

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.  $(\text{ALE before implementing safeguard}) - (\text{ALE after implementing safeguard}) - (\text{annual cost of safeguard}) = \text{value of safeguard to the organization}$
  - B.  $(\text{ALE before implementing safeguard}) - (\text{ALE during implementing safeguard}) - (\text{annual cost of safeguard}) = \text{value of safeguard to the organization}$
  - C.  $(\text{ALE before implementing safeguard}) - (\text{ALE while implementing safeguard}) - (\text{annual cost of safeguard}) = \text{value of safeguard to the organization}$
  - D.  $(\text{ALE before implementing safeguard}) - (\text{ALE after implementing safeguard}) - (\text{annual cost of asset}) = \text{value of safeguard to the organization}$
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) <sup>2</sup> Code of Professional Ethics	1	(ISC) <sup>2</sup> 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

Domain	Objective	All-in-One Coverage	
		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



Domain	Objective	All-in-One Coverage	
		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

Domain	Objective	All-in-One Coverage	
		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*



---

# 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](http://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](http://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](http://www.totalsem.com)** or e-mail **[support@totalsem.com](mailto:support@totalsem.com)**.
- For questions regarding the flash cards, e-mail **[info@humanelementsecurity.com](mailto:info@humanelementsecurity.com)**.
- For questions regarding book content, visit **[www.mheducation.com/customerservice](http://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.

$$\text{single loss expectancy (SLE)} \times \text{annualized rate of occurrence (ARO)} = \text{ALE}$$



**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

$$\text{threats} \times \text{vulnerability} \times \text{asset value} = \text{total risk}$$

$$(\text{threats} \times \text{vulnerability} \times \text{asset value}) \times \text{controls gap} = \text{residual risk}$$



**risk** The likelihood of a threat agent taking advantage of a vulnerability and the resulting business impact. A risk is the loss potential, or probability, that a threat will exploit a vulnerability.

**risk analysis** A detailed examination of the components of risk that is used to ensure that security is cost-effective, relevant, timely, and responsive to threats.

**risk assessment** A method of identifying vulnerabilities and threats and assessing the possible impacts to determine where to implement security controls.

**risk management** The process of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level of risk.

**risk-based access control** An authorization mechanism that 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.

**role-based access control (RBAC)** Type of access control model that provides access to resources based on the role the user holds within the organization or the tasks that the user has been assigned.

**rule-based access control (RB-RBAC)** Type of access control model that uses specific rules that indicate what can and cannot happen between a subject and an object; built on top of traditional RBAC and is thus commonly called RB-RBAC to disambiguate the otherwise overloaded RBAC acronym.

**safeguard** 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 control.

**sandboxing** A type of control that isolates processes from the operating system to prevent security violations.

**scoping** The process of taking a broader standard and trimming out the irrelevant or otherwise unwanted parts.

**secure defaults** A secure design principle that entails having every system start off in a state where security trumps user friendliness and functionality, and then has controls deliberately relaxed to enable additional features and generally make the system more user friendly.

**Security Assertion Markup Language (SAML)** An XML standard that allows the exchange of authentication and authorization data to be shared between security domains.

**security awareness** The knowledge and attitude of an individual concerning likely threats.

**security control** Any measure taken by an organization to mitigate information security risks.



**security evaluation** Assesses the degree of trust and assurance that can be placed in systems for the secure handling of sensitive information.

**security information and event management (SIEM)** A software platform that aggregates security information and security events and presents them in a single, consistent, and cohesive manner.

**security label** An identifier that represents the security level of an object.

**security orchestration, automation, and response (SOAR)** Integrated systems that enable more efficient security operations through automation of various workflows.

**security testing** Testing all security mechanisms and features within a system to determine the level of protection they provide. Security testing can include penetration testing, formal design and implementation verification, and functional testing.

**sensitive information** Information that would cause a negative effect on the organization if it were lost or compromised.

**sensitivity label** A piece of information that represents the security level of an object. Sensitivity labels are used as the basis for mandatory access control (MAC) decisions.

