Corporate Computer Security, 4e **(Boyle/Panko)**
Chapter 2 Planning and Policy

1) This book focuses on _____.
A) offense
B) defense
C) offense and defense about equally
D) None of the above
Answer: B
Diff: 1
Question: 1

2) Closing all routes of attack into an organization's system(s) is called _____.
A) defense in depth
B) comprehensive security
C) total security
D) access control
Answer: B
Diff: 1
Question: 2b

3) A _____ occur(s) when a single security element failure defeats the overall security of a system.
A) spot failure
B) weakest link failure
C) defense in depth departure
D) critical failure
Answer: B
Diff: 1
Question: 2c

4) Which of the following is a formal process?
A) Annual corporate planning
B) Planning and developing individual countermeasures
C) Both A and B
D) Neither A nor B
Answer: C
Diff: 1
Question: 3a

5) A planned series of actions in a corporation is a(n) _____.
A) strategy
B) sequence
C) process
D) anomaly
Answer: C
Diff: 2
Question: 3a

6) The growing number of compliance laws and regulations is driving firms to use formal governance frameworks to guide their security processes.
Answer: TRUE
Diff: 1
Question: 3b

7) Many compliance regimes require firms to adopt specific formal governance framework to drive security planning and operational management.
Answer: TRUE
Diff: 2
Question: 3b

8) Planning, protection, and response follow a fairly strict sequence from one stage to another.
Answer: FALSE
Diff: 1
Question: 4b

9) The stage of the plan-protect response cycle that consumes the most time is _____.
A) planning
B) protection
C) response
D) each of the above consumes about the same amount of time
Answer: B
Diff: 1
Question: 4c

10) _____ is the plan-based creation and operation of countermeasures.
A) Planning
B) Protection
C) Response
D) All of the above
Answer: B
Diff: 1
Question: 4d

11) What is missing from the definition of response as "recovery?"
A) The phrase "according to plan" must be added to "recovery."
B) The definition must refer to specific resources.
C) The phrase "Reasonable degree of" must begin the definition.
D) The phrase "and prosecution" must be added after "recovery."
Answer: A
Diff: 3
Question: 4e

12) Strong security can be an enabler, allowing a company to do things it could not do otherwise.
Answer: TRUE
Diff: 1
Question: 5a

13) The key to security being an enabler is _____.
A) getting it involved early within the project
B) having strong corporate policies
C) extensive training
D) adequate spending on security
Answer: A
Diff: 2
Question: 5b

14) IT security people should maintain a negative view of users.
Answer: FALSE
Diff: 1
Question: 5c

15) It is a good idea to view the security function as a police force or military organization.
Answer: FALSE
Diff: 1
Question: 5d

16) The first step in developing an IT security plan is to _____.
A) determine needs
B) assess the current state of the company's security
C) create comprehensive security
D) prioritize security projects
Answer: B
Diff: 3
Question: 6a

17) Once a company's resources are enumerated, the next step is to _____.
A) create a protection plan for each
B) assess the degree to which each is already protected
C) enumerate threats to each
D) classify them according to sensitivity
Answer: D
Diff: 3
Question: 6c

18) After performing a preliminary security assessment, a company should develop a remediation plan for EVERY security gap identified.
Answer: TRUE
Diff: 1
Question: 6d

19) A company should consider list of possible remediation plans as an investment portfolio.
Answer: TRUE
Diff: 1
Question: 6e

20) The factors that require a firm to change its security planning, protection, and response are called driving forces.
Answer: TRUE
Diff: 1
Question: 7a

21) Compliance laws and regulations _____.
A) create requirements to which security must respond
B) can be expensive for IT security
C) Both A and B
D) Neither A nor B
Answer: C
Diff: 1
Question: 7b

22) A _____ is a material deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement in the annual or interim financial statements will not be prevented or detected.
A) material control failure
B) material control deficiency
C) critical control deficiency
D) critical control failure
Answer: B
Diff: 2
Question: 8a

23) When companies studied where they stored private information, they found that much of this information was stored inside spreadsheets and word processing documents.
Answer: TRUE
Diff: 1
Question: 9b

24) _____ specifically addresses data protection requirements at financial institutions.
A) GLBA
B) HIPAA
C) The Revised SEC Act
D) Sarbanes-Oxley
Answer: A
Diff: 1
Question: 9c

