CHAPTER 3

Information Risk Management

This domain includes questions from the following topics:

- Benefits and outcomes from an information risk management perspective
- Risk assessment and risk management frameworks
- Developing a risk management strategy
- The risk management lifecycle process
- Integrating risk management into an organization's practices and culture
- The components of a risk assessment: asset value, vulnerabilities, threats, and probability and impact of occurrence
- Risk treatment options: mitigate, accept, transfer, avoid
- The risk register
- Monitoring and reporting risk

The topics in this chapter represent 30 percent of the Certified Information Security Manager (CISM) examination. This chapter discusses CISM job practice 2, "Information Risk Management."

ISACA defines this domain as follows: "Manage information risk to an acceptable level based on risk appetite in order to meet organizational goals and objectives."

When properly implemented, security governance is the foundation that supports security-related strategic decisions and all other security activities. Governance is a process whereby senior management exerts strategic control over business functions through policies, objectives, delegation of authority, and monitoring. Governance is management's oversight for all other business processes to ensure that business processes continue to meet the organization's business vision and objectives effectively.

Organizations usually establish governance through a steering committee that is responsible for setting long-term business strategy and by making changes to ensure that business processes continue to support business strategy and the organization's overall needs. This is accomplished through the development and enforcement of documented policies, standards, requirements, and various reporting metrics.

QUESTIONS

1. An organization has a process whereby security-related hazards are identified, followed by analysis and decisions about what to do about these hazards. What kind of a business process is this?
   - **A.** Vulnerability management
   - **B.** Risk treatment
   - **C.** Risk management
   - **D.** Risk assessment
2. What is the purpose of a cyber-risk management program in an organization?
   - **A.** Consume information from a centralized risk register
   - **B.** Identify and make decisions about information security risks
   - **C.** Plan for future cybersecurity projects and initiatives
   - **D.** Develop mitigating controls
3. All of the following activities are typical inputs into a risk management process *except* which one?
   - **A.** Code reviews
   - **B.** Risk assessments
   - **C.** Threat assessments
   - **D.** Internal audits
4. What should be the primary objective of a risk management strategy?
   - **A.** Determine the organization's risk appetite.
   - **B.** Identify credible risks and transfer them to an external party.
   - **C.** Identify credible risks and reduce them to an acceptable level.
   - **D.** Eliminate credible risks.
5. What are possible outcomes of a risk that has been identified and analyzed in a risk management process?
   - **A.** Acceptance, avoidance, mitigation, transfer, residual
   - **B.** Acceptance, elimination, reduction, transfer
   - **C.** Acceptance, avoidance, elimination, mitigation, transfer
   - **D.** Acceptance, avoidance, mitigation, transfer

6. Dawn, a new CISO in a pharmaceutical company, is reviewing an existing risk management process. The process states that the CISO alone makes all risk treatment decisions. What should Dawn conclude from this observation?

- **A.** The process should be changed so that other business leaders may collaborate on risk treatment decisions.
- **B.** The process is appropriate, as it is the CISO's responsibility to make risk treatment decisions.
- **C.** The process should be changed so that the internal audit department approves risk treatment decisions.
- **D.** The process should be changed so that external regulators approve risk treatment decisions.

7. Marie, a CISO at a manufacturing company, is building a new cyber-risk governance process. For this process to be successful, what is the best first step for Marie to take?

- **A.** Develop a RACI matrix that defines executive roles and responsibilities.
- **B.** Charter a security steering committee consisting of IT and cybersecurity leaders.
- **C.** Develop a risk management process similar to what is found in ISO/IEC 27001.
- **D.** Charter a security steering committee consisting of IT, security, and business leaders.

8. To what audience should communication about new information risks be sent?

- **A.** Customers
- **B.** Security steering committee and executive management
- **C.** All personnel
- **D.** Board of directors

9. An organization's internal audit department is assessing the organization's compliance with PCI-DSS. Internal audit finds that the organization is not compliant with a PCI-DSS control regarding workers' annual acknowledgement of security policy. What kind of a risk has been identified?

- **A.** Insider threat risk
- **B.** Disclosure risk
- **C.** Compliance risk
- **D.** Administrative risk

10. An internal audit team has completed a comprehensive internal audit and has determined that several controls are ineffective. What is the next step that should be performed?

- **A.** Correlate these results with an appropriately scoped penetration test.
- **B.** Develop compensating controls to reduce risk to acceptable levels.
- **C.** Perform a risk assessment.
- **D.** Develop a risk-based action plan to remediate ineffective controls.

11. Which of the following statements is correct regarding applicable regulation and the selection of a security controls framework?

- **A.** An appropriate framework will make it easier to map regulatory details to required activities.
- **B.** It makes no difference which controls framework is selected for regulatory compliance matters.
- **C.** Applicable laws and security control framework have little to do with each other.
- **D.** For regulated organizations, wise selection of control frameworks will result in lower cyber-insurance premiums.

12. In the use of FAIR (Factor Analysis of Information Risk), how does a risk manager determine the potential types of loss?

- **A.** A risk assessment is used to determine what types of loss may occur.
- **B.** The record of prior losses is used.
- **C.** Losses in similar companies are used.
- **D.** Loss types are defined by the FAIR method.

13. Dawn, a CISO in a pharmaceutical organization, is partnering with the company's legal department on the topic of new applicable regulations. Which of the following approaches is most likely to be successful?

- **A.** Examine each new regulation for impact to the organization. Confirm applicability if impact is significant.
- **B.** Examine each new regulation for impact to the organization. Confirm applicability for regulations from other countries.
- **C.** Examine each new regulation for applicability. If applicable, analyze for impact to the organization.
- **D.** Subscribe to a service that informs the organization of new laws. Implement them in the following budget year.

14. What steps must be completed prior to the start of a risk assessment in an organization?

- **A.** Determine the qualifications of the firm that will perform the audit.
- **B.** Determine scope, purpose, and criteria for the audit.
- **C.** Determine the qualifications of the person(s) who will perform the audit.
- **D.** Determine scope, applicability, and purpose for the audit.

15. A risk manager recently completed a risk assessment in an organization. Executive management asked the risk manager to remove one of the findings from the final report. This removal is an example of what?

- **A.** Gerrymandering
- **B.** Internal politics

C. Risk avoidance

D. Risk acceptance

16. Which of the following is *not* a risk management methodology?

A. FRAP

B. ISO/IEC 27005

C. NIST Special Publication 800-39

D. FAIR

17. What is the primary objective of the Factor Analysis of Information Risk (FAIR) methodology?

A. Determine the probability of a threat event.

B. Determine the impact of a threat event.

C. Determine the cost of a threat event.

D. Determine the type of a threat event.

18. Why might the first control objective of CIS be "Inventory of Authorized and Unauthorized Devices"?

A. Most organizations are required to have effective asset inventory processes.

B. The CIS controls framework is hardware asset–centric.

C. Several IT and security processes depend upon an effective hardware inventory.

D. The CIS controls framework is an antiquated controls framework.

19. Why is hardware asset inventory critical for the success of security operations?

A. Critical processes such as software asset and software licensing depend upon accurate asset inventory.

B. Critical processes such as vulnerability management, event management, and antimalware depend upon accurate asset inventory.

C. Vulnerability scans need to cover all hardware assets so that all assets are scanned.

D. Penetration tests need to cover all hardware assets so that all assets are scanned.

20. What are the most important security-related criteria for system classification?

A. Data sensitivity

B. Data sensitivity and operational criticality

C. Operational criticality

D. Location

21. A new CISO in a financial service organization is working to get asset inventory processes under control. The organization uses on-premises and IaaS-based virtualization services. What approach will most effectively identify all assets in use?

- **A.** Perform discovery scans on all networks.
- **B.** Obtain a list of all assets from the patch management platform.
- **C.** Obtain a list of all assets from the security event and information management (SIEM) system.
- **D.** Count all of the servers in each data center.

22. Which of the following security-based metrics is most likely to provide value when reported to management?

- **A.** Number of firewall packets dropped per server per day
- **B.** Number of persons who have completed security awareness training
- **C.** Number of phishing messages blocked per month
- **D.** Percent of production servers that have been patched within SLA

23. Ravila, a CISO, reports security-related metrics to executive management. The trend for the past several months for the metric "Percent of patches applied within SLA for servers supporting manufacturing" is 100 percent, 99.5 percent, 100 percent, 100 percent, 99.2 percent, and 74.5 percent. What action should Ravila take with regard to these metrics?

- **A.** Explain that risk levels have dropped correspondingly.
- **B.** No action is required because this is normal for patch management processes.
- **C.** Investigate the cause of the reduction in patching and report to management.
- **D.** Wait until the next month to see if the metric returns to normal.

24. Duncan is the CISO in a large electric utility. Duncan received an advisory that describes a serious flaw in Intel CPUs that permits an attacker to take control of an affected system. Knowing that much of the utility's industrial control system (ICS) is Intel-based, what should Duncan do next?

- **A.** Report the situation to executive management.
- **B.** Create a new entry in the risk register.
- **C.** Analyze the situation to understand business impact.
- **D.** Declare a security incident.

25. Duncan is the CISO in a large electric utility. Duncan received an advisory that describes a serious flaw in Intel CPUs that permits an attacker to take control of an affected system. After analyzing the advisory, Duncan realizes that many of the ICS devices in the environment are vulnerable. Knowing that much of the utility's industrial control system (ICS) is Intel-based, what should Duncan do next?

A. Create a new entry in the risk register.

B. Report the situation to executive management.

C. Create a new entry in the vulnerability register.

D. Declare a security incident.

26. An internal audit examination of the employee termination process determined that in 20 percent of employee terminations, one or more terminated employee user accounts were not locked or removed. The internal audit department also found that routine monthly user access reviews identified 100 percent of missed account closures, resulting in those user accounts being closed no more than 60 days after users were terminated. What corrective actions, if any, are warranted?

A. Increase user access review process frequency to twice per week.

B. Increase user access review process frequency to weekly.

C. No action is necessary since monthly user access review process is effective.

D. Improve the user termination process to reduce the number of missed account closures.

27. To optimize security operations processes, the CISO in an organization wants to establish an asset classification scheme. The organization has no data classification program. How should the CISO proceed?

A. Establish an asset classification scheme based upon operational criticality.

B. Establish an asset classification scheme based upon operational criticality and data classification.

C. First establish a data classification scheme and then an asset classification scheme based on data classification.

D. Treat all assets equally until a data classification program has been established.

28. A CISO in a U.S.-based healthcare organization is considering implementation of a data classification program. What criteria should be considered for classifying information?

A. Sensitivity, in scope for HIPAA, in scope for HITECH.

B. Monetary value, operational criticality, sensitivity.

C. Information system, storage, business owner.

D. Data at rest, data in motion, data in transit.

29. The Good Doctor healthcare organization has initiated its data management program. One of the early activities is a data discovery project to learn about the extent of sensitive data in unstructured data stores. What is the best method for conducting this data discovery?

- **A.** Implement passive DLP tools on servers and endpoints.
- **B.** Implement intrusive DLP tools on servers and endpoints.
- **C.** Manually examine a randomly chosen set of files to see if they contain sensitive data.
- **D.** Run a data discovery tool against file servers and SharePoint servers.

30. What is typically the greatest challenge when implementing a data classification program?

- **A.** Difficulty with industry regulators
- **B.** Understanding the types of data in use
- **C.** Training end users on data handling procedures
- **D.** Implementing and tuning DLP agents on servers and endpoints

31. Russ, a security manager at a small online retailer, is completing a self-assessment questionnaire for PCI-DSS compliance. In studying the questionnaire, Russ has noted that his organization is not in compliance with all requirements. No auditor will be verifying the accuracy of the questionnaire. What is Russ's best course of action?

- **A.** Complete the form truthfully and notify senior management of the exceptions.
- **B.** Complete the form truthfully and submit it to authorities.
- **C.** Mark each control as compliant and submit it to authorities.
- **D.** Mark each control as compliant and notify senior management that he must be truthful on the next such submission.

32. Russ, a security manager at a small online retailer, learned recently about the European General Data Protection Regulation (GDPR). The retailer has customers all over the world. The organization has outsourced its online catalog, order acceptance, and payment functions to a cloud-based e-commerce platform. Russ is unaware of any efforts that the retailer may have made to be compliant with GDPR. What should Russ do about this?

- **A.** Ask senior management or the legal department about this matter.
- **B.** Assume that the organization is compliant with GDPR.
- **C.** Nothing, because the cloud-based e-commerce platform is required to be GDPR compliant.
- **D.** Contact the cloud-based e-commerce platform and confirm its compliance to GDPR.

33. Russ, a security leader at a global online retailer, is developing a system classification plan. Systems are classified as High, Moderate, or Low, depending upon operational criticality, data sensitivity, and exposure to threats. In a given environment, how should servers that support (such as DNS servers, time servers) High, Moderate, and Low production servers be classified?

- **A.** Support servers should be classified as High, since some servers they support are High.
- **B.** Support servers should be classified as Low, since they do not perform critical transactions, nor do they contain sensitive data.
- **C.** Support servers should be classified at the same level as the lowest-level servers they support.
- **D.** Support servers should be classified at the same level as the highest-level servers they support.

