Managed Services

As our organizations continue to migrate to cloud services (IaaS, PaaS, and SaaS, discussed in depth in Chapter 7), we should also assess the security impact of those services. This is highlighted by a 2020 study by global intelligence firm IDC, which found that nearly 80 percent of the companies surveyed had experienced at least one cloud data breach in the past 18 months. The top three reasons were misconfigurations, lack of visibility into access settings and activities, and improper access control. The major cloud services provide tools to help you avoid these pitfalls, but the bottom line is that, if you don't have the in-house expertise to secure and assess your cloud services, you really should consider contracting an expert to help you out.

Chapter Review

Building secure code requires commitment from many parts of the organization, not just the development and security teams. It starts at the very top with a policy document that is implemented through standards, procedures, and guidelines. A key part of these is the inclusion of the various types of tests that must be run regularly (even continuously) on the software as it is being written, integrated, and prepared for delivery. Software development environments are complex and could require different approaches from those you'd take in a normal network environment. For this reason, teamwork among all stakeholders is absolutely critical. A really good way to facilitate this collaboration is by using the DevSecOps approach introduced in Chapter 24 and highlighted in this one.

Even if your organization doesn't develop software, it most certainly uses applications and services developed by others. That's why the concepts discussed in this chapter are universally applicable to any cybersecurity leader. You must understand how secure code is built, so that you can determine whether the software you're getting from others presents any undue risks to your organization's cybersecurity.

Quick Review

- Machine language, which consists of 1's and 0's, is the only format that a computer's processor can understand directly and is considered a first-generation language.
- Assembly language is considered a second-generation programming language and uses symbols (called mnemonics) to represent complicated binary codes.
- Third-generation programming languages, such as C/C++, Java, and Python, are known as high-level languages due to their refined programming structures, which allow programmers to leave low-level (system architecture) intricacies to the programming language and focus on their programming objectives.
- Fourth-generation languages (aka very high-level languages) use natural language processing to allow inexpert programmers to develop code in less time than it would take an experienced software engineer to do so using a third-generation language.

- Fifth-generation programming languages (aka natural languages) approach programming by defining the constraints for achieving a specified result and allowing the development environment to solve problems by itself instead of a programmer having to develop code to deal with individual and specific problems.
- Assemblers are tools that convert assembly language source code into machine code.
- Compilers transform instructions from a source language (high-level) to a target language (machine), sometimes using an external assembler along the way.
- A garbage collector identifies blocks of memory that were once allocated but are no longer in use and deallocates the blocks and marks them as free.
- A runtime environment (RTE) functions as a miniature operating system for the program and provides all the resources portable code needs.
- In object-oriented programming (OOP), related functions and data are encapsulated together in classes, which may then be instantiated as objects.
- Objects in OOP communicate with each other by using messages that conform to the receiving object's application programming interface (API) definition.
- Cohesion reflects how many different types of tasks a module can carry out, with the goal being to perform only one task (high cohesion), which makes modules easier to maintain.
- Coupling is a measure of how much a module depends on others; the more dependencies it has, the more complex and difficult the module is to maintain, so we want low (or loose) coupling.
- An API specifies the manner in which a software component interacts with other software components.
- Parameter validation refers to confirming that the parameter values being received by an application are within defined limits before they are processed by the system.
- A software library is a collection of components that do specific tasks that are useful to many other components.
- Secure coding is a set of practices that reduce (to acceptable levels) the risk of vulnerabilities in our software.
- A source code vulnerability is a defect in code that provides a threat actor an opportunity to compromise the security of a software system.
- Secure coding standards are verifiable, mandatory practices that reduce the risk of particular types of vulnerabilities in the source code.
- Secure coding guidelines are recommended practices that tend to be less specific than standards.

- Software-defined security (SDS or SDSec) is a security model in which security functions such as firewalling, IDS/IPS, and network segmentation are implemented in software within an SDN environment.
- Software development tools should be authorized, implemented, and maintained just like any other software product through the organization's change management process; developers should not be allowed to install and use arbitrary tools.
- Static application security testing (SAST) is a technique meant to help identify software defects or security policy violations and is carried out by examining the source code without executing the program.
- Dynamic application security testing (DAST) refers to the evaluation of a program in real time, while it is running.
- Fuzzing is a technique used to discover flaws and vulnerabilities in software by sending large amounts of malformed, unexpected, or random data to the target program in order to trigger failures.
- Continuous integration means that all new code is integrated into the rest of the system as soon as the developer writes it.
- Continuous delivery is incrementally building a software product that can be released at any time and requires continuous integration.
- A software configuration management (SCM) platform identifies the attributes of software at various points in time and performs a methodical control of changes for the purpose of maintaining software integrity and traceability throughout the SDLC.
- The purpose of a software security assessment is to verify that this entire development process, from organizational policy to delivered product, is working as it should.
- Security assessments of acquired software are essential to mitigate the risk they could pose to the organization that acquired it.
- The most practical way to assess the security of commercial software is to research what vulnerabilities and exploits have been discovered by others and decide for ourselves whether or not the vendor uses effective secure coding practices.
- The greatest risk in using open-source software is relying on outdated versions of it.
- The best way to assess the security of third-party (i.e., custom or customized) software is to perform external or third-party audits.

Questions

Please remember that these questions are formatted and asked in a certain way for a reason. Keep in mind that the CISSP exam is asking questions at a conceptual level. Questions may not always have the perfect answer, and the candidate is advised against always looking for the perfect answer. Instead, the candidate should look for the best answer in the list.

1. What language is the only one that a computer processor can natively understand and execute?
   - **A.** Machine language
   - **B.** Register language
   - **C.** Assembly language
   - **D.** High-level language
2. To which generation do programming languages such as such as C/C++, Java, and Python belong?
   - **A.** Second generation
   - **B.** Third generation
   - **C.** Fourth generation
   - **D.** Fifth generation
3. Which type of tool is specifically designed to convert assembly language into machine language?
   - **A.** Compiler
   - **B.** Integrated development environment (IDE)
   - **C.** Assembler
   - **D.** Fuzzer
4. Which of the following is not very useful in assessing the security of acquired software?
   - **A.** The reliability and maturity of the vendor
   - **B.** The vendor's software escrow framework
   - **C.** Third-party vulnerability assessments
   - **D.** In-house code reviews if source code is available
5. Cohesion and coupling are characteristics of quality code. Which of the following describes the goals for these two characteristics?
   - **A.** Low cohesion, low coupling
   - **B.** Low cohesion, high coupling
   - **C.** High cohesion, low coupling
   - **D.** High cohesion, high coupling

6. Yichen is a new software engineer at Acme Software, Inc. During his first code review, he is told by his boss that he should use descriptive names for variables in his code. What is this observation an example of?

   A. Secure coding guidelines

   B. Secure coding standards

   C. Secure software development policy

   D. Use of fifth-generation language

7. On what other technology does software-defined security depend?

   A. Software-defined storage (SDS)

   B. Software-defined networking (SDN)

   C. Security orchestration, automation, and response (SOAR)

   D. Continuous integration (CI)

8. If you wanted to test source code for vulnerabilities without running it, which approach would be best?

   A. Static application security testing (SAST)

   B. Fuzzing

   C. Dynamic application security testing (DAST)

   D. Manual penetration testing

9. If you wanted to test software for vulnerabilities by executing it and then exposing it to large amounts of random inputs, which testing technique would you use?

   A. Static application security testing (SAST)

   B. Fuzzing

   C. Dynamic application security testing (DAST)

   D. Manual penetration testing

10. Which of the following is not a common reason for data breaches in managed cloud services?

    A. Misconfigurations

    B. Lack of visibility into access settings and activities

    C. Hardware failures

    D. Improper access control

Answers

1. **A.** Machine language, which consists of 1's and 0's, is the only format that a computer's processor can understand directly and is considered a first-generation language.

2. **B.** Third-generation programming languages, such as C/C++, Java, and Python, are known as high-level languages due to their refined programming structures, which allow programmers to leave low-level (system architecture) intricacies to the programming language and focus on their programming objectives.
3. **C.** Assemblers are tools that convert assembly language source code into machine code. Compilers also generate machine language, but do so by transforming high-level language code, not assembly language.
4. **B.** In a software escrow framework, a third party keeps a copy of the source code, and possibly other materials, which it will release to the customer in specific circumstances such as the developer going out of business. While software escrow is a good business continuity practice, it wouldn't normally tell us anything about the security of the software itself. All three other answers are part of a rigorous assessment of the security of acquired software.
5. **C.** Cohesion reflects how many different types of tasks a module can carry out, with the goal being to perform only one task (high cohesion), which makes modules easier to maintain. Coupling is a measure of how much a module depends on others; the more dependencies it has, the more complex and difficult the module is to maintain, so we want low (or loose) coupling.
6. **A.** Secure coding guidelines are recommended practices that tend to be less specific than standards. They might encourage programmers to use variable names that are self-explanatory and to keep functions short (without specifying how short). Secure coding standards, on the other hand, are verifiable, mandatory practices that reduce the risk of particular types of vulnerabilities in the source code.
7. **B.** Software-defined security (SDS or SDSec) is a security model in which security functions such as firewalling, IDS/IPS, and network segmentation are implemented in software within an SDN environment.
8. **A.** Static application security testing (SAST) is a technique meant to help identify software defects or security policy violations and is carried out by examining the source code without executing the program. All the other answers require that the code be executed.
9. **B.** Fuzzing is a technique used to discover flaws and vulnerabilities in software by sending large amounts of malformed, unexpected, or random data to the target program in order to trigger failures.
10. **C.** The top three reasons for data breaches in cloud services are misconfigurations, lack of visibility into access settings and activities, and improper access control.

This page intentionally left blank

APPENDIX A

Comprehensive Questions

Use the following scenario to answer Questions 1–3. Josh has discovered that an organized hacking ring in China has been targeting his company's research and development department. If these hackers have been able to uncover his company's research findings, this means they probably have access to his company's intellectual property. Josh thinks that an e-mail server in his company's DMZ may have been successfully compromised and a rootkit loaded.

1. Based upon this scenario, what is most likely the biggest risk Josh's company needs to be concerned with?

A. Market share drop if the attackers are able to bring the specific product to market more quickly than Josh's company.

B. Confidentiality of e-mail messages. Attackers may post all captured e-mail messages to the Internet.

C. Impact on reputation if the customer base finds out about the attack.

D. Depth of infiltration of attackers. If attackers have compromised other systems, more confidential data could be at risk.

2. The attackers in this situation would be seen as which of the following?

A. Vulnerability

B. Threat

C. Risk

D. Threat agent

3. If Josh is correct in his assumptions, which of the following best describes the vulnerability, threat, and exposure, respectively?

A. E-mail server is hardened, an entity could exploit programming code flaw, server is compromised and leaking data.

B. E-mail server is not patched, an entity could exploit a vulnerability, server is hardened.

C. E-mail server misconfiguration, an entity could exploit misconfiguration, server is compromised and leaking data.

D. DMZ firewall misconfiguration, an entity could exploit misconfiguration, internal e-mail server is compromised.

4. Aaron is a security manager who needs to develop a solution to allow his company's mobile devices to be authenticated in a standardized and centralized manner using digital certificates. The applications these mobile clients use require a TCP connection. Which of the following is the best solution for Aaron to implement?
   - **A.** TACACS+
   - **B.** RADIUS
   - **C.** Diameter
   - **D.** Mobile IP
5. Terry is a security manager for a credit card processing company. His company uses internal DNS servers, which are placed within the LAN, and external DNS servers, which are placed in the DMZ. The company also relies on DNS servers provided by its service provider. Terry has found out that attackers have been able to manipulate several DNS server caches to point employee traffic to malicious websites. Which of the following best describes the solution this company should implement?
   - **A.** IPSec
   - **B.** PKI
   - **C.** DNSSEC
   - **D.** MAC-based security
6. Which of the following is not a key provision of the GDPR?
   - **A.** Requirement for consent from data subjects
   - **B.** Right to be informed
   - **C.** Exclusion for temporary workers
   - **D.** Right to be forgotten
7. Jane is suspicious that an employee is sending sensitive data to one of the company's competitors but is unable to confirm this. The employee has to use this data for daily activities, thus it is difficult to properly restrict the employee's access rights. In this scenario, which best describes the company's vulnerability, threat, risk, and necessary control?
   - **A.** Vulnerability is employee access rights, threat is internal entities misusing privileged access, risk is the business impact of data loss, and the necessary control is detailed network traffic monitoring.
   - **B.** Vulnerability is lack of user monitoring, threat is internal entities misusing privileged access, risk is the business impact of data loss, and the necessary control is detailed user activity logs.
   - **C.** Vulnerability is employee access rights, threat is internal employees misusing privileged access, risk is the business impact of confidentiality, and the necessary control is multifactor authentication.
   - **D.** Vulnerability is employee access rights, threat is internal users misusing privileged access, risk is the business impact of confidentiality, and the necessary control is CCTV.

8. Which of the following best describes what role-based access control offers organizations in reducing administrative burdens?

A. It allows entities closer to the resources to make decisions about who can and cannot access resources.

B. It provides a centralized approach for access control, which frees up department managers.

C. User membership in roles can be easily revoked and new ones established as job assignments dictate.

D. It enforces an enterprise-wide security policy, standards, and guidelines.

9. Mark works for a large corporation operating in multiple countries worldwide. He is reviewing his company's policies and procedures dealing with data breaches. Which of the following is an issue that he must take into consideration?

A. Each country may or may not have unique notification requirements.

B. All breaches must be announced to affected parties within 24 hours.

C. Breach notification is a "best effort" process and not a guaranteed process.

D. Breach notifications are avoidable if all PII is removed from data stores.

10. A software development company released a product that committed several errors that were not expected once deployed in their customers' environments. All of the software code went through a long list of tests before being released. The team manager found out that after a small change was made to the code, the program was not tested before it was released. Which of the following tests was most likely not conducted?

A. Unit

B. Compiled

C. Integration

D. Regression

11. Which of the following should not be considered as part of the supply chain risk management process for a smartphone manufacturer?

A. Hardware Trojans inserted by downstream partners

B. ISO/IEC 27001

C. Hardware Trojans inserted by upstream partners

D. NIST Special Publication 800-161

12. Data sovereignty is increasingly becoming an issue that most of us in cybersecurity should address within our organizations. What does the term data sovereignty mean?

A. Certain types of data concerning a country's citizens must be stored and processed in that country.

B. Data on a country's citizens must be stored and processed according to that country's laws, regardless of where the storing/processing takes place.

C. Certain types of data concerning a country's citizens are the sovereign property of that data subject.

D. Data on a country's citizens must never cross the sovereign borders of another country.

Use the following scenario to answer Questions 13–15. Jack has just been hired as the security officer for a large hospital system. The organization develops some of its own proprietary applications. The organization does not have as many layers of controls when it comes to the data processed by these applications, since it is assumed that external entities will not understand the internal logic of the applications. One of the first things that Jack wants to carry out is a risk assessment to determine the organization's current risk profile. He also tells his boss that the hospital should become ISO certified to bolster its customers' and partners' confidence in its risk management processes.

13. Which of the following approaches has been implemented in this scenario?

A. Defense-in-depth

B. Security through obscurity

C. Information security management system

D. ISO/IEC 27001

14. Which ISO/IEC standard would be best for Jack to follow to meet his goals?

A. ISO/IEC 27001

B. ISO/IEC 27004

C. ISO/IEC 27005

D. ISO/IEC 27006

15. Which standard should Jack suggest to his boss for compliance with best practices regarding storing and processing sensitive medical information?

A. ISO/IEC 27004

B. ISO/IEC 27001

C. ISO/IEC 27799

D. ISO/IEC 27006

16. You just received an e-mail from one of your hardware manufacturers notifying you that it will no longer manufacture a certain product and, after the end of the year, you won't be able to send it in for repairs, buy spare parts, or get technical assistance from that manufacturer. What term describes this?

A. End-of-support (EOS)

B. End-of-service-life (EOSL)

C. Deprecation

D. End-of-life (EOL)

17. The confidentiality of sensitive data is protected in different ways depending on the state of the data. Which of the following is the best approach to protecting data in transit?

A. SSL

B. VPN

C. IEEE 802.1X

D. Whole-disk encryption

18. Your boss asks you to put together a report describing probable adverse effects on your assets caused by specific threat sources. What term describes this?

A. Risk analysis

B. Threat modeling

C. Attack trees

D. MITRE ATT&CK

19. A(n) ___________ is the graphical representation of data commonly used on websites. It is a skewed representation of characteristics a person must enter to prove that the subject is a human and not an automated tool, as in a software robot.

A. anti-spoofing symbol

B. CAPTCHA

C. spam anti-spoofing symbol

D. CAPCHAT

20. Mark has been asked to interview individuals to fulfill a new position in his company, chief privacy officer (CPO). What is the function of this type of position?

A. Ensuring that company financial information is correct and secure

B. Ensuring that customer, company, and employee data is protected

C. Ensuring that security policies are defined and enforced

D. Ensuring that partner information is kept safe

21. A risk management program must be developed properly and in the right sequence. Which of the following provides the correct sequence for the steps listed?

i. Develop a risk management team.

ii. Calculate the value of each asset.

iii. Identify the vulnerabilities and threats that can affect the identified assets.

iv. Identify company assets to be assessed.

A. i, iii, ii, iv

B. ii, i, iv, iii

C. iii, i, iv, ii

D. i, iv, ii, iii

22. Juan needs to assess the performance of a critical web application that his company recently upgraded. Some of the new features are very profitable, but not frequently used. He wants to ensure that the user experience is positive, but doesn't want to wait for the users to report problems. Which of the following techniques should Juan use?

A. Real user monitoring

B. Synthetic transactions

C. Log reviews

D. Management review

23. Which of the following best describes a technical control for dealing with the risks presented by data remanence?

A. Encryption

B. Data retention policies

C. File deletion

D. Using solid-state drives (SSDs)

24. George is the security manager of a large bank, which provides online banking and other online services to its customers. George has recently found out that some of the bank's customers have complained about changes to their bank accounts that they did not make. George worked with the security team and found out that all changes took place after proper authentication steps were completed. Which of the following describes what most likely took place in this situation?

A. Web servers were compromised through cross-scripting attacks.

B. TLS connections were decrypted through a man-in-the-middle attack.

C. Personal computers were compromised with malware that installed keyloggers.

D. Web servers were compromised and masquerading attacks were carried out.

25. Internet Protocol Security (IPSec) is actually a suite of protocols. Each protocol within the suite provides different functionality. Which of the following is not a function or characteristic of IPSec?

A. Encryption

B. Link layer protection

C. Authentication

D. Protection of packet payloads and the headers

26. In what order would a typical PKI perform the following transactions?

i. Receiver decrypts and obtains session key.

ii. Public key is verified.

iii. Public key is sent from a public directory.

iv. Sender sends a session key encrypted with receiver's public key.

A. iv, iii, ii, i

B. ii, i, iii, iv

C. iii, ii, iv, i

D. ii, iv, iii, i

Use the following scenario to answer Questions 27–28. Tim is the CISO for a large distributed financial investment organization. The company's network is made up of different network devices and software applications, which generate their own proprietary logs and audit data. Tim and his security team have become overwhelmed with trying to review all of the log files when attempting to identify if anything suspicious is taking place within the network. Another issue Tim's team needs to deal with is that many of the network devices have automated IPv6-to-IPv4 tunneling enabled by default, which is not what the organization needs.

27. Which of the following is the best solution to Tim's difficulties handling the quantity and diversity of logs and audit data?

A. Event correlation tools

B. Intrusion detection systems

C. Security information and event management

D. Hire more analysts

28. How could Tim best address the IP version issue described in the scenario?

A. Change management

B. Zero trust

C. Converged protocols

D. Configuration management

29. Which of the following is not a concern of a security professional considering adoption of Internet of Things (IoT) devices?

A. Weak or nonexistent authentication mechanisms

B. Vulnerability of data at rest and data in motion

C. Difficulty of deploying patches and updates

D. High costs associated with connectivity

30. What is an advantage of microservices compared to traditional server-based architectures?

A. Web services support

B. Security

C. Scalability

D. Database connectivity

31. __________, a declarative access control policy language implemented in XML and a processing model, describes how to interpret security policies. __________ is an XML-based language that allows for the exchange of provisioning data between applications, which could reside in one organization or many.