**separation of duties** A secure design principle that splits up a critical task among two or more individuals to ensure that one person cannot complete a risky task by himself.

**serverless architecture** A computing architecture in which the services offered to end users, such as compute, storage, or messaging, along with their required configuration and management, can be performed without a requirement from the user to set up any server infrastructure.

**service level agreement (SLA)** A contract between a service provider and a service user that specifies the minimum acceptable parameters of the services being provided.

**shared responsibility** A secure design principle that addresses situations in which a service provider is responsible for certain security controls, while the customer is responsible for others.

**shoulder surfing** When a person looks over another person's shoulder and watches keystrokes or watches data as it appears on the screen in order to uncover information in an unauthorized manner.

**simple security property** A Bell-LaPadula security model rule that stipulates that a subject cannot read data at a higher security level.

**single loss expectancy (SLE)** A monetary value that is assigned to a single event that represents the organization's potential loss amount if a specific threat were to take place.

$$\text{asset value} \times \text{exposure factor} = \text{SLE}$$

**single sign-on (SSO)** A technology that allows a user to authenticate one time and then access resources in the environment without needing to reauthenticate.

**social engineering** The act of tricking another person into providing confidential information by posing as an individual who is authorized to receive that information.

**Software as a Service (SaaS)** A cloud computing model that provides users access to a specific application that executes in the service provider's environment.

**Software Assurance Maturity Model (SAMM)** A maturity model that is specifically focused on secure software development and allows organizations of any size to decide their target maturity levels within each of five critical business functions.

**software-defined networking (SDN)** An approach to networking that relies on distributed software to provide improved agility and efficiency by centralizing the configuration and control of networking devices.

**software-defined security (SDS or SDsec)** A security model in which security functions such as firewalling, IDS/IPS, and network segmentation are implemented in software within an SDN environment.

**spoofing** Presenting false information, usually within packets, to trick other systems and hide the origin of the message. This is usually done by hackers so that their identity cannot be successfully uncovered.

**standards** Rules indicating how hardware and software should be implemented, used, and maintained. Standards provide a means to ensure that specific technologies, applications, parameters, and procedures are carried out in a uniform way across the organization. They are compulsory.

**star property (\*-property)** A Bell-LaPadula security model rule that stipulates that a subject cannot write data to an object at a lower security level.

**static application security testing (SAST)** A technique, also called static analysis, that identifies certain software defects or security policy violations by examining the source code without executing the program.

**subject** An active entity, generally in the form of a person, process, or device, that causes information to flow among objects or that changes the system state.

**supervisory control and data acquisition (SCADA)** A system for remotely monitoring and controlling physical systems such as power and manufacturing plants.

**supply chain** An interconnected network of interdependent suppliers and consumers involved in delivering some product or service.

**symmetric key cryptography** A cryptographic method that uses instances of the same key (called the secret key) for encryption and decryption.

**synthetic transaction** A transaction that is executed in real time by a software agent to test or monitor the performance of a distributed system.

**tabletop exercise (TTX)** A type of exercise in which participants respond to notional events to test out procedures and ensure they actually do what they're intended to and that everyone knows their role in responding to the events.

**TACACS (Terminal Access Controller Access Control System)** A client/server authentication protocol that provides the same type of functionality as RADIUS and is used as a central access control mechanism mainly for remote users.

**tailoring** The practice of making changes to specific provisions of a standard so they better address organizational requirements.

**technical controls** Controls that work in software to provide availability, integrity, or confidentiality protection; also called logical access control mechanisms. Some examples are passwords, identification and authentication methods, security devices, auditing, and the configuration of the network.

**test coverage** A measure of how much of a system is examined by a specific test (or group of tests), which is typically expressed as a percentage.

**threat** A potential cause of an unwanted incident, which can result in harm to a system or organization.

**threat intelligence** Evidence-based knowledge about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding responses to that menace or hazard.

**threat modeling** The process of describing probable adverse effects on an organization's assets caused by specific threat sources.

**top-down approach** An approach in which the initiation, support, and direction for a project come from top management and work their way down through middle management and then to staff members.