34. Russ, a security leader at a global online retailer, is designing a facilities classification plan to provide more consistency and purpose for physical security controls at the organization's worldwide business and processing locations. What criteria should be used to classify facilities for this purpose?

- **A.** Sensitivity of data stored or accessed there
- **B.** Sensitivity of data stored or accessed there and criticality of operations performed there
- **C.** Criticality of operations performed there
- **D.** Size of facilities and whether there are regulations requiring facilities protection

35. Which of the following is *not* a valid method for assigning asset value?

- **A.** Net present value
- **B.** Replacement cost
- **C.** Repair cost
- **D.** Book value

36. Dylan is an executive security consultant who is assessing a client organization for compliance to various applicable information security and privacy regulations. Dylan has identified compliance issues and recommends that these issues be documented in the client organization's business. How should these issues be documented?

- **A.** Separate entries for each regulation should be made in the organization's risk register.
- **B.** A single entry should be made in the organization's risk register.
- **C.** Separate entries for each regulation should be made in the organization's security incident log.
- **D.** A single entry should be made in the organization's security incident log.

37. For disaster recovery purposes, why is book value *not* a preferred method for determining the value of assets?

A. Information assets have no book value.

B. Book value may vary based on location if a recovery site is located elsewhere.

C. Some assets may not be tracked for depreciation.

D. The cost to replace damaged or destroyed assets could exceed book value.

38. A security analyst has identified a critical server that is missing an important security-related operating system patch. What has the security analyst identified?

A. A vulnerability

B. A threat

C. A risk

D. An incident

39. A security analyst has identified a new technique that cybercriminals are using to break into server operating systems. What has the security analyst identified?

A. A vulnerability

B. A threat

C. A risk

D. An incident

40. Threat actors consist of all of the following *except* which one?

A. Trojans

B. Hacktivists

C. Cybercriminal organizations

D. Employees

41. While deliberating an item in an organization's risk register, members of the cybersecurity steering committee have decided that the organization should discontinue a new feature in its online social media platform. This decision is an example of what?

A. Risk transfer

B. Risk acceptance

C. Risk mitigation

D. Risk avoidance

42. NotPetya is an example of what?

A. Threat

B. Spyware

C. Mass-mailing worm

D. Password-cracking tool

43. Randi, a security architect, is seeking ways to improve a defense-in-depth to defend against ransomware. Randi's organization employs advanced antimalware on all endpoints and antivirus software on its e-mail servers. Endpoints also have an IPS capability that functions while endpoints are onsite or remote. What other solutions should Randi consider to improve defenses against ransomware?

A. Data replication

B. Spam and phishing e-mail filtering

C. File integrity monitoring

D. Firewalls

44. Which European law enforces users' rights to privacy?

A. GLBA

B. GDPR

C. 95/46/EC

D. SB-1386

45. Which mechanism does GDPR provide for multinational organizations to make internal transfers of PII?

A. Model clauses

B. Privacy Shield

C. Safe Harbor

D. Binding corporate rules

46. Which mechanism provides the legal framework for the transfer of information from Europe to the United States?

A. Model clauses

B. Privacy Shield

C. Safe Harbor

D. Binding corporate rules

47. What language is used in legal agreements between organizations regarding the protection of personally identifiable information?

- **A.** Model clauses
- **B.** Privacy Shield
- **C.** Safe Harbor
- **D.** Binding corporate rules

48. Which mechanism was formally used as the legal framework for the transfer of information from Europe to the United States?

- **A.** Model clauses
- **B.** Privacy Shield
- **C.** Safe Harbor
- **D.** Binding corporate rules

49. The internal audit department in a public company recently audited key controls in the vulnerability management process and found that the control "Production servers will be patched within 30 days of receipt of critical patches" fails 30 percent of the time. What finding should the internal audit make?

- **A.** A new control is needed for vulnerability management.
- **B.** The control is ineffective and needs to be corrected.
- **C.** The control should be changed from 30 days to 45 days.
- **D.** The control should be changed from 30 days to 21 days.

50. The internal audit department in an organization recently audited the control "User accounts for terminated workers shall be locked or removed within 48 hours of termination" and found that user accounts for terminated workers are not locked or removed 20 percent of the time. What recommendation should internal audit make?

- **A.** Change the timeframe in the control from 48 hours to 7 days.
- **B.** Add a new compensating control for monthly review of terminated user accounts.
- **C.** Add more staff to the team that manages user accounts.
- **D.** No changes are needed since 20 percent is an acceptable failure rate.

51. Upon examining the change control process in a SaaS provider organization, a new security manager has discovered that the change control process lacks a security impact procedure. What should the security management recommend for this matter?

- **A.** Systems impacted by a change should be scanned before and after changes are made.
- **B.** A post-change security review should be added to the change control process.
- **C.** No change is needed because security is not needed in change control processes.
- **D.** Add a security impact procedure to the change control process so that the security impact of each proposed change can be identified.

52. A SaaS provider performs penetration tests on its services once per year, and many findings are identified each time. The organization's CISO wants to make changes so that penetration test results will improve. The CISO should recommend all of the following changes *except* which one?

A. Add a security review of all proposed software changes into the SDLC.

B. Introduce safe coding training for all software developers.

C. Increase the frequency of penetration tests from annually to quarterly.

D. Add the inclusion of security and privacy requirements into the SDLC.

53. A SaaS provider performs penetration tests on its services once per year, and many findings are identified each time. What is the best way to report this matter to executive management?

A. Develop a KRI that reports the trend of security defects over time.

B. Penetration test reports should be distributed to executive management so that they can have a better understanding of the problem.

C. The executive summary section of penetration test reports should be distributed to executive management.

D. Report the number of defects found to executive management.

54. A SaaS provider performs penetration tests on its services once per year, and many findings are identified each time. What is the best KRI that would highlight risks to executives?

A. Number of software vulnerabilities that exist on production SaaS applications

B. Number of days that critical software vulnerabilities exist on production SaaS applications

C. Number of vulnerability scans performed on production SaaS applications

D. Names of developers who introduced the greatest number of security defects onto production SaaS applications

55. The security leader at a SaaS provider has noticed that the number of security defects in the SaaS application is gradually climbing over time to unacceptable levels. What is the best first step the security leader should take?

A. Contact the software development leader and report that more security defects are being created.

B. Initiate the procurement process for a web application firewall.

C. Initiate a low-severity security incident.

D. Create a new risk register entry that describes the problem along with potential fixes.

56. Why is the KRI "Number of days that critical software vulnerabilities exist on production SaaS applications" considered a leading risk indicator?

- **A.** This is the first KRI that executives are likely to pay attention to.
- **B.** This KRI provides a depiction of the probability of a security incident through the exploitation of vulnerabilities. The risk of an incident is elevated with each successive day that unpatched vulnerabilities exist.
- **C.** Critical software vulnerabilities are the leading cause of security incidents.
- **D.** The KRI indicates that critical software vulnerabilities are the most likely cause of a future incident.

57. Which is the best method for reporting risk matters to senior management?

- **A.** Sending after-action reviews of security incidents
- **B.** Sending the outcomes of risk treatment decisions
- **C.** Periodic briefing on the contents of the risk register
- **D.** Sending memos each time a new risk is identified

58. Janice has worked in the Telco Company for many years and is now the CISO. For several years, Janice has recognized that the engineering organization contacts information security just prior to the release of new products and features so that security can be added in at the end. Now that Janice is the CISO, what is the best long-range solution to this problem?

- **A.** Introduce security at the conceptual, requirements, and design steps in the product development process.
- **B.** Train engineering in the use of vulnerability scanning tools so that they can find and fix vulnerabilities on their own.
- **C.** Add security requirements to other requirements that are developed in product development projects.
- **D.** There is no problem to fix: it is appropriate for engineering to contact security prior to product release to add in necessary security controls.

59. Janice has worked in the Telco Company for many years and is now the CISO. For several years, Janice has recognized that the engineering organization contacts information security just prior to the release of new products and features so that security can be added in at the end. Now that Janice is the CISO, what is the best first step for Janice to take?

- **A.** Initiate a low-severity security incident.
- **B.** Create a new risk register entry that describes the problem along with potential fixes.
- **C.** Initiate a high-severity security incident.
- **D.** Write a memo to the leader of the engineering organization requesting that security be added to the product development lifecycle.

60. The term "insider threat" includes all of the following *except* which one?

- **A.** End users who are ignorant and make unwise decisions
- **B.** Employees who have a grudge against their employer
- **C.** Customers who attempt to break into systems while onsite
- **D.** End users who are doing the right thing but make mistakes

61. Examples of employees gone rogue include all of the following *except* which one?

- **A.** A developer who inserts a time bomb in application source code
- **B.** A securities trader who makes unauthorized trades resulting in huge losses
- **C.** An engineer who locks co-workers out of the network because they are not competent
- **D.** A systems engineer who applies security patches that cause applications to malfunction

62. Janice, a new CISO in a healthcare delivery organization, has discovered that virtually all employees are local administrators on their laptop/desktop computers. This is an example of what?

- **A.** Insider threat
- **B.** Vulnerability
- **C.** Threat
- **D.** Incident

63. An end user in an organization opened an attachment in e-mail, which resulted in ransomware running on the end user's workstation. This is an example of what?

- **A.** Incident
- **B.** Vulnerability
- **C.** Threat
- **D.** Insider threat

64. What is the purpose of the third-party risk management process?

- **A.** Identify risks that can be transferred to third parties.
- **B.** Identify a party responsible for a security breach.
- **C.** Identify a party that can perform risk assessments.
- **D.** Identify and treat risks associated with the use of third-party services.

65. What is the correct sequence of events when onboarding a third-party service provider?

- **A.** Contract negotiation, examine services, identify risks, risk treatment
- **B.** Examine services, identify risks, risk treatment, contract negotiation
- **C.** Examine services, contract negotiation, identify risks, risk treatment
- **D.** Examine services, identify risks, risk treatment

66. A campaign by a cybercriminal to perform reconnaissance on a target organization and develop specialized tools to build a long-term presence in the organization's environment is known as what?

- **A.** Watering hole attack
- **B.** Hacktivism
- **C.** Advanced persistent campaign (APC)
- **D.** Advanced persistent threat (APT)

67. Joel, a CISO in a manufacturing company, has identified a new cybersecurity-related risk to the business and is discussing it privately with the chief risk officer (CRO). The CRO has asked Joel not to put this risk in the risk register. What form of risk treatment does this represent?

- **A.** This is not risk treatment, but the avoidance of managing the risk altogether.
- **B.** This is risk avoidance, where the organization elects to avoid the risk altogether.
- **C.** This is risk transfer, as the organization has implicitly transferred this risk to insurance.
- **D.** This is risk acceptance, as the organization is accepting the risk as-is.

68. Which of the following factors in risk analysis is the most difficult to determine?

- **A.** Exposure factor
- **B.** Single-loss expectancy
- **C.** Event probability
- **D.** Event impact

69. An estimate on the number of times that a threat might occur in a given year is known as what?

- **A.** Annualized loss expectancy (ALE)
- **B.** Annualized rate of occurrence (ARO)
- **C.** Exposure factor (EF)
- **D.** Annualized exposure factor (AEF)

70. Which is the best method for prioritizing risks and risk treatment?

- **A.** Threat event probability times asset value, from highest to lowest
- **B.** Threat event probability, followed by asset value
- **C.** Professional judgment
- **D.** A combination of threat event probability, asset value, and professional judgment

71. Joel is a security manager in a large manufacturing company. The company uses primarily Microsoft, Cisco, and Oracle products. Joel subscribes to security bulletins from these three vendors. Which of the following statements best describes the adequacy of these advisory sources?

- **A.** Joel should also subscribe to nonvendor security sources such as US-CERT and InfraGard.
- **B.** Joel's security advisory sources are adequate.
- **C.** Joel should discontinue vendor sources and subscribe to nonvendor security sources such as US-CERT and InfraGard.
- **D.** Joel should focus on threat hunting in the dark web.

72. The primary advantage of automatic controls versus manual controls includes all of the following *except* which one?

- **A.** Automatic controls are generally more reliable than manual controls.
- **B.** Automatic controls are less expensive than manual controls.
- **C.** Automatic controls are generally more consistent than manual controls.
- **D.** Automatic controls generally perform better in audits than manual controls.

73. Which of the following statements about PCI-DSS compliance is true?

- **A.** Only organizations that store, transfer, or process more than 6 million credit card numbers are required to undergo an annual PCI audit.
- **B.** Service providers are not required to submit an attestation of compliance (AOC) annually.
- **C.** Merchants that process fewer than 15,000 credit card transactions are not required to submit an attestation of compliance (AOC).
- **D.** All organizations that store, transfer, or process credit card data are required to submit an attestation of compliance (AOC) annually.

74. A security leader wants to commission an outside company to assess the organization's performance against the NIST SP800-53 control framework to see which controls the organization is operating properly and which controls require improvement. What kind of an assessment does the security leader need to commission?

- **A.** Controls risk assessment
- **B.** Controls maturity assessment
- **C.** Controls gap assessment
- **D.** Risk assessment

75. An organization needs to better understand how well organized its operations are from a controls point of view. What kind of an assessment will best reveal this?