A. Service Provisioning Markup Language (SPML), Extensible Access Control Markup Language (XACML)

B. Extensible Access Control Markup Language (XACML), Service Provisioning Markup Language (SPML)

C. Extensible Access Control Markup Language (XACML), Security Assertion Markup Language (SAML)

D. Security Assertion Markup Language (SAML), Service Provisioning Markup Language (SPML)

32. Doors configured in fail-safe mode assume what position in the event of a power failure?

A. Open and locked

B. Closed and locked

C. Closed and unlocked

D. Open

33. Next-generation firewalls combine the best attributes of other types of firewalls. Which of the following is not a common characteristic of these firewall types?

A. Integrated intrusion prevention system

B. Sharing signatures with cloud-based aggregators

C. Automated incident response

D. High cost

34. The purpose of security awareness training is to expose personnel to security issues so that they may be able to recognize them and better respond to them. Which of the following is not normally a topic covered in security awareness training?

A. Social engineering

B. Phishing

C. Whaling

D. Trolling

Use the following scenario to answer Questions 35–36. Zack is a security consultant who has been hired to help an accounting company improve some of its current e-mail security practices. The company wants to ensure that when its clients send the company accounting files and data, the clients cannot later deny sending these messages. The company also wants to integrate a more granular and secure authentication method for its current mail server and clients.

35. Which of the following best describes how client messages can be dealt with and addresses the first issue outlined in the scenario?

A. The company needs to integrate a public key infrastructure and the Diameter protocol.

B. The company needs to require that clients encrypt messages with their public key before sending them to the company.

C. The company needs to have all clients sign a formal document outlining nonrepudiation requirements.

D. The company needs to require that clients digitally sign messages that contain financial information.

36. Which of the following would be the best solution to integrate to meet the authentication requirements outlined in the scenario?

A. TLS

B. IPSec

C. 802.1X

D. SASL

37. Which of the following is not considered a secure coding practice?

A. Validate user inputs

B. Default deny

C. Defense in depth

D. High (tight) coupling

38. A __________ is the amount of time it should take to recover from a disaster, and a __________ is the amount of data, measured in time, that can be lost and be tolerable from that same event.

A. recovery time objective, recovery point objective

B. recovery point objective, recovery time objective

C. maximum tolerable downtime, work recovery time

D. work recovery time, maximum tolerable downtime

39. Mary is doing online research about prospective employers and discovers a way to compromise a small company's personnel files. She decides to take a look around, but does not steal any information. Is she still committing a crime even if she does not steal any of the information?

- **A.** No, since she does not steal any information, she is not committing a crime.
- **B.** Probably, because she has gained unauthorized access.
- **C.** Not if she discloses the vulnerability she exploited to the company.
- **D.** Yes, she could jeopardize the system without knowing it.

40. In the structure of Extensible Access Control Markup Language (XACML), a Subject element is the ___________, a Resource element is the ___________, and an Action element is the ___________.

- **A.** requesting entity, requested entity, types of access
- **B.** requested entity, requesting entity, types of access
- **C.** requesting entity, requested entity, access control
- **D.** requested entity, requesting entity, access control

41. The Mobile IP protocol allows location-independent routing of IP datagrams on the Internet. Each mobile node is identified by its ___________, disregarding its current location in the Internet. While away from its home network, a mobile node is associated with a ___________.

- **A.** prime address, care-of address
- **B.** home address, care-of address
- **C.** home address, secondary address
- **D.** prime address, secondary address

42. Because she has many different types of security products and solutions, Joan wants to purchase a product that integrates her many technologies into one user interface. She would like her staff to analyze all security alerts from the same application environment. Which of the following would best fit Joan's needs?

- **A.** Dedicated appliance
- **B.** Data analytics platform
- **C.** Hybrid IDS\IPS integration
- **D.** Security information and event management (SIEM)

43. When classifying an information asset, which of the following is true concerning its sensitivity?

- **A.** It is commensurate with how its loss would impact the fundamental business processes of the organization.
- **B.** It is determined by its replacement cost.

C. It is determined by the product of its replacement cost and the probability of its compromise.

D. It is commensurate with the losses to an organization if it were revealed to unauthorized individuals.

44. Which of the following is an international organization that helps different governments come together and tackle the economic, social, and governance challenges of a globalized economy and provides guidelines on the protection of privacy and transborder flows of personal data rules?

A. Council of Global Convention on Cybercrime

B. Council of Europe Convention on Cybercrime

C. Organisation for Economic Co-operation and Development

D. Organisation for Cybercrime Co-operation and Development

45. System ports allow different computers to communicate with each other's services and protocols. The Internet Assigned Numbers Authority (IANA) has assigned registered ports to be __________ and dynamic ports to be __________.

A. 0–1024, 49152–65535

B. 1024–49151, 49152–65535

C. 1024–49152, 49153–65535

D. 0–1024, 1025–49151

46. When conducting a quantitative risk analysis, items are gathered and assigned numeric values so that cost/benefit analysis can be carried out. Which of the following formulas could be used to understand the value of a safeguard?

A. (ALE before implementing safeguard) – (ALE after implementing safeguard) – (annual cost of safeguard) = value of safeguard to the organization

B. (ALE before implementing safeguard) – (ALE during implementing safeguard) – (annual cost of safeguard) = value of safeguard to the organization

C. (ALE before implementing safeguard) – (ALE while implementing safeguard) – (annual cost of safeguard) = value of safeguard to the organization

D. (ALE before implementing safeguard) – (ALE after implementing safeguard) – (annual cost of asset) = value of safeguard to the organization

47. Patty is giving a presentation next week to the executive staff of her company. She wants to illustrate the benefits of the company using specific cloud computing solutions. Which of the following does not properly describe one of these benefits or advantages?

A. Organizations have more flexibility and agility in IT growth and functionality.

B. Cost of computing can be increased since it is a shared delivery model.

C. Location independence can be achieved because the computing is not centralized and tied to a physical data center.

D. Scalability and elasticity of resources can be accomplished in near real-time through automation.

Use the following scenario to answer Questions 48–49. Francisca is the new manager of the in-house software designers and programmers. She has been telling her team that before design and programming on a new product begins, a formal architecture needs to be developed. She also needs this team to understand security issues as they pertain to software design. Francisca has shown the team how to follow a systematic approach that allows them to understand different ways in which the software products they develop could be compromised by specific threat actors.

48. Which of the following best describes what an architecture is in the context of this scenario?

A. Tool used to conceptually understand the structure and behavior of a complex entity through different views

B. Formal description and representation of a system and the components that make it up

C. Framework used to create individual architectures with specific views

D. Framework that is necessary to identify needs and meet all of the stakeholder requirements

49. Which of the following best describes the approach Francisca has shown her team as outlined in the scenario?

A. Attack surface analysis

B. Threat modeling

C. Penetration testing

D. Double-blind penetration testing

50. Barry was told that the IDS product that is being used on the network has heuristic capabilities. Which of the following best describes this functionality?

A. Gathers packets and reassembles the fragments before assigning anomaly values

B. Gathers data and assesses the likelihood of it being malicious in nature

C. Gathers packets and compares their payload values to a signature engine

D. Gathers packet headers to determine if something suspicious is taking place within the network traffic

51. Bringing in third-party auditors has advantages over using an internal team. Which of the following is not true about using external auditors?

A. They are required by certain governmental regulations.

B. They bring experience gained by working in many other organizations.

C. They know the organization's processes and technology better than anyone else.

D. They are less influenced by internal culture and politics.

52. Don is a senior manager of an architectural firm. He has just found out that a key contract was renewed, allowing the company to continue developing an operating system that was idle for several months. Excited to get started, Don begins work on the operating system privately, but cannot tell his staff until the news is announced publicly in a few days. However, as Don begins making changes in the software, various staff members notice changes in their connected systems, even though they have a lower security level than Don. What kind of model could be used to ensure this does not happen?

A. Biba

B. Bell-LaPadula

C. Noninterference

D. Clark-Wilson

53. Betty has received several e-mail messages from unknown sources that try and entice her to click a specific link using a "Click Here" approach. Which of the following best describes what is most likely taking place in this situation?

A. DNS pharming attack

B. Embedded hyperlink is obfuscated

C. Malware back-door installation

D. Bidirectional injection attack

54. Rebecca is an internal auditor for a large retail company. The company has a number of web applications that run critical business processes with customers and partners around the world. Her company would like to ensure the security of technical controls on these processes. Which of the following would not be a good approach to auditing these technical controls?

A. Log reviews

B. Code reviews

C. Personnel background checks

D. Misuse case testing

55. Which of the following multiplexing technologies analyzes statistics related to the typical workload of each input device and makes real-time decisions on how much time each device should be allocated for data transmission?

A. Time-division multiplexing

B. Wave-division multiplexing

C. Frequency-division multiplexing

D. Statistical time-division multiplexing

56. In a VoIP environment, the Real-time Transport Protocol (RTP) and RTP Control Protocol (RTCP) are commonly used. Which of the following best describes the difference between these two protocols?

A. RTCP provides a standardized packet format for delivering audio and video over IP networks. RTP provides out-of-band statistics and control information to provide feedback on QoS levels.

B. RTP provides a standardized packet format for delivering data over IP networks. RTCP provides control information to provide feedback on QoS levels.

C. RTP provides a standardized packet format for delivering audio and video over MPLS networks. RTCP provides control information to provide feedback on QoS levels.

D. RTP provides a standardized packet format for delivering audio and video over IP networks. RTCP provides out-of-band statistics and control information to provide feedback on QoS levels.

57. Which of the following is not descriptive of an edge computing architecture?

A. It eliminates the need for cloud infrastructure.

B. Processing and storage assets are close to where they're needed.

C. It reduces latency and network traffic.

D. It typically has three layers.

58. Which cryptanalytic attack method is characterized by the identification of statistically significant patterns in the ciphertext generated by a cryptosystem?

A. Differential attack

B. Implementation attack

C. Frequency analysis

D. Side-channel attack

59. IPSec's main protocols are AH and ESP. Which of the following services does AH provide?

A. Confidentiality and authentication

B. Confidentiality and availability

C. Integrity and accessibility

D. Integrity and authentication

60. When multiple databases exchange transactions, each database is updated. This can happen many times and in many different ways. To protect the integrity of the data, databases should incorporate a concept known as an ACID test. What does this acronym stand for?

A. Availability, confidentiality, integrity, durability

B. Availability, consistency, integrity, durability

C. Atomicity, confidentiality, isolation, durability

D. Atomicity, consistency, isolation, durability

Use the following scenario to answer Questions 61–63. Jim works for a large energy company. His senior management just conducted a meeting with Jim's team with the purpose of reducing IT costs without degrading their security posture. The senior management decided to move all administrative systems to a cloud provider. These systems are proprietary applications currently running on Linux servers.

61. Which of the following services would allow Jim to transition all administrative custom applications to the cloud while leveraging the service provider for security and patching of the cloud platforms?

A. IaaS

B. PaaS

C. SaaS

D. IDaaS

62. Which of the following would *not* be an issue that Jim would have to consider in transitioning administrative services to the cloud?

A. Privacy and data breach laws in the country where the cloud servers are located

B. Loss of efficiencies, performance, reliability, scalability, and security

C. Security provisions in the terms of service

D. Total cost of ownership compared to the current systems

63. Which of the following secure design principles would be most important to consider as Jim plans the transition to the cloud?

A. Defense in depth

B. Secure defaults

C. Shared responsibility

D. Zero trust

64. A group of software designers are at a stage in their software development project where they need to reduce the amount of code running, reduce entry points available to untrusted users, reduce privilege levels as much as possible, and eliminate unnecessary services. Which of the following best describes the first step the team needs to carry out to accomplish these tasks?

A. Attack surface analysis

B. Software development life cycle

C. Risk assessment

D. Unit testing

65. Jenny needs to engage a new software development company to create her company's internal banking software. The software needs to be created specifically for her company's environment, so it must be proprietary in nature. Which of the following would be useful for Jenny to use as a gauge to determine how advanced the various software development companies are in their processes?

A. Waterfall methodology

B. Capability Maturity Model Integration level

C. Auditing results

D. Key performance metrics

66. Which type of organization would be likeliest to implement Virtual eXtensible Local Area Network (VxLAN) technology?

A. Organizations that need to support more than 2,048 VLANs

B. Small and medium businesses

C. Organizations with hosts in close proximity to each other

D. Cloud service providers with hundreds of customers

67. Kerberos is a commonly used access control and authentication technology. It is important to understand what the technology can and cannot do and its potential downfalls. Which of the following is not a potential security issue that must be addressed when using Kerberos?

i. The KDC can be a single point of failure.

ii. The KDC must be scalable.

iii. Secret keys are temporarily stored on the users' workstations.

iv. Kerberos is vulnerable to password guessing.

A. i, iv

B. iii

C. All of them

D. None of them

68. If the annualized loss expectancy (ALE) for a specific asset is $100,000, and after implementation of a control to safeguard the asset the new ALE is $45,000 and the annual cost of the control is $30,000, should the company implement this control?

A. Yes

B. No

C. Not enough information

D. Depends on the annualized rate of occurrence (ARO)

69. ISO/IEC 27000 is a growing family of ISO/IEC information security management system (ISMS) standards. Which of the following provides an incorrect mapping of the individual standard number to its description?

A. ISO/IEC 27002: Code of practice for information security controls

B. ISO/IEC 27003: ISMS implementation guidance

C. ISO/IEC 27004: ISMS monitoring, measurement, analysis, and evaluation

D. ISO/IEC 27005: ISMS auditing guidelines

70. Yazan leads the IT help desk at a large manufacturing company. He is concerned about the amount of time his team spends resetting passwords for the various accounts that each of his organizational users has. All of the following would be good approaches to alleviating this help desk load *except* which one?

A. Single sign-on (SSO)

B. Just-in-time (JIT) access

C. Password managers

D. Self-service password reset

71. Encryption and decryption can take place at different layers of an operating system, application, and network stack. End-to-end encryption happens within the ___________. IPSec encryption takes place at the ___________ layer. PPTP encryption takes place at the ___________ layer. Link encryption takes place at the ___________ and ___________ layers.

A. applications, transport, data link, data link, physical

B. applications, transport, network, data link, physical

C. applications, network, data link, data link, physical

D. network, transport, data link, data link, physical

72. Which of the following best describes the difference between hierarchical storage management (HSM) and storage area network (SAN) technologies?

A. HSM uses optical or tape jukeboxes, and SAN is a network of connected storage systems.

B. SAN uses optical or tape jukeboxes, and HSM is a network of connected storage systems.

C. HSM and SAN are one and the same. The difference is in the implementation.

D. HSM uses optical or tape jukeboxes, and SAN is a standard of how to develop and implement this technology.

73. Which legal system is characterized by its reliance on previous interpretations of the law?

A. Tort

B. Customary

C. Common

D. Civil (code)

74. In order to be admissible in court, evidence should normally be which of the following?

A. Subpoenaed

B. Relevant

C. Motioned

D. Adjudicated

75. Which type of authorization mechanism can incorporate historical data into its access control decision-making in real time?

A. Rule-based access control

B. Risk-based access control

C. Attribute-based access control

D. Discretionary access control

76. Which of the following is an XML-based protocol that defines the schema of how web service communication takes place over HTTP transmissions?

A. Service-Oriented Protocol

B. Active X Protocol

C. SOAP

D. Web Ontology Language

77. Which of the following has an incorrect definition mapping?

i. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Team-oriented approach that assesses organizational and IT risks through facilitated workshops

ii. Facilitated Risk Analysis Process (FRAP) Stresses prescreening activities so that the risk assessment steps are only carried out on the item(s) that need(s) it the most

iii. ISO/IEC 27005 International standard for the implementation of a risk management program that integrates into an information security management system (ISMS)

iv. Failure Modes and Effect Analysis (FMEA) Approach that dissects a component into its basic functions to identify flaws and those flaws' effects

v. Fault tree analysis Approach to map specific flaws to root causes in complex systems

A. None of them

B. ii

C. iii, iv

D. v

78. For an enterprise security architecture to be successful in its development and implementation, which of the following items must be understood and followed?

i. Strategic alignment

ii. Process enhancement

iii. Business enablement

iv. Security effectiveness

A. i, ii

B. ii, iii

C. i, ii, iii, iv

D. iii, iv

79. Which of the following best describes the purpose of the Organisation for Economic Co-operation and Development (OECD)?

A. An international organization where member countries come together and tackle the economic, social, and governance challenges of a globalized economy

B. A national organization that helps different governments come together and tackle the economic, social, and governance challenges of a globalized economy

C. A United Nations body that regulates economic, social, and governance issues of a globalized economy

D. A national organization that helps different organizations come together and tackle the economic, social, and governance challenges of a globalized economy

80. Many enterprise architecture models have been developed over the years for specific purposes. Some of them can be used to provide structure for information security processes and technology to be integrated throughout an organization. Which of the following provides an incorrect mapping between the architecture type and the associated definition?

A. **Zachman Framework** Model and methodology for the development of information security enterprise architectures

B. **TOGAF** Model and methodology for the development of enterprise architectures developed by The Open Group

C. **DoDAF** U.S. Department of Defense architecture framework that ensures interoperability of systems to meet military mission goals

D. **SABSA** Framework and methodology for enterprise security architecture and service management

81. Which of the following best describes the difference between the role of the ISO/IEC 27000 series and COBIT?

A. COBIT provides a high-level overview of security program requirements, while the ISO/IEC 27000 series provides the objectives of the individual security controls.

B. The ISO/IEC 27000 series provides a high-level overview of security program requirements, while COBIT maps IT goals to enterprise goals to stakeholder needs.

C. COBIT is process oriented, and the ISO/IEC 27000 series is solution oriented.

D. The ISO/IEC 27000 series is process oriented, and COBIT is solution oriented.

82. The Capability Maturity Model Integration (CMMI) approach is being used more frequently in security program and enterprise development. Which of the following provides an incorrect characteristic of this model?

A. It provides a pathway for how incremental improvement can take place.

B. It provides structured steps that can be followed so an organization can evolve from one level to the next and constantly improve its processes.

C. It was created for process improvement and developed by Carnegie Mellon.

D. It was built upon the SABSA model.

83. If Jose wanted to use a risk assessment methodology across the entire organization and allow the various business owners to identify risks and know how to deal with them, what methodology would he use?

A. Qualitative

B. COBIT

C. FRAP

D. OCTAVE

84. Information security is a field that is maturing and becoming more organized and standardized. Organizational security models should be based on an enterprise architecture framework. Which of the following best describes what an enterprise architecture framework is and why it would be used?

A. Mathematical model that defines the secure states that various software components can enter and still provide the necessary protection

B. Conceptual model that is organized into multiple views addressing each of the stakeholder's concerns

C. Business enterprise framework that is broken down into six conceptual levels to ensure security is deployed and managed in a controllable manner

D. Enterprise framework that allows for proper security governance

85. Which of the following provides a true characteristic of a fault tree analysis?

A. Fault trees are assigned qualitative values to faults that can take place over a series of business processes.

B. Fault trees are assigned failure mode values.

C. Fault trees are labeled with actual numbers pertaining to failure probabilities.

D. Fault trees are used in a stepwise approach to software debugging.

86. It is important that organizations ensure that their security efforts are effective and measurable. Which of the following is not a common method used to track the effectiveness of security efforts?

A. Service level agreement

B. Return on investment

C. Balanced scorecard system

D. Provisioning system

87. Capability Maturity Model Integration (CMMI) is a process improvement approach that is used to help organizations improve their performance. The CMMI model may also be used as a framework for appraising the process maturity of the organization. Which of the following is an incorrect mapping of the levels that may be assigned to an organization based upon this model?

i. Maturity Level 2 – Managed or Repeatable

ii. Maturity Level 3 – Defined

iii. Maturity Level 4 – Quantitatively Managed

iv. Maturity Level 5 – Optimizing

A. i

B. i, ii

C. All of them

D. None of them

88. An organization's information systems risk management (ISRM) policy should address many items to provide clear direction and structure. Which of the following is not a core item that should be covered in this type of policy?

i. The objectives of the ISRM team

ii. The level of risk the organization will accept and what is considered an acceptable level of risk

iii. Formal processes of risk identification

iv. The connection between the ISRM policy and the organization's strategic planning processes

v. Responsibilities that fall under ISRM and the roles to fulfill them

vi. The mapping of risk to specific physical controls

vii. The approach toward changing staff behaviors and resource allocation in response to risk analysis

viii. The mapping of risks to performance targets and budgets

ix. Key metrics and performance indicators to monitor the effectiveness of controls

A. ii, v, ix

B. vi

C. v

D. vii, ix

89. More organizations are outsourcing supporting functions to allow them to focus on their core business functions. Organizations use hosting companies to maintain websites and e-mail servers, service providers for various telecommunication connections, disaster recovery companies for co-location capabilities, cloud computing providers for infrastructure or application services, developers for software creation, and security companies to carry out vulnerability management. Which of the following items should be included during the analysis of an outsourced partner or vendor?

i. Conduct onsite inspection and interviews

ii. Review contracts to ensure security and protection levels are agreed upon

iii. Ensure service level agreements are in place

iv. Review internal and external audit reports and third-party reviews

v. Review references and communicate with former and existing customers

A. ii, iii, iv

B. iv, v

C. All of them

D. i, ii, iii

90. Which of the following is normally not an element of e-discovery?

A. Identification

B. Preservation

C. Production

D. Remanence

91. A financial institution has developed its internal security program based upon the ISO/IEC 27000 series. The security officer has been told that metrics need to be developed and integrated into this program so that effectiveness can be gauged. Which of the following standards should be followed to provide this type of guidance and functionality?

