vulnerability
D) Technical security architecture
Answer: A
Page Ref: 76
Learning Objective: 2.5 Describe technical security infrastructure
Difficulty: Moderate

Copyright © 2021 Pearson Education, Inc.

68) _____ is being able to manage security technologies from a single security management console or at least from a relatively few consoles.
A) Technical security architecture
B) A single point of vulnerability
C) Centralized security management
D) Defense in depth
Answer: C
Page Ref: 78
Learning Objective: 2.5 Describe technical security infrastructure
Difficulty: Moderate

69) It is preferable if a firm's security systems evolve naturally and organically without major coordination.
Answer: FALSE
Page Ref: 75
Learning Objective: 2.5 Describe technical security infrastructure
Difficulty: Easy

70) If a legacy technology is a serious threat to security, it must be replaced.
Answer: TRUE
Page Ref: 75
Learning Objective: 2.5 Describe technical security infrastructure
Difficulty: Easy

71) In defense in depth, there are multiple independent countermeasures placed in a series.
Answer: TRUE
Page Ref: 75
Learning Objective: 2.5 Describe technical security infrastructure
Difficulty: Moderate

72) All single points of failure can be eliminated.
Answer: FALSE
Page Ref: 76
Learning Objective: 2.5 Describe technical security infrastructure
Difficulty: Moderate

73) Firewalls are only for borders between external networks and internal networks and do not exist for solely an internal purpose.
Answer: FALSE
Page Ref: 76
Learning Objective: 2.5 Describe technical security infrastructure
Difficulty: Moderate

Copyright © 2021 Pearson Education, Inc.

74) In interorganizational systems, two companies link some of their IT assets.
Answer: TRUE
Page Ref: 78
Learning Objective: 2.5 Describe technical security infrastructure
Difficulty: Easy

75) The goal of _____ is to emphasize a firm's commitment to strong security.
A) corporate security policies
B) centralized security management
C) technical security architecture
D) acceptable use policies
Answer: A
Page Ref: 80
Learning Objective: 2.6 Explain policy-driven implementation
Difficulty: Moderate

76) It is common for companies to require users to read and sign a(n) _____.
A) corporate security policy
B) personally identifiable information policy
C) e-mail policy
D) acceptable use policy
Answer: D
Page Ref: 80
Learning Objective: 2.6 Explain policy-driven implementation
Difficulty: Moderate

77) _____ are mandatory implementation guidance, meaning that employees are not free to opt out of them.
A) Standards
B) Policies
C) Guidelines
D) Procedures
Answer: A
Page Ref: 82
Learning Objective: 2.6 Explain policy-driven implementation
Difficulty: Moderate

78) _____ are mandatory implementation guidance, meaning that employees are not free to opt out of them.
A) Standards
B) Policies
C) Guidelines
D) Procedures
Answer: A
Page Ref: 82
Learning Objective: 2.6 Explain policy-driven implementation
Difficulty: Moderate

Copyright © 2021 Pearson Education, Inc.

79) Of the following, _____ are the most detailed.
A) policies
B) standards
C) guidelines
D) procedures
Answer: D
Page Ref: 82
Learning Objective: 2.6 Explain policy-driven implementation
Difficulty: Moderate

80) In the _____, a specific, full act should require two or more people to complete.
A) implementation guidance
B) weakest link
C) segregation of duties
D) request/authorization control
Answer: C
Page Ref: 83
Learning Objective: 2.6 Explain policy-driven implementation
Difficulty: Moderate

81) _____ describe the details of what is to be done but without specifically describing how to do something.
A) Baselines
B) Standards
C) Best practices
D) Procedures
Answer: A
Page Ref: 84
Learning Objective: 2.6 Explain policy-driven implementation
Difficulty: Moderate

82) _____ are descriptions of what the best firms in the industry are doing about security.
A) Baselines
B) Standards
C) Procedures
D) Best practices
Answer: D
Page Ref: 84
Learning Objective: 2.6 Explain policy-driven implementation
Difficulty: Moderate

Copyright © 2021 Pearson Education, Inc.

83) _____ can simply be described as a person's system of values.
A) Baselines
B) Ethics
C) Procedures
D) Best practices
Answer: B
Page Ref: 85
Learning Objective: 2.6 Explain policy-driven implementation
Difficulty: Easy

84) Which of the following is NOT a general guideline to handling exceptions?
A) Only some people should be allowed to request exceptions.
B) The person who requests an exception must never be the same person who authorizes the exception.
C) More people should be allowed to authorize exceptions than can request exceptions.
D) Each exception must be carefully documented in terms of specifically what was done and who did each action.
Answer: C
Page Ref: 87
Learning Objective: 2.6 Explain policy-driven implementation
Difficulty: Difficult

85) _____ is a process, function, or group of tools that are used to improve policy implementation and enforcement.
A) Promulgation
B) Oversight
C) Monitoring
D) Auditing
Answer: B
Page Ref: 88
Learning Objective: 2.6 Explain policy-driven implementation
Difficulty: Easy

86) In a 2018 report, it was reported that _____ of fraud is detected through anonymous tips.
A) approximately 25 percent
B) more than 40 percent
C) approximately 48 percent
D) more than 65 percent
Answer: B
Page Ref: 89
Learning Objective: 2.6 Explain policy-driven implementation
Difficulty: Easy

Copyright © 2021 Pearson Education, Inc.