A. Controls risk assessment

B. Controls maturity assessment

C. Controls gap assessment

D. Risk assessment

76. An organization needs to better understand which of its controls are more important than others. What kind of an assessment will best reveal this?

A. Controls risk assessment

B. Controls maturity assessment

C. Controls gap assessment

D. Risk assessment

77. An organization needs to better understand whether its control framework is adequately protecting the organization from known and unknown hazards. What kind of an assessment will best reveal this?

A. Controls risk assessment

B. Controls maturity assessment

C. Controls gap assessment

D. Risk assessment

78. An organization recently suffered a significant security incident. The organization was surprised by the incident and believed that this kind of an event would not occur. To avoid a similar event in the future, what should the organization do next?

A. Commission an enterprise-wide risk assessment.

B. Commission a controls maturity assessment.

C. Commission an internal and external penetration test.

D. Commission a controls gap assessment.

79. Stephen is a security leader for a SaaS company that provides file storage services to corporate clients. Stephen is examining proposed contract language from a prospective customer that is requiring the SaaS company implement "best practices" for protecting customer information. How should Stephen respond to this contract language?

A. Stephen should accept the contract language as-is.

B. Stephen should not accept a customer's contract but instead use his company's contract language.

C. Stephen should change the language from "best practices" to "industry-standard practices."

D. Stephen should remove the security-related language as it is unnecessary for a SaaS environment.

80. Security analysts in the SOC have noticed that the organization's firewall is being scanned by a port scanner in a hostile country. Security analysts have notified the security manager. How should the security manager respond to this matter?

A. Declare a high-severity security event.

B. Declare a low-severity security event.

C. Take no action.

D. Direct the SOC to blackhole the scan's originating IP address.

81. A security leader recently commissioned a controls maturity assessment and has received the final report. Control maturity in the assessment is classified as "Initial," "Managed," "Defined," "Quantitatively Managed," and "Optimized." What maturity scale was used in this maturity assessment?

A. Organizational Project Maturity Model

B. Open Source Maturity Model

C. Capability Maturity Model

D. Capability Maturity Model Integrated

82. Security analysts in the SOC have noticed a large volume of phishing e-mails that are originating from a single "from" address. Security analysts have notified the security manager. How should the security manager respond to the matter?

A. Declare a high-level security incident.

B. Block all incoming e-mail from that address at the e-mail server or spam filter.

C. Issue an advisory to all employees to be on the lookout for suspicious messages and to disregard them.

D. Blackhole the originating IP address.

83. The corporate controller in an organization recently received an e-mail from the CEO with instructions to wire a large amount of money to an offshore bank account that is part of secret merger negotiations. How should the corporate controller respond?

A. Contact the CEO and ask for confirmation.

B. Wire the money as directed.

C. Reply to the e-mail and ask for confirmation.

D. Direct the wire transfer clerk to wire the money as directed.

84. An organization's information security department conducts quarterly user access reviews of the financial accounting system. Who is the best person to approve users' continued access to roles in the system?

- **A.** Security manager
- **B.** IT manager
- **C.** Corporate controller
- **D.** Users' respective managers

85. All of the following are possible techniques for setting the value of information in a database *except* which one?

- **A.** Recovery cost
- **B.** Replacement cost
- **C.** Lost revenue
- **D.** Book value

86. For disaster recovery scenarios, which of the following methods for setting the value of computer equipment is most appropriate?

- **A.** Recovery cost
- **B.** Replacement cost
- **C.** Lost revenue
- **D.** Book value

87. A security leader in a SaaS services organization has recently commissioned a controls maturity assessment. The consultants who performed the assessment used the CMMI model for rating individual control maturity. The assessment report rated most controls from 2.5 to 3.5 on a scale of 1 to 5. How should the security leader interpret these results?

- **A.** Acceptable: the maturity scores are acceptable and align with those of other software companies.
- **B.** Unacceptable: develop a strategy to improve control maturity to 4.5–5.0 over the next three to four years.
- **C.** Unacceptable: develop a strategy to improve control maturity to 3.4–4.5 over the next three to four years.
- **D.** Irrelevant: too little is known to make a determination of long-term maturity targets.

88. In a mature third-party risk management (TPRM) program, how often are third parties typically assessed?

- **A.** At the time of onboarding and annually thereafter
- **B.** At the time of onboarding
- **C.** At the time of onboarding and annually thereafter if the third party is rated as high risk
- **D.** At the time of onboarding and later on if the third party has a security incident

89. David, a security analyst in a financial services firm, has requested the Expense Management Company, a service provider, to furnish him with a SOC1 audit report. The Expense Management Company furnished David with a SOC1 audit report for the hosting center where Expense Management Company servers are located. How should David respond?

- **A.** File the report and consider the Expense Management Company as assessed.
- **B.** Analyze the report for significant findings.
- **C.** Thank them for the report.
- **D.** Thank them for the report and request a SOC1 audit report for the Expense Management Company itself.

90. A healthcare delivery organization has a complete inventory of third-party service providers and keeps good records on initial and follow-up assessments. What information should be reported to management?

- **A.** Metrics related to the number of third-party assessments that are performed
- **B.** A risk dashboard that indicates patterns and trends of risks associated with third parties
- **C.** Metrics related to the number of third-party assessments, along with their results
- **D.** Status on whether there are sufficient resources to perform third-party risk assessments

QUICK ANSWER KEY

1. C	**31.** A	**61.** D
2. B	**32.** A	**62.** B
3. A	**33.** D	**63.** A
4. C	**34.** B	**64.** D
5. D	**35.** C	**65.** B
6. A	**36.** B	**66.** D
7. D	**37.** D	**67.** A
8. B	**38.** A	**68.** C
9. C	**39.** B	**69.** B
10. D	**40.** A	**70.** D
11. A	**41.** D	**71.** A
12. D	**42.** A	**72.** B
13. C	**43.** B	**73.** D
14. B	**44.** B	**74.** C
15. D	**45.** D	**75.** B
16. D	**46.** B	**76.** A
17. A	**47.** A	**77.** D
18. C	**48.** C	**78.** A
19. B	**49.** B	**79.** C
20. B	**50.** B	**80.** D
21. A	**51.** D	**81.** D
22. D	**52.** C	**82.** B
23. C	**53.** A	**83.** A
24. C	**54.** B	**84.** C
25. B	**55.** D	**85.** D
26. D	**56.** B	**86.** B
27. A	**57.** C	**87.** A
28. B	**58.** A	**88.** C
29. D	**59.** B	**89.** D
30. C	**60.** C	**90.** B

ANSWERS

A

1. An organization has a process whereby security-related hazards are identified, followed by analysis and decisions about what to do about these hazards. What kind of a business process is this?

A. Vulnerability management

B. Risk treatment

C. Risk management

D. Risk assessment

☑ **C**. The risk management process consists of risk assessments, analysis about risks that are identified by risk assessment, followed by discussions, and finally decisions about what to do about these risks.

☒ **A**, **B**, and **D** are incorrect. **A** is incorrect because the steps in the question do not describe a vulnerability management process. **B** is incorrect because the steps in the question do not describe a risk treatment process. However, risk treatment is a part of the risk management process. **D** is incorrect because the steps in the question do not describe a risk management process. Risk assessment is a part of the risk management process.

2. What is the purpose of a cyber-risk management program in an organization?

A. Consume information from a centralized risk register

B. Identify and make decisions about information security risks

C. Plan for future cybersecurity projects and initiatives

D. Develop mitigating controls

☑ **B**. The purpose of a risk management program is to use various means to identify risks in an organization and then study and make decisions about those risks through a process known as risk treatment.

☒ **A**, **C**, and **D** are incorrect. **A** is incorrect because the purpose of a risk management program is not to consume information from the risk register, but instead to populate it and manage information there. **C** is incorrect because the core purpose of risk management is not long-term planning, but the management of risk. An *output* of the risk treatment process is a series of decisions that may result in one or more initiatives and projects to take place in the future. **D** is incorrect because this is too narrow a definition of risk management; while mitigating controls will sometimes be developed as a result of risk management, there are other outcomes as well.

3. All of the following activities are typical inputs into a risk management process *except* which one?

A. Code reviews

B. Risk assessments

C. Threat assessments

D. Internal audits

☑ **A**. A code review is not a typical input to a risk management process, primarily because a code review represents a narrow, tactical examination of a program's source code. Output from a code review would likely be fed into a software defect tracking process or a vulnerability management process.

☒ **B**, **C**, and **D** are incorrect. They are incorrect because risk assessments, threat assessments, and internal audits *would* typically result in issues being processed by a risk management process. The distinction is this: A standard risk management process is designed to tackle cyber risks that are systemic in an organization. Examples of such risks include weaknesses in business processes and overarching design problems in complex information systems. Issues such as missing patches, security configuration problems, and software vulnerabilities are instead handled by tactical vulnerability management and software defect management processes.

4. What should be the primary objective of a risk management strategy?

A. Determine the organization's risk appetite.

B. Identify credible risks and transfer them to an external party.

C. Identify credible risks and reduce them to an acceptable level.

D. Eliminate credible risks.

☑ **C**. The primary objective of a risk management strategy is the identification of risks, followed by the reduction of those risks to levels acceptable to executive management.

☒ **A**, **B**, and **D** are incorrect. **A** is incorrect because the determination of risk appetite, while important—and essential to the proper functioning of a risk management program—is not the main purpose of a risk management strategy. **B** is incorrect because transferring risks to external parties is but one of several possible outcomes for risks that are identified. **D** is incorrect because risks cannot be eliminated, only reduced to acceptable levels.

5. What are possible outcomes of a risk that has been identified and analyzed in a risk management process?

A. Acceptance, avoidance, mitigation, transfer, residual

B. Acceptance, elimination, reduction, transfer

C. Acceptance, avoidance, elimination, mitigation, transfer

D. Acceptance, avoidance, mitigation, transfer

☑ **D**. The four possible outcomes of a risk in a risk management process are acceptance, avoidance, mitigation, and transfer. These are known as *risk treatment* options.

☒ **A**, **B**, and **C** are incorrect because these are not the outcomes of risk treatment in a risk management process. Elimination is not a valid risk treatment option because risks cannot be eliminated altogether. Residual is not a valid risk treatment option; instead, residual risk is defined as the "leftover" risk after the original risk has been reduced through mitigation or transfer.

6. Dawn, a new CISO in a pharmaceutical company, is reviewing an existing risk management process. The process states that the CISO alone makes all risk treatment decisions. What should Dawn conclude from this observation?

A. The process should be changed so that other business leaders may collaborate on risk treatment decisions.

B. The process is appropriate, as it is the CISO's responsibility to make risk treatment decisions.

C. The process should be changed so that the internal audit department approves risk treatment decisions.

D. The process should be changed so that external regulators approve risk treatment decisions.

☑ **A**. Risk treatment decisions are business decisions that should be made by business leaders in collaboration with the CISO. The CISO should not be making unilateral decisions on behalf of the business.

☒ **B**, **C**, and **D** are incorrect. **B** is incorrect because the CISO should not be making unilateral decisions about risk on behalf of the business. Business leaders should *at least* participate in, and agree with, these decisions. **C** is incorrect because it is not appropriate for an internal audit department to make risk treatment decisions (except, possibly, for risk treatment decisions that are directly related to the internal audit function). **D** is incorrect because it is not appropriate for outside regulators to make an organization's risk treatment decisions; at most, regulators may be informed of such decisions.

7. Marie, a CISO at a manufacturing company, is building a new cyber-risk governance process. For this process to be successful, what is the best first step for Marie to take?

A. Develop a RACI matrix that defines executive roles and responsibilities.

B. Charter a security steering committee consisting of IT and cybersecurity leaders.

C. Develop a risk management process similar to what is found in ISO/IEC 27001.

D. Charter a security steering committee consisting of IT, security, and business leaders.

☑ **D**. The best course of action is the formation of a chartered information security steering committee that consists of IT and security leaders, as well as business leaders. For security governance to succeed, business leaders need to be involved and participate in discussions and decisions.

☒ **A**, **B**, and **C** are incorrect. **A** is incorrect because a RACI matrix, while important, is but a small part of a chartered information security steering committee. **B** is incorrect because a security steering committee must include business leaders. **C** is incorrect because this question is about security governance, which is more than just a risk management process.

8. To what audience should communication about new information risks be sent?

A. Customers

B. Security steering committee and executive management

C. All personnel

D. Board of directors

☑ **B**. New developments concerning information risk should be sent to the information security steering committee and executive management. This is a part of a typical risk management process that includes risk communication.

☒ **A**, **C**, and **D** are incorrect. **A** is incorrect because information risk matters are generally internal matters that are not shared with outside parties. Exceptions, of course, may include disclosures about risks and incidents as required by law, as well as through private legal obligations. **C** is incorrect because matters of information risk should not be shared to a wide audience such as all internal staff. **D** is incorrect because a board of directors does not necessarily need to know about all risks.

9. An organization's internal audit department is assessing the organization's compliance with PCI-DSS. Internal audit finds that the organization is not compliant with a PCI-DSS control regarding workers' annual acknowledgement of security policy. What kind of a risk has been identified?

A. Insider threat risk

B. Disclosure risk

C. Compliance risk

D. Administrative risk

☑ **C**. This is primarily a matter of compliance risk. Organizations handling credit card data are required to comply with all controls in PCI-DSS, whether they represent actual risks or not.