**topology** The physical construction of how nodes are connected to form a network.

**total risk** The risk an organization faces if it chooses not to implement any type of safeguard.

**trade secret** Something that is proprietary to a company and important for its survival and profitability.

**trademark** A legal right that protects a word, name, product shape, symbol, color, or a combination of these used to identify a product or an organization.

**transborder data flow (TDF)** The movement of machine-readable data across a political boundary such as a country's border.

**Trojan horse** A computer program that has an apparently or actually useful function, but that also contains hidden malicious capabilities to exploit a vulnerability and/or provide unauthorized access into a system.

**trust but verify** A secure design principle that requires that even when an entity and its behaviors are trusted, they should be monitored and verified.

**user** A person or process that is accessing a computer system.

**user and entity behavior analytics (UEBA)** Processes that determine normal patterns of behavior so that abnormalities can be detected and investigated.

**user ID** A unique set of characters or code that is used to identify a specific user to a system.

**validation** The act of performing tests and evaluations to test a system's security level to see if it complies with security specifications and requirements.

**Virtual eXtensible Local Area Network (VxLAN)** A network virtualization technology that encapsulates layer 2 frames onto UDP (layer 4) datagrams for distribution anywhere in the world.

**virtualization** The practice of running a virtual computing system in an environment that is abstracted from the actual hardware.

**virus** A small application, or string of code, that infects applications. The main function of a virus is to reproduce, and it requires a host application to do this. It can damage data directly or degrade system performance.

**vulnerability** A weakness in a system that allows a threat source to compromise its security. It can be a software, hardware, procedural, or human weakness that can be exploited.

**Waterfall methodology** A software development methodology that uses a strictly linear, sequential life-cycle approach in which each phase must be completed in its entirety before the next phase can begin.

**whitelist (or allow list)** A set of known-good resources such as IP addresses, domain names, or applications.

**work factor** The estimated time and effort required for an attacker to overcome a security control.

**worm** An independent program that can reproduce by copying itself from one system to another. It may damage data directly or degrade system performance by tying up resources.

**zero trust** A secure design principle that assumes that every entity is hostile until proven otherwise.

*This page intentionally left blank*

---

# INDEX

## A

AARs (after-action reviews) in disaster recovery, 869, 1061

ABAC (attribute-based access control)  
characteristics, 776  
description, 774

ABR (available bit rate) in ATM, 551

abstract machines, 766

abstraction

- containers, 298
- network architectures, 597, 634
- object-oriented programming, 1129
- programming languages, 1119–1120
- system architectures, 283, 297

academic software, 153

acceptable use policies (AUPs)

- software, 226
- user accounts, 858
- web proxies, 664

acceptance risk strategy

- ISO/IEC 27005, 178
- overview, 79–80

acceptance testing in software development, 1091

access control

- authorization mechanisms.

*See authentication; authorization*

CPTED, 430–431

facilities, 443–446, 916–924

identity and access, 796

information, 801

just-in-time, 738

locks, 917–923

logical, 717

markup languages, 776–781

models, 766

physical and logical access,  
801–803

physical security. *See physical security and controls*

remote, 789–795

access control lists (ACLs)

DAC, 767

data historians, 293

identity management, 747

incident response, 996

network sockets, 703

packet-filtering firewalls, 946–948

RBAC, 771

routers, 660

server-based systems, 284

switches, 657

VPNs, 697

WPANs, 571

access doors for data processing facilities, 443

access points (APs)