- **A.** ISO/IEC 27002
- **B.** ISO/IEC 27003
- **C.** ISO/IEC 27004
- **D.** ISO/IEC 27005

92. Which of the following is not an advantage of using content distribution networks?

- **A.** Improved responsiveness to regional users
- **B.** Resistance to ARP spoofing attacks
- **C.** Customization of content for regional users
- **D.** Resistance to DDoS attacks

93. Sana has been asked to install a cloud access security broker (CASB) product for her company's environment. What is the best description for what CASBs are commonly used for?

- **A.** Monitor end-user behavior and enforce policies across cloud services
- **B.** Provision secure cloud services
- **C.** Enforce access controls to cloud services through X.500 databases
- **D.** Protect cloud services from certain types of attacks

94. Which of the following allows a user to be authenticated across multiple IT systems and enterprises?

- **A.** Single sign-on (SSO)
- **B.** Session management
- **C.** Federated identity
- **D.** Role-based access control (RBAC)

95. Which of the following is a true statement pertaining to markup languages?

- **A.** Hypertext Markup Language (HTML) came from Generalized Markup Language (GML), which came from Standard Generalized Markup Language (SGML).
- **B.** Hypertext Markup Language (HTML) came from Standard Generalized Markup Language (SGML), which came from Generalized Markup Language (GML).

C. Standard Generalized Markup Language (SGML) came from Hypertext Markup Language (HTML), which came from Generalized Markup Language (GML).

D. Standard Generalized Markup Language (SGML) came from Generalized Markup Language (GML), which came from Hypertext Markup Language (HTML).

96. What is Extensible Markup Language (XML) and why was it created?

A. A specification that provides a structure for creating other markup languages and still allow for interoperability

B. A specification that is used to create static and dynamic websites

C. A specification that outlines a detailed markup language dictating all formats of all companies that use it

D. A specification that does not allow for interoperability for the sake of security

97. Which access control policy is based on the necessary operations and tasks users need to fulfill their responsibilities within an organization and allows for implicit permission inheritance using a nondiscretionary model?

A. Rule-based

B. Role-based

C. Identity-based

D. Mandatory

98. Which of the following centralized access control protocols would a security professional choose if her network consisted of multiple protocols, including Mobile IP, and had users connecting via wireless and wired transmissions?

A. RADIUS

B. TACACS+

C. Diameter

D. Kerberos

99. Javad is the security administrator at a credit card processing company. The company has many identity stores, which are not properly synchronized. Javad is going to oversee the process of centralizing and synchronizing the identity data within the company. He has determined that the data in the HR database will be considered the most up-to-date data, which cannot be overwritten by the software in other identity stores during their synchronization processes. Which of the following best describes the role of this database in the identity management structure of the company?

A. Authoritative system of record

B. Infrastructure source server

C. Primary identity store

D. Hierarchical database primary

100. Proper access control requires a structured user provisioning process. Which of the following best describes user provisioning?

A. The creation, maintenance, and deactivation of user objects and attributes as they exist in one or more systems, directories, or applications, in response to business processes

B. The creation, maintenance, activation, and delegation of user objects and attributes as they exist in one or more systems, directories, or applications, in response to compliance processes

C. The maintenance of user objects and attributes as they exist in one or more systems, directories, or applications, in response to business processes

D. The creation and deactivation of user objects and attributes as they exist in one or more systems, directories, or applications, in response to business processes

101. Which of the following protocols would an Identity as a Service (IDaaS) provider use to authenticate you to a third party?

A. Diameter

B. OAuth

C. Kerberos

D. OpenID Connect

102. Johana needs to ensure that her company's application can accept provisioning data from the company's partner's application in a standardized method. Which of the following best describes the technology that Johana should implement?

A. Service Provisioning Markup Language

B. Extensible Provisioning Markup Language

C. Security Assertion Markup Language

D. Security Provisioning Markup Language

103. Lynn logs into a website and purchases an airline ticket for her upcoming trip. The website also offers her pricing and package deals for hotel rooms and rental cars while she is completing her purchase. The airline, hotel, and rental companies are all separate and individual companies. Lynn decides to purchase her hotel room through the same website at the same time. The website is using Security Assertion Markup Language to allow for this type of federated identity management functionality. In this example which entity is the principal, which entity is the identity provider, and which entity is the service provider, respectively?

A. Portal, Lynn, hotel company

B. Lynn, airline company, hotel company

C. Lynn, hotel company, airline company

D. Portal, Lynn, airline company

104. John is the new director of software development within his company. Several proprietary applications offer individual services to the employees, but the employees have to log into each and every application independently to gain access to these discrete services. John would like to provide a way that allows each of the services provided by the various applications to be centrally accessed and controlled. Which of the following best describes the architecture that John should deploy?

A. Service-oriented architecture

B. Web services architecture

C. Single sign-on architecture

D. Hierarchical service architecture

105. Which security model is defined by three main rules: simple security, star property, and strong star property?

A. Biba

B. Bell-LaPadula

C. Brewer-Nash

D. Noninterference

106. Khadijah is leading a software development team for her company. She knows the importance of conducting an attack surface analysis and developing a threat model. During which phase of the software development life cycle should she perform these actions?

A. Requirements gathering

B. Testing and validation

C. Release and maintenance

D. Design

107. Bartosz is developing a new web application for his marketing department. One of the requirements for the software is that it allows users to post specific content to LinkedIn and Twitter directly from the web app. Which technology would allow him to do this?

A. OpenID Connect

B. OAuth

C. SSO

D. Federated Identity Management

108. Applications may not work on systems with specific processors. Which of the following best describes why an application may work on an Intel processor but not on an AMD processor?

A. The application was not compiled to machine language that is compatible with the AMD architecture.

B. It is not possible for the same application to run on both Intel and AMD processors.

C. The application was not compiled to machine language that is compatible with the Windows architecture.

D. Only applications written in high-level languages will work on different processor architectures.

109. Which of the following is *not* true about software libraries?

A. They make software development more efficient through code reuse.

B. They are typically accessed through an application programming interface (API).

C. They almost never introduce vulnerabilities into programs that use them.

D. They are used in most major software development projects.

110. Kim is tasked with testing the security of an application but has no access to its source code. Which of the following tests could she use in this scenario?

A. Dynamic application security testing

B. Static application security testing

C. Regression testing

D. Code review

111. Hanna is a security manager of a company that relies heavily on one specific operating system. The operating system is used in the employee workstations and is embedded within devices that support the automated production line software. She has uncovered a vulnerability in the operating system that could allow an attacker to force applications to not release memory segments after execution. Which of the following best describes the type of threat this vulnerability introduces?

A. Injection attacks

B. Memory corruption

C. Denial of service

D. Software locking

112. Which of the following access control mechanisms gives you the most granularity in defining access control policies?

A. Attribute-based access control (ABAC)

B. Role-based access control (RBAC)

C. Mandatory access control (MAC)

D. Discretionary access control (DAC)

113. All of the following are weaknesses of Kerberos *except* which one?

A. Principals don't trust each other.

B. Only the KDC can vouch for individuals' identities and entitlements.

C. Secret keys are stored on the users' workstations temporarily.

D. Susceptibility to password guessing and brute-force attacks.

114. A company needs to implement a CCTV system that will monitor a large area of the facility. Which of the following is the correct lens combination for this?

A. A wide-angle lens and a small lens opening

B. A wide-angle lens and a large lens opening

C. A wide-angle lens and a large lens opening with a small focal length

D. A wide-angle lens and a large lens opening with a large focal length

115. What is the name of a water sprinkler system that keeps pipes empty and doesn't release water until a certain temperature is met and a "delay mechanism" is instituted?

A. Wet

B. Preaction

C. Delayed

D. Dry

116. There are different types of fire suppression systems. Which of the following answers best describes the difference between a deluge system and a preaction system?

A. A deluge system provides a delaying mechanism that allows someone to deactivate the system in case of a false alarm or if the fire can be extinguished by other means. A preaction system provides similar functionality but has wide open sprinkler heads that allow a lot of water to be dispersed quickly.

B. A preaction system provides a delaying mechanism that allows someone to deactivate the system in case of a false alarm or if the fire can be extinguished by other means. A deluge system has wide open sprinkler heads that allow a lot of water to be dispersed quickly.

C. A dry pipe system provides a delaying mechanism that allows someone to deactivate the system in case of a false alarm or if the fire can be extinguished by other means. A deluge system has wide open sprinkler heads that allow a lot of water to be dispersed quickly.

D. A preaction system provides a delaying mechanism that allows someone to deactivate the system in case of a false alarm or if the fire can be extinguished by other means. A deluge system provides similar functionality but has wide open sprinkler heads that allow a lot of water to be dispersed quickly.

117. Which of the following best describes why Crime Prevention Through Environmental Design (CPTED) would integrate benches, walkways, and bike paths into a site?

A. These features are designed to provide natural access control.

B. These features are designed to emphasize or extend the organization's physical sphere of influence so legitimate users feel a sense of ownership of that space.

C. These features are designed to make criminals think that those in the site are more attentive, well resourced, and possibly alert.

D. These features are designed to make criminals feel uncomfortable by providing many ways observers could potentially see them.

118. Which of the following frameworks is a two-dimensional model that uses six basic communication interrogatives intersecting with different viewpoints to give a holistic understanding of the enterprise?

A. SABSA

B. TOGAF

C. CMMI

D. Zachman

119. Not every data transmission incorporates the session layer. Which of the following best describes the functionality of the session layer?

A. End-to-end data transmission

B. Application client/server communication mechanism in a distributed environment

C. Application-to-computer physical communication

D. Provides application with the proper syntax for transmission

120. What is the purpose of the Logical Link Control (LLC) layer in the OSI model?

A. Provides a standard interface for the network layer protocol

B. Provides the framing functionality of the data link layer

C. Provides addressing of the packet during encapsulation

D. Provides the functionality of converting bits into electrical signals

121. Which of the following best describes why classless interdomain routing (CIDR) was created?

A. To allow IPv6 traffic to tunnel through IPv4 networks

B. To allow IPSec to be integrated into IPv4 traffic

C. To allow an address class size to meet an organization's need

D. To allow IPv6 to tunnel IPSec traffic

122. Johnetta is a security engineer at a company that develops highly confidential products for various government agencies. Her company has VPNs set up to protect traffic that travels over the Internet and other nontrusted networks, but she knows that internal traffic should also be protected. Which of the following is the best type of approach Johnetta's company should take?

A. Implement a data link technology that provides 802.1AE security functionality.

B. Implement a network-level technology that provides 802.1AE security functionality.

C. Implement TLS over L2TP.

D. Implement IPSec over L2TP.

123. IEEE __________ provides a unique ID for a device. IEEE __________ provides data encryption, integrity, and origin authentication functionality. IEEE __________ carries out key agreement functions for the session keys used for data encryption. Each of these standards provides specific parameters to work within an IEEE __________ framework.

A. 802.1AF, 802.1AE, 802.1AR, 802.1X EAP-TLS

B. 802.1AT, 802.1AE, 802.1AM, 802.1X EAP-SSL

C. 802.1AR, 802.1AE, 802.1AF, 802.1X EAP-SSL

D. 802.1AR, 802.1AE, 802.1AF, 802.1X EAP-TLS

124. Under the principle of ethical disclosure, information systems security professionals must properly disclose __________ to the appropriate parties.

A. Vulnerabilities

B. Threats

C. Exploits

D. Incidents

125. Larry is a seasoned security professional and knows the potential dangers associated with using an ISP's DNS server for Internet connectivity. When Larry stays at a hotel or uses his laptop in any type of environment he does not fully trust, he updates values in his HOSTS file. Which of the following best describes why Larry carries out this type of task?

A. Reduces the risk of an attacker sending his system a corrupt ARP address that points his system to a malicious website

B. Ensures his host-based IDS is properly updated

C. Reduces the risk of an attacker sending his system an incorrect IP address-to-host mapping that points his system to a malicious website

D. Ensures his network-based IDS is properly synchronized with his host-based IDS

126. John has uncovered a rogue system on the company network that emulates a switch. The software on this system is being used by an attacker to modify frame tag values. Which of the following best describes the type of attack that has most likely been taking place?

A. DHCP snooping

B. VLAN hopping

C. Network traffic shaping

D. Network traffic hopping

127. Frank is a new security manager for a large financial institution. He has been told that the organization needs to reduce the total cost of ownership for many components of the network and infrastructure. The organization currently maintains many distributed networks, software packages, and applications. Which of the following best describes the cloud service models that Frank could leverage to obtain cloud services to replace on-premises network and infrastructure components

A. Infrastructure as a Service provides an environment similar to an operating system, Platform as a Service provides operating systems and other major processing platforms, and Software as a Service provides specific application-based functionality.

B. Infrastructure as a Service provides an environment similar to a data center, Platform as a Service provides operating systems and other major processing platforms, and Software as a Service provides specific application-based functionality.

C. Infrastructure as a Service provides an environment similar to a data center, Platform as a Service provides application-based functionality, and Software as a Service provides specific operating system functionality.

D. Infrastructure as a Service provides an environment similar to a database, Platform as a Service provides operating systems and other major processing platforms, and Software as a Service provides specific application-based functionality.

128. Terry works in a training services provider where the network topology and access controls change very frequently. His boss tells him that he needs to implement a network infrastructure that enables changes to be made quickly and securely with minimal effort. What does Terry need to roll out?

A. Wi-Fi

B. Infrastructure as a Service

C. Software-defined networking

D. Software-defined wide area networking

129. On a Tuesday morning, Jami is summoned to the office of the security director, where she finds six of her peers from other departments. The security director gives them instructions about an event that will be taking place in two weeks. Each of the individuals will be responsible for removing specific systems from the facility, bringing them to the offsite facility, and implementing them. Each individual will need to test the installed systems and ensure the configurations are correct for production activities. What event is Jami about to take part in?

A. Parallel test

B. Full-interruption test

C. Simulation test

D. Structured walk-through test

130. While disaster recovery planning (DRP) and business continuity planning (BCP) are directed at the development of "plans," ___________ is the holistic management process that should cover both of them. It provides a framework for integrating resilience with the capability for effective responses that protects the interests of the organization's key stakeholders.

A. continuity of operations

B. business continuity management

C. risk management

D. enterprise management architecture

131. Your company enters into a contract with another company as part of which your company requires the other company to abide by specific security practices. Six months into the effort, you decide to verify that the other company is satisfying these security requirements. Which of the following would you conduct?

A. Third-party audit

B. External (second-party) audit

C. Structured walk-through test

D. Full-interruption test

132. Which of the following statements is true about employee duress?

A. Its risks can be mitigated by installing panic buttons.

B. Its risks can be mitigated by installing panic rooms.

C. Its risks can be mitigated by enforcing forced vacations.

D. It can more easily be detected using the right clipping levels.

133. The main goal of the Wassenaar Arrangement is to prevent the buildup of military capabilities that could threaten regional and international security and stability. How does this relate to technology?

A. Cryptography is a dual-use tool.

B. Technology is used in weaponry systems.

C. Military actions directly relate to critical infrastructure systems.

D. Critical infrastructure systems can be at risk under this agreement.

134. Which world legal system is used in continental European countries, such as France and Spain, and is rule-based law, not precedent-based?

A. Civil (code) law system

B. Common law system

C. Customary law system

D. Mixed law system

135. Which of the following is not a correct characteristic of the Failure Modes and Effect Analysis (FMEA) method?

A. Determining functions and identifying functional failures

B. Assessing the causes of failure and their failure effects through a structured process

C. Structured process carried out by an identified team to address high-level security compromises

D. Identifying where something is most likely going to break and either fixing the flaws that could cause this issue or implementing controls to reduce the impact of the break

136. A risk analysis can be carried out through qualitative or quantitative means. It is important to choose the right approach to meet the organization's goals. In a quantitative analysis, which of the following items would not be assigned a numeric value?

i. Asset value

ii. Threat frequency

iii. Severity of vulnerability

iv. Impact damage

v. Safeguard costs

vi. Safeguard effectiveness

vii. Probability

A. All of them

B. None of them

C. ii

D. vii

137. Uncovering restricted information by using permissible data is referred to as ___________.

A. inference

B. data mining

C. perturbation

D. cell suppression

138. Meeta recently started working at an organization with no defined security processes. One of the areas she'd like to improve is software patching. Consistent with the organizational culture, she is considering a decentralized or unmanaged model for patching. Which of the following is not one of the risks her organization would face with such a model?

A. This model typically requires users to have admin credentials, which violates the principle of least privilege.

B. It will be easier to ensure that all software products are updated, since they will be configured to do so automatically.

C. It may be difficult (or impossible) to attest to the status of every application in the organization.

D. Having each application or service independently download the patches will lead to network congestion.

139. Clustering is an unsupervised machine learning approach that determines where data samples naturally clump together. It does this by calculating the distance between a new data point and the existing clusters and assigning the point to the closest cluster if, indeed, it is close to any of them. What is this approach typically used for in cybersecurity?

A. Spam filtering

B. Anomaly detection

C. Network flow analysis

D. Signature matching

140. Sam wants to test the ability of her technical security controls to stop realistic attacks. Her organization is going through significant growth, which is also increasing the complexity of the networks and systems. To ensure she stays ahead of the adversaries, Sam wants to run these tests frequently. Which approach should she use?

A. Breach and attack simulations

B. Tabletop exercises

C. Red teaming

D. Synthetic transactions

Use the following scenario to answer Questions 141–142. Ron is in charge of updating his company's business continuity and disaster recovery plans and processes. After conducting a business impact analysis, his team has told him that if the company's e-commerce payment gateway was unable to process payments for 24 hours or more, this could drastically affect the survivability of the company. The analysis indicates that after an outage, the payment gateway and payment processing should be restored within 13 hours. Ron's team needs to integrate solutions that provide redundancy, fault tolerance, and failover capability.

141. In the scenario, what does the 24-hour time period represent and what does the 13-hour time period represent, respectively?

A. Maximum tolerable downtime, recovery time objective

B. Recovery time objective, maximum tolerable downtime

C. Maximum tolerable downtime, recovery data period

D. Recovery time objective, data recovery period

142. Which of the following best describes the type of solution Ron's team needs to implement?

A. RAID and clustering

B. Storage area networks

C. High availability

D. Grid computing and clustering

Answers

1. D. While they are all issues to be concerned with, risk is a combination of probability and business impact. The largest business impact out of this list and in this situation is the fact that intellectual property for product development has been lost. If a competitor can produce the product and bring it to market quickly, this can have a long-lasting financial impact on the company.

2. D. The attackers are the entities that have exploited a vulnerability; thus, they are the threat agent.

3. C. In this situation the e-mail server most likely is misconfigured or has a programming flaw that can be exploited. Either of these would be considered a vulnerability. The threat is that someone would find out about this vulnerability and exploit it. The exposure is allowing sensitive data to be accessed in an unauthorized manner.

4. C. Diameter is a protocol that has been developed to build upon the functionality of RADIUS and TACACS+ while overcoming some of their limitations, particularly with regard to mobile clients. RADIUS uses UDP and cannot effectively deal well with remote access, IP mobility, and policy control. Mobile IP is not an authentication and authorization protocol, but rather a technology that allows users to move from one network to another and still use the same IP address.