25) _____ specifically addresses data protection requirements at health care institutions.
A) GLBA
B) HIPAA
C) Sarbanes-Oxley
D) The SEC Act
Answer: B
Diff: 1
Question: 9d

26) Data breach notification laws typically _____.
A) require companies to notify affected people if sensitive personally identifiable information is stolen or even lost
B) have caused companies to think more about security
C) Both A and B
D) Neither A nor B
Answer: C
Diff: 2
Question: 10a

27) The FTC can act against companies that fail to take reasonable precautions to protect privacy information.
Answer: TRUE
Diff: 1
Question: 11a

28) The FTC can _____.
A) impose fines
B) require annual audits by external auditing firms for many years
C) Both A and B
D) Neither A nor B
Answer: C
Diff: 1
Question: 11b

29) Which companies do PCI-DSS affect?
A) E-commerce firms
B) Medical firms
C) Government organizations
D) Companies that accept credit card payments
Answer: D
Diff: 1
Question: 13

30) What type of organization is subject to FISMA?
A) E-commerce firms
B) Medical firms
C) Government organizations
D) Companies that accept credit card payments
Answer: C
Diff: 1
Question: 14a

31) In FISMA, _____ is done internally by the organization.
A) certification
B) accreditation
C) Both A and B
D) Neither A nor B
Answer: C
Diff: 2
Question: 14b

32) The manager of the security department often is called _____.
A) the chief security officer (CSO)
B) the chief information security officer (CISO)
C) Either A and B
D) Neither A nor B
Answer: C
Diff: 1
Question: 15a

33) Placing security within IT _____.
A) creates independence
B) is likely to give security stronger backing from the IT department
C) Both A and B
D) Neither A nor B
Answer: B
Diff: 2
Question: 16a

34) Independence is best provided for IT security by placing it within the IT department.
Answer: FALSE
Diff: 1
Question: 16a

35) Most IT security analysts recommend placing IT security functions within the IT department.
Answer: FALSE
Diff: 1
Question: 16c

36) In order to demonstrate support for security, top management must _____.
A) ensure that security has an adequate budget
B) support security when there are conflicts between the needs of security and the needs of other business functions
C) follow security procedures themselves
D) All of the above
Answer: D
Diff: 1
Question: 17b

37) _____ examines organizational units for efficiency, effectiveness, and adequate controls.
A) Internal auditing
B) Financial auditing
C) IT auditing
D) None of the above
Answer: A
Diff: 1
Question: 18b

38) _____ examines financial processes for efficiency, effectiveness, and adequate controls.
A) Internal auditing
B) Financial auditing
C) IT auditing
D) None of the above
Answer: B
Diff: 1
Question: 18b

39) _____ examines IT processes for efficiency, effectiveness, and adequate controls.
A) Internal auditing
B) Financial auditing
C) IT auditing
D) None of the above
Answer: C
Diff: 1
Question: 18b

40) Placing IT auditing in an existing auditing department would give independence from IT security.
Answer: TRUE
Diff: 1
Question: 18c

41) _____ entails investigating the IT security of external companies and the implications of close IT partnerships before implementing interconnectivity.
A) Auditing
B) Due diligence
C) Peer-to-peer security
D) Vulnerability testing
Answer: B
Diff: 1
Question: 18h

42) To outsource some security functions, a firm can use an MISP.
Answer: FALSE
Diff: 2
Question: 19a

43) A benefit of using MSSPs is that they provide _____.
A) cost savings
B) independence
C) Both A and B
D) Neither A nor B
Answer: C
Diff: 2
Question: 19b

44) What security functions typically are outsourced?
A) Intrusion detection
B) Vulnerability testing
C) Both A and B
D) Neither A nor B
Answer: C
Diff: 2
Question: 19c

45) What security functions typically are outsourced?
A) Policy
B) Vulnerability testing
C) Both A and B
D) Neither A nor B
Answer: B
Diff: 2
Question: 19c

46) What security function(s) usually is(are) *not* outsourced?
A) Planning
B) Intrusion detection
C) Vulnerability testing
D) All of the above
Answer: A
Diff: 2
Question: 19e

47) Vulnerability testing typically is *not* outsourced.
Answer: FALSE
Diff: 2
Question: 19e

48) According to the author, *information assurance* is a good name for IT security.
Answer: FALSE
Diff: 1
Question: 20a

49) The goal of IT security is *risk elimination*.
Answer: FALSE
Diff: 2
Question: 20b