collision domains, 493

DSL modems, 683

WLANs, 564–565

access triples in Clark-Wilson model, 400

accountability

audits, 741–745

credential management, 736

description, 161, 716

logical access controls, 717

overview, 887–888

Accountability Principle in OECD, 142

accounting in Diameter, 795

accounts

adding, 858

modifying, 859

registration and proofing of identity,  
738–740

suspending, 860

accuracy

biometric systems, 724–725, 727

data loss prevention, 270

threat intelligence, 941

ACID properties of database systems, 286

ACK (acknowledgment packets) in TCP

handshakes, 508, 949–951

ACLs. *See access control lists (ACLs)*

acoustical detection IDSs, 927

- acquired software security concerns, 1145–1148
- acquiring
  - data, 230
  - evidence, 1012–1013
- acrylic windows, 441
- Act phase in Plan-Do-Check-Act loop, 875
- actionability in security metrics, 854
- actions in ABAC, 774
- actions on objectives stage in Cyber Kill Chain framework, 994
- active attacks on cryptography, 367
- Active Directory (AD) environment, 747
- active monitors
  - computer surveillance, 1020
  - Token Ring, 496
- actors
  - defined, 8
  - internal, 61–62
- ad hoc WLANs, 565
- adapters in forensics field kits, 1015
- Address Resolution Protocol (ARP), 515–517
- Adleman, Leonard, 340
- ADM (Architecture Development Method), 194–195
- administrative controls
  - digital asset management, 261
  - risk responses, 83, 86–87
- administrative investigations, 161–162
- administrative law system, 128
- administrative/regulatory law, 130
- administrative responsibilities for locks, 922
- admissibility of evidence, 1013–1014
- ADSL (asymmetric DSL), 684
- Advanced Encryption Standard (AES)
  - DES replacement, 321
  - meeting applications, 694
  - SEDs, 407
  - TLS, 603–604
  - WPA2, 578
  - WPANs, 571
- Advanced Micro Devices (AMD)
  - trade secrets, 149
- Advanced Mobile Phone System (AMPS), 584
- advanced persistent threats (APTs), 135–136
- Advanced Research Project Agency Network (ARPANET) program, 471
- advisory policies, 30
- AE (authenticated encryption), 604
- AEAD (authenticated encryption with additional data), 604
- AES. *See* Advanced Encryption Standard (AES)
- after-action reviews (AARs) in disaster recovery, 869, 1061
- agent based patch management, 904
- agentless patch management, 904
- agents
  - data loss prevention, 273
  - SNMP, 522–523
- aggregation in database systems, 286–287
- Agile methodologies
  - Extreme Programming, 1102
  - Kanban, 1102–1103
  - overview, 1100–1101
  - Scrum, 1101–1102
- agreements
  - disasters recovery, 1047–1048
  - employment, 36–37
  - service level. *See* service level agreements (SLAs)
- AH (Authentication Header) in IPSec, 608
- AIKs (attestation identity keys) in Trusted Platform Modules, 406
- alarms
  - CPTED, 428
  - doors, 444
  - duress codes, 931
  - human-machine interface, 292
  - perimeter security, 803
- ALE (annualized loss expectancy)
  - control selection, 82
  - power backup, 448
  - quantitative risk analysis, 73–75
- algorithms
  - cryptography attacks on, 367–370
  - cryptology, 320–321
  - hashing functions, 351–352
  - patents for, 151
  - public vs. secret, 369
- Align, Plan and Organize (APO) domain in COBIT 2019, 189
- alignment
  - COBIT goals, 188
  - security to business strategy, 13–16, 182, 202
  - strategic, 15–16