5. **C.** DNS Security Extensions (DNSSEC, which is part of the many current implementations of DNS server software) works within a PKI and uses digital signatures, which allows DNS servers to validate the origin of a message to ensure that it is not spoofed and potentially malicious. Suppose DNSSEC were enabled on server A, and a client sends it a DNS request for a resource that is not cached locally. Server A would relay the request to one or more external DNS servers and, upon receiving a response, validate the digital signature on the message before accepting the information to make sure that it is from an authorized DNS server. So even if an attacker sent a message to a DNS server, the DNS server would discard it because the message would not contain a valid digital signature. DNSSEC allows DNS servers to send and receive only authenticated and authorized messages between themselves and thwarts the attacker's goal of poisoning a DNS cache table.
6. **C.** The General Data Protection Regulation (GDPR) impacts every organization that holds or uses European personal data both inside and outside of Europe. In other words, if your company is a U.S.-based company that has never done business with the EU but it has an EU citizen working even as temporary staff (e.g., a summer intern), it probably has to comply with the GDPR or risk facing stiff penalties. There is no exclusion based on the nature of the relations between the data subjects and the data controllers and processors.
7. **B.** A vulnerability is a lack or weakness of a control. The vulnerability is that the user, who must be given access to the sensitive data, is not properly monitored to deter and detect a willful breach of security. The threat is that any internal entity might misuse given access. The risk is the business impact of losing sensitive data. One control that could be put into place is monitoring so that access activities can be closely watched.
8. **C.** A role-based access control (RBAC) model uses a centrally administrated set of controls to determine how subjects and objects interact. An administrator does not need to revoke and reassign permissions to individual users as they change jobs. Instead, the administrator assigns permissions and rights to a role, and users are plugged into those roles.
9. **A.** Many (but not all) countries have data breach notification requirements, and these vary greatly in their specifics. While some countries have very strict requirements, others have laxer requirement, or lack them altogether. This requires the security professional to ensure compliance in the appropriate territory. Applying the most stringent rules universally (e.g., 24-hour notification) is usually not a good idea from a business perspective. The term "best effort" is not acceptable in countries with strict rules, nor is the notion that personally identifiable information (PII) is the only type of data that would trigger a mandatory notification.
10. **D.** Regression testing should take place after a change to a system takes place, retesting to ensure functionality, performance, and protection.

11. **B.** ISO/IEC 27001 is a standard covering information security management systems (ISMSs), which is a much broader topic than supply chain risk management. The other three options are better answers because they are directly tied to this process: NIST Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, directly addresses supply chain risk, and the insertion of hardware Trojans could happen at any point in the chain, upstream or downstream.
12. **B.** Various countries have data sovereignty laws that stipulate that anyone who stores or processes certain types of data (typically personal data on their citizens), whether or not they do so locally, must comply with those countries' laws. Data localization laws, on the other hand, require certain types of data to be stored and processed in that country (examples include laws in China and Russia).
13. **B.** Security through obscurity depends upon complexity or secrecy as a protection method. Some organizations feel that since their proprietary code is not standards based, outsiders will not know how to compromise its components. This is an insecure approach. Defense-in-depth is a better approach, with the assumption that anyone can figure out how something works.
14. **C.** ISO/IEC 27005 is the international standard for risk assessments and analysis.
15. **C.** ISO/IEC 27799 is a guideline for information security management in health organizations. It deals with how organizations that store and process sensitive medical information should protect it.
16. **D.** End-of-life (EOL) for an asset is that point in time when its manufacturer is neither manufacturing nor sustaining it. In other words, you can't send it in for repairs, buy spare parts, or get technical assistance from the manufacturer. The related term, end-of-support (EOS), which is sometimes also called end-of-service-life (EOSL), means that the manufacturer is no longer patching bugs or vulnerabilities on the product.
17. **B.** A virtual private network (VPN) provides confidentiality for data being exchanged between two endpoints. While the use of VPNs may not be sufficient in every case, it is the only answer among those provided that addresses the question. The use of Secure Sockets Layer (SSL) is not considered secure. IEEE 802.1X is an authentication protocol that does not protect data in transit. Finally, whole-disk encryption may be a good approach to protecting sensitive data, but only while it is at rest.
18. **B.** Threat modeling is the process of describing probable adverse effects on an organization's assets caused by specific threat sources. This modeling can use a variety of approaches, including attack trees and the MITRE ATT&CK framework. However, since the question refers to a report and neither of those approaches specifically points to a report, the more general answer of threat modeling is the best one.
19. **B.** A CAPTCHA is a skewed representation of characteristics a person must enter to prove that the subject is a human and not an automated tool, as in a software robot. It is the graphical representation of data.

20. **B.** The CPO position was created mainly because of the increasing demands on organizations to protect a long laundry list of different types of data. This role is responsible for ensuring that customer, organizational, and employee data is secure and kept secret, which keeps the organization out of criminal and civil courts and hopefully out of the headlines.

21. **D.** The correct sequence for the steps listed in the question is as follows:

    i. Develop a risk management team.

    ii. Identify company assets to be assessed.

    iii. Calculate the value of each asset.

    iv. Identify the vulnerabilities and threats that can affect the identified assets.

22. **B.** Synthetic transactions are scripted events that mimic the behaviors of real users and allow security professionals to systematically test the performance of critical services. They are the best approach, because they can detect problems before users notice them. Real user monitoring (RUM) would rely on users encountering the problem, whereupon the system would automatically report it.

23. **A.** Data remanence refers to the persistence of data on storage media after it has been deleted. Encrypting this data is the best of the listed choices because the recoverable data will be meaningless to an adversary without the decryption key. Retention policies are important, but are considered administrative controls that don't deal with remanence directly. Simply deleting the file will not normally render the data unrecoverable, nor will the use of SSDs even though these devices will sometimes (though not always) make it difficult to recover the deleted data.

24. **C.** While all of these situations could have taken place, the most likely attack type in this scenario is the use of a keylogger. Attackers commonly compromise personal computers by tricking the users into installing Trojan horses that have the capability to install keystroke loggers. The keystroke logger can capture authentication data that the attacker can use to authenticate as a legitimate user and carry out malicious activities.

25. **B.** IPSec is a suite of protocols used to provide VPNs that use strong encryption and authentication functionality. It can work in two different modes: tunnel mode (payload and headers are protected) or transport mode (payload protection only). IPSec works at the network layer, not the data link layer.

26. **C.** In a typical public key infrastructure, the sender first needs to obtain the receiver's public key, which could be from the receiver or a public directory, and then verify it. The sender needs to protect the symmetric session key as it is being sent, so the sender encrypts it with the receiver's public key. The receiver decrypts the session key with the receiver's private key.

27. **C.** Today, more organizations are implementing security information and event management (SIEM) systems. These products gather logs from various devices (servers, firewalls, routers, etc.) and attempt to correlate the log data and provide analysis capabilities. Organizations also have different types of systems on a network (routers, firewalls, IDS, IPS, servers, gateways, proxies) collecting logs in various proprietary formats, which requires centralization, standardization, and normalization. Log formats are different per product type and vendor.

28. **D.** Configuration management is a process aimed at ensuring that systems and controls are configured correctly and are responsive to the current threat and operational environments. Since the IPv6-to-IPv4 tunneling is not desirable, ensuring all devices are properly configured is the best approach of those listed. Change management is a broader term that includes configuration management but is not the best answer listed because it is more general.

29. **D.** IoT devices run the gamut of cost, from the very cheap to the very expensive. Cost, among the listed options, is the least likely to be a direct concern for a security professional. Lack of authentication, encryption, and update mechanisms are much more likely to be significant issues in any IoT adoption plan.

30. **C.** Each microservice lives in its own container and gets called as needed. If, for example, you see a spike in orders, you can automatically deploy a new container (in seconds), perhaps in a different host, and destroy it when you no longer need it. This contrasts with traditional servers that have fixed resources available and don't scale as well. Both approaches deal equally well with both web and database services and (properly deployed) have comparable security.

31. **B.** Extensible Access Control Markup Language (XACML), a declarative access control policy language implemented in XML and a processing model, describes how to interpret security policies. Service Provisioning Markup Language (SPML) is an XML-based language that allows for the exchange of provisioning data between applications, which could reside in one organization or many; allows for the automation of user management (account creation, amendments, revocation) and access entitlement configuration related to electronically published services across multiple provisioning systems; and allows for the integration and interoperation of service provisioning requests across various platforms. Security Assertion Markup Language (SAML) is an XML-based language that allows for the exchange of provisioning data between applications, which could reside in one organization or many.

32. **C.** A company must decide how to handle physical access control in the event of a power failure. In fail-safe mode, doorways are automatically unlocked. This is usually dictated by fire codes to ensure that people do not get stuck inside of a burning building. Fail-secure means that the door will default to lock.

33. **C.** Incident response typically requires humans in the loop. Next-generation firewalls (NGFWs) do not completely automate the process of responding to security incidents. NGFWs typically involve integrated IPS and signature sharing capabilities with cloud-based aggregators, but are also significantly more expensive than other firewall types.

34. **D.** Trolling is the term used to describe people who sow discord on various social platforms on the Internet by starting arguments or making inflammatory statements aimed at upsetting others. This is not a topic normally covered in security awareness training. Social engineering, phishing, and whaling are important topics to include in any security awareness program.

35. **D.** When clients digitally sign messages, this ensures nonrepudiation. Since the client should be the only person who has the client's private key, and only the client's public key can decrypt it, the e-mail must have been sent from the client. Digital signatures provide nonrepudiation protection, which is what this company needs.

36. **D.** Simple Authentication and Security Layer (SASL) is a protocol-independent authentication framework for authentication and data security in Internet protocols. It decouples authentication mechanisms from application protocols, with the goal of allowing any authentication mechanism supported by SASL to be used in any application protocol that uses SASL. SASL's design is intended to allow new protocols to reuse existing mechanisms without requiring redesign of the mechanisms, and allows existing protocols to make use of new mechanisms without redesign of protocols.

37. **D.** Coupling is not considered a secure coding practice, though it does affect the quality (and hence the security) of software. It is a measurement that indicates how much interaction one module requires to carry out its tasks. High (tight) coupling means a module depends upon many other modules to carry out its tasks. Low (loose) coupling means a module does not need to communicate with many other modules to carry out its job, which is better because the module is easier to understand and easier to reuse, and changes can take place to one module and not affect many modules around it.

38. **A.** A recovery time objective (RTO) is the amount of time it takes to recover from a disaster, and a recovery point objective (RPO) is the amount of data, measured in time, that can be lost and be tolerable from that same event. The RPO is the acceptable amount of data loss measured in time. This value represents the earliest point in time by which data must be recovered. The higher the value of data, the more funds or other resources that can be put into place to ensure a smaller amount of data is lost in the event of a disaster. RTO is the maximum time period within which a business process must be restored to a designated service level after a disaster to avoid unacceptable consequences associated with a break in business continuity.

39. **B.** Though laws vary around the world, many countries criminalize unauthorized access, even if it lacked malicious intent.

40. A. XACML uses a Subject element (requesting entity), a Resource element (requested entity), and an Action element (types of access). XACML defines a declarative access control policy language implemented in XML.

41. B. The Mobile IP protocol allows location-independent routing of IP packets on web-based environments. Each mobile device is identified by its home address. While away from its home network, a mobile node is associated with a care-of address, which identifies its current location, and its home address is associated with the local endpoint of a tunnel to its home agent. Mobile IP specifies how a mobile device registers with its home agent and how the home agent routes packets to the mobile device.

42. D. A SIEM solution is a software platform that aggregates security information and security events and presents them in a single, consistent, and cohesive manner.

43. D. The sensitivity of information is commensurate with the losses to an organization if that information were revealed to unauthorized individuals. Its criticality, on the other hand, is an indicator of how the loss of the information would impact the fundamental business processes of the organization. While replacement costs could factor into a determination of criticality, they almost never do when it comes to sensitivity.

44. C. Global organizations that move data across other country boundaries must be aware of and follow the Organisation for Economic Co-operation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Since most countries have a different set of laws pertaining to the definition of private data and how it should be protected, international trade and business get more convoluted and can negatively affect the economy of nations. The OECD is an international organization that helps different governments come together and tackle the economic, social, and governance challenges of a globalized economy. Because of this, the OECD came up with guidelines for the various countries to follow so that data is properly protected and everyone follows the same type of rules.

45. B. Registered ports are 1024–49151, which can be registered with the Internet Assigned Numbers Authority (IANA) for a particular use. Vendors register specific ports to map to their proprietary software. Dynamic ports are 49152–65535 and are available to be used by any application on an "as needed" basis. Port numbers from 0 to 1023 are well-known ports.

46. A. The correct answer for cost/benefit analysis is the formula: (ALE before implementing safeguard) – (ALE after implementing safeguard) – (annual cost of safeguard) = value of safeguard to the organization.

47. B. Each of the listed items are correct benefits or characteristics of cloud computing except "Cost of computing can be increased since it is a shared delivery model." The correct answer would be "Cost of computing can be *decreased* since it is a shared delivery model."

48. **A.** An architecture is a tool used to conceptually understand the structure and behavior of a complex entity through different views. An architecture provides different views of the system, based upon the needs of the stakeholders of that system.

49. **B.** Threat modeling is a systematic approach used to understand how different threats could be realized and how a successful compromise could take place. A threat model is a description of a set of security aspects that can help define a threat and a set of possible attacks to consider. It may be useful to define different threat models for one software product. Each model defines a narrow set of possible attacks to focus on. A threat model can help to assess the probability, the potential harm, and the priority of attacks, and thus help to minimize or eradicate the threats.

50. **B.** Many IDSs have "heuristic" capabilities, which means that the system gathers different "clues" from the network or system and calculates the probability an attack is taking place. If the probability hits a set threshold, then the alarm sounds.

51. **C.** External auditors have certain advantages over in-house teams, but they will almost certainly not be as knowledgeable of internal processes and technology as the folks who deal with them on a daily basis.

52. **C.** In this example, staffers with lower security clearance than Don has could have deduced that the contract had been renewed by paying attention to the changes in their systems. The noninterference model addresses this specifically by dictating that no action or state in higher levels can impact or be visible to lower levels. In this example, the staff could learn something indirectly or infer something that they do not have a right to know yet.

53. **B.** HTML documents and e-mails allow users to attach or embed hyperlinks in any given text, such as the "Click Here" links you commonly see in e-mail messages or web pages. Attackers misuse hyperlinks to deceive unsuspecting users into clicking rogue links. The most common approach is known as URL hiding.

54. **C.** Personnel background checks are a common administrative (not technical) control. This type of audit would have nothing to do with the web applications themselves. The other three options (log reviews, code reviews, misuse case testing) are typical ways to verify the effectiveness of technical controls.

55. **D.** Statistical time-division multiplexing (STDM) transmits several types of data simultaneously across a single transmission line. STDM technologies analyze statistics related to the typical workload of each input device and make real-time decisions on how much time each device should be allocated for data transmission.

56. **D.** The actual voice stream is carried on media protocols such as RTP. RTP provides a standardized packet format for delivering audio and video over IP networks. RTP is a session layer protocol that carries data in media stream format, as in audio

and video, and is used extensively in VoIP, telephony, video conferencing, and other multimedia streaming technologies. It provides end-to-end delivery services and is commonly run over the transport layer protocol UDP. RTCP is used in conjunction with RTP and is also considered a session layer protocol. It provides out-of-band statistics and control information to provide feedback on QoS levels of individual streaming multimedia sessions.

57. **A.** Edge computing is a distributed system in which some computational and data storage assets are deployed close to where they are needed in order to reduce latency and network traffic. An edge computing architecture typically has three layers: end devices, edge devices, and cloud infrastructure.

58. **C.** A frequency analysis, also known as a statistical attack, identifies statistically significant patterns in the ciphertext generated by a cryptosystem. For example, the number of zeroes may be significantly higher than the number of ones. This could show that the pseudorandom number generator (PRNG) in use may be biased.

59. **D.** IPSec is made up of two main protocols, Authentication Header (AH) and Encapsulating Security Payload (ESP). AH provides system authentication and integrity, but not confidentiality or availability. ESP provides system authentication, integrity, and confidentiality, but not availability. Nothing within IPSec can ensure the availability of the system it is residing on.

60. **D.** The ACID test concept should be incorporated into the software of a database. ACID stands for:

    - **Atomicity** Either the entire transaction succeeds or the database rolls it back to its previous state.
    - **Consistency** A transaction strictly follows all applicable rules on all data affected.
    - **Isolation** If transactions are allowed to happen in parallel (which most of them are), then they will be isolated from each other so that the effects of one don't corrupt another. In other words, isolated transactions have the same effect whether they happen in parallel or one after the other.
    - **Durability** Ensures that a completed transaction is permanently stored (for instance, in nonvolatile memory) so that it cannot be wiped by a power outage or other such failure.

61. **B.** In a Platform as a Service (PaaS) contract, the service provider normally takes care of all configuration, patches, and updates for the virtual platform. Jim would only have to worry about porting the applications and running them.

62. **B.** The biggest advantages of cloud computing are enhanced efficiency, performance, reliability, scalability, and security. Still, cloud computing is not a panacea. An organization must still carefully consider legal, contractual, and cost issues since they could potentially place the organization in a difficult position.

63. C. Shared responsibility addresses situations in which a cloud service provider is responsible for certain security controls, while the customer is responsible for others. It will be critical for Jim to delineate where these responsibilities lie. The other principles listed would presumably be equally important before and after the transition.

64. A. The aim of an attack surface analysis is to identify and reduce the amount of code accessible to untrusted users. The basic strategies of attack surface reduction are to reduce the amount of code running, reduce entry points available to untrusted users, reduce privilege levels as much as possible, and eliminate unnecessary services. Attack surface analysis is generally carried out through specialized tools to enumerate different parts of a product and aggregate their findings into a numerical value. Attack surface analyzers scrutinize files, registry keys, memory data, session information, processes, and services details.

65. B. The Capability Maturity Model Integration (CMMI) model outlines the necessary characteristics of an organization's security engineering process. It addresses the different phases of a secure software development life cycle, including concept definition, requirements analysis, design, development, integration, installation, operations, and maintenance, and what should happen in each phase. It can be used to evaluate security engineering practices and identify ways to improve them. It can also be used by customers in the evaluation process of a software vendor. Ideally, software vendors would use the model to help improve their processes, and customers would use the model to assess the vendor's practices.

66. D. VxLANs are designed to overcome two limitations of traditional VLANs: the limit of no more than 4,096 VLANs imposed by the 12-bit VLAN ID (VID) field, and the need for VLANs to be connected to the same router port. Accordingly, VxLANs are mostly used by cloud service providers with hundreds of customers and by large organizations with a global presence.

67. D. These are all issues that are directly related to Kerberos. These items are as follows:

- The Key Distribution Center (KDC) can be a single point of failure. If the KDC goes down, no one can access needed resources. Redundancy is necessary for the KDC.
- The KDC must be scalable to handle the number of requests it receives in a timely manner.
- Secret keys are temporarily stored on the users' workstations, which means it is possible for an intruder to obtain these cryptographic keys.
- Session keys are decrypted and reside on the users' workstations, either in a cache or in a key table. Again, an intruder can capture these keys.
- Kerberos is vulnerable to password guessing. The KDC does not know if a dictionary attack is taking place.

68. **A.** Yes, the company should implement the control, as the value would be $25,000. The cost/benefit calculation is (ALE before implementing safeguard) – (ALE after implementing safeguard) – (annual cost of safeguard) = value of safeguard to the organization, which in this case is $100,000 – $45,000 – $30,000 = $25,000.

69. **D.** The correct mappings for the individual standards are as follows:
    - ISO/IEC 27002: Code of practice for information security controls
    - ISO/IEC 27003: ISMS implementation guidance
    - ISO/IEC 27004: ISMS monitoring, measurement, analysis, and evaluation
    - ISO/IEC 27005: Information security risk management
    - ISO/IEC 27007: ISMS auditing guidelines

70. **B.** Just-in-time (JIT) access temporarily elevates users to the necessary privileged access to perform a specific task, on a specific asset, for a short time. This approach mitigates the risk of privileged account abuse by reducing the time a threat actor has to gain access to a privileged account. While this could reduce some of the workload on the IT staff, it would have no impact on the time needed to reset a multitude of passwords.

71. **C.** End-to-end encryption happens within the applications. IPSec encryption takes place at the network layer. PPTP encryption takes place at the data link layer. Link encryption takes place at the data link and physical layers.