☒ **A**, **B**, and **D** are incorrect. These are not the appropriate terms for this type of risk. In addition to risks related to information theft, disclosure, and destruction, organizations need to understand matters of compliance risk, which may result in fines or sanctions and may become public matters in some circumstances.

10. An internal audit team has completed a comprehensive internal audit and has determined that several controls are ineffective. What is the next step that should be performed?

A. Correlate these results with an appropriately scoped penetration test.

B. Develop compensating controls to reduce risk to acceptable levels.

C. Perform a risk assessment.

D. Develop a risk-based action plan to remediate ineffective controls.

☑ **D**. Typically, organizations are compelled to remediate most or all findings identified by an internal audit department. Taking a risk-based approach is sensible because this serves to remediate findings by addressing the highest-risk findings first.

☒ **A**, **B**, and **C** are incorrect. **A** is incorrect because correlation with a penetration test would rarely be a prudent next step (unless the internal audit was solely focused on security configuration of target systems). **B** is incorrect because compensating controls are not the "go-to" remedy for curing control ineffectiveness; in some cases, compensating controls may be used, but this is not a typical approach. **C** is incorrect because a risk assessment does nothing to remediate control effectiveness findings.

11. Which of the following statements is correct regarding applicable regulation and the selection of a security controls framework?

A. An appropriate framework will make it easier to map regulatory details to required activities.

B. It makes no difference which controls framework is selected for regulatory compliance matters.

C. Applicable laws and security control framework have little to do with each other.

D. For regulated organizations, wise selection of control frameworks will result in lower cyber-insurance premiums.

☑ **A**. Applicable regulations may or may not be specific to required activities. In some cases, control frameworks are available that closely resemble required activities. Selection of a control framework that corresponds to an applicable law or regulation may help an organization to better align regulatory requirements with required activities.

☒ **B**, **C**, and **D** are incorrect. **B** is incorrect because there are cases where specific frameworks have coverage for specific regulations. For example, U.S. federal government agencies as well as service providers that provide information-related services to one or more of those agencies often follow NIST SP800-53, as the controls in NIST SP800-53 are required of these organizations. Similarly, organizations that manage credit card payment information often adopt PCI-DSS as a control framework because they are specifically required to comply with all PCI-DSS requirements. (Note that PCI-DSS is not actually a law, but its position in the payments ecosystem gives it strong resemblance to regulation.) **C** is incorrect since this blanket statement is not true. **D** is incorrect because the question is not addressing cyber-risk insurance.

12. In the use of FAIR (Factor Analysis of Information Risk), how does a risk manager determine the potential types of loss?

A. A risk assessment is used to determine what types of loss may occur.

B. The record of prior losses is used.

C. Losses in similar companies are used.

D. Loss types are defined by the FAIR method.

☑ **D**. The FAIR (Factor Analysis of Information Risk) analysis method contains six types of loss, which are Productivity, Response, Replacement, Fines and Judgments, Competitive Advantage, and Reputation. According to the FAIR method, any cybersecurity incident would result in one or more of these losses.

☒ **A**, **B**, and **C** are incorrect because the FAIR methodology does not employ these means. Instead, FAIR uses six types of loss: Productivity, Response, Replacement, Fines and Judgments, Competitive Advantage, and Reputation. The FAIR method does not accommodate any other types of loss.

13. Dawn, a CISO in a pharmaceutical organization, is partnering with the company's legal department on the topic of new applicable regulations. Which of the following approaches is most likely to be successful?

A. Examine each new regulation for impact to the organization. Confirm applicability if impact is significant.

B. Examine each new regulation for impact to the organization. Confirm applicability for regulations from other countries.

C. Examine each new regulation for applicability. If applicable, analyze for impact to the organization.

D. Subscribe to a service that informs the organization of new laws. Implement them in the following budget year.

☑ **C**. Because there are so many regulations of different kinds, it is first necessary to determine which ones are applicable to the organization. For regulations that are applicable, the next best course of action is to understand the impact of the regulation on business processes and costs and then develop an action plan for complying with the regulation.

☒ **A**, **B**, and **D** are incorrect. **A** and **B** are incorrect because these approaches will cause unnecessary burden on the organization. Regulations should first be vetted for applicability; if they are not applicable, no further work needs to be done. **D** is incorrect because this answer does not include the vital step of determining applicability. That said, a subscription service for new and emerging laws and regulations may be cost-effective for many organizations.

14. What steps must be completed prior to the start of a risk assessment in an organization?

A. Determine the qualifications of the firm that will perform the audit.

B. Determine scope, purpose, and criteria for the audit.

C. Determine the qualifications of the person(s) who will perform the audit.

D. Determine scope, applicability, and purpose for the audit.

☑ **B**. According to ISO/IEC 27005 and other risk management frameworks, it is first necessary to establish the context of an audit. This means making a determination of the scope of the audit—which parts of the organization are to be included. Also, it is necessary to determine the purpose of the risk assessment; for example, determining control coverage, control effectiveness, or business process effectiveness. Finally, the criteria for the audit need to be determined.

☒ **A**, **C**, and **D** are incorrect. **A** and **C** are incorrect because any confirmation of qualifications would be determined prior to this point. **D** is incorrect because an audit that was not applicable should not be performed.

15. A risk manager recently completed a risk assessment in an organization. Executive management asked the risk manager to remove one of the findings from the final report. This removal is an example of what?

A. Gerrymandering

B. Internal politics

C. Risk avoidance

D. Risk acceptance

☑ **D**. Although this is a questionable approach, removal of a risk finding in a report is, implicitly, risk acceptance. It could, however, be even worse than that, and in some industries, this could be considered negligent and a failure of due care. A risk manager should normally object to such an action and may consider documenting the matter or even filing a formal protest.

☒ **A**, **B**, and **C** are incorrect. **A** is incorrect because the term "gerrymandering" is related to the formation of electoral districts in government. **B** is incorrect because, although the situation may be an example of internal politics, this is not the best answer. **C** is incorrect because risk avoidance is defined as a discontinuation of the activity related to the risk.

16. Which of the following is *not* a risk management methodology?

A. FRAP

B. ISO/IEC 27005

C. NIST Special Publication 800-39

D. FAIR

☑ **D**. FAIR (Factor Analysis of Information Risk) is not a risk management framework, but a risk *assessment* methodology. Though closely related, a risk management framework is concerned with the outcomes of risk assessments, but not the performance of the risk assessments themselves.

☒ **A**, **B**, and **C** are incorrect because FRAP, ISO/IEC 27005, and NIST SP 800-39 are examples of risk management frameworks.

17. What is the primary objective of the Factor Analysis of Information Risk (FAIR) methodology?

A. Determine the probability of a threat event.

B. Determine the impact of a threat event.

C. Determine the cost of a threat event.

D. Determine the type of a threat event.

☑ **A**. The primary objective of FAIR is to determine the probability of an event using "what if" analysis, which cannot be easily done using maturity models or checklists.

☒ **B**, **C**, and **D** are incorrect because FAIR is not used to determine the impact, cost, or type of a threat or threat event.

18. Why might the first control objective of CIS be "Inventory of Authorized and Unauthorized Devices"?

A. Most organizations are required to have effective asset inventory processes.

B. The CIS controls framework is hardware asset–centric.

C. Several IT and security processes depend upon an effective hardware inventory.

D. The CIS controls framework is an antiquated controls framework.

☑ **C**. It is postulated that CIS places hardware asset inventory as its first control because hardware inventory is central to critical processes such as vulnerability management, security event monitoring, and malware prevention and response.

☒ **A**, **B**, and **D** are incorrect. **A** is incorrect because this answer is a distractor. **B** and **D** are incorrect because these statements about CIS are untrue.

19. Why is hardware asset inventory critical for the success of security operations?

A. Critical processes such as software asset and software licensing depends upon accurate asset inventory.

B. Critical processes such as vulnerability management, event management, and antimalware depend upon accurate asset inventory.

C. Vulnerability scans need to cover all hardware assets so that all assets are scanned.

D. Penetration tests need to cover all hardware assets so that all assets are scanned.

☑ **B**. Vulnerability management, event visibility, and malware control are among the most critical security operations processes. When these processes are effective, the chances of a successful attack diminish significantly. When asset inventory processes are ineffective, it is possible that there will be assets that are not scanned for vulnerabilities, monitored for events, or protected by antimalware. Intruders are able to identify these assets, which makes asset inventory a critically important activity in information security.

☒ **A**, **C**, and **D** are incorrect. **A** is incorrect because software inventory, while important for security operations, is not as important as vulnerability management, event management, and malware control. **C** and **D** are incorrect because vulnerability management and penetration tests, while important, are only a portion of critical activities that depend upon effective asset management.

20. What are the most important security-related criteria for system classification?

A. Data sensitivity

B. Data sensitivity and operational criticality

C. Operational criticality

D. Location

☑ **B**. Generally, the operational criticality of a system and the sensitivity of information stored in or processed by the system are the two most important criteria that determine a system's classification.

☒ **A**, **C**, and **D** are incorrect. **A** is incorrect because data sensitivity alone does not take into account operational criticality. **C** is incorrect because operational criticality alone does not take into account data sensitivity. **D** is incorrect because location alone does not take into account operational criticality or data sensitivity.

21. A new CISO in a financial service organization is working to get asset inventory processes under control. The organization uses on-premises and IaaS-based virtualization services. What approach will most effectively identify all assets in use?

A. Perform discovery scans on all networks.

B. Obtain a list of all assets from the patch management platform.

C. Obtain a list of all assets from the security event and information management (SIEM) system.

D. Count all of the servers in each data center.

☑ **A**. Although none of these approaches is ideal, performing discovery scans on all networks is the best first step. Even so, it will be necessary to consult with network engineers to ensure that discovery scans will scan all known networks in on-premises and IaaS environments. Other helpful steps include interviewing system engineers to understand virtual machine management systems and obtain inventory information from them.

☒ **B**, **C**, and **D** are incorrect. **B** is incorrect because patch management systems may not be covering all assets in the organization's environment. **C** is incorrect because the SIEM may not be receiving log data from all assets in the organization's environment. **D** is incorrect because the organization is using virtualization technology, as well as IaaS-based platforms; counting servers in an on-premises data center will fail to discover virtual assets and IaaS-based assets.

22. Which of the following security-based metrics is most likely to provide value when reported to management?

A. Number of firewall packets dropped per server per day

B. Number of persons who have completed security awareness training

C. Number of phishing messages blocked per month

D. Percent of production servers that have been patched within SLA

☑ **D**. Of the choices listed, this metric will provide the most value and meaning to management, because this helps to reveal the security posture of production servers that support the business.

☒ **A**, **B**, and **C** are incorrect. **A** is incorrect because the number of packets dropped by the firewall does not provide any business value to management. **B** is incorrect because, although it does provide some value to management, this is not as good an answer as **D**. **C** is incorrect because the number of phishing messages blocked does not provide much business value to management.

23. Ravila, a CISO, reports security-related metrics to executive management. The trend for the past several months for the metric "Percent of patches applied within SLA for servers supporting manufacturing" is 100 percent, 99.5 percent, 100 percent, 100 percent, 99.2 percent, and 74.5 percent. What action should Ravila take with regards to these metrics?

A. Explain that risk levels have dropped correspondingly.

B. No action is required because this is normal for patch management processes.

C. Investigate the cause of the reduction in patching and report to management.

D. Wait until the next month to see if the metric returns to normal.

☑ **C**. As patching is an important activity, and because the servers support critical business operations, this sudden drop in patch coverage needs to be investigated immediately and corrected as quickly as possible.

☒ **A**, **B**, and **D** are incorrect. **A** is incorrect because a reduction in risk levels would not result in a decrease in patching. **B** is incorrect because the reduction in patch coverage is *not* a normal event. **D** is incorrect because it would be unwise to "wait and see" regarding such an important activity as server patching.

24. Duncan is the CISO in a large electric utility. Duncan received an advisory that describes a serious flaw in Intel CPUs that permits an attacker to take control of an affected system. Knowing that much of the utility's industrial control system (ICS) is Intel-based, what should Duncan do next?

A. Report the situation to executive management.

B. Create a new entry in the risk register.

C. Analyze the situation to understand business impact.

D. Declare a security incident.

☑ **C**. Though it's tempting to notify executive management immediately, without first understanding any potential business impact, there's little to tell. For this reason, the best first step is to analyze the matter so that any business impact can be determined.

☒ **A**, **B**, and **D** are incorrect. **A** is incorrect because the impact is not yet known. **B** is incorrect because it is not the best answer. After understanding the matter, it may indeed be prudent to create a risk register entry, particularly if the matter is complicated and likely to persist for some time. **D** is incorrect because the impact of the advisory on the organization is not yet known. In some incident response plans, however, organizations may use advisories like this as a trigger for emergency analysis to take place.

25. Duncan is the CISO in a large electric utility. Duncan received an advisory that describes a serious flaw in Intel CPUs that permits an attacker to take control of an affected system. After analyzing the advisory, Duncan realizes that many of the ICS devices in the environment are vulnerable. Knowing that much of the utility's industrial control system (ICS) is Intel-based, what should Duncan do next?