50) The goal of IT security is *reasonable risk reduction*.
Answer: TRUE
Diff: 2
Question: 20b

51) Security tends to impede functionality.
Answer: TRUE
Diff: 1
Question: 20c

52) In benefits, costs and benefits are expressed on a per-year basis.
Answer: TRUE
Diff: 1
Question: 21a

53) SLE times APO gives the _____.
A) expected per-event loss
B) expected annual loss
C) expected life cycle loss
D) expected per-event benefit
Answer: B
Diff: 3
Question: 21b

54) When risk analysis deals with costs and benefits that vary by year, the computations should use _____.
A) NPV
B) IRR
C) Either A or B
D) Neither A nor B
Answer: C
Diff: 2
Question: 23a

55) Which of the following gives the best estimate of the complete cost of a compromise?
A) ALE
B) ARO
C) TCI
D) Life cycle cost
Answer: C
Diff: 2
Question: 23b

56) The worst problem with classic risk analysis is that _____.
A) protections often protect multiple resources
B) resources often are protected by multiple resources
C) we cannot estimate the annualized rate of occurrence
D) costs and benefits are not the same each year
Answer: C
Diff: 2
Question: 23d

57) The book recommends hard-headed thinking about security ROI analysis.
Answer: FALSE
Diff: 1
Question: 23e

58) Which of the following is a way of responding to risk with active countermeasures?
A) Risk reduction
B) Risk acceptance
C) Risk avoidance
D) All of the above
Answer: A
Diff: 1
Question: 24a

59) _____ means implementing no countermeasures and absorbing any damages that occur.
A) Risk reduction
B) Risk acceptance
C) Risk avoidance
D) None of the above
Answer: B
Diff: 1
Question: 24b

60) _____ means responding to risk by taking out insurance.
A) Risk reduction
B) Risk acceptance
C) Risk avoidance
D) Risk transference
Answer: D
Diff: 1
Question: 24c

61) _____ means responding to risk by not taking a risky action.
A) Risk reduction
B) Risk acceptance
C) Risk avoidance
D) Risk transference
Answer: C
Diff: 1
Question: 24e

62) Responding to risk through risk avoidance is likely to be acceptable to other units of the firm.
Answer: FALSE
Diff: 2
Question: 24f

63) A technical security architecture includes _____.
A) all of a firm's countermeasures
B) how countermeasures are organized
C) Both A and B
D) Neither A nor B
Answer: C
Diff: 1
Question: 25a

64) A technical security architecture should be created _____.
A) annually
B) before a firm creates individual countermeasures
C) before a firm creates a specific countermeasure
D) after each major compromise
Answer: B
Diff: 2
Question: 25c

65) Companies should replace their legacy security technologies immediately.
Answer: FALSE
Diff: 2
Question: 25d

66) Using both a firewall and host hardening to protect a host is _____.
A) defense in depth
B) risk acceptance
C) an anti-weakest link strategy
D) adding berms
Answer: A
Diff: 1
Question: 26a

67) _____ requires multiple countermeasures to be defeated for an attack to succeed.
A) Defense in depth
B) Weakest link analysis
C) Both A and B
D) Neither A nor B
Answer: A
Diff: 1
Question: 26b

68) _____ is a single countermeasure composed of multiple interdependent components in series that require all components to succeed if the countermeasure is to succeed.
A) Defense in depth
B) Weakest link
C) Both A and B
D) Neither A nor B
Answer: B
Diff: 2
Question: 26b

69) Central security consoles _____.
A) are dangerous
B) allow policies to be applied consistently
C) Both A and B
D) Neither A nor B
Answer: C
Diff: 1
Question: 26d

70) Security professionals should minimize burdens on functional departments.
Answer: TRUE
Diff: 1
Question: 26e

71) Having realistic goals for reducing vulnerabilities _____.
A) is giving in to the problem
B) helps to focus on the most critical threats
C) is a cost-saving method
D) is risk avoidance
Answer: B
Diff: 2
Question: 26f

72) Border management _____.
A) is no longer important because there are so many ways to bypass borders
B) is close to a complete solution to access control
C) Both A and B
D) Neither A nor B
Answer: D
Diff: 2
Question: 27b

73) A(n) _____ is a statement of *what* should be done under specific circumstances.
A) implementation control
B) policy
C) policy guidance document
D) procedure
Answer: B
Diff: 1
Question: 28a