72. **A.** Hierarchical storage management (HSM) provides continuous online backup functionality. It combines hard disk technology with the cheaper and slower optical or tape jukeboxes. Storage area network (SAN) is made up of several storage systems that are connected together to form a single backup network.

73. **C.** The common law system is the only one that is based on previous interpretations of the law. This means that the system consists of both laws and court decisions in specific cases. Torts can be (and usually are) part of a common law system, but that would be an incomplete answer to this question.

74. **B.** It is important that evidence be relevant, complete, sufficient, and reliable to the case at hand. These four characteristics of evidence provide a foundation for a case and help ensure that the evidence is legally permissible.

75. **B.** Risk-based access control estimates the risk associated with a particular request in real time and, if it doesn't exceed a given threshold, grants the subject access to the requested resource. This estimate can be based on multiple factors, including the risk history of similar requests. It is possible to improve a rule-based access control mechanism over time (based on historical data), but that would have to be a manual process and wouldn't happen in real time.

76. **C.** SOAP enables programs running on different operating systems and written in different programming languages to communicate over web-based communication methods. SOAP is an XML-based protocol that encodes messages in a web service environment. SOAP actually defines an XML schema or a structure of how

communication is going to take place. The SOAP XML schema defines how objects communicate directly.

77. A. Each answer lists the correct definition mapping.

78. C. For an enterprise security architecture to be successful in its development and implementation, the following items must be understood and followed: strategic alignment, process enhancement, business enablement, and security effectiveness.

79. A. The OECD is an international organization where member countries come together to address economic, social, and governance challenges of a globalized economy. Thus, the OECD came up with guidelines for the various countries to follow so data is properly protected and everyone follows the same type of rules.

80. A. The Zachman Framework is for business enterprise architectures, not security enterprises. The proper definition mappings are as follows:

- **Zachman Framework** Model for the development of enterprise architectures developed by John Zachman
- **TOGAF** Model and methodology for the development of enterprise architectures developed by The Open Group
- **DoDAF** U.S. Department of Defense architecture framework that ensures interoperability of systems to meet military mission goals
- **SABSA** Model and methodology for the development of information security enterprise architectures

81. B. The ISO/IEC 27000 series provides a high-level overview of security program requirements, while COBIT maps IT goals to enterprise goals to stakeholder needs through a series of transforms called cascading goals. COBIT specifies 13 enterprise and 13 alignment goals that take the guesswork out of ensuring we consider all dimensions in our decision-making processes.

82. D. This model was not built upon the SABSA model. All other characteristics are true.

83. D. The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) relies on the idea that the people working in a given environment best understand what is needed and what kind of risks they are facing. This places the people who work inside the organization in the power positions of being able to make the decisions regarding what is the best approach for evaluating the security of their organization.

84. B. An enterprise architecture framework is a conceptual model in which an architecture description is organized into multiple architecture views, where each view addresses specific concerns originating with the specific stakeholders. Individual stakeholders have a variety of system concerns, which the architecture must address. To express these concerns, each view applies the conventions of its architecture viewpoint.

85. C. Fault tree analysis follows this general process. First, an undesired effect is taken as the root, or top, event of a tree of logic. Then, each situation that has the potential to cause that effect is added to the tree as a series of logic expressions. Fault trees are then labeled with actual numbers pertaining to failure probabilities.

86. D. Security effectiveness deals with metrics, meeting service level agreement (SLA) requirements, achieving return on investment (ROI), meeting set baselines, and providing management with a dashboard or balanced scorecard system. These are ways to determine how useful the current security solutions and architecture as a whole are performing.

87. D. Each answer provides the correct definition of the four levels that can be assigned to an organization during its evaluation against the CMMI model. This model can be used to determine how well the organization's processes compare to CMMI best practices and to identify areas where improvement can be made. Maturity Level 1 is Initial.

88. B. The ISRM policy should address all of the items listed except specific physical controls. Policies should not specify any type of controls, whether they are administrative, physical, or technical.

89. C. Each of these items should be considered before committing to an outsource partner or vendor.

90. D. The steps normally involved in the discovery of electronically stored information, or e-discovery, are identifying, preserving, collecting, processing, reviewing, analyzing, and producing the data in compliance with the court order. Data remanence is not part of e-discovery, though it could influence the process.

91. C. ISO/IEC 27004:2016, which is used to assess the effectiveness of an ISMS and the controls that make up the security program as outlined in ISO/IEC 27001. ISO/IEC 27004 provides guidance for ISMS monitoring, measurement, analysis, and evaluation.

92. B. Content distribution networks (CDNs) work by replicating content across geographically dispersed nodes. This means that regional users (those closest to a given node) will see improved responsiveness and could have tailored content delivered to them. It also means that mounting a successful DDoS attack is much more difficult. An ARP spoofing attack, however, takes place on the local area network and is therefore unrelated to the advantages of CDNs.

93. A. A CASB is a system that provides visibility and security controls for cloud services. A CASB monitors what users do in the cloud and applies whatever policies and controls are applicable to that activity.

94. C. A federated identity is a portable identity, and its associated entitlements, that can be used across business boundaries. It allows a user to be authenticated across multiple IT systems and enterprises. Single sign-on (SSO) allows users to enter credentials one time and be able to access all resources in primary and secondary network domains, but is not the best answer because it doesn't specifically address the capability to provide authentication across enterprises. A federated identity is a kind of SSO, but not every SSO implementation is federated.

95. **B.** HTML came from SGML, which came from GML. A markup language is a way to structure text and data sets, and it dictates how these will be viewed and used. When developing a web page, a markup language enables you to control how the text looks and some of the actual functionality the page provides.

96. **A.** XML is a universal and foundational standard that provides a structure for other independent markup languages to be built from and still allow for interoperability. Markup languages with various functionalities were built from XML, and while each language provides its own individual functionality, if they all follow the core rules of XML, then they are interoperable and can be used across different web-based applications and platforms.

97. **B.** A role-based access control (RBAC) model is based on the necessary operations and tasks a user needs to carry out to fulfill her responsibilities within an organization. This type of model lets access to resources be based on the user's roles. In hierarchical RBAC, role hierarchies define an inheritance relation among roles.

98. **C.** Diameter is a more diverse centralized access control administration technique than RADIUS and TACACS+ because it supports a wide range of protocols that often accompany wireless technologies. RADIUS supports PPP, SLIP, and traditional network connections. TACACS+ is a RADIUS-like protocol that is Cisco-proprietary. Kerberos is a single sign-on technology, not a centralized access control administration protocol that supports all stated technologies.

99. **A.** An authoritative system of record (ASOR) is a hierarchical tree-like structure system that tracks subjects and their authorization chains. The authoritative source is the "system of record," or the location where identity information originates and is maintained. It should have the most up-to-date and reliable identity information.

100. **A.** User provisioning refers to the creation, maintenance, and deactivation of user objects and attributes as they exist in one or more systems, directories, or applications, in response to business processes.

101. **D.** OpenID Connect (OIDC) is a simple authentication layer built on top of the OAuth 2.0 protocol. It allows transparent authentication and authorization of client resource requests. Though it is possible to use OAuth, which is an authorization standard, for authentication, you would do so by leveraging its OpenID Connect layer. Diameter and Kerberos are not well-suited for IDaaS.

102. **A.** The Service Provisioning Markup Language (SPML) allows for the exchange of provisioning data between applications, which could reside in one organization or many. SPML allows for the automation of user management (account creation, amendments, revocation) and access entitlement configuration related to electronically published services across multiple provisioning systems. SPML also allows for the integration and interoperation of service provisioning requests across various platforms.

103. B. In this scenario, Lynn is considered the principal, the airline company is considered the identity provider, and the hotel company that receives the user's authentication information from the airline company web server is considered the service provider. Security Assertion Markup Language (SAML) provides the authentication pieces to federated identity management systems to allow business-to-business (B2B) and business-to-consumer (B2C) transactions.

104. A. A service-oriented architecture (SOA) is way to provide independent services residing on different systems in different business domains in one consistent manner. This architecture is a set of principles and methodologies for designing and developing software in the form of interoperable services.

105. B. The Bell-LaPadula model enforces the confidentiality aspects of access control and consists of three main rules. The simple security rule states that a subject at a given security level cannot read data that resides at a higher security level. The *-property rule (star property rule) states that a subject in a given security level cannot write information to a lower security level. Finally, the strong star property rule states that a subject who has read and write capabilities can only perform both of those functions at the same security level; nothing higher and nothing lower.

106. D. In the system design phase, the software development team gathers system requirement specifications and determines how the system will accomplish design goals, such as required functionality, compatibility, fault tolerance, extensibility, security, usability, and maintainability. The attack surface analysis, together with the threat model, inform the developers' decisions because they can look at proposed architectures and competing designs from the perspective of an attacker. This allows them to develop a more defensible system. Though it is possible to start the threat model during the earlier phase of requirements gathering, this modeling effort is normally not done that early. Furthermore, the attack surface cannot be properly studied until there is a proposed architecture to analyze. Performing this activity later in the SDLC is less effective and usually results in security being "bolted on" instead of "baked in."

107. B. OAuth is an open standard for authorization to third parties. It lets you authorize a web application to use something that you control at a different website. For instance, if users wanted to share an article in the web app directly to their LinkedIn account, the system would ask them for access to their accounts in LinkedIn. If they agree, they'd see a pop-up from LinkedIn asking whether they want to authorize the web app to share a post. If they agree to this, the web app gains access to all their contacts until they rescind this authorization.

108. A. Each CPU type has a specific architecture and set of instructions that it can carry out. The application must be developed to work within this CPU architecture and compiled into machine code that can run on it. This is why one application may work on an Intel processor but not on an AMD processor. There are portable applications that can work on multiple architectures and operating systems, but these rely on a runtime environment.

109. C. According to Veracode, seven in ten applications use at least one open-source software library with a security flaw, which makes those applications vulnerable. This estimate doesn't include proprietary libraries, which are probably even more insecure because they haven't been subjected to the same amount of scrutiny as open-source ones. This is the main risk in using software libraries.

110. A. Dynamic application security testing (DAST), which is also known as dynamic analysis, refers to the evaluation of a program in real time, while it is running. It is the only one of the answers that is effective for analyzing software without having access to the actual source code.

111. C. Attackers have identified programming errors in operating systems that allow them to "starve" the system of its own memory. This means the attackers exploit a software vulnerability that ensures that processes do not properly release their memory resources. Memory is continually committed and not released, and the system is depleted of this resource until it can no longer function. This is an example of a denial-of-service attack.

112. A. Attribute-based access control (ABAC) is based on attributes of any component of the system. It is the most granular of the access control models.

113. A. The primary reason to use Kerberos is that the principals do not trust each other enough to communicate directly; they only trust the Key Distribution Center (KDC). This is a strength, not a weakness, of the system, but it does point to the fact that if only the KDC can vouch for identities, this creates a single point of failure. The fact that secret keys are stored on users' workstations, albeit temporarily, presents an attack opportunity for threat actors, who can also perform password attacks on the system.

114. A. The depth of field refers to the portion of the environment that is in focus when shown on the monitor. The depth of field varies, depending upon the size of the lens opening, the distance of the object being focused on, and the focal length of the lens. The depth of field increases as the size of the lens opening decreases, the subject distance increases, or the focal length of the lens decreases. So if you want to cover a large area and not focus on specific items, it is best to use a wide-angle lens and a small lens opening.

115. B. In a preaction system, a link must melt before the water will pass through the sprinkler heads, which creates the delay in water release. This type of suppression system is best in data-processing environments because it allows time to deactivate the system if there is a false alarm.

116. B. A preaction system has a link that must melt before water is released. This is the mechanism that provides the delay in water release. A deluge system has wide open sprinkler heads that allow a lot of water to be released quickly. It does not have a delaying component.

117. D. CPTED encourages natural surveillance, the goal of which is to make criminals feel uncomfortable by providing many ways observers could potentially see them and to make all other people feel safe and comfortable by providing an open and well-designed environment. The other answers refer to the other three CPTED strategies, which are natural access control, territorial reinforcement, and maintenance, respectively.

118. D. The Zachman Framework is a two-dimensional model that uses six basic communication interrogatives (What, How, Where, Who, When, and Why) intersecting with different viewpoints (Executives, Business Managers, System Architects, Engineers, Technicians, and Enterprise-wide) to give a holistic understanding of the enterprise. This framework was developed in the 1980s and is based on the principles of classical business architecture that contain rules that govern an ordered set of relationships.

119. B. The communication between two pieces of the same software product that reside on different computers needs to be controlled, which is why session layer protocols even exist. Session layer protocols take on the functionality of middleware, enabling software on two different computers to communicate.

120. A. The data link layer has two sublayers: the Logical Link Control (LLC) and Media Access Control (MAC) layers. The LLC sublayer provides a standard interface for whatever network protocol is being used. This provides an abstraction layer so that the network protocol does not need to be programmed to communicate with all of the possible MAC-level protocols (Ethernet, WLAN, frame relay, etc.).

121. C. A Class B address range is usually too large for most companies, and a Class C address range is too small, so CIDR provides the flexibility to increase or decrease the class sizes as necessary. CIDR is the method to specify more flexible IP address classes.

122. A. 802.1AE is the IEEE MAC Security (MACSec) standard, which defines a security infrastructure to provide data confidentiality, data integrity, and data origin authentication. Where a VPN connection provides protection at the higher networking layers, MACSec provides hop-by-hop protection at layer 2.

123. D. 802.1AR provides a unique ID for a device. 802.1AE provides data encryption, integrity, and origin authentication functionality. 802.1AF carries out key agreement functions for the session keys used for data encryption. Each of these standards provides specific parameters to work within an 802.1X EAP-TLS framework.

124. A. As information systems security professionals, if we discover a vulnerability, we have an ethical obligation to properly disclose it to the appropriate parties. If the vulnerability is in our own product, we need to notify our customers and partners as soon as possible. If it is in someone else's product, we need to notify the vendor or manufacturer immediately so they can fix it. The goal of ethical disclosure is to inform anyone who might be affected as soon as feasible, so a patch can be developed before any threat actors become aware of the vulnerability.

125. C. The HOSTS file resides on the local computer and can contain static hostname-to-IP mapping information. If you do not want your system to query a DNS server, you can add the necessary data in the HOSTS file, and your system will first check its contents before reaching out to a DNS server. Some people use these files to reduce the risk of an attacker sending their system a bogus IP address that points them to a malicious website.

126. B. VLAN hopping attacks allow attackers to gain access to traffic in various VLAN segments. An attacker can have a system act as though it is a switch. The system understands the tagging values being used in the network and the trunking protocols, and can insert itself between other VLAN devices and gain access to the traffic going back and forth. Attackers can also insert tagging values to manipulate the control of traffic at the data link layer.

127. B. The most common cloud service models are

- **Infrastructure as a Service (IaaS)** Cloud service providers offer the infrastructure environment of a traditional data center in an on-demand delivery method.
- **Platform as a Service (PaaS)** Cloud service providers deliver a computing platform, which can include an operating system, database, and web server as a holistic execution environment.
- **Software as a Service (SaaS)** Cloud service providers give users access to specific application software (e.g., CRM, e-mail, and games).

128. C. Software-defined networking (SDN) is an approach to networking that relies on distributed software to provide unprecedented agility and efficiency. Using SDN, it becomes much easier to dynamically route traffic to and from newly provisioned services and platforms. It also means that a service or platform can be quickly moved from one location to another and the SDN will just as quickly update traffic-flow rules in response to this change.

129. A. Parallel tests are similar to simulation tests, except that parallel tests include moving some of the systems to the offsite facility. Simulation tests stop just short of the move. Parallel tests are effective because they ensure that specific systems work at the new location, but the test itself does not interfere with business operations at the main facility.

130. B. While DRP and BCP are directed at the development of plans, business continuity management (BCM) is the holistic management process that should cover both of them. BCM provides a framework for integrating resilience with the capability for effective responses in a manner that protects the interests of the organization's key stakeholders. The main objective of BCM is to allow the organization to continue to perform business operations under various conditions. BCM is the overarching approach to managing all aspects of BCP and DRP.

131. B. An external audit (sometimes called a second-party audit) is one conducted by (or on behalf of) a business partner to verify contractual obligations. Though this audit could be conducted by a third party (e.g., an auditing firm hired by either party), it is still considered an external audit because it is being done to satisfy an external entity.

132. A. Duress is the use of threats or violence against someone in order to force them to do something they don't want to do. A popular example of a countermeasure for duress is the use of panic buttons by bank tellers. A panic room could conceivably be another solution, but it would only work if employees are able to get in and lock the door before an assailant can stop them, which makes it a generally poor approach.

133. A. The Wassenaar Arrangement implements export controls for "Conventional Arms and Dual-Use Goods and Technologies." The main goal of this arrangement is to prevent the buildup of military capabilities that could threaten regional and international security and stability. So, everyone is keeping an eye on each other to make sure no one country's weapons can take everyone else out. One item the agreement deals with is cryptography, which is considered a dual-use good because it can be used for both military and civilian purposes. The agreement recognizes the danger of exporting products with cryptographic functionality to countries that are in the "offensive" column, meaning that they are thought to have friendly ties with terrorist organizations and/or want to take over the world through the use of weapons of mass destruction.

134. A. The civil (code) law system is used in continental European countries such as France and Spain. It is a different legal system from the common law system used in the United Kingdom and United States. A civil law system is rule-based law, not precedent-based. For the most part, a civil law system is focused on codified law—or written laws.

135. C. FMEA is a method for determining functions, identifying functional failures, and assessing the causes of failure and their failure effects through a structured process. It is commonly used in product development and operational environments. The goal is to identify where something is most likely going to break and either fix the flaws that could cause this issue or implement controls to reduce the impact of the break.

136. B. Each of these items would be assigned a numeric value in a quantitative risk analysis. Each element is quantified and entered into equations to determine total and residual risks. Quantitative risk analysis is more of a scientific or mathematical approach to risk analysis compared to qualitative.

137. A. Aggregation and inference go hand in hand. For example, a user who uses data from a public database to figure out classified information is exercising aggregation (the collection of data) and can then infer the relationship between that data and the data the user does not have access to. This is called an inference attack.

138. B. This option is not a risk, but a (probably unrealistic) benefit, so it cannot be the right answer. The other three options are all risks associated with an unmanaged patching model.

139. B. Clustering algorithms are frequently used for anomaly detection. Classifiers are helpful when trying to determine whether a binary file is malware or detect whether an e-mail is spam. Predictive machine learning models can be applied wherever historical numerical data is available and work by estimating what the value of the next data point should be, which makes them very useful for network flow analysis (e.g., when someone is exfiltrating large amounts of data from the network).

140. A. Breach and attack simulations (BAS) are automated systems that launch simulated attacks against a target environment and then generate reports on their findings. They are meant to be run regularly (even frequently) and be realistic, but not to cause any adverse effect to the target systems. They are usually a much more affordable approach than red teaming, even if you use an internal team.

141. A. Maximum tolerable downtime (MTD) is the outage time that can be endured by an organization, and the recovery time objective (RTO) is an allowable amount of downtime. The RTO value (13 hours) is smaller than the MTD value (24 hours) because the MTD value represents the time after which an inability to recover significant operations will mean severe and perhaps irreparable damage to the organization's reputation or bottom line. The RTO assumes that there is a period of acceptable downtime. This means that a company can be out of production for a certain period of time (RTO) and still get back on its feet. But if the company cannot get production up and running within the MTD window, the company is sinking too fast to properly recover.

142. C. High availability (HA) is a combination of technologies and processes that work together to ensure that critical functions are always up and running at the necessary level. To provide this level of high availability, a company has to have a long list of technologies and processes that provide redundancy, fault tolerance, and failover capabilities.