A. Create a new entry in the risk register.

B. Report the situation to executive management.

C. Create a new entry in the vulnerability register.

D. Declare a security incident.

☑ **B**. Because the CISO has analyzed the advisory, the impact to the organization can be known. This matter should be reported to executive management, along with an explanation of business impact and a remediation plan.

☒ **A**, **C**, and **D** are incorrect. **A** is incorrect because this matter has greater urgency than the risk management lifecycle is likely to provide. If, however, it is determined that there is no easy or quick fix, a risk register entry might be warranted. **C** is incorrect because it may be necessary to create many entries instead of a single entry. There may be many different types of devices that are affected by the advisory, necessitating an entry for each time, or an entry for each device, depending upon how the organization manages its vulnerabilities. **D** is incorrect because most organizations' incident response plans do not address vulnerabilities, but actual threat events.

26. An internal audit examination of the employee termination process determined that in 20 percent of employee terminations, one or more terminated employee user accounts were not locked or removed. The internal audit department also found that routine monthly user access reviews identified 100 percent of missed account closures, resulting in those user accounts being closed no more than 60 days after users were terminated. What corrective actions, if any, are warranted?

A. Increase user access review process frequency to twice per week.

B. Increase user access review process frequency to weekly.

C. No action is necessary since monthly user access review process is effective.

D. Improve the user termination process to reduce the number of missed account closures.

☑ **D**. The rate that user terminations are not performed properly is too high. Increasing the frequency of user access reviews will likely take too much time. The best remedy is to find ways of improving the user termination process. Since the "miss" rate is 20 percent, it is assumed that all processes are manual.

☒ **A**, **B**, and **C** are incorrect. **A** and **B** are incorrect because the user access review process likely takes too much effort. Since the "miss" rate is 20 percent, it is assumed that all processes are manual. **C** is incorrect, since the "miss" rate of 20 percent would be considered too high in most organizations. An acceptable rate would be under 2 percent.

27. To optimize security operations processes, the CISO in an organization wants to establish an asset classification scheme. The organization has no data classification program. How should the CISO proceed?

A. Establish an asset classification scheme based upon operational criticality.

B. Establish an asset classification scheme based upon operational criticality and data classification.

C. First establish a data classification scheme and then an asset classification scheme based on data classification.

D. Treat all assets equally until a data classification program has been established.

☑ **A**. Even in the absence of a data classification program, an asset classification program can be developed. In such a case, asset classification cannot be based on data classification, but assets can be classified according to business operational criticality. For example, assets can be mapped to a business impact analysis (BIA) to determine which assets are the most critical to the business.

☒ **B**, **C**, and **D** are incorrect. **B** is incorrect because there is no data classification scheme upon which to base an asset classification scheme. **C** is incorrect because it can take a great deal of time to develop a data classification scheme and map data to assets. It is assumed that the CISO wants to establish the asset classification scheme quickly. **D** is incorrect because there should be an opportunity to classify assets according to operational criticality. If, however, there is little or no sense of business process priority and criticality, then, yes, it might be premature to develop an asset classification scheme.

28. A CISO in a U.S.-based healthcare organization is considering implementation of a data classification program. What criteria should be considered for classifying information?

A. Sensitivity, in scope for HIPAA, in scope for HITECH.

B. Monetary value, operational criticality, sensitivity.

C. Information system, storage, business owner.

D. Data at rest, data in motion, data in transit.

☑ **B**. Monetary value, operational criticality, and sensitivity are typical considerations for data classification. Some organizations may have additional considerations, such as intellectual property.

☒ **A**, **C**, and **D** are incorrect. **A** is incorrect because these are not the best criteria. **C** is incorrect because these considerations are not the best criteria. **D** is incorrect because these are not classification considerations, but data-handling use cases.

29. The Good Doctor healthcare organization has initiated its data management program. One of the early activities is a data discovery project to learn about the extent of sensitive data in unstructured data stores. What is the best method for conducting this data discovery?

A. Implement passive DLP tools on servers and endpoints.

B. Implement intrusive DLP tools on servers and endpoints.

C. Manually examine a randomly chosen set of files to see if they contain sensitive data.

D. Run a data discovery tool against file servers and SharePoint servers.

☑ **D**. The best first activity is to run special-purpose data discovery tools against all unstructured data stores such as file servers, SharePoint servers, and cloud provider data stores. This will help the organization better understand the extent of sensitive data in these systems. Results from this activity can be used to determine what next steps are appropriate.

☒ **A**, **B**, and **C** are incorrect. **A** and **B** are incorrect because these are more intrusive and time-consuming options that may or may not be needed. **C** is incorrect because random sampling may miss significant instances, and this option may require excessive time.

30. What is typically the greatest challenge when implementing a data classification program?

A. Difficulty with industry regulators

B. Understanding the types of data in use

C. Training end users on data handling procedures

D. Implementing and tuning DLP agents on servers and endpoints

☑ **C**. The most difficult challenge associated with implementing a data classification program is ensuring that workers understand and are willing to comply with data handling procedures. By comparison, automation is simpler primarily because it is deterministic.

☒ **A**, **B**, and **D** are incorrect. **A** is incorrect because regulators are not typically as concerned with data classification as they are with the protection of relevant information. **B** is incorrect because, although it can be a challenge understanding the data in use in an organization, user compliance is typically the biggest challenge. **D** is incorrect because implementing and tuning agents are not usually as challenging as end user behavior training.

31. Russ, a security manager at a small online retailer, is completing a self-assessment questionnaire for PCI-DSS compliance. In studying the questionnaire, Russ has noted that his organization is not in compliance with all requirements. No auditor will be verifying the accuracy of the questionnaire. What is Russ's best course of action?

A. Complete the form truthfully and notify senior management of the exceptions.

B. Complete the form truthfully and submit it to authorities.

C. Mark each control as compliant and submit it to authorities.

D. Mark each control as compliant and notify senior management that he must be truthful on the next such submission.

☑ **A**. Security professionals, particularly those who have industry certifications that have a code of conduct (including ISACA's CISM certification), must be truthful, even when there may be personal, professional, or organizational consequences. In this situation, the form must be completed accurately, even though this means that the organization may have some short-term compliance issues with authorities.

☒ **B**, **C**, and **D** are incorrect. **B** is incorrect because executive management should also be made aware of the compliance issue. **C** and **D** are incorrect because it would be unethical to falsify answers on the questionnaire.

32. Russ, a security manager at a small online retailer, learned recently about the European General Data Protection Regulation (GDPR). The retailer has customers all over the world. The organization has outsourced its online catalog, order acceptance, and payment functions to a cloud-based e-commerce platform. Russ is unaware of any efforts that the retailer may have made to be compliant with GDPR. What should Russ do about this?

A. Ask senior management or the legal department about this matter.

B. Assume that the organization is compliant with GDPR.

C. Nothing, because the cloud-based e-commerce platform is required to be GDPR compliant.

D. Contact the cloud-based e-commerce platform and confirm its compliance to GDPR.

☑ **A**. A responsible security manager would always reach out to the legal department or another member of senior management to inquire about the organization's state of compliance to a law or regulation.

☒ **B**, **C**, and **D** are incorrect. **B** is incorrect because it is unwise to assume that others in an organization have all matters taken care of. **C** is incorrect because the retailer itself must be GDPR compliant, regardless of whether any part of its operations is outsourced. **D** is incorrect because the organization itself must be GDPR compliant. That said, the outsourcing organization must also be GDPR compliant.

33. Russ, a security leader at a global online retailer, is developing a system classification plan. Systems are classified as High, Moderate, or Low, depending upon operational criticality, data sensitivity, and exposure to threats. In a given environment, how should servers that support (such as DNS servers, time servers) High, Moderate, and Low production servers be classified?

A. Support servers should be classified as High, since some servers they support are High.

B. Support servers should be classified as Low, since they do not perform critical transactions, nor do they contain sensitive data.

C. Support servers should be classified at the same level as the lowest-level servers they support.

D. Support servers should be classified at the same level as the highest-level servers they support.

☑ **D**. The best option is to classify support servers at the same level as the highest-rated servers they support. For instance, if support servers provide support to servers that are rated Medium, then the support servers should be rated as Medium. This will ensure that the support servers are protected (whether for security, resilience, or both) at the same levels as the servers they support.

☒ **A**, **B**, and **C** are incorrect. **A** is incorrect because the question does not specify the classification level of servers they're supporting. **B** is incorrect because it would be imprudent to classify support servers as Low. It would be better to classify them at the same level as the highest-rated servers they support. **C** is incorrect because the support servers might be supporting higher-rated servers.

34. Russ, a security leader at a global online retailer, is designing a facilities classification plan to provide more consistency and purpose for physical security controls at the organization's worldwide business and processing locations. What criteria should be used to classify facilities for this purpose?

A. Sensitivity of data stored or accessed there

B. Sensitivity of data stored or accessed there and criticality of operations performed there

C. Criticality of operations performed there

D. Size of facilities, and whether there are regulations requiring facilities protection

☑ **B**. Facilities classification is typically established based on two main criteria: sensitivity of information stored at, or accessed at, a location and operational criticality of activities being performed there. For example, a work facility would be classified as High if data classified as High was stored there, or if personnel who worked there routinely accessed data classified as High. A work facility could also be classified as High if critical operations were performed there, such as a hosting facility or a call center.

☒ **A**, **C**, and **D** are incorrect. **A** is incorrect because facilities classification should be determined by more than just the sensitivity of data stored or accessed there. **C** is incorrect because facilities classification should be based on more than just the criticality of operations performed there. **D** is incorrect because data classification and operational criticality should also be considerations for facilities classification.

35. Which of the following is *not* a valid method for assigning asset value?

A. Net present value

B. Replacement cost

C. Repair cost

D. Book value

☑ **C**. Repair cost is *not* a valid method for assigning asset valuation. Valid methods include replacement cost, book value, net present value, redeployment cost, creation cost, reacquisition cost, and consequential financial cost.

☒ **A**, **B**, and **D** are incorrect. These *are* valid methods for assigning asset value.

36. Dylan is an executive security consultant who is assessing a client organization for compliance to various applicable information security and privacy regulations. Dylan has identified compliance issues and recommends that these issues be documented in the client organization's business. How should these issues be documented?

A. Separate entries for each regulation should be made in the organization's risk register.

B. A single entry should be made in the organization's risk register.

C. Separate entries for each regulation should be made in the organization's security incident log.

D. A single entry should be made in the organization's security incident log.

☑ **B**. The best way to document these findings is to create a single risk register entry for the matter. There could be dozens of similar issues that have common remedies, making it impractical to create potentially dozens of similar entries.

☒ **A**, **C**, and **D** are incorrect. **A** is incorrect because there could be numerous similar entries that would create unnecessary clutter in the risk register. **C** and **D** are incorrect because the security incident log is not the best place to record this matter.

37. For disaster recovery purposes, why is book value *not* a preferred method for determining the value of assets?

A. Information assets have no book value.

B. Book value may vary based on location if a recovery site is located elsewhere.

C. Some assets may not be tracked for depreciation.

D. The cost to replace damaged or destroyed assets could exceed book value.

☑ **D**. For disaster recovery purposes, organizations should use replacement or redeployment cost versus book value for asset value. If assets are damaged or destroyed in a disaster, they must be replaced; costs for replacements may be much higher than book value.

☒ **A**, **B**, and **C** are incorrect. **A** is incorrect because this question is not specifically about information assets. **B** is incorrect because this is not a true statement. **C** is incorrect because this statement is not relevant.

38. A security analyst has identified a critical server that is missing an important security-related operating system patch. What has the security analyst identified?

A. A vulnerability

B. A threat

C. A risk

D. An incident

☑ **A**. The security analysist has identified a vulnerability, which is a weakness that could more easily permit one or more types of threats to occur.

☒ **B**, **C**, and **D** are incorrect. **B** is incorrect because the missing patch is not a threat, but a vulnerability that could permit a threat to occur. **C** is incorrect because this is not the best answer. **D** is incorrect because the missing patch is not an incident, although it may permit an incident to occur.

39. A security analyst has identified a new technique that cybercriminals are using to break into server operating systems. What has the security analyst identified?

A. A vulnerability

B. A threat

C. A risk

D. An incident

☑ **B**. The security analysis has identified a threat that, if realized, could result in an intrusion into the organization's systems.

☒ **A**, **C**, and **D** are incorrect. **A** is incorrect because these techniques are not a vulnerability, but a threat. **C** is incorrect because this is not the best answer. **D** is incorrect because the new technique is not an incident, although it might be possible for an incident to occur because of the threat.

40. Threat actors consist of all of the following *except* which one?

A. Trojans

B. Hacktivists

C. Cybercriminal organizations

D. Employees

☑ **A**. Trojans are threats, but they are not threat actors. Threat actors consist of external parties such as hackers, cybercriminal organizations, hacktivists, and more; internal users are also considered threat actors in the context of "insider threat."

☒ **B**, **C**, and **D** are incorrect because hacktivists, employees, and cybercriminals are all considered threat actors.

41. While deliberating an item in an organization's risk register, members of the cybersecurity steering committee have decided that the organization should discontinue a new feature in its online social media platform. This decision is an example of what?