74) Policies should specify the details of how protections are to be applied.
Answer: FALSE
Diff: 1
Question: 28b

75) Policies should specify implementation in detail.
Answer: FALSE
Diff: 1
Question: 28c

76) When you wish to create a specific firewall, you should create a security policy for that firewall specifically.
Answer: TRUE
Diff: 2
Question: 29d

77) Policies should be written by _____.
A) IT security
B) corporate teams involving people from multiple departments
C) a senior executive
D) an outside consultant, to maintain independence
Answer: B
Diff: 1
Question: 30

78) _____ are mandatory.
A) Standards
B) Guidelines
C) Both A and B
D) Neither A nor B
Answer: A
Diff: 1
Question: 31a

79) _____ are discretionary.
A) Standards
B) Guidelines
C) Both A and B
D) Neither A nor B
Answer: B
Diff: 1
Question: 31a

80) It is mandatory for decision makers to consider guidelines.
Answer: TRUE
Diff: 2
Question: 31b

81) Guidelines are appropriate in simple and highly certain circumstances.
Answer: FALSE
Diff: 1
Question: 31c

82) _____ specify the low-level detailed actions that must be taken by specific employees.
A) Procedures
B) Processes
C) Both A and B
D) Neither A nor B
Answer: A
Diff: 1
Question: 32a

83) The steps required to issue a new employee a password should be specified in a _____.
A) procedure
B) process
C) Both A and B
D) Neither A nor B
Answer: A
Diff: 2
Question: 32b

84) In manual procedures, the segregation of duties _____.
A) reduces risk
B) increases risk by creating blind spots
C) increases risk by reducing accountability
D) can only be done safely through information technology
Answer: A
Diff: 2
Question: 32c

85) When someone requests to take an action that is potentially dangerous, what protection should be put into place?
A) Limit the number of people that may request an approval
B) Ensure that the approver is the same as the requestor
C) Both A and B
D) Neither A nor B
Answer: A
Diff: 2
Question: 32d

86) Mandatory vacations should be enforced _____.
A) to improve employee diligence to threats
B) to reduce the possibility of collusion between employees
C) to be in compliance with state and federal law
D) for ethical purposes
Answer: B
Diff: 1
Question: 32e

87) _____ are check lists of *what* should be done in a specific procedure.
A) Baselines
B) Guidelines
C) Standards
D) Procedures
Answer: A
Diff: 2
Question: 32f

88) _____ are descriptions of what the best firms in the industry are doing about security.
A) Best practices
B) Recommended practices
C) Both A and B
D) Neither A nor B
Answer: A
Diff: 1
Question: 32g

89) _____ are prescriptive statements about what companies should do and are put together by trade associations and government agencies.
A) Best practices
B) Recommended practices
C) Both A and B
D) Neither A nor B
Answer: B
Diff: 1
Question: 32g

90) The party that is ultimately held accountable for a resource or control is _____.
A) the owner
B) the trustee
C) the accredited security officer
D) the certified security officer
Answer: A
Diff: 2
Question: 32h

91) The owner can delegate _____ to the trustee.
A) the work of implementation of a resource or control
B) accountability for a resource or control
C) Both A and B
D) Neither A nor B
Answer: A
Diff: 2
Question: 32i

92) Different honest people can make different ethical decisions in a given situation.
Answer: TRUE
Diff: 1
Question: 33a

93) Companies create codes of ethics in order to make ethical decision making more predictable.
Answer: TRUE
Diff: 1
Question: 33b

94) In a firm, codes of ethics apply to _____.
A) part-time employees
B) senior managers
C) Both A and B
D) Neither A nor B
Answer: C
Diff: 1
Question: 33d

95) Senior officers often have an additional code of ethics.
Answer: TRUE
Diff: 2
Question: 33e

96) Which of the following is an example of a conflict of interest?
A) Preferential dealings with relatives
B) Investing in competitors
C) Competing with the company while still employed by the company
D) All of the above
Answer: D
Diff: 2
Question: 33h

97) _____ are monetary gifts to induce an employee to favor a supplier or other party.
A) Bribes
B) Kickbacks
C) Both A and B
D) Neither A nor B
Answer: A
Diff: 1
Question: 33k

98) _____ are payments made by a supplier to a corporate buyer when a purchase is made.
A) Bribes
B) Kickbacks
C) Both A and B
D) Neither A nor B
Answer: B
Diff: 1
Question: 33k