Objective Map

		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 1: Security and Risk Management			
1.1	**Understand, adhere to, and promote professional ethics**	1	Professional Ethics
1.1.1	(ISC)^2 Code of Professional Ethics	1	(ISC)^2 Code of Professional Ethics
1.1.2	Organizational code of ethics	1	Organizational Code of Ethics
1.2	**Understand and apply security concepts (confidentiality, integrity, and availability, authenticity and nonrepudiation)**	1	Fundamental Cybersecurity Concepts and Terms
1.3	**Evaluate and apply security governance principles**	1	Security Governance Principles
1.3.1	Alignment of the security function to business strategy, goals, mission, and objectives	1	Aligning Security to Business Strategy
1.3.2	Organizational processes (e.g., acquisitions, divestitures, governance committees)	1	Organizational Processes
1.3.3	Organizational roles and responsibilities	1	Organizational Roles and Responsibilities
1.3.4	Security control frameworks	4	Security Control Frameworks
1.3.5	Due care/due diligence	3	Due Care vs. Due Diligence
1.4	**Determine compliance and other requirements**	3	Compliance Requirements
1.4.1	Contractual, legal, industry standards, and regulatory requirements	3	Contractual, Legal, Industry Standards, and Regulatory Requirements
1.4.2	Privacy requirements	3	Privacy Requirements
1.5	**Understand legal and regulatory issues that pertain to information security in a holistic context**	3	Laws and Regulations

		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 1: Security and Risk Management			
1.5.1	Cybercrimes and data breaches	3	Cybercrimes and Data Breaches
1.5.2	Licensing and Intellectual Property (IP) requirements	3	Licensing and Intellectual Property Requirements
1.5.3	Import/export controls	3	Import/Export Controls
1.5.4	Transborder data flow	3	Transborder Data Flow
1.5.5	Privacy	3	Privacy
1.6	**Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)**	3	Requirements for Investigations
1.7	**Develop, document, and implement security policy, standards, procedures, and guidelines**	1	Security Policies, Standards, Procedures, and Guidelines
1.8	**Identify, analyze, and prioritize Business Continuity (BC) requirements**	2	Business Continuity
1.8.1	Business Impact Analysis (BIA)	2	Business Impact Analysis
1.8.2	Develop and document the scope and the plan	2	Business Continuity
1.9	**Contribute to and enforce personnel security policies and procedures**	1	Personnel Security
1.9.1	Candidate screening and hiring	1	Candidate Screening and Hiring
1.9.2	Employment agreements and policies	1	Employment Agreements and Policies
1.9.3	Onboarding, transfers, and termination processes	1	Onboarding, Transfers and Termination Processes
1.9.4	Vendor, consultant, and contractor agreements and controls	1	Vendors, Consultants, and Contractors
1.9.5	Compliance policy requirements	1	Compliance Policies
1.9.6	Privacy policy requirements	1	Privacy Policies
1.10	**Understand and apply risk management concepts**	2	Risk Management Concepts
1.10.1	Identify threats and vulnerabilities	2	Identifying Threats and Vulnerabilities
1.10.2	Risk assessment/analysis	2	Assessing Risks
1.10.3	Risk response	2	Responding to Risks
1.10.4	Countermeasure selection and implementation	2	Countermeasure Selection and Implementation

		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 1: Security and Risk Management			
1.10.5	Applicable types of controls (e.g., preventive, detective, corrective)	2	Types of Controls
1.10.6	Control assessments (security and privacy)	2	Control Assessments
1.10.7	Monitoring and measurement	2	Monitoring Risks
1.10.8	Reporting	2	Risk Reporting
1.10.9	Continuous improvement (e.g., Risk maturity modeling)	2	Continuous Improvement
1.10.10	Risk frameworks	4	Risk Frameworks
1.11	**Understand and apply threat modeling concepts and methodologies**	9	Threat Modeling
1.12	**Apply Supply Chain Risk Management (SCRM) concepts**	2	Supply Chain Risk Management
1.12.1	Risks associated with hardware, software, and services	2	Risks Associated with Hardware, Software, and Services
1.12.2	Third-party assessment and monitoring	2	Other Third-Party Risks
1.12.3	Minimum security requirements	2	Minimum Security Requirements
1.12.4	Service level requirements	2	Service Level Agreements
1.13	**Establish and maintain a security awareness, education, and training program**	1	Security Awareness, Education, and Training Programs
1.13.1	Methods and techniques to present awareness and training (e.g., social engineering, phishing, security champions, gamification)	1	Methods and Techniques to Present Awareness and Training
1.13.2	Periodic content reviews	1	Periodic Content Reviews
1.13.3	Program effectiveness evaluation	1	Program Effectiveness Evaluation
Domain 2: Asset Security			
2.1	**Identify and classify information and assets**	5	Information and Assets
2.1.1	Data classification	5	Data Classification
2.1.2	Asset classification	5	Asset Classification
2.2	**Establish information and asset handling requirements**	5	Classification
2.3	**Provision resources securely**	5	Secure Provisioning
2.3.1	Information and asset ownership	5	Ownership

		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 2: Asset Security			
2.3.2	Asset inventory (e.g., tangible, intangible)	5	Inventories
2.3.3	Asset management	5	Managing the Life Cycle of Assets
2.4	**Manage data lifecycle**	5	Data Life Cycle
2.4.1	Data roles (i.e., owners, controllers, custodians, processors, users/subjects)	5	Data Roles
2.4.2	Data collection	5	Data Collection
2.4.3	Data location	5	Where in the World Is My Data?
2.4.4	Data maintenance	5	Data Maintenance
2.4.5	Data retention	5	Data Retention
2.4.6	Data remanence	5	Data Remanence
2.4.7	Data destruction	5	Data Destruction
2.5	**Ensure appropriate asset retention (e.g., End-of-Life (EOL), End-of-Support (EOS))**	5	Asset Retention
2.6	**Determine data security controls and compliance requirements**	6	Data Security Controls
2.6.1	Data states (e.g., in use, in transit, at rest)	6	Data States
2.6.2	Scoping and tailoring	6	Scoping and Tailoring
2.6.3	Standards selection	6	Standards
2.6.4	Data protection methods (e.g., Digital Rights Management (DRM), Data Loss Prevention (DLP), Cloud Access Security Broker (CASB))	6	Data Protection Methods
Domain 3: Security Architecture and Engineering			
3.1	**Research, implement and manage engineering processes using secure design principles**	9	Secure Design Principles
3.1.1	Threat modeling	9	Threat Modeling
3.1.2	Least privilege	9	Least Privilege
3.1.3	Defense in depth	9	Defense in Depth
3.1.4	Secure defaults	9	Secure Defaults
3.1.5	Fail securely	9	Fail Securely
3.1.6	Separation of Duties (SoD)	9	Separation of Duties
3.1.7	Keep it simple	9	Keep It Simple
3.1.8	Zero Trust	9	Zero Trust
3.1.9	Privacy by design	9	Privacy by Design

		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 3: Security Architecture and Engineering			
3.1.10	Trust but verify	9	Trust But Verify
3.1.11	Shared responsibility	9	Shared Responsibility
3.2	**Understand the fundamental concepts of security models (e.g., Biba, Star Model, Bell-LaPadula)**	9	Security Models
3.3	**Select controls based upon systems security requirements**	9	Security Requirements
3.4	**Understand security capabilities of Information Systems (IS) (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)**	9	Security Capabilities of Information Systems
3.5	**Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements**	7	General System Architectures
3.5.1	Client-based systems	7	Client-Based Systems
3.5.2	Server-based systems	7	Server-Based Systems
3.5.3	Database systems	7	Database Systems
3.5.4	Cryptographic systems	8	Cryptosystems
3.5.5	Industrial Control Systems (ICS)	7	Industrial Control Systems
3.5.6	Cloud-based systems (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))	7	Cloud-Based Systems
3.5.7	Distributed systems	7	Distributed Systems
3.5.8	Internet of Things (IoT)	7	Internet of Things
3.5.9	Microservices	7	Microservices
3.5.10	Containerization	7	Containerization
3.5.11	Serverless	7	Serverless
3.5.12	Embedded systems	7	Embedded Systems
3.5.13	High-Performance Computing (HPC) systems	7	High-Performance Computing Systems
3.5.14	Edge computing systems	7	Edge Computing Systems
3.5.15	Virtualized systems	7	Virtualized Systems
3.6	**Select and determine cryptographic solutions**	8	Cryptography Definitions and Concepts
3.6.1	Cryptographic life cycle (e.g., keys, algorithm selection)	8	Cryptographic Life Cycle

		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 3: Security Architecture and Engineering			
3.6.2	Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves, quantum)	8	Cryptographic Methods
3.6.3	Public Key Infrastructure (PKI)	8	Public Key Infrastructure
3.6.4	Key management practices	8	Key Management
3.6.5	Digital signatures and digital certificates	8	Digital Signatures Digital Certificates
3.6.6	Non-repudiation	8	Cryptosystems
3.6.7	Integrity (e.g., hashing)	8	Cryptosystems
3.7	**Understand methods of cryptanalytic attacks**	8	Integrity
3.7.1	Brute force	8	Brute Force
3.7.2	Ciphertext only	8	Ciphertext-Only Attacks
3.7.3	Known plaintext	8	Known-Plaintext Attacks
3.7.4	Frequency analysis	8	Frequency Analysis
3.7.5	Chosen ciphertext	8	Chosen-Ciphertext Attacks
3.7.6	Implementation attacks	8	Implementation Attacks
3.7.7	Side-channel	8	Side-Channel Attacks
3.7.8	Fault injection	8	Fault Injection
3.7.9	Timing	8	Side-Channel Attacks
3.7.10	Man-in-the-Middle (MITM)	8	Man-in-the-Middle
3.7.11	Pass the hash	8	Replay Attacks
3.7.12	Kerberos exploitation	17	Weaknesses of Kerberos
3.7.13	Ransomware	8	Ransomware
3.8	**Apply security principles to site and facility design**	10	Security Principles
3.9	**Design site and facility security controls**	10	Site and Facility Controls
3.9.1	Wiring closets/intermediate distribution facilities	10	Distribution Facilities
3.9.2	Server rooms/data centers	10	Data Processing Facilities
3.9.3	Media storage facilities	10	Media Storage
3.9.4	Evidence storage	10	Evidence Storage
3.9.5	Restricted and work area security	10	Restricted Areas

		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 3: Security Architecture and Engineering			
3.9.6	Utilities and Heating, Ventilation, and Air Conditioning (HVAC)	10	Utilities
3.9.7	Environmental issues	10	Environmental Issues
3.9.8	Fire prevention, detection, and suppression	10	Fire Safety
3.9.9	Power (e.g., redundant, backup)	10	Electric Power
Domain 4: Communication and Network Security			
4.1	**Assess and implement secure design principles in network architectures**	13	Applying Secure Design Principles to Network Architectures
4.1.1	Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models	11	Network Reference Models
4.1.2	Internet Protocol (IP) networking (e.g., Internet Protocol Security (IPSec), Internet Protocol (IP) v4/6)	11	Internet Protocol Networking
4.1.3	Secure protocols	13	Secure Protocols
4.1.4	Implications of multilayer protocols	13	Multilayer Protocols
4.1.5	Converged protocols (e.g., Fiber Channel Over Ethernet (FCoE), Internet Small Computer Systems Interface (iSCSI), Voice over Internet Protocol (VoIP))	13	Converged Protocols
4.1.6	Micro-segmentation (e.g., Software Defined Networks (SDN), Virtual eXtensible Local Area Network (VXLAN), Encapsulation, Software-Defined Wide Area Network (SD-WAN))	13	Network Segmentation
4.1.7	Wireless networks (e.g., Li-Fi, Wi-Fi, Zigbee, satellite)	12	Wireless Networking Fundamentals
4.1.8	Cellular networks (e.g., 4G, 5G)	12	Mobile Wireless Communication
4.1.9	Content Distribution Networks (CDN)	14	Content Distribution Networks
4.2	**Secure network components**	14	Network Devices
4.2.1	Operation of hardware (e.g., redundant power, warranty, support)	14	Operation of Hardware
4.2.2	Transmission media	14	Transmission Media
4.2.3	Network Access Control (NAC) devices	14	Network Access Control Devices
4.2.4	Endpoint security	14	Endpoint Security

		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 4: Communication and Network Security			
4.3	**Implement secure communication channels according to design**	15	All of Chapter 15
4.3.1	Voice	15	Voice Communications
4.3.2	Multimedia collaboration	15	Multimedia Collaboration
4.3.3	Remote access	15	Remote Access
4.3.4	Data communications	11	Data Communications Foundations
4.3.5	Virtualized networks	15	Virtualized Networks
4.3.6	Third-party connectivity	15	Third-Party Connectivity
Domain 5: Identity and Access Management (IAM)			
5.1	**Control physical and logical access to assets**	17	Controlling Physical and Logical Access
5.1.1	Information	17	Information Access Control
5.1.2	Systems	17	System and Application Access Control
5.1.3	Devices	17	Access Control to Devices
5.1.4	Facilities	17	Facilities Access Control
5.1.5	Applications	17	System and Application Access Control
5.2	**Manage identification and authentication of people, devices, and services**	16	Identification, Authentication, Authorization, and Accountability
5.2.1	Identity Management (IdM) implementation	16	Identity Management
5.2.2	Single/Multi-Factor Authentication (MFA)	16	Identification and Authentication
5.2.3	Accountability	16	Accountability
5.2.4	Session management	16	Session Management
5.2.5	Registration, proofing, and establishment of identity	16	Registration and Proofing of Identity
5.2.6	Federated Identity Management (FIM)	16	Federated Identity Management
5.2.7	Credential management systems	16	Credential Management
5.2.8	Single Sign On (SSO)	16	Single Sign-On
5.2.9	Just-In-Time (JIT)	16	Just-in-Time Access
5.3	**Federated identity with a third-party service**	16	Federated Identity with a Third-Party Service
5.3.1	On-premise	16	On-Premise

		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 5: Identity and Access Management (IAM)			
5.3.2	Cloud	16	Cloud
5.3.3	Hybrid	16	Hybrid
5.4	**Implement and manage authorization mechanisms**	17	Authorization Mechanisms
5.4.1	Role Based Access Control (RBAC)	17	Role-Based Access Control
5.4.2	Rule based access control	17	Rule-Based Access Control
5.4.3	Mandatory Access Control (MAC)	17	Mandatory Access Control
5.4.4	Discretionary Access Control (DAC)	17	Discretionary Access Control
5.4.5	Attribute Based Access Control (ABAC)	17	Attribute-Based Access Control
5.4.6	Risk based access control	17	Risk-Based Access Control
5.5	**Manage the identity and access provisioning lifecycle**	17	Managing the Identity and Access Provisioning Life Cycle
5.5.1	Account access review (e.g., user, system, service)	17	System Account Access Review
5.5.2	Provisioning and deprovisioning (e.g., on /off boarding and transfers)	17	Provisioning Deprovisioning
5.5.3	Role definition (e.g., people assigned to new roles)	17	Role Definitions
5.5.4	Privilege escalation (e.g., managed service accounts, use of sudo, minimizing its use)	17	Privilege Escalation Managed Service Accounts
5.6	**Implement authentication systems**	17	Implementing Authentication and Authorization Systems
5.6.1	OpenID Connect (OIDC)/Open Authorization (Oauth)	17	OpenID Connect Oauth
5.6.2	Security Assertion Markup Language (SAML)	17	Access Control and Markup Languages
5.6.3	Kerberos	17	Kerberos
5.6.4	Remote Authentication Dial-In User Service (RADIUS)/Terminal Access Controller Access Control System Plus (TACACS+)	17	Remote Access Control Technologies

		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 6: Security Assessment and Testing			
6.1	**Design and validate assessment, test, and audit strategies**	18	Test, Assessment, and Audit Strategies
6.1.1	Internal	18	Internal Audits
6.1.2	External	18	External Audits
6.1.3	Third-party	18	Third-Party Audits
6.2	**Conduct security control testing**	18	Testing Technical Controls
6.2.1	Vulnerability assessment	18	Vulnerability Testing
6.2.2	Penetration testing	18	Penetration Testing
6.2.3	Log reviews	18	Log Reviews
6.2.4	Synthetic transactions	18	Synthetic Transactions
6.2.5	Code review and testing	18	Code Reviews
6.2.6	Misuse case testing	18	Misuse Case Testing
6.2.7	Test coverage analysis	18	Test Coverage
6.2.8	Interface testing	18	Interface Testing
6.2.9	Breach attack simulations	18	Breach Attack Simulations
6.2.10	Compliance checks	18	Compliance Checks
6.3	**Collect security process data (e.g., technical and administrative)**	19	Security Process Data
6.3.1	Account management	19	Account Management
6.3.2	Management review and approval	19	Management Review and Approval
6.3.3	Key performance and risk indicators	19	Key Performance and Risk Indicators
6.3.4	Backup verification data	19	Backup Verification
6.3.5	Training and awareness	19	Security Training and Security Awareness Training
6.3.6	Disaster Recovery (DR) and Business Continuity (BC)	19	Disaster Recovery and Business Continuity
6.4	**Analyze test output and generate report**	19	Reporting
6.4.1	Remediation	19	Remediation
6.4.2	Exception handling	19	Exception Handling
6.4.3	Ethical disclosure	19	Ethical Disclosure

		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 6: Security Assessment and Testing			
6.5	**Conduct or facilitate security audits**	18	Conducting Security Audits
6.5.1	Internal	18	Conducting Internal Audits
6.5.2	External	18	Conducting and Facilitating External Audits
6.5.3	Third-party	18	Facilitating Third-Party Audits
Domain 7: Security Operations			
7.1	**Understand and comply with investigations**	22	Investigations
7.1.1	Evidence collection and handling	22	Evidence Collection and Handling
7.1.2	Reporting and documentation	22	Reporting and Documenting
7.1.3	Investigative techniques	22	Other Investigative Techniques
7.1.4	Digital forensics tools, tactics, and procedures	22	Digital Forensics Tools, Tactics, and Procedures
7.1.5	Artifacts (e.g., computer, network, mobile device)	22	Forensic Artifacts
7.2	**Conduct logging and monitoring activities**	21	Logging and Monitoring
7.2.1	Intrusion detection and prevention	21	Intrusion Detection and Prevention Systems
7.2.2	Security Information and Event Management (SIEM)	21	Security Information and Event Management
7.2.3	Continuous monitoring	21	Continuous Monitoring
7.2.4	Egress monitoring	21	Egress Monitoring
7.2.5	Log management	21	Log Management
7.2.6	Threat intelligence (e.g., threat feeds, threat hunting)	21	Threat Intelligence
7.2.7	User and Entity Behavior Analytics (UEBA)	21	User and Entity Behavior Analytics
7.3	**Perform Configuration Management (CM) (e.g., provisioning, baselining, automation)**	20	Configuration Management

		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 7: Security Operations			
7.4	**Apply foundational security operations concepts**	20	Foundational Security Operations Concepts
7.4.1	Need-to-know/least privilege	20	Need-to-Know/Least Privilege
7.4.2	Separation of Duties (SoD) and responsibilities	20	Separation of Duties and Responsibilities
7.4.3	Privileged account management	20	Privileged Account Management
7.4.4	Job rotation	20	Job Rotation
7.4.5	Service Level Agreements (SLAs)	20	Service Level Agreements
7.5	**Apply resource protection**	20	Resource Protection
7.5.1	Media management	20	Hierarchical Storage Management
7.5.2	Media protection techniques	20	Resource Protection
7.6	**Conduct incident management**	22	Overview of Incident Management
7.6.1	Detection	22	Detection
7.6.2	Response	22	Response
7.6.3	Mitigation	22	Mitigation
7.6.4	Reporting	22	Reporting
7.6.5	Recovery	22	Recovery
7.6.6	Remediation	22	Remediation
7.6.7	Lessons learned	22	Lessons Learned
7.7	**Operate and maintain detective and preventative measures**	21	Preventive and Detective Measures
7.7.1	Firewalls (e.g., next generation, web application, network)	21	Firewalls
7.7.2	Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)	21	Intrusion Detection and Prevention Systems
7.7.3	Whitelisting/blacklisting	21	Whitelisting and Blacklisting
7.7.4	Third-party provided security services	21	Outsourced Security Services
7.7.5	Sandboxing	21	Sandboxing
7.7.6	Honeypots/honeynets	21	Honeypots and Honeynets