A. Risk transfer

B. Risk acceptance

C. Risk mitigation

D. Risk avoidance

☑ **D**. Risk avoidance is one of four risk treatment options. In risk avoidance, the activity associated with an identified risk is discontinued.

☒ **A**, **B**, and **C** are incorrect. Risk acceptance, risk mitigation, and risk transfer are not the correct terms associated with the organization's decision to discontinue the business activity discussed here.

42. NotPetya is an example of what?

A. Threat

B. Spyware

C. Mass-mailing worm

D. Password-cracking tool

☑ **A**. NotPetya is a threat. More specifically, NotPetya is malware that resembles ransomware but lacks the ability to decrypt data; thus, it is considered by many to be destructware, or software that destroys data files.

☒ **B**, **C**, and **D** are incorrect. **B** is incorrect because NotPetya is not spyware. **C** is incorrect because NotPetya is not a mass-mailing worm. **D** is incorrect because NotPetya is not a password cracker.

43. Randi, a security architect, is seeking ways to improve a defense-in-depth to defend against ransomware. Randi's organization employs advanced antimalware on all endpoints and antivirus software on its e-mail servers. Endpoints also have an IPS capability that functions while endpoints are onsite or remote. What other solutions should Randi consider to improve defenses against ransomware?

A. Data replication

B. Spam and phishing e-mail filtering

C. File integrity monitoring

D. Firewalls

☑ **B**. The next solution that should be considered is a solution that will block all incoming spam and phishing e-mail messages from reaching end users. This will provide a better defense-in-depth for ransomware since several other good controls are in place.

☒ **A**, **C**, and **D** are incorrect. **A** is incorrect because data replication is not an adequate defense against ransomware, because files encrypted by ransomware are likely to be replicated onto backup file stores. Instead, offline backup such as magnetic tape or e-vaulting should be used. **C** is incorrect because file integrity monitoring (FIM) is generally not chosen as a defense against ransomware. **D** is incorrect because firewalls are not an effective defense against ransomware, unless they also have an IPS component that can detect and block command-and-control traffic.

44. Which European law enforces users' rights to privacy?

A. GLBA

B. GDPR

C. 95/46/EC

D. SB-1386

☑ **B**. GDPR, or the European General Data Protection Regulation, which took effect in 2018, provides several means to improve privacy for European residents.

☒ **A**, **C**, and **D** are incorrect. **A** is incorrect because GLBA is a U.S. law that requires financial services organizations to protect information about its customers. **C** is incorrect because 95/46/EC, otherwise known as the European Privacy Directive, is the former European privacy law that has been superseded by GDPR. **D** is incorrect because SB-1386 is the original data breach disclosure law in the state of California.

45. Which mechanism does GDPR provide for multinational organizations to make internal transfers of PII?

A. Model clauses

B. Privacy Shield

C. Safe Harbor

D. Binding corporate rules

☑ **D**. Binding corporate rules were established by European privacy laws that permit multinational organizations to perform internal transfers of sensitive information. Typically this is applied to internal human resources information.

☒ **A**, **B**, and **C** are incorrect. **A** is incorrect because model clauses are used between organizations to legally obligate them to comply with GDPR and other privacy regulations. **B** is incorrect because Privacy Shield is used by organizations to register their obligation to comply with GDPR. **C** is incorrect because Safe Harbor is the now-defunct means for organizations to register their obligation to comply with the former European privacy directive, 95/46/EC.

46. Which mechanism provides the legal framework for the transfer of information from Europe to the United States?

A. Model clauses

B. Privacy Shield

C. Safe Harbor

D. Binding corporate rules

☑ **B**. The E.U.-U.S. Privacy Shield is the new legal framework for regulating the flow of information from Europe to the United States. Privacy Shield supersedes Safe Harbor, which was invalidated in 2015.

☒ **A**, **C**, and **D** are incorrect. **A** is incorrect because model clauses are a set of legal language used in legal agreements between organizations regarding the protection of PII of European residents. **C** is incorrect because Safe Harbor was invalidated in 2015. **D** is incorrect as binding corporate rules are used for the internal transfer of PII within a multinational organization.

47. What language is used in legal agreements between organizations regarding the protection of personally identifiable information?

A. Model clauses

B. Privacy Shield

C. Safe Harbor

D. Binding corporate rules

☑ **A**. Model clauses are used in legal contracts between organizations regarding the protection of PII of European citizens. Model clauses are a set of specific language included in privacy regulations such as the former European Privacy Directive and the current Global Data Privacy Regulation (GDPR).

☒ **B**, **C**, and **D** are incorrect. **B** is incorrect because Privacy Shield is a legal framework for the protection of PII, but it does not include language used in contracts between organizations. **C** is incorrect because Safe Harbor is the former legal framework that is superseded by Privacy Shield. **D** is incorrect because binding corporate rules are the legal framework for the internal transfer of sensitive information in multinational companies.

48. Which mechanism was formally used as the legal framework for the transfer of information from Europe to the United States?

A. Model clauses

B. Privacy Shield

C. Safe Harbor

D. Binding corporate rules

☑ **C**. International Safe Harbor Privacy Principles, known primarily as Safe Harbor, is the former framework for the legal transfer of European PII to the United States. Safe Harbor was invalidated in 2015 by the European Court of Justice.

☒ **A**, **B**, and **D** are incorrect. **A** is incorrect because model clauses are legal agreement templates used for agreements between organizations. **B** is incorrect because Privacy Shield is the functional replacement for Safe Harbor. **D** is incorrect because binding corporate rules are used in the context of intracompany data transfers of PII.

49. The internal audit department in a public company recently audited key controls in the vulnerability management process and found that the control "Production servers will be patched within 30 days of receipt of critical patches" fails 30 percent of the time. What finding should the internal audit make?

A. A new control is needed for vulnerability management.

B. The control is ineffective and needs to be corrected.

C. The control should be changed from 30 days to 45 days.

D. The control should be changed from 30 days to 21 days.

☑ **B**. There is a control in place that is not effective. The best remedy is to fix the existing control, which is still reasonable and appropriate.

☒ **A**, **C**, and **D** are incorrect. **A** is incorrect because creating an additional control should not be considered until the existing control is fixed. **C** and **D** are incorrect because the SLA for critical patches does not necessarily need to be changed.

50. The internal audit department in an organization recently audited the control "User accounts for terminated workers shall be locked or removed within 48 hours of termination" and found that user accounts for terminated workers are not locked or removed 20 percent of the time. What recommendation should internal audit make?

A. Change the timeframe in the control from 48 hours to 7 days.

B. Add a new compensating control for monthly review of terminated user accounts.

C. Add more staff to the team that manages user accounts.

D. No changes are needed since 20 percent is an acceptable failure rate.

☑ **B**. A compensating control in the form of a periodic access review is the best answer. Periodic access reviews are common and used for this purpose.

☒ **A**, **C**, and **D** are incorrect. **A** is incorrect because seven days is far too long for user accounts to be active after a worker is terminated. **C** is incorrect because staffing levels are not necessarily the cause of this control failure. **D** is incorrect because 20 percent is considered too high a failure rate for a terminated user account access control.

51. Upon examining the change control process in a SaaS provider organization, a new security manager has discovered that the change control process lacks a security impact procedure. What should the security management recommend for this matter?

A. Systems impacted by a change should be scanned before and after changes are made.

B. A post-change security review should be added to the change control process.

C. No change is needed because security is not needed in change control processes.

D. Add a security impact procedure to the change control process so that the security impact of each proposed change can be identified.

☑ **D**. The best remedy is the addition of a security impact procedure that is performed for each proposed change. This will help to identify any security-related issues associated with a proposed change that can be discussed prior to the change being made. This is preferable to the alternative: accepting a change that may have one or more security issues that may increase the risk of a security incident.

☒ **A**, **B**, and **C** are incorrect. **A** is incorrect because not all security-related issues will be manifested in a vulnerability scan. **B** is incorrect because a security review should be performed prior to a change being made so that an organization can consider modifying the nature of the change so that there is no increase in risk. **C** is incorrect because security *is* an important consideration in a change control process.

52. A SaaS provider performs penetration tests on its services once per year, and many findings are identified each time. The organization's CISO wants to make changes so that penetration test results will improve. The CISO should recommend all of the following changes *except* which one?

A. Add a security review of all proposed software changes into the SDLC.

B. Introduce safe coding training for all software developers.

C. Increase the frequency of penetration tests from annually to quarterly.

D. Add the inclusion of security and privacy requirements into the SDLC.

☑ **C**. Increasing the frequency of penetration tests is not likely to get to the root cause of the problem, which is the creation of too many security-related software defects.

☒ **A**, **B**, and **D** are incorrect. **A** is incorrect because the addition of a security review for proposed changes is likely to reveal issues that can be corrected prior to development. **B** is incorrect because safe coding training can help developers better understand coding practices that will result in fewer security defects. **D** is incorrect because the addition of security and privacy requirements will help better define the nature of new and changed features.

53. A SaaS provider performs penetration tests on its services once per year, and many findings are identified each time. What is the best way to report this matter to executive management?

A. Develop a KRI that reports the trend of security defects over time.

B. Penetration test reports should be distributed to executive management so that they can have a better understanding of the problem.

C. The executive summary section of penetration test reports should be distributed to executive management.

D. Report the number of defects found to executive management.

☑ **A**. A key risk indicator (KRI) should be developed that illustrates the risk that security defects make on the organization. An example KRI for this situation could read, "Number of critical software defects introduced into SAAS Product."

☒ **B**, **C**, and **D** are incorrect. **B** is incorrect because penetration test reports are quite detailed and technical, and they provide little, if any, business insight to an executive. **C** is incorrect because even an executive summary section in a penetration test report is unlikely to express business risk in a meaningful way. **D** is incorrect because the number of defects alone is not a good risk indicator.

54. A SaaS provider performs penetration tests on its services once per year, and many findings are identified each time. What is the best KRI that would highlight risks to executives?

A. Number of software vulnerabilities that exist on production SaaS applications

B. Number of days that critical software vulnerabilities exist on production SaaS applications

C. Number of vulnerability scans performed on production SaaS applications

D. Names of developers who introduced the greatest number of security defects onto production SaaS applications

☑ **B**. The total number of days that unmitigated software defects existed on production applications is the best risk indicator, particularly when tracked over a period of time.

☒ **A**, **C**, and **D** are incorrect. **A** is incorrect because the number of vulnerabilities alone does not sufficiently convey risk; a better depiction of risk is the number of days that unpatched vulnerabilities were present on production systems. **C** is incorrect because the number of scans does not provide an indication of risk. **D** is incorrect because a list of offenders is not a key risk indicator.

55. The security leader at a SaaS provider has noticed that the number of security defects in the SaaS application is gradually climbing over time to unacceptable levels. What is the best first step the security leader should take?

A. Contact the software development leader and report that more security defects are being created.

B. Initiate the procurement process for a web application firewall.

C. Initiate a low-severity security incident.

D. Create a new risk register entry that describes the problem along with potential fixes.

☑ **D**. When there is a disturbing trend developing, such as an increase in the number of security vulnerabilities being identified, creating an entry in the risk register is the best first step. This will facilitate action in the organization's risk management process that will enable business and technology leaders to discuss the matter and make decisions to manage the risk.

☒ **A**, **B**, and **C** are incorrect. **A** is incorrect because this is not the best first choice. Contacting the development leader is, however, a prudent move so that the development leader will not feel blindsided by later proceedings. **B** is incorrect because a WAF may not be the best solution here; besides, this represents a unilateral decision on the part of the security leader, when a better approach would be a discussion with stakeholders. **C** is incorrect because a situation like this is not commonly regarded as a security incident.

56. Why is the KRI "Number of days that critical software vulnerabilities exist on production SaaS applications" considered a leading risk indicator?

A. This is the first KRI that executives are likely to pay attention to.

B. This KRI provides a depiction of the probability of a security incident through the exploitation of vulnerabilities. The risk of an incident is elevated with each successive day that unpatched vulnerabilities exist.

C. Critical software vulnerabilities are the leading cause of security incidents.

D. The KRI indicates that critical software vulnerabilities are the most likely cause of a future incident.

☑ **B**. A KRI is a leading risk indicator because it portends the likelihood of a future event. The KRI in this question points to the likelihood of a security breach that occurs through the exploitation of a defect in an organization's Internet-facing software application.

☒ **A**, **C**, and **D** are incorrect. **A** is incorrect because leading risk indicators are so-named because they help predict the likelihood of future events. **C** is incorrect because the meaning of a leading risk indicator is related to the likelihood of a specific future event. The fact that the KRI in this question is related to a leading cause of incidents is coincidental. **D** is incorrect because the KRI does not attempt to identify the most likely cause of a future incident.

57. Which is the best method for reporting risk matters to senior management?

A. Sending after-action reviews of security incidents

B. Sending the outcomes of risk treatment decisions

C. Periodic briefing on the contents of the risk register

D. Sending memos each time a new risk is identified

☑ **C**. The best method available here is to provide a summary briefing on the contents of the risk register. Providing a summary overview of the items of the risk register will enable the leadership team to focus on the key areas or emerging risks that need their attention. This will help senior management better understand the entire catalog of unmanaged risks in the organization.