99) It is acceptable for an employee to reveal _____.
A) confidential information
B) private information
C) trade secrets
D) None of the above
Answer: D
Diff: 1
Question: 33l

100) Exceptions in policies and procedures should be forbidden.
Answer: FALSE
Diff: 1
Question: 34a

101) Which of the following is a good rule for handling exceptions?
A) Only some people should be allowed to request exceptions.
B) The requestor and approver should be different people.
C) The exception should be documented.
D) All of the above.
Answer: D
Diff: 1
Question: 34c

102) Policies drive _____.
A) implementation
B) oversight
C) Both A and B
D) Neither A nor B
Answer: C
Diff: 1
Question: 35b

103) Conducting stings on employees _____.
A) raises awareness
B) raises resentment
C) Both A and B
D) Neither A nor B
Answer: C
Diff: 1
Question: 35f

104) Electronic employee monitoring is rare.
Answer: FALSE
Diff: 1
Question: 35g

105) Informing employees that monitoring will be done is a bad idea.
Answer: FALSE
Diff: 2
Question: 35h

106) Security metrics allow a company to know if it is improving in its implementation of policies.
Answer: TRUE
Diff: 1
Question: 35j

107) The purpose(s) of auditing is(are) to _____.
A) develop opinions on the health of controls
B) find punishable instances of noncompliance
C) Both A and B
D) Neither A nor B
Answer: A
Diff: 2
Question: 36a

108) Audits place special attention on _____.
A) compliance avoidance
B) noncompliance
C) memo log files
D) absences from duty
Answer: A
Diff: 2
Question: 36c

109) _____ audits are done by an organization on itself.
A) Internal
B) External
C) Both A and B
D) Neither A nor B
Answer: A
Diff: 1
Question: 36d

110) Hotlines for reporting improper behavior are required by law to be non-anonymous.
Answer: FALSE
Diff: 1
Question: 37a

111) Internal corporate attackers often have a history of overt unacceptable behavior.
Answer: TRUE
Diff: 1
Question: 37c

112) Which of the following is *not* one of the three elements in the fraud and abuse triangle?
A) Opportunity
B) Resistance
C) Rationalization
D) Pressure
Answer: B
Diff: 1
Question: 37d

113) Employees usually must rationalize bad behavior.
Answer: TRUE
Diff: 1
Question: 37f

114) Before doing a vulnerability test, a security employee must ensure that _____.
A) doing a vulnerability test is in his or her job description
B) no damage will be done
C) he or she has a specific contract to do a specific test
D) the test is a surprise to everyone, including the tester's superior, who may be engaged in illicit activities
Answer: C
Diff: 1
Question: 38b

115) Which of the following are examples of opportunity?
A) Weak security controls
B) Insufficient oversight from management
C) An unlocked safe
D) All of the above
Answer: D
Diff: 1

116) An example of "pressure" from the fraud triangle would include paying back embezzled money.
Answer: FALSE
Diff: 2

117) A governance framework specifies how to do _____.
A) planning
B) implementation
C) oversight
D) All of the above.
Answer: D
Diff: 1
Question: 40a

118) COSO focuses on _____.
A) corporate internal and financial controls
B) IT governance
C) IT security governance
D) All of the above
Answer: A
Diff: 1
Question: 40b

119) CobiT focuses on _____.
A) corporate governance
B) controlling entire IT function
C) IT security governance
D) All of the above about equally
Answer: B
Diff: 1
Question: 40b

120) In COSO, a company's overall control culture is called its _____.
A) control culture
B) tone at the top
C) control environment
D) security culture
Answer: C
Diff: 1
Question: 41c

121) Which CobiT domain has the most control objectives?
A) Planning & Organization
B) Acquisition & Implementation
C) Delivery & Support
D) Monitoring
Answer: C
Diff: 3
Question: 42d

122) _____ is preferred by U.S. auditors.
A) ISO/IEC 27000 family
B) COSO
C) CobiT
D) PCI-DSS
Answer: C
Diff: 2
Question: 42e

123) The ISO/IEC 2700 family focuses on _____.
A) corporate governance
B) IT governance
C) IT security governance
D) All of the above about equally
Answer: C
Diff: 1
Question: 40c

124) Which of the following specifies how to do certification by external parties?
A) COSO
B) CobiT
C) ISO/IEC 27000
D) All of the above have certification by external parties.
Answer: C
Diff: 2
Question: 43d