		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 7: Security Operations			
7.7.7	Anti-malware	21	Antimalware Software
7.7.8	Machine learning and Artificial Intelligence (AI) based tools	21	Artificial Intelligence Tools
7.8	**Implement and support patch and vulnerability management**	20	Vulnerability and Patch Management
7.9	**Understand and participate in change management processes**	20	Change Management
7.10	**Implement recovery strategies**	23	Recovery Strategies
7.10.1	Backup storage strategies	23	Data Backup
7.10.2	Recovery site strategies	23	Recovery Site Strategies
7.10.3	Multiple processing sites	23	Multiple Processing Sites
7.10.4	System resilience, High Availability (HA), Quality of Service (QoS), and fault tolerance	23	Availability
7.11	**Implement Disaster Recovery (DR) processes**	23	Disaster Recovery Processes
7.11.1	Response	23	Response
7.11.2	Personnel	23	Personnel
7.11.3	Communications	23	Communications
7.11.4	Assessment	23	Assessment
7.11.5	Restoration	23	Restoration
7.11.6	Training and awareness	23	Training and Awareness
7.11.7	Lessons learned	23	Lessons Learned
7.12	**Test Disaster Recovery Plans (DRP)**	23	Testing Disaster Recovery Plans
7.12.1	Read-through/tabletop	23	Checklist Test Tabletop Exercises
7.12.2	Walkthrough	23	Structured Walkthrough Test
7.12.3	Simulation	23	Simulation Test
7.12.4	Parallel	23	Parallel Test
7.12.5	Full interruption	23	Full-Interruption Test
7.13	**Participate in Business Continuity (BC) planning and exercises**	23	Business Continuity
7.14	**Implement and manage physical security**	20	Physical Security
7.14.1	Perimeter security controls	20	External Perimeter Security Controls
7.14.2	Internal security controls	20	Internal Security Controls

		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 7: Security Operations			
7.15	**Address personnel safety and security concerns**	20	Personnel Safety and Security
7.15.1	Travel	20	Travel
7.15.2	Security training and awareness	20	Security Training and Awareness
7.15.3	Emergency management	20	Emergency Management
7.15.4	Duress	20	Duress
Domain 8: Software Development Security			
8.1	**Understand and integrate security in the Software Development Life Cycle (SDLC)**	24	Software Development Life Cycle
8.1.1	Development methodologies (e.g., Agile, Waterfall, DevOps, DevSecOps)	24	Development Methodologies
8.1.2	Maturity models (e.g., Capability Maturity Model (CMM), Software Assurance Maturity Model (SAMM))	24	Maturity Models
8.1.3	Operation and maintenance	24	Operations and Maintenance Phase
8.1.4	Change management	24	Change Management
8.1.5	Integrated Product Team (IPT)	24	Integrated Product Team
8.2	**Identify and apply security controls in software development ecosystems**	25	Security Controls for Software Development
8.2.1	Programming languages	25	Programming Languages and Concepts
8.2.2	Libraries	25	Software Libraries
8.2.3	Tool sets	25	Tool Sets
8.2.4	Integrated Development Environment (IDE)	25	Development Platforms
8.2.5	Runtime	25	Runtime Environments
8.2.6	Continuous Integration and Continuous Delivery (CI/CD)	25	Continuous Integration and Delivery
8.2.7	Security Orchestration, Automation, and Response (SOAR)	25	Security Orchestration, Automation, and Response
8.2.8	Software Configuration Management (SCM)	25	Software Configuration Management
8.2.9	Code repositories	25	Code Repositories
8.2.10	Application security testing (e.g., Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST))	25	Application Security Testing

		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 8: Software Development Security			
8.3	**Assess the effectiveness of software security**	25	Software Security Assessments
8.3.1	Auditing and logging of changes	25	Change Management
8.3.2	Risk analysis and mitigation	25	Risk Analysis and Mitigation
8.4	**Assess security impact of acquired software**	25	Assessing the Security of Acquired Software
8.4.1	Commercial-off-the-shelf (COTS)	25	Commercial Software
8.4.2	Open source	25	Open-Source Software
8.4.3	Third-party	25	Third-Party Software
8.4.4	Managed services (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))	25	Managed Services
8.5	**Define and apply secure coding guidelines and standards**	25	Secure Software Development
8.5.1	Security weaknesses and vulnerabilities at the source-code level	25	Source Code Vulnerabilities
8.5.2	Security of Application Programming Interfaces (APIs)	25	Application Programming Interfaces
8.5.3	Secure coding practices	25	Secure Coding Practices
8.5.4	Software-defined security	25	Software-Defined Security

This page intentionally left blank

APPENDIX C

About the Online Content

This book comes complete with TotalTester Online customizable practice exam software with more than 1,400 practice exam questions, separate graphical questions, and access to online CISSP flash cards.

System Requirements

The current and previous major versions of the following desktop browsers are recommended and supported: Chrome, Microsoft Edge, Firefox, and Safari. These browsers update frequently, and sometimes an update may cause compatibility issues with the TotalTester Online or other content hosted on the Training Hub. If you run into a problem using one of these browsers, please try using another until the problem is resolved.

Your Total Seminars Training Hub Account

To get access to the online content you will need to create an account on the Total Seminars Training Hub. Registration is free, and you will be able to track all your online content using your account. You may also opt in if you wish to receive marketing information from McGraw Hill or Total Seminars, but this is not required for you to gain access to the online content.

Privacy Notice

McGraw Hill values your privacy. Please be sure to read the Privacy Notice available during registration to see how the information you have provided will be used. You may view our Corporate Customer Privacy Policy by visiting the McGraw Hill Privacy Center. Visit the **mheducation.com** site and click **Privacy** at the bottom of the page.

Single User License Terms and Conditions

Online access to the digital content included with this book is governed by the McGraw Hill License Agreement outlined next. By using this digital content you agree to the terms of that license.

Access To register and activate your Total Seminars Training Hub account, simply follow these easy steps.

1. Go to this URL: **hub.totalsem.com/mheclaim**
2. To register and create a new Training Hub account, enter your e-mail address, name, and password on the **Register** tab. No further personal information (such as credit card number) is required to create an account.

   If you already have a Total Seminars Training Hub account, enter your e-mail address and password on the **Log in** tab.
3. Enter your Product Key: **`khth-vc35-9bqs`**
4. Click to accept the user license terms.
5. For new users, click the **Register and Claim** button to create your account. For existing users, click the **Log in and Claim** button.

   You will be taken to the Training Hub and have access to the content for this book.

Duration of License Access to your online content through the Total Seminars Training Hub will expire one year from the date the publisher declares the book out of print.

Your purchase of this McGraw Hill product, including its access code, through a retail store is subject to the refund policy of that store.

The Content is a copyrighted work of McGraw Hill, and McGraw Hill reserves all rights in and to the Content. The Work is © 2022 by McGraw Hill.

Restrictions on Transfer The user is receiving only a limited right to use the Content for the user's own internal and personal use, dependent on purchase and continued ownership of this book. The user may not reproduce, forward, modify, create derivative works based upon, transmit, distribute, disseminate, sell, publish, or sublicense the Content or in any way commingle the Content with other third-party content without McGraw Hill's consent.

Limited Warranty The McGraw Hill Content is provided on an "as is" basis. Neither McGraw Hill nor its licensors make any guarantees or warranties of any kind, either express or implied, including, but not limited to, implied warranties of merchantability or fitness for a particular purpose or use as to any McGraw Hill Content or the information therein or any warranties as to the accuracy, completeness, correctness, or results to be obtained from, accessing or using the McGraw Hill Content, or any material referenced in such Content or any information entered into licensee's product by users or other persons and/or any material available on or that can be accessed through the licensee's product (including via any hyperlink or otherwise) or as to non-infringement of third-party rights. Any warranties of any kind, whether express or implied, are disclaimed. Any material or data obtained through use of the McGraw Hill Content is at your own discretion and risk and user understands that it will be solely responsible for any resulting damage to its computer system or loss of data.

Neither McGraw Hill nor its licensors shall be liable to any subscriber or to any user or anyone else for any inaccuracy, delay, interruption in service, error or omission, regardless of cause, or for any damage resulting therefrom.

In no event will McGraw Hill or its licensors be liable for any indirect, special or consequential damages, including but not limited to, lost time, lost money, lost profits or good will, whether in contract, tort, strict liability or otherwise, and whether or not such damages are foreseen or unforeseen with respect to any use of the McGraw Hill Content.

TotalTester Online

TotalTester Online provides you with a simulation of the CISSP exam. Exams can be taken in Practice Mode or Exam Mode. Practice Mode provides an assistance window with hints, references to the book, explanations of the correct and incorrect answers, and the option to check your answer as you take the test. Exam Mode provides a simulation of the actual exam. The number of questions, the types of questions, and the time allowed are intended to be an accurate representation of the exam environment. The option to customize your quiz allows you to create custom exams from selected domains or chapters, and you can further customize the number of questions and time allowed.

To take a test, follow the instructions provided in the previous section to register and activate your Total Seminars Training Hub account. When you register you will be taken to the Total Seminars Training Hub. From the Training Hub Home page, select your certification from the Study drop-down menu at the top of the page to drill down to the TotalTester for your book. You can also scroll to it from the list of Your Topics on the Home page and then click the TotalTester link to launch the TotalTester. Once you've launched your TotalTester, you can select the option to customize your quiz and begin testing yourself in Practice Mode or Exam Mode. All exams provide an overall grade and a grade broken down by domain.

Graphical Questions

In addition to multiple-choice questions, the CISSP exam includes graphical questions. You can access the practice questions included with this book by navigating to the Resources tab and selecting Graphical Questions Quizzes. After you have selected the quizzes, they will appear in your browser, organized by domain.

Hotspot questions are graphical in nature and require the test taker to understand the concepts of the question from a practical and graphical aspect. You will have to point to the correct component within the graphic to properly answer the exam question. For example, you might be required to point to a specific area in a network diagram, point to a location in a network stack graphic, or choose the right location of a component within a graphic illustrating e-commerce–based authentication. It is not as easy to memorize answers for these types of questions, and they in turn make passing the exam more difficult.

The drag-and-drop questions are not as drastically different in format as compared to the hotspot questions. These questions just require the test taker to choose the correct answer or answers and drag them to the right location.

Online Flash Cards

Access to *Shon Harris' Online CISSP Flash Cards* from CISSP learning products company Human Element, LLC is also provided. These flash cards are another great way to study for the CISSP exam.

Privacy Notice Human Element, LLC values your privacy. Please be sure to read the Privacy Notice available during registration to see how the information you have provided will be used. You may view Human Element's Privacy Policy by visiting https://www.humanelementsecurity.com/content/Privacy-Policy.aspx.

To access the flash cards:

1. Go to www.humanelementsecurity.com and navigate to the CISSP Flash Cards page.
2. Choose the desired product and click the Add to Cart button.
3. Enter all required information (name and e-mail address) to set up your free online account.
4. On the payment method page enter the following code: 7YKL3

After following these instructions, you will have access to the CISSP Flash Cards. The Flash Card application is compatible with all Microsoft, Apple, and Android operating systems and browsers.

Single User License Terms and Conditions

Online access to the flash cards included with this book is governed by the McGraw Hill License Agreement outlined next. By using this digital content you agree to the terms of that license.

Duration of License Access to your online content through the Human Element website will expire one year from the date the publisher declares the book out of print.

Your purchase of this McGraw Hill product, including its access code, through a retail store is subject to the refund policy of that store.

Restrictions on Transfer The user is receiving only a limited right to use the Content for user's own internal and personal use, dependent on purchase and continued ownership of this book. The user may not reproduce, forward, modify, create derivative works based upon, transmit, distribute, disseminate, sell, publish, or sublicense the Content or in any way commingle the Content with other third-party content, without Human Element's consent. The Content is a copyrighted work of Human Element, LLC and Human Element reserves all rights in and to the Content.

Limited Warranty The Content is provided on an "as is" basis. Neither McGraw Hill, Human Element nor their licensors make any guarantees or warranties of any kind, either express or implied, including, but not limited to, implied warranties of merchantability or fitness for a particular purpose or use as to any Content or the information therein or any warranties as to the accuracy, completeness, correctness, or results to be obtained from, accessing or using the Content, or any material referenced in such Content or any information entered into licensee's product by users or other persons and/or any material available on or that can be accessed through the licensee's product (including via any hyperlink or otherwise) or as to non-infringement of thirdparty rights. Any warranties of any kind, whether express or implied, are disclaimed. Any material or data obtained through use of the Content is at your own discretion and risk and user understands that it will be solely responsible for any resulting damage to its computer system or loss of data.

Neither McGraw Hill nor its licensors shall be liable to any subscriber or to any user or anyone else for any inaccuracy, delay, interruption in service, error or omission, regardless of cause, or for any damage resulting therefrom.

In no event will McGraw Hill, Human Element or their licensors be liable for any indirect, special or consequential damages, including but not limited to, lost time, lost money, lost profits or good will, whether in contract, tort, strict liability or otherwise, and whether or not such damages are foreseen or unforeseen with respect to any use of the Content.

Technical Support

- For questions regarding the TotalTester or operation of the Training Hub, visit **www.totalsem.com** or e-mail **support@totalsem.com**.
- For questions regarding the flash cards, e-mail **info@humanelementsecurity.com**.
- For questions regarding book content, visit **www.mheducation.com/customerservice**.

This page intentionally left blank

access A subject's ability to view, modify, or communicate with an object. Access enables the flow of information between the subject and the object.

access control Mechanisms, controls, and methods of limiting access to resources to authorized subjects only.

access control list (ACL) A list of subjects that are authorized to access a particular object. Typically, the types of access are read, write, execute, append, modify, delete, and create.

access control mechanism Administrative, physical, or technical control that is designed to detect and prevent unauthorized access to a resource or environment.

accountability A security principle indicating that individuals must be identifiable and must be held responsible for their actions.

accredited A computer system or network that has received official authorization and approval to process sensitive data in a specific operational environment. There must be a security evaluation of the system's hardware, software, configurations, and controls by technical personnel.

acquisition The act of acquiring an asset. In organizational processes, this can mean either acquiring infrastructure (e.g., hardware, software, services) or another organization.

administrative controls Security mechanisms that are management's responsibility and referred to as "soft" controls. These controls include the development and publication of policies, standards, procedures, and guidelines; the screening of personnel; security-awareness training; the monitoring of system activity; and change control procedures.

aggregation The act of combining information from separate sources of a lower classification level that results in the creation of information of a higher classification level that the subject does not have the necessary rights to access.

Agile development An umbrella term for several development methodologies that focus on incremental and iterative development methods and promote cross-functional teamwork and continuous feedback mechanisms.

annualized loss expectancy (ALE) A dollar amount that estimates the loss potential from a risk in a span of a year.

single loss expectancy (SLE) × annualized rate of occurrence (ARO) = ALE

annualized rate of occurrence (ARO) The value that represents the estimated possibility of a specific threat taking place within a one-year timeframe.

antimalware Software whose principal functions include the identification and mitigation of malware; also known as antivirus, although this term could be specific to only one type of malware.

artificial intelligence (AI) A multidisciplinary field concerned with how knowledge is organized, how inference proceeds to support decision-making, and how systems learn.

asset Anything that is useful or valuable to an organization.

assurance A measurement of confidence in the level of protection that a specific security control delivers and the degree to which it enforces the security policy.

asymmetric key cryptography A cryptographic method that uses two different, or asymmetric, keys (also called public and private keys).

attribute-based access control (ABAC) An access control model in which access decisions are based on attributes of any component of or action on the system.

audit A systematic assessment of significant importance to the organization that determines whether the system or process being audited satisfies some external standards.

audit trail A chronological set of logs and records used to provide evidence of a system's performance or activity that took place on the system. These logs and records can be used to attempt to reconstruct past events and track the activities that took place, and possibly detect and identify intruders.

authentication Verification of the identity of a subject requesting the use of a system and/or access to network resources. The steps to giving a subject access to an object should be identification, authentication, and authorization.

authorization Granting a subject access to an object after the subject has been properly identified and authenticated.

availability The reliability and accessibility of data and resources to authorized individuals in a timely manner.

back door An undocumented way of gaining access to a computer system. After a system is compromised, an attacker may load a program that listens on a port (back door) so that the attacker can enter the system at any time. A back door is also referred to as a maintenance hook.

back up Copy and move data to a medium so that it may be restored if the original data is corrupted or destroyed. A full backup copies all the data from the system to the backup medium. An incremental backup copies only the files that have been modified since the previous backup. A differential backup backs up all files since the last full backup.

baseline The minimum level of security necessary to support and enforce a security policy.

Bell-LaPadula model A formal security model for access control that enforces the confidentiality of data (but not its integrity) using three rules: simple security, star property (*-property), and strong star property.

Biba model A formal security model for access control that enforces data integrity (but not confidentiality) using three rules: the *-integrity axiom (referred to as "no write up"), the simple integrity axiom (referred to as "no read down"), and the invocation property.

biometrics When used within computer security, identifies individuals by physiological characteristics, such as a fingerprint, hand geometry, or pattern in the iris.

blacklist (or deny list) A set of known-bad resources such as IP addresses, domain names, or applications.

breach attack simulation An automated system that launches simulated attacks against a target environment and then generates reports on its findings.

brute-force attack An attack that continually tries different inputs to achieve a predefined goal, which can be used to obtain credentials for unauthorized access.

business continuity (BC) Practices intended to keep the organization in business after a major disruption takes place.

business impact analysis (BIA) A functional analysis in which a team collects data through interviews and documentary sources; documents business functions, activities, and transactions; develops a hierarchy of business functions; and applies a classification scheme to indicate each individual function's criticality level.

Capability Maturity Model Integration (CMMI) A process model that captures the organization's maturity and fosters continuous improvement.

certificate authority (CA) A trusted third party that vouches for the identity of a subject, issues a certificate to that subject, and then digitally signs the certificate to assure its integrity.

certification The technical evaluation of the security components and their compliance for the purpose of accreditation. A certification process can use safeguard evaluation, risk analysis, verification, testing, and auditing techniques to assess the appropriateness of a specific system processing a certain level of information within a particular environment. The certification is the testing of the security component or system, and the accreditation is the approval from management of the security component or system.

challenge/response method A method used to verify the identity of a subject by sending the subject an unpredictable or random value. If the subject responds with the expected value in return, the subject is authenticated.

change management A business process aimed at deliberately regulating the changing nature of business activities such as projects.

chosen-ciphertext attack A cryptanalysis technique in which the attacker can choose the ciphertext to be decrypted and has access to the resulting decrypted plaintext, with the goal of determining the key that was used for decryption.

chosen-plaintext attack A cryptanalysis technique in which the attacker has the plaintext and ciphertext, but can choose the plaintext that gets encrypted to see the corresponding ciphertext in an effort to determine the key being used.

CIA triad The three primary security principles: confidentiality, integrity, and availability. Sometimes also presented as AIC: availability, integrity, and confidentiality.

ciphertext Data that has been encrypted and is unreadable until it has been converted into plaintext.

ciphertext-only attack A cryptanalysis technique in which the attacker has the ciphertext of one or more messages, each of which has been encrypted using the same encryption algorithm and key, and attempts to discover the key used in the encryption process.