☒ **A**, **B**, and **D** are incorrect. **A** is incorrect because risks often exist, apart from security incidents. **B** is incorrect because senior management should participate in risk treatment decisions, not merely be informed about them (implying that others are making those decisions). **D** is incorrect because sending memos is unstructured, and memos may not always be read. Further, a briefing from the risk register is much better, because this is an interactive event where senior management can ask questions about risks in the risk register.

58. Janice has worked in the Telco Company for many years and is now the CISO. For several years, Janice has recognized that the engineering organization contacts information security just prior to the release of new products and features so that security can be added in at the end. Now that Janice is the CISO, what is the best long-range solution to this problem?

A. Introduce security at the conceptual, requirements, and design steps in the product development process.

B. Train engineering in the use of vulnerability scanning tools so that they can find and fix vulnerabilities on their own.

C. Add security requirements to other requirements that are developed in product development projects.

D. There is no problem to fix: it is appropriate for engineering to contact security prior to product release to add in necessary security controls.

☑ **A**. The best long-term solution is the introduction of appropriate security activities throughout the product development lifecycle, starting at the conceptual stage where new products and features are initially discussed. Security steps at the requirements and design stages will help ensure that products are secure by design.

☒ **B**, **C**, and **D** are incorrect. **B** is incorrect because vulnerability scanning will fail to identify many types of security problems. **C** is incorrect because adding security requirements alone, while helpful, is not the best choice. **D** is incorrect because responsible organizations ensure that their products are secure by design.

59. Janice has worked in the Telco Company for many years and is now the CISO. For several years, Janice has recognized that the engineering organization contacts information security just prior to the release of new products and features so that security can be added in at the end. Now that Janice is the CISO, what is the best first step for Janice to take?

A. Initiate a low-severity security incident.

B. Create a new risk register entry that describes the problem along with potential fixes.

C. Initiate a high-severity security incident.

D. Write a memo to the leader of the engineering organization requesting that security be added to the product development lifecycle.

☑ **B**. Creation of a risk register entry is the best first step. Presuming that a cross-functional cybersecurity council exists, the next step will be discussion of the matter that will lead to an eventual decision.

☒ **A**, **C**, and **D** are incorrect. **A** and **C** are incorrect because initiation of a security incident is not an appropriate response. **D** is incorrect because a wider conversation should be conducted by cybersecurity steering committee members.

60. The term "insider threat" includes all of the following *except* which one?

A. End users who are ignorant and make unwise decisions

B. Employees who have a grudge against their employer

C. Customers who attempt to break into systems while onsite

D. End users who are doing the right thing but make mistakes

☑ **C**. Customers, even while onsite, are not considered insiders.

☒ **A**, **B**, and **D** are incorrect. Each of these is considered an insider threat.

61. Examples of employees gone rogue include all of the following *except* which one?

A. A developer who inserts a time bomb in application source code

B. A securities trader who makes unauthorized trades resulting in huge losses

C. An engineer who locks co-workers out of the network because they are not competent

D. A systems engineer who applies security patches that cause applications to malfunction

☑ **D**. The systems engineer who applies patches to fix feature or security defects is the best choice, because there is little or no sign of malice. In this example, the change control process should be improved so that there is an opportunity to test software applications in a nonproduction environment prior to applying patches to production.

☒ **A**, **B**, and **C** are incorrect. Each of these is an example of an employee who has gone rogue and is consequently harming the organization.

62. Janice, a new CISO in a healthcare delivery organization, has discovered that virtually all employees are local administrators on their laptop/desktop computers. This is an example of what?

A. Insider threat

B. Vulnerability

C. Threat

D. Incident

☑ **B**. The matter of end users being local administrators means that they have administrative control of the computers they use, namely their laptop and/or desktop computers. This means they can install software and security patches and change the configuration of the operating system. This also means that malware introduced by the user onto the system will probably be able to run with administrative privileges, which may result in significantly more harm to the system and the organization.

☒ **A**, **C**, and **D** are incorrect. **A** is incorrect because this configuration setting is not, by itself, an insider threat. However, an insider threat situation can be made worse through end users having local administrative privileges. **C** is incorrect because this is not a threat, but a vulnerability (these terms are often misused). **D** is incorrect because this is not an incident. However, an incident is somewhat more likely to occur and more likely to have greater impact because end users have local administrative privileges.

63. An end user in an organization opened an attachment in e-mail, which resulted in ransomware running on the end user's workstation. This is an example of what?

A. Incident

B. Vulnerability

C. Threat

D. Insider threat

☑ **A**. Ransomware executing on an end user's workstation is considered an incident. It may have been allowed to execute because of one or more vulnerabilities.

☒ **B**, **C**, and **D** are incorrect. **B** is incorrect because a vulnerability is a configuration setting or a software defect that can, if exploited, result in an incident. **C** is incorrect because ransomware, by itself, is considered a threat, but ransomware executing on a system is considered an incident. **D** is incorrect because this is not considered an insider threat. However, users having poor judgment (which may include clicking on phishing messages) is considered an insider threat.

64. What is the purpose of the third-party risk management process?

A. Identify risks that can be transferred to third parties.

B. Identify a party responsible for a security breach.

C. Identify a party that can perform risk assessments.

D. Identify and treat risks associated with the use of third-party services.

☑ **D**. Third-party risk management encompasses processes and procedures for identifying risks associated with third-party service providers and suppliers; assessments of third parties enable management to make decisions regarding whether to do business with specific third parties and under what conditions.

☒ **A**, **B**, and **C** are incorrect. **A** is incorrect because third-party risk management is not related to risk transfer. **B** is incorrect because third-party risk management is not involved in security breach response and investigation. **C** is incorrect because third-party risk management is not related to the process of performing internal risk assessments.

65. What is the correct sequence of events when onboarding a third-party service provider?

A. Contract negotiation, examine services, identify risks, risk treatment

B. Examine services, identify risks, risk treatment, contract negotiation

C. Examine services, contract negotiation, identify risks, risk treatment

D. Examine services, identify risks, risk treatment

☑ **B**. The best sequence here is to examine the services offered by the third party, identify risks associated with doing service with the third party, make decisions about what to do about these risks, and enter into contract negotiations.

☒ **A**, **C**, and **D** are incorrect. **A** and **C** are incorrect because contract negotiation should not take place prior to identifying risks that may need to be addressed in a contract. **D** is incorrect because contract negotiation is not included.

66. A campaign by a cybercriminal to perform reconnaissance on a target organization and develop specialized tools to build a long-term presence in the organization's environment is known as what?

A. Watering hole attack

B. Hacktivism

C. Advanced persistent campaign (APC)

D. Advanced persistent threat (APT)

☑ **D**. A long-term campaign of patient reconnaissance, development of tools, and establishment of a long-term quiet presence inside an organization's environment is known as an advanced persistent threat (APT). It is "advanced" on account of the reconnaissance and the development of an intrusion strategy with specialized tools; it is "persistent" by design, so that the intruder can maintain a long-term presence in the environment; it is a "threat" because the criminal actor is performing all of this to reach a long-term objective, whether the acquisition or destruction of sensitive information or the disruption of the organization's operations.

☒ **A**, **B**, and **C** are incorrect. **A** is incorrect because a watering hole attack is an attack on an organization via a compromised website that will automatically download malware onto visitors' systems. **B** is incorrect because hacktivism refers to an ideology wherein an attacker seeks to expose or disrupt an organization for ideological reasons. **C** is incorrect because the term "advanced persistent campaign" is not in use.

67. Joel, a CISO in a manufacturing company, has identified a new cybersecurity-related risk to the business and is discussing it privately with the chief risk officer (CRO). The CRO has asked Joel not to put this risk in the risk register. What form of risk treatment does this represent?

A. This is not risk treatment, but the avoidance of managing the risk altogether.

B. This is risk avoidance, where the organization elects to avoid the risk altogether.

C. This is risk transfer, as the organization has implicitly transferred this risk to insurance.

D. This is risk acceptance, as the organization is accepting the risk as-is.

☑ **A**. The deliberate "burying" of a risk is not risk treatment, but the refusal to deal with the risk altogether. Although there may be legitimate reasons for this action, based on the information here, there is an appearance of negligence on the part of the CRO.

☒ **B**, **C**, and **D** are incorrect. **B** is incorrect because risk avoidance is a formal decision wherein the organization will discontinue the activity that manifests the identified risk. **C** is incorrect because there is no indication in this question that cyber insurance will assume this risk. **D** is incorrect because formal risk acceptance involves the use of the risk management lifecycle that includes the risk being recorded in the risk ledger, followed by analysis and a risk treatment decision.

68. Which of the following factors in risk analysis is the most difficult to determine?

A. Exposure factor

B. Single-loss expectancy

C. Event probability

D. Event impact

☑ **C**. Event probability is the most difficult of these values to determine accurately, particularly for high-impact events. Because event probability is so difficult to determine, much risk analysis work performed is qualitative in nature.

☒ **A**, **B**, and **D** are incorrect. **A** is incorrect because exposure factor (which is calculated as a percentage of an asset's value) is relatively easy to determine. **B** is incorrect because single-loss expectancy (which is calculated as asset value times exposure factor) is relatively easy to determine. **D** is incorrect because event impact (formally known as event cost) is not altogether difficult to determine.

69. An estimate on the number of times that a threat might occur in a given year is known as what?

A. Annualized loss expectancy (ALE)

B. Annualized rate of occurrence (ARO)

C. Exposure factor (EF)

D. Annualized exposure factor (AEF)

☑ **B**. Annualized rate of occurrence (ARO) is defined as an estimate of the number of times that a threat will occur per year.

☒ **A**, **C**, and **D** are incorrect. **A** is incorrect because annualized loss expectancy (ALE) is defined as the annualized rate of occurrence (ARO) times the single loss expectancy (SLE). **C** is incorrect as exposure factor (EF) is the loss that represents a percentage of an asset's value (because in some cases, an asset is not completely destroyed). **D** is incorrect because there is no such term is annualized exposure factor (AEF).

70. Which is the best method for prioritizing risks and risk treatment?

A. Threat event probability times asset value, from highest to lowest

B. Threat event probability, followed by asset value

C. Professional judgment

D. A combination of threat event probability, asset value, and professional judgment

☑ **D**. The best method for prioritizing risks and risk treatment is to examine the probability of event occurrence (difficult though that may be), asset value, and impact to the organization. Professional judgment plays a big role as well because factors such as business reputation are difficult to quantify.

☒ **A**, **B**, and **C** are incorrect. **A** is incorrect because this approach allows no room for professional judgment. **B** is incorrect because there is no logical sequence based on these two items that are measured differently. **C** is incorrect because professional judgment alone risks the failure to consider high-value assets, high impact, and high probability of occurrence.

71. Joel is a security manager in a large manufacturing company. The company uses primarily Microsoft, Cisco, and Oracle products. Joel subscribes to security bulletins from these three vendors. Which of the following statements best describes the adequacy of these advisory sources?

A. Joel should also subscribe to nonvendor security sources such as US-CERT and InfraGard.

B. Joel's security advisory sources are adequate.

C. Joel should discontinue vendor sources and subscribe to nonvendor security sources such as US-CERT and InfraGard.

D. Joel should focus on threat hunting in the dark web.

☑ **A**. The best set of security advisories includes those from all IT product vendors, as well as a number of nonvendor sources such as US-CERT and InfraGard.

☒ **B**, **C**, and **D** are incorrect. **B** is incorrect because Joel should also have at least one good nonvendor source such as US-CERT. **C** is incorrect because it is important to continue to receive vendor advisories. **D** is incorrect because "threat hunting on the dark web" is not a real activity.

72. The primary advantage of automatic controls versus manual controls includes all of the following *except* which one?

A. Automatic controls are generally more reliable than manual controls.

B. Automatic controls are less expensive than manual controls.

C. Automatic controls are generally more consistent than manual controls.

D. Automatic controls generally perform better in audits than manual controls.

☑ **B**. Automatic controls are not necessarily less expensive than manual controls; in some cases, they may be considerably more expensive than manual controls.

☒ **A**, **C**, and **D** are incorrect. **A** is incorrect because automated controls are typically more reliable and accurate than manual controls. **C** is incorrect because automated controls are typically more consistent than manual controls. **D** is incorrect because automated controls generally perform better in audits.

73. Which of the following statements about PCI-DSS compliance is true?

A. Only organizations that store, transfer, or process more than 6 million credit card numbers are required to undergo an annual PCI audit.

B. Service providers are not required to submit an attestation of compliance (AOC) annually.

C. Merchants that process fewer than 15,000 credit card transactions are not required to submit an attestation of compliance (AOC).

D. All organizations that store, transfer, or process credit card data are required to submit an attestation of compliance (AOC) annually.

☑ **D**. All organizations that store, process, or transmit credit card data are required to submit an attestation of compliance (AOC) annually to their acquiring bank, processing bank, or card brand.

☒ **A**, **B**, and **C** are incorrect. **A** is incorrect because some organizations that process fewer credit card numbers are also required to undergo annual PCI audits—for example, organizations that have suffered a breach may be required to undergo audits. **B** is incorrect because service providers are required to submit attestations of compliance (AOC) annually. **C** is incorrect because all merchants are required to submit attestations of compliance (AOC).