87) The _____ was a replacement for the controversial Protect America Act of 2007.
A) USA Freedom Act
B) Communications Assistance for Law Enforcement Act
C) Foreign Intelligence Surveillance Act
D) General Data Protection Regulation
Answer: A
Page Ref: 94
Learning Objective: 2.6 Explain policy-driven implementation
Difficulty: Easy

88) A policy is a statement of what should be done under specific circumstances.
Answer: TRUE
Page Ref: 79
Learning Objective: 2.6 Explain policy-driven implementation
Difficulty: Easy

89) E-mail policies exist in almost all firms.
Answer: TRUE
Page Ref: 80
Learning Objective: 2.6 Explain policy-driven implementation
Difficulty: Easy

90) Team-written policies are usually less respected by employees than policies written exclusively by IT security.
Answer: FALSE
Page Ref: 80
Learning Objective: 2.6 Explain policy-driven implementation
Difficulty: Moderate

91) Implementation guidance limits the discretion of implementers.
Answer: TRUE
Page Ref: 81
Learning Objective: 2.6 Explain policy-driven implementation
Difficulty: Moderate

92) Accountability refers to the liability for sanctions if implementation is not done properly.
Answer: TRUE
Page Ref: 84
Learning Objective: 2.6 Explain policy-driven implementation
Difficulty: Moderate

93) Formally announcing, publishing, or making users aware of new policies of the company is called oversight.
Answer: FALSE
Page Ref: 88
Learning Objective: 2.6 Explain policy-driven implementation
Difficulty: Easy

Copyright © 2021 Pearson Education, Inc.

94) All publicly traded companies must have their financial statements audited.
Answer: TRUE
Page Ref: 89
Learning Objective: 2.6 Explain policy-driven implementation
Difficulty: Moderate

95) The Communications Assistance for Law Enforcement Act was passed in the late 1960s.
Answer: FALSE
Page Ref: 94
Learning Objective: 2.6 Explain policy-driven implementation
Difficulty: Moderate

96) Which of the following focuses broadly on corporate internal and financial controls?
A) COBIT
B) ISO/IEC 27000
C) COSO
D) ISO/IEC 27002
Answer: C
Page Ref: 95
Learning Objective: 2.7 Know governance frameworks
Difficulty: Moderate

97) Which of the following is a series of standards specifically addressing IT security?
A) COBIT
B) ISO/IEC 27000
C) COSO
D) ISO/IEC 27002
Answer: A
Page Ref: 95
Learning Objective: 2.7 Know governance frameworks
Difficulty: Moderate

98) Which of the following is NOT an objective in the COSO framework?
A) Strategic
B) Reporting
C) Compliance
D) Implementation
Answer: D
Page Ref: 96
Learning Objective: 2.7 Know governance frameworks
Difficulty: Moderate

Copyright © 2021 Pearson Education, Inc.

99) Which of the following is NOT a COSO framework component?
A) Internal environment
B) Event identification
C) Training practices
D) Risk assessment
Answer: C
Page Ref: 96
Learning Objective: 2.7 Know governance frameworks
Difficulty: Moderate

100) Which of the following COSO framework components encompasses the tone of the organization?
A) Internal environment
B) Event identification
C) Objective setting
D) Control activities
Answer: A
Page Ref: 96
Learning Objective: 2.7 Know governance frameworks
Difficulty: Moderate

101) In which of the following COSO framework components are policies and procedures established?
A) Internal environment
B) Control activities
C) Information and communication
D) Objective setting
Answer: B
Page Ref: 96
Learning Objective: 2.7 Know governance frameworks
Difficulty: Moderate

102) Which of the following is NOT one of the major domains of the COBIT framework?
A) Evaluate, direct, and monitor
B) Build, acquire, and implement
C) Deliver, service, and support
D) Promote, hire, and train
Answer: D
Page Ref: 99
Learning Objective: 2.7 Know governance frameworks
Difficulty: Moderate

Copyright © 2021 Pearson Education, Inc.

103) The ISO/IEC 27001 standard specifies how to certify organizations as being compliant with _____.
A) ISO/IEC 27000
B) ISO/IEC 27043
C) COSO
D) COBIT
Answer: A
Page Ref: 100
Learning Objective: 2.7 Know governance frameworks
Difficulty: Moderate

104) Objective setting and risk assessment are both COSO framework components.
Answer: TRUE
Page Ref: 96
Learning Objective: 2.7 Know governance frameworks
Difficulty: Moderate

105) The IT Governance Institute was created by the Association of Certified Fraud Examiners.
Answer: FALSE
Page Ref: 96
Learning Objective: 2.7 Know governance frameworks
Difficulty: Moderate

106) The ISO/IEC 27002 standard divides security into 14 broad areas.
Answer: TRUE
Page Ref: 96
Learning Objective: 2.7 Know governance frameworks
Difficulty: Moderate

107) The EDM domain of the COBIT framework evaluates strategic alternatives.
Answer: TRUE
Page Ref: 96
Learning Objective: 2.7 Know governance frameworks
Difficulty: Moderate

108) COBIT is a general control planning and assessment tool for corporations.
Answer: FALSE
Page Ref: 98
Learning Objective: 2.7 Know governance frameworks
Difficulty: Moderate

109) There is no time ordering for the five components of the COSO framework.
Answer: TRUE
Page Ref: 98
Learning Objective: 2.7 Know governance frameworks
Difficulty: Moderate

Copyright © 2021 Pearson Education, Inc.

110) The first standard in the series was originally called ISO/IEC 17799.
Answer: TRUE
Page Ref: 99
Learning Objective: 2.7 Know governance frameworks
Difficulty: Moderate

Copyright © 2021 Pearson Education, Inc.