Clark-Wilson model An integrity model that addresses all three integrity goals: prevent unauthorized users from making modifications, prevent authorized users from making improper modifications, and maintain internal and external consistency through auditing. A distinctive feature of this model is that it focuses on well-formed transactions and separation of duties.

classification A systematic arrangement of objects into groups or categories according to a set of established criteria. Data and resources can be assigned a level of sensitivity as they are being created, amended, enhanced, stored, or transmitted. The classification level then determines the extent to which the resource needs to be controlled and secured and is indicative of its value in terms of information assets.

cleartext In data communications, describes the form of a message or data that is transferred or stored without cryptographic protection.

cloud access security broker (CASB) A system that provides visibility and security controls for cloud services, monitors user activity in the cloud, and enforces policies and controls that are applicable to that activity.

cloud computing The use of shared, remote computing devices for the purpose of providing improved efficiencies, performance, reliability, scalability, and security.

code review A systematic examination of the instructions that comprise a piece of software, performed by someone other than the author of that code.

collusion Two or more people working together to carry out a fraudulent activity. More than one person would need to work together to cause some type of destruction or fraud; this drastically reduces its probability.

compensating controls Alternative controls that provide similar protection as the original controls but have to be used because they are more affordable or allow specifically required business functionality.

compliance Verifiable adherence to applicable laws, regulations, policies, and standards. The term is typically used to refer to compliance with governmental regulations.

compromise A violation of the security policy of a system or an organization such that unauthorized disclosure or modification of sensitive information occurs.

confidentiality A security principle that works to ensure that information is not disclosed to unauthorized subjects.

configuration management An operational process aimed at ensuring that systems and controls are configured correctly and are responsive to the current threat and operational environments.

containerization A type of virtualization in which individual applications run in their own isolated user space (called a container), which allows for more efficient use of computing resources.

content distribution network Multiple servers distributed across a large region, each of which provides content that is optimized for users closest to it. These networks are used not only to improve the user experience but also to mitigate the risk of denial-of-service attacks.

continuous improvement The practice of constantly measuring, analyzing, and improving processes.

continuous integration and continuous delivery (CI/CD) Processes and technologies that allow source code to be integrated, tested, and prepared for delivery to production environments as soon as a change to the code is submitted.

continuous monitoring Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

control A policy, method, technique, or procedure that is put into place to reduce the risk that a threat agent exploits a vulnerability. Also called a countermeasure or safeguard.

control zone The space within a facility that is used to protect sensitive processing equipment. Controls are in place to protect equipment from physical or technical unauthorized entry or compromise. The zone can also be used to prevent electrical waves carrying sensitive data from leaving the area.

converged protocols Protocols that started off independent and distinct from one another but over time converged to become one.

copyright A legal right that protects the expression of ideas.

corrective controls Controls that fix components or systems after an incident has occurred.

cost/benefit analysis An assessment that is performed to ensure that the cost of a safeguard does not outweigh the benefit of the safeguard. Spending more to protect an asset than the asset is actually worth does not make good business sense. All possible safeguards must be evaluated to ensure that the most security-effective and cost-effective choice is made.

countermeasure A policy, method, technique, or procedure that is put into place to reduce the risk that a threat agent exploits a vulnerability. Also called a safeguard or control.

covert channel A communications path that enables a process to transmit information in a way that violates the system's security policy.

covert storage channel A covert channel that involves writing to a storage location by one process and the direct or indirect reading of the storage location by another process. Covert storage channels typically involve a resource (for example, sectors on a disk) that is shared by two subjects at different security levels.

covert timing channel A covert channel in which one process modulates its system resource (for example, CPU cycles), which is interpreted by a second process as some type of communication.

cryptanalysis The practice of breaking cryptosystems and algorithms used in encryption and decryption processes.

cryptography The science of secret writing that enables storage and transmission of data in a form that is available only to the intended individuals.

cryptology The study of cryptography and cryptanalysis.

cryptosystem The hardware or software implementation of cryptography.

data at rest Data that resides in external or auxiliary storage devices such as hard disk drives, solid-state drives, or optical discs.

data classification Assignments to data that indicate the level of availability, integrity, and confidentiality that is required for each type of information.

data controller A senior leader that sets policies with regard to the management of the data life cycle, particularly with regard to sensitive data such as personal data.

data custodian An individual who is responsible for the maintenance and protection of the data. This role is usually filled by the IT department (usually the network administrator). The duties include performing regular backups of the data; implementing and maintaining security controls; periodically validating the integrity of the data; restoring data from backup media; retaining records of activity; and fulfilling the requirements specified in the organization's security policy, standards, and guidelines that pertain to information security and data protection.

data in transit (or data in motion) Data that is moving between computing nodes over a data network such as the Internet.

data in use Data that temporarily resides in primary storage such as registers, caches, or RAM while the CPU is using it.

data loss (or leak) prevention (DLP) The actions that organizations take to prevent unauthorized external parties from gaining access to sensitive data.

data mining The analysis of the data held in data warehouses in order to produce new and useful information.

data owner The person who has final responsibility of data protection and would be the one held liable for any negligence when it comes to protecting the organization's information assets. The person who holds this role—usually a senior executive within the management group—is responsible for assigning a classification to the information and dictating how the information should be protected.

data processor Any person who carries out operations (e.g., querying, modifying, analyzing) on data under the authority of the data controller.

data remanence A measure of the magnetic flux density remaining after removal of the applied magnetic force, which is used to erase data. Refers to any data remaining on magnetic storage media.

data subject The person about whom the data is concerned.

data warehousing The process of combining data from multiple databases or data sources into a large data store for the purpose of providing more extensive information retrieval and data analysis.

declassification An administrative decision or procedure to remove or reduce the security classification of information.

defense in depth A secure design principle that entails the coordinated use of multiple security controls in a layered approach.

degauss Process that demagnetizes magnetic media so that a very low residue of magnetic induction is left on the media. Used to effectively erase data from media.

Delphi technique A group decision method used to ensure that each member of a group gives an honest and anonymous opinion pertaining to what the result of a particular threat will be.

denial of service (DoS) Any action, or series of actions, that prevents a system, or its resources, from functioning in accordance with its intended purpose.

detective controls Controls that help identify an incident's activities and potentially an intruder.

DevOps The practice of incorporating development, IT, and quality assurance (QA) staff into software development projects to align their incentives and enable frequent, efficient, and reliable releases of software products.

DevSecOps The integration of development, security, and operations professionals into a software development team. It's DevOps with the security team added in.

dial-up The service whereby a computer terminal can use telephone lines, usually via a modem, to initiate and continue communication with another computer system.

dictionary attack A form of attack in which an attacker uses a large set of likely combinations to guess a secret, usually a password.

digital certificate A mechanism used to associate a public key with a collection of components in a manner that is sufficient to uniquely identify the claimed owner. The most commonly used standard for digital certificates is the International Telecommunications Union's X.509.

Digital Rights Management (DRM) A set of technologies that is applied to controlling access to copyrighted data.

digital signature A hash value that has been encrypted with the sender's private key.

disaster recovery (DR) The set of practices that enables an organization to minimize loss of, and restore, mission-critical technology infrastructure after a catastrophic incident.

disaster recovery plan (DRP) A plan developed to help an organization recover from a disaster. It provides procedures for emergency response, extended backup operations, and post-disaster recovery when an organization suffers a loss of computer processing capability or resources and physical facilities.

discretionary access control (DAC) An access control model and policy that restricts access to objects based on the identity of the subjects and the groups to which those subjects belong. The data owner has the discretion of allowing or denying others access to the resources it owns.

Distributed Network Protocol 3 (DNP3) A communications protocol designed for use in SCADA systems, particularly those within the power sector, that does not include routing functionality.

domain The set of objects that a subject is allowed to access. Within this domain, all subjects and objects share a common security policy, procedures, and rules, and they are managed by the same management system.

due care The precautions that a reasonable and competent person would take in a given situation.

due diligence The process of systematically evaluating information to identify vulnerabilities, threats, and issues relating to an organization's overall risk.

duress The use of threats or violence against someone in order to force them to do something they don't want to do.

dynamic application security testing (DAST) Also known as dynamic analysis, the evaluation of a program in real time, while it is running.

edge computing A distributed system in which some computational and data storage assets are deployed close to where they are needed in order to reduce latency and network traffic.

egress monitoring Maintaining awareness of the information that is flowing out of a network, whether it appears to be malicious or not.

electronic discovery (e-discovery) The process of producing for a court or external attorney all electronically stored information pertinent to a legal proceeding.

electronic vaulting The transfer of backup data to an offsite location. This process is primarily a batch process of transmitting data through communications lines to a server at an alternative location.

elliptic curve cryptography A cryptographic method that uses complex mathematical equations (plotted as elliptic curves) that are more efficient than traditional asymmetric key cryptography but also much more difficult to cryptanalyze.

emanations Electrical and electromagnetic signals emitted from electrical equipment that can transmit through the airwaves. These signals carry information that can be captured and deciphered, which can cause a security breach. These are also called *emissions*.

embedded system A self-contained, typically ruggedized, computer system with its own processor, memory, and input/output devices that is designed for a very specific purpose.

encryption The transformation of plaintext into unreadable ciphertext.

end-of-life (EOL) The point in time when a manufacturer ceases to manufacture or sustain a product.

end-of-support (EOS) The point in time when a manufacturer is no longer patching bugs or vulnerabilities on a product, which is typically a few years after EOL.

endpoint A networked computing device that initiates or responds to network communications.

endpoint detection and response (EDR) An integrated security system that continuously monitors endpoints for security violations and uses rules-based automated response and analysis capabilities.

end-to-end encryption A technology that encrypts the data payload of a packet.

ethical disclosure The practice of informing anyone who might be affected by a discovered vulnerability as soon as feasible, so a patch can be developed before any threat actors become aware of the vulnerability.

exposure An instance of being exposed to losses from a threat. A weakness or vulnerability can cause an organization to be exposed to possible damages.

exposure factor The percentage of loss a realized threat could have on a certain asset.

failover A backup operation that automatically switches to a standby system if the primary system fails or is taken offline. It is an important fault-tolerant function that provides system availability.

fail-safe A functionality that ensures that when software or a system fails for any reason, it does not compromise anyone's safety. After a failure, a fail-safe electronic lock might default to an unlocked state, which would prevent it from interfering with anyone trying to escape in an emergency.

fail-secure A functionality that ensures that when software or a system fails for any reason, it does not end up in a vulnerable state. After a failure, a fail-secure lock might default to a locked state, which would ensure the security of whatever it is protecting.

federated identity management (FIM) The management of portable identities, and their associated entitlements, that can be used across business boundaries.

Fibre Channel over Ethernet (FCoE) A converged protocol that allows Fibre Channel frames to ride over Ethernet networks.

firmware Software instructions that have been written into read-only memory (ROM) or a programmable ROM (PROM) chip.

forensic artifact Anything that has evidentiary value.

formal verification Validating and testing of highly trusted systems. The tests are designed to show design verification, consistency between the formal specifications and the formal security policy model, implementation verification, consistency between the formal specifications, and the actual implementation of the product.

full-interruption test A type of security test in which a live system or facility is shut down, forcing the recovery team to switch processing to an alternate system or facility.

gamification The application of elements of game play to other activities such as security awareness training.

gateway A system or device that connects two unlike environments or systems. The gateway is usually required to translate between different types of applications or protocols.

guidelines Recommended actions and operational guides for users, IT staff, operations staff, and others when a specific standard does not apply.

handshaking procedure A dialog between two entities for the purpose of identifying and authenticating the entities to one another. The dialog can take place between two computers or two applications residing on different computers. It is an activity that usually takes place within a protocol.

high-performance computing (HPC) The aggregation of computing power in ways that exceed the capabilities of general-purpose computers for the specific purpose of solving large problems.

honeynet A network of honeypots designed to keep adversaries engaged (and thus under observation) for longer than would be possible with a single honeypot.

honeypot A network device that is intended to be exploited by attackers, with the administrator's goal being to gain information on the attackers' tactics, techniques, and procedures (TTPs).

identification A subject provides some type of data to an authentication service. Identification is the first step in the authentication process.

Identity as a Service (IDaaS) A type of Software as a Service (SaaS) offering that normally provides single sign-on (SSO), federated identity management (IdM), and password management services.

identity management (IdM) A broad term that encompasses the use of different products to identify, authenticate, and authorize users through automated means. It usually includes user account management, access control, credential management, single sign-on (SSO) functionality, managing rights and permissions for user accounts, and auditing and monitoring all of these items.

industrial control system (ICS) Information technology that is specifically designed to control physical devices in industrial processes. The two main types of ICS are distributed control systems (DCSs) and supervisory control and data acquisition (SCADA) systems. The main difference between them is that a DCS controls local processes while SCADA is used to control things remotely.

inference The ability to derive information not explicitly available.

Infrastructure as a Service (IaaS) A cloud computing model that provides users unfettered access to a cloud device, such as an instance of a server, which includes both the operating system and the virtual machine on which it runs.

Integrated Product Team (IPT) A multidisciplinary software development team with representatives from many or all the stakeholder populations.

integrity A security principle that makes sure that information and systems are not modified maliciously or accidentally.

Internet of Things (IoT) The global network of connected, uniquely addressable, embedded systems.

Internet Small Computer System Interface (iSCSI) A converged protocol that encapsulates SCSI data in TCP segments in order to allow peripherals to be connected to computers across networks.

intrusion detection system (IDS) Software employed to monitor and detect possible attacks and behaviors that vary from the normal and expected activity. The IDS can be network based, which monitors network traffic, or host based, which monitors activities of a specific system and protects system files and control mechanisms.

intrusion prevention system (IPS) An intrusion detection system (IDS) that is also able to take actions to stop a detected intrusion.

IP Security (IPSec) A suite of protocols that was developed to specifically protect IP traffic. It includes the Authentication Header (AH), Encapsulating Security Payload (ESP), Internet Security Association and Key Management Protocol (ISAKMP), and Internet Key Exchange (IKE) protocols.

isolation The containment of processes in a system in such a way that they are separated from one another to ensure integrity and confidentiality.

job rotation The practice of ensuring that, over time, more than one person fulfills the tasks of one position within the organization. This enables the organization to have staff backup and redundancy, and helps detect fraudulent activities.

just in time (JIT) access A provisioning methodology that elevates users to the necessary privileged access to perform a specific task.

Kerberos A client/server authentication protocol based on symmetric key cryptography that is the default authentication mechanism in Microsoft Active Directory environments.

kernel The core of an operating system, manages the machine's hardware resources (including the processor and the memory) and provides and controls the way any other software component accesses these resources.

key A discrete data set that controls the operation of a cryptography algorithm. In encryption, a key specifies the particular transformation of plaintext into ciphertext, or vice versa, during decryption. Keys are also used in other cryptographic algorithms, such as digital signature schemes and keyed-hash functions (also known as HMACs), which are often used for authentication and integrity.

keystroke monitoring A type of auditing that can review or record keystrokes entered by a user during an active session.

known-plaintext attack A cryptanalysis technique in which the attacker has the plaintext and corresponding ciphertext of one or more messages and wants to discover the key used to encrypt the message(s).

least privilege The secure design principle that requires each subject to be granted the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

Li-Fi A wireless networking technology that uses light rather than radio waves to transmit and receive data.

Lightweight Directory Access Protocol (LDAP) A directory service based on a subset of the X.500 standard that allows users and applications to interact with a directory.

link encryption A type of encryption technology that encrypts packets' headers, trailers, and the data payload. Each network communications node, or hop, must decrypt the packets to read their addresses and routing information and then re-encrypt the packets. This is different from end-to-end encryption.

machine learning (ML) Systems that acquire their knowledge, in the form of numeric parameters (i.e., weights), through training with data sets consisting of millions of examples. In supervised learning, ML systems are told whether or not they made the right decision. In unsupervised training they learn by observing an environment. Finally, in reinforcement learning they get feedback on their decisions from the environment.

maintenance hook Instructions within a program's code that enable the developer or maintainer to enter the program without having to go through the usual access control and authentication processes. Maintenance hooks should be removed from the code before it is released to production; otherwise, they can cause serious security risks. Also called a back door.

malware Malicious software. Code written to perform activities that circumvent the security policy of a system. Examples are viruses, malicious applets, Trojan horses, logic bombs, and worms.

mandatory access control (MAC) An access policy that restricts subjects' access to objects based on the security clearance of the subject and the classification of the object. The system enforces the security policy, and users cannot share their files with other users.

message authentication code (MAC) In cryptography, a generated value used to authenticate a message. A MAC can be generated by HMAC or CBC-MAC methods. The MAC protects both a message's integrity (by ensuring that a different MAC will be produced if the message has changed) and its authenticity, because only someone who knows the secret key could have modified the message.

microsegmentation The practice of isolating individual assets (e.g., data servers) in their own protected network environment.

microservice An architectural style that consists of small, decentralized, loosely coupled, individually deployable services built around business capabilities.

multifactor authentication (MFA) Authentication mechanisms that employ more than one factor. Factors are something a person knows (e.g., password), something a person has (e.g., a hardware token), and something a person is (e.g., biometrics).

multilayer protocol A protocol that works across multiple layers of the OSI model.

multilevel security A class of systems containing information with different classifications. Access decisions are based on the subject's security clearances, need to know, and formal approval.

Multiprotocol Label Switching (MPLS) A converged data communications protocol designed to improve the routing speed of high-performance networks.

need to know A security principle stating that users should have access only to the information and resources necessary to complete their tasks that fulfill their roles within an organization. Need to know is commonly used in access control criteria by operating systems and applications.

network detection and response (NDR) Systems that monitor network traffic for malicious actors and suspicious behavior, and react and respond to the detection of cyberthreats to the network.

nonrepudiation A service that ensures the sender cannot later falsely deny sending a message or taking an action.

OAuth An open standard for authorization (not authentication) to third parties that lets users authorize a web system to use something that they control at a different website.

object A passive entity that contains or receives information. Access to an object potentially implies access to the information that it contains. Examples of objects include records, pages, memory segments, files, directories, directory trees, and programs.

onboarding The process of turning a candidate into a trusted employee who is able to perform all assigned duties.

one-time pad A method of encryption in which the plaintext is combined with a random "pad," which should be the same length as the plaintext. This encryption process uses a nonrepeating set of random bits that are combined bitwise (XOR) with the message to produce ciphertext. A one-time pad is a perfect encryption scheme because it is unbreakable and each pad is used exactly once, but it is impractical because of all of the required overhead.

Open System Interconnection (OSI) model A conceptual framework used to describe the functions of a networking system along seven layers in which each layer relies on services provided by the layer below it and provides services to the layer above it.

OpenID Connect A simple authentication layer built on top of the OAuth 2.0 protocol that allows transparent authentication and authorization of client resource requests.

password A sequence of characters used to prove one's identity. It is used during a logon process and should be highly protected.

patent A grant of legal ownership given to an individual or organization to exclude others from using or copying the invention covered by the patent.

Payment Card Industry Data Security Standard (PCI DSS) An information security standard for organizations that are involved in payment card transactions.

penetration testing A method of evaluating the security of a computer system or network by simulating an attack that a malicious hacker would carry out. Pen testing is performed to uncover vulnerabilities and weaknesses.

personnel security The procedures that are established to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearances. Procedures confirm a person's background and provide assurance of necessary trustworthiness.

physical controls Controls that pertain to controlling individual access into the facility and different departments, locking systems and removing unnecessary USB and optical drives, protecting the perimeter of the facility, monitoring for intrusion, and checking environmental controls.

physical security Controls and procedures put into place to prevent intruders from physically accessing a system or facility. The controls enforce access control and authorized access.

piggyback Unauthorized access to a facility or area by using another user's legitimate credentials or access rights.

plaintext In cryptography, the original readable text before it is encrypted.

Platform as a Service (PaaS) A cloud computing model that provides users access to a computing platform but not to the operating system or to the virtual machine on which it runs.

preventive controls Controls that are intended to keep an incident from occurring.

privacy A security principle that protects an individual's information and employs controls to ensure that this information is not disseminated or accessed in an unauthorized manner.

privacy by design A secure design principle that ensures privacy of user data is an integral part of the design of an information system, not an afterthought or later-stage feature.

procedure Detailed step-by-step instructions to achieve a certain task, which are used by users, IT staff, operations staff, security members, and others.

protocol A set of rules and formats that enables the standardized exchange of information between different systems.

public key encryption A type of encryption that uses two mathematically related keys to encrypt and decrypt messages. The private key is known only to the owner, and the public key is available to anyone.

public key infrastructure (PKI) A framework of programs, procedures, communication protocols, and public key cryptography that enables a diverse group of individuals to communicate securely.

qualitative risk analysis A risk analysis method that uses opinion and experience to judge an organization's exposure to risks. It uses scenarios and ratings systems. Compare to quantitative risk analysis.

quantitative risk analysis A risk analysis method that attempts to use percentages in damage estimations and assigns real numbers to the costs of countermeasures for particular risks and the amount of damage that could result from the risk. Compare to qualitative risk analysis.

quantum key distribution (QKD) A system that generates and securely distributes encryption keys of any length between two parties.

RADIUS (Remote Authentication Dial-In User Service) A security service that authenticates and authorizes dial-up users and is a centralized access control mechanism.

recovery point objective (RPO) The acceptable amount of data loss measured in time.

recovery time objective (RTO) The maximum time period within which a mission-critical system must be restored to a designated service level after a disaster to avoid unacceptable consequences associated with a break in business continuity.

reference monitor concept An abstract machine that mediates all access subjects have to objects, both to ensure that the subjects have the necessary access rights and to protect the objects from unauthorized access and destructive modification.

registration authority (RA) A trusted entity that establishes and confirms the identity of an individual, initiates the certification process with a CA on behalf of an end user, and performs certificate life-cycle management functions.

reliability The assurance of a given system, or individual component, performing its mission adequately for a specified period of time under the expected operating conditions.

remote journaling A method of transmitting changes to data to an offsite facility. This takes place as parallel processing of transactions, meaning that changes to the data are saved locally and to an offsite facility. These activities take place in real time and provide redundancy and fault tolerance.

repudiation When the sender of a message denies sending the message. The countermeasure to this is to implement digital signatures.

residual risk The remaining risk after the security controls have been applied. The conceptual formulas that explain the difference between total risk and residual risk are

threats × vulnerability × asset value = total risk

(threats × vulnerability × asset value) × controls gap = residual risk