74. A security leader wants to commission an outside company to assess the organization's performance against the NIST SP800-53 control framework to see which controls the organization is operating properly and which controls require improvement. What kind of an assessment does the security leader need to commission?

A. Controls risk assessment

B. Controls maturity assessment

C. Controls gap assessment

D. Risk assessment

☑ **C**. The organization needs to commission a controls gap assessment, which will reveal which controls are being operated properly and which ones require improvement of some kind.

☒ **A**, **B**, and **D** are incorrect. **A** is incorrect because a risk assessment will not provide the desired results. **B** is incorrect because a maturity assessment will not provide the desired results. **D** is incorrect because a risk assessment will not provide the desired results.

75. An organization needs to better understand how well organized its operations are from a controls point of view. What kind of an assessment will best reveal this?

A. Controls risk assessment

B. Controls maturity assessment

C. Controls gap assessment

D. Risk assessment

☑ **B**. A controls maturity assessment will reveal, control by control, the level of organization and consistency of each control in the organization.

☒ **A**, **C**, and **D** are incorrect. **A** is incorrect because a controls risk assessment will not provide the desired results. **C** is incorrect because a controls gap assessment will not provide the desired results. **D** is incorrect because a risk assessment will not provide the desired results.

76. An organization needs to better understand which of its controls are more important than others. What kind of an assessment will best reveal this?

A. Controls risk assessment

B. Controls maturity assessment

C. Controls gap assessment

D. Risk assessment

☑ **A**. A controls risk assessment will reveal which controls have greater risk associated with them. This will help the organization better understand which controls warrant greater attention and scrutiny.

☒ **B**, **C**, and **D** are incorrect. **B** is incorrect because a controls maturity assessment will not provide the desired results. **C** is incorrect because a controls gap assessment will not provide the desired results. **D** is incorrect because a risk assessment will not provide the desired results.

77. An organization needs to better understand whether its control framework is adequately protecting the organization from known and unknown hazards. What kind of an assessment will best reveal this?

A. Controls risk assessment

B. Controls maturity assessment

C. Controls gap assessment

D. Risk assessment

☑ **D**. A risk assessment will best help the organization understand the entire array of risks and potential impacts facing the organization and whether its control framework is adequately covering them.

☒ **A**, **B**, and **C** are incorrect. **A** is incorrect because a controls risk assessment (the next best choice) will not provide the desired results. **B** is incorrect because a controls maturity assessment will not provide the desired results. **C** is incorrect because a controls gap assessment will not provide the desired results.

78. An organization recently suffered a significant security incident. The organization was surprised by the incident and believed that this kind of an event would not occur. To avoid a similar event in the future, what should the organization do next?

A. Commission an enterprise-wide risk assessment.

B. Commission a controls maturity assessment.

C. Commission an internal and external penetration test.

D. Commission a controls gap assessment.

☑ **A**. An enterprise-wide risk assessment is the best option here so that risks of all kinds can be identified and remedies suggested for mitigating them.

☒ **B**, **C**, and **D** are incorrect. **B** is incorrect because it's possible that there are missing controls; a controls maturity assessment takes too narrow a view here and focuses only on existing controls, when the problem might be controls that are nonexistent. **C** is incorrect because the nature of the incident is unknown and may not be related to technical vulnerabilities that a penetration test would reveal (for example, it may have been phishing or fraud). **D** is incorrect because a controls gap assessment takes too narrow a view here and focuses only on existing controls, when the problem might be controls that are nonexistent.

79. Stephen is a security leader for a SaaS company that provides file storage services to corporate clients. Stephen is examining proposed contract language from a prospective customer that is requiring the SaaS company implement "best practices" for protecting customer information. How should Stephen respond to this contract language?

A. Stephen should accept the contract language as-is.

B. Stephen should not accept a customer's contract but instead use his company's contract language.

C. Stephen should change the language from "best practices" to "industry-standard practices."

D. Stephen should remove the security-related language as it is unnecessary for a SaaS environment.

☑ **C**. The term "best practices" is good to impose on others but bad to accept from others. "Best practices" in this case implies that Stephen's company will use the best available processes and tools that are superior to all others. Instead, a phrase such as "industry-standard practices" should be used.

☒ **A**, **B**, and **D** are incorrect. **A** is incorrect because few companies can afford to truly implement "best practices" controls, particularly a SaaS company that stores information. **B** is incorrect because it is commonplace to accept a customer's contract (just as it is commonplace to use one's own). **D** is incorrect because complete removal of the security language will likely be unacceptable by the customer.

80. Security analysts in the SOC have noticed that the organization's firewall is being scanned by a port scanner in a hostile country. Security analysts have notified the security manager. How should the security manager respond to this matter?

A. Declare a high-severity security event.

B. Declare a low-severity security event.

C. Take no action.

D. Direct the SOC to blackhole the scan's originating IP address.

☑ **D**. The best course of action is to blackhole the IP address that is the origination of the port scan. However, even this may not be necessary because a port scan is not, by itself, a serious matter. However, it may represent reconnaissance by an intruder that is targeting the organization.

☒ **A**, **B**, and **C** are incorrect. **A** is incorrect because a port scan is not a high-severity security matter. **B** is incorrect because this is not the best answer; however, some organizations might consider a port scan a low-level security incident and respond in some way, such as blackholing the IP address. **C** is incorrect because taking no action at all is not the best course of action.

81. A security leader recently commissioned a controls maturity assessment and has received the final report. Control maturity in the assessment is classified as "Initial," "Managed," "Defined," "Quantitatively Managed," and "Optimized." What maturity scale was used in this maturity assessment?

A. Organizational Project Maturity Model

B. Open Source Maturity Model

C. Capability Maturity Model

D. Capability Maturity Model Integrated

☑ **D**. The maturity model used for this assessment was the Capability Maturity Model Integrated.

☒ **A**, **B**, and **C** are incorrect. The maturity levels in the question do not correspond to any of these other maturity models.

82. Security analysts in the SOC have noticed a large volume of phishing e-mails that are originating from a single "from" address. Security analysts have notified the security manager. How should the security manager respond to the matter?

A. Declare a high-level security incident.

B. Block all incoming e-mail from that address at the e-mail server or spam filter.

C. Issue an advisory to all employees to be on the lookout for suspicious messages and to disregard them.

D. Blackhole the originating IP address.

☑ **B**. Of the choices available, the best one is to block any new incoming e-mail messages from the offending e-mail address. A better solution would be the use of a system that would do this automatically, as well as retrieve any offending messages already delivered to some users before the message was recognized as harmful.

☒ **A**, **C**, and **D** are incorrect. **A** is incorrect because this is not the best choice. However, depending on the nature of the threat (which is not revealed in this question), if the phishing is known to carry a malicious payload known to infect user machines successfully in the organization, then perhaps a high-severity incident is the right course of action. **C** is incorrect because this is not the best choice. However, in the absence of antiphishing controls, this may be the organization's best choice. **D** is incorrect because this is not the best choice; the adversary may be able to continue sending e-mails from different servers.

83. The corporate controller in an organization recently received an e-mail from the CEO with instructions to wire a large amount of money to an offshore bank account that is part of secret merger negotiations. How should the corporate controller respond?

A. Contact the CEO and ask for confirmation.

B. Wire the money as directed.

C. Reply to the e-mail and ask for confirmation.

D. Direct the wire transfer clerk to wire the money as directed.

☑ **A**. The best course of action is to contact the CEO directly, via phone or e-mail, asking for confirmation of the directive. On the surface, this appears to be a case of business e-mail compromise (BEC).

☒ **B**, **C**, and **D** are incorrect. **B** is incorrect because this may be a case of business e-mail compromise (BEC) that could result in large financial losses. **C** is incorrect because this may be a case of business e-mail compromise. A better response would be to initiate a new e-mail to the CEO; better yet would be a phone call. **D** is incorrect because this appears to be a case of business e-mail compromise (BEC) that could result in large financial losses.

84. An organization's information security department conducts quarterly user access reviews of the financial accounting system. Who is the best person to approve users' continued access to roles in the system?

A. Security manager

B. IT manager

C. Corporate controller

D. Users' respective managers

☑ **C**. The best person to approve ongoing user access in an application is a business unit leader or department head, or someone in the business responsible for the business process(es) supported by the information system.

☒ **A**, **B**, and **D** are incorrect. **A** is incorrect because the security manager is not going to be as familiar with finance department operations to know which persons should continue to have access to roles. **B** is incorrect because the IT manager is not going to be as familiar with finance department operations to know which persons should continue to have access to roles. **D** is incorrect because users' managers are not going to be as familiar with finance department operations to know which persons should continue to have access to roles.

85. All of the following are possible techniques for setting the value of information in a database *except* which one?

A. Recovery cost

B. Replacement cost

C. Lost revenue

D. Book value

☑ **D**. Book value is the least likely method to be used to assign value to information in a database. Book value is generally used for hardware assets only.

☒ **A**, **B**, and **C** are incorrect. Recovery cost, replacement cost, and lost revenue are all feasible methods for assigning value to information in a database.

86. For disaster recovery scenarios, which of the following methods for setting the value of computer equipment is most appropriate?

A. Recovery cost

B. Replacement cost

C. Lost revenue

D. Book value

☑ **B**. Replacement cost may be best suited for disaster recovery scenarios. In a disaster situation, computer equipment may need to be replaced rather than repaired.

☒ **A**, **C**, and **D** are incorrect. **A** is incorrect because recovery cost is not usually associated with computer equipment, but instead with information. **C** is incorrect because this is not the best method. If in cases where revenue derived from computer equipment is greater than its replacement value, this would underscore the need for rapid replacement or use of an alternative processing center. **D** is incorrect because it may be difficult to replace lost assets if only book value is available to obtain replacements.

87. A security leader in a SaaS services organization has recently commissioned a controls maturity assessment. The consultants who performed the assessment used the CMMI model for rating individual control maturity. The assessment report rated most controls from 2.5 to 3.5 on a scale of 1 to 5. How should the security leader interpret these results?

A. Acceptable: the maturity scores are acceptable and align with those of other software companies.

B. Unacceptable: develop a strategy to improve control maturity to 4.5–5.0 over the next three to four years.

C. Unacceptable: develop a strategy to improve control maturity to 3.4–4.5 over the next three to four years.

D. Irrelevant: too little is known to make a determination of long-term maturity targets.

☑ **A**. These results are acceptable, and they may even be interpreted as pretty good. The maturity of security controls in a SaaS or software company is generally in the 2.5–3.5 range.

☒ **B**, **C**, and **D** are incorrect. **B** is incorrect because few organizations aspire to bring their control maturity to the 4.5–5.0 range. **C** is incorrect because few software companies aspire to bring their control maturity to the 3.5–4.5 range. **D** is incorrect because this is not the best answer. That said, the question did not specify the industry or type of software in use.

88. In a mature third-party risk management (TPRM) program, how often are third parties typically assessed?

A. At the time of onboarding and annually thereafter

B. At the time of onboarding

C. At the time of onboarding and annually thereafter if the third party is rated as high risk

D. At the time of onboarding and later on if the third party has a security incident

☑ **C**. Better organizations' TPRM programs assess all third parties at the time of onboarding. High-risk third parties are assessed annually thereafter; medium-risk third parties might be assessed every two to three years, and low-risk third parties might not be reassessed at all.

☒ **A**, **B**, and **D** are incorrect. **A** is incorrect because not all third parties warrant reassessment. **B** is incorrect because assessing third parties only at the time of onboarding is considered insufficient, particularly for medium- and high-risk third parties. **D** is incorrect because high-risk third parties should be assessed annually.

89. David, a security analyst in a financial services firm, has requested the Expense Management Company, a service provider, to furnish him with a SOC1 audit report. The Expense Management Company furnished David with a SOC1 audit report for the hosting center where Expense Management Company servers are located. How should David respond?

A. File the report and consider the Expense Management Company as assessed.

B. Analyze the report for significant findings.

C. Thank them for the report.

D. Thank them for the report and request a SOC1 audit report for the Expense Management Company itself.

☑ **D**. The SOC1 report that the Expense Management Company provided is not for its business, but instead for its hosting provider. Most of the time this is insufficient, as a SOC1 report is needed also for the company itself.

☒ **A**, **B**, and **C** are incorrect. **A** is incorrect because little is still known about the Expense Management Company controls. **B** is incorrect because little is still known about the Expense Management Company controls. **C** is incorrect because little is still known about the Expense Management Company controls.

90. A healthcare delivery organization has a complete inventory of third-party service providers and keeps good records on initial and follow-up assessments. What information should be reported to management?

A. Metrics related to the number of third-party assessments that are performed

B. A risk dashboard that indicates patterns and trends of risks associated with third parties

C. Metrics related to the number of third-party assessments, along with their results

D. Status on whether there are sufficient resources to perform third-party risk assessments

☑ **B**. The best thing to report to management is a risk dashboard that shows them which third parties have the highest risks or greatest potential impact to the organization, as well as the trends of risk over time.

☒ **A**, **C**, and **D** are incorrect. **A** is incorrect because this does not portray risk. **C** is incorrect because this does not portray risk as well as a risk dashboard. **D** is incorrect because this does not directly portray risk. This is, however, an important item to report on so that management knows whether there are sufficient resources to manage third-party risk effectively.