- allow lists in IDS/IPS, 968–969
- alternate category in PACE plans, 1057
- always invoked property in reference monitors, 766
- always-on VPN, 697
- AMD (Advanced Micro Devices)
  - trade secrets, 149
- amplification DNS attacks, 620
- amplitude
  - analog signals, 644–645
  - multiplexing systems, 544
  - radio signals, 559–560
- AMPS (Advanced Mobile Phone System), 584
- analog transmission, 644–645
- analysis
  - antimalware software, 970
  - application security, 1139
  - forensics investigations, 1016–1018
  - qualitative risk, 72, 76–78
  - quantitative risk, 72–76, 78–79
  - software security, 1144–1145
- Analysis practice in Good Practice Guidelines, 106
- Android Data company, 150
- annualized loss expectancy (ALE)
  - control selection, 82
  - power backup, 448
  - quantitative risk analysis, 73–75
- annualized rate of occurrence (ARO), 74–75
- annunciator systems in CCTV systems, 916
- anomalies, session termination from, 741
- anomaly-based IDS/IPS, 967–968
- antimalware software, 969–972
- anycast addresses in IPv6, 513
- APIs. *See* application programming interfaces (APIs)
- APO (Align, Plan and Organize) domain
  - in COBIT 2019, 189
- apparent power, 671
- appendices in reports, 873
- Apple lawsuit, 151
- appliances, 958
- application errors in risk management, 54
- application layer
  - functions and protocols, 483
  - OSI model, 474–475
- application-level events in audits, 743
- application-level proxies, 953–955, 957
- application programming interfaces (APIs)
  - application layer, 475
  - CASBs, 275–276
  - containers, 298
  - description, 837
  - object-oriented programming, 1126–1128
  - SDNs, 635
  - software libraries, 1132–1133
  - software security, 1132
  - TEE, 409
  - web services, 613
- applications
  - access control, 802
  - connections, 479
  - security testing, 1139–1140
  - whitelisting, 225
- approval by management, 877
- APs (access points)
  - collision domains, 493
  - DSL modems, 683
  - WLANs, 564–565
- APT32, 389
- APTs (advanced persistent threats), 135–136
- architects for software development, 1080
- Architecture Development Method (ADM), 194–195
- architectures. *See* system architectures
- archive bits for backups, 1035
- archives for data, 239–240
- Arnold, Benedict, 319
- ARO (annualized rate of occurrence), 74–75
- ARP (Address Resolution Protocol), 515–517
- ARPANET (Advanced Research Project Agency Network) program, 471
- artifacts in digital forensics, 1020–1021
- ASOR (authoritative system of record), 739
- ASs (autonomous systems), 533
- assemblers, 1118, 1120–1122
- assembly language, 1118, 1120
- assessments
  - audits, 838–844
  - chapter questions, 846–849
  - chapter review, 844–846
  - designing, 814–815
  - disaster recovery plans, 1058
  - overview, 813
  - physical security, 908
  - preventive and detective measures, 945



- assessments (*cont.*)
  - risk. *See* risk assessment
  - Risk Management Framework, 176
  - social engineering, 903
  - software security, 1144–1148
  - strategies, 813–816
  - technical controls. *See* testing
  - validating, 815–816
- assets
  - business impact analysis, 112–115
  - chapter questions, 247–251
  - chapter review, 245–246
  - classification, 219
  - data life cycle. *See* data life cycle
  - digital, 258–259, 261–263
  - information, 214–219
  - inventories, 224–227
  - life cycle, 222–230
  - overview, 213–214
  - ownership, 223
  - physical security, 220–222
  - provisioning, 227–228
  - retention, 228–230
  - valuation, 65–66
- assisted password resets, 738
- associations in misuse case testing, 835
- ASTM International fire resistance ratings, 456
- asymmetric DSL (ADSL), 684
- asymmetric key cryptography, 328
  - Diffie-Hellman algorithm, 337–340
  - overview, 335–337
  - RSA, 340–342
  - summary, 337
  - with symmetric, 346–349
- asynchronous replication, 1039
- asynchronous token devices for one-time passwords, 731
- Asynchronous Transfer Mode (ATM) in WANs, 550–552
- asynchronous transmissions, 645–647
- atbash cryptology, 317–318
- ATM (Asynchronous Transfer Mode) in WANs, 550–552
- atomic execution in trusted execution environments, 410
- atomicity in ACID properties, 286
- attack surface analysis in software development design, 1085
- attack trees in threat modeling, 386–387
- attacks, evolution of, 134–138
- attenuation in cabling, 652
- attestation identity keys (AIKs) in Trusted Platform Modules, 406
- attocells in Li-Fi standard, 568
- attribute-based access control (ABAC)
  - characteristics, 776
  - description, 774
- attribute-value pairs (AVPs) in RADIUS, 792
- attributes
  - LDAP, 749
  - object-oriented programming, 1125
- audience for reports, 872
- audit-reduction tools, 744
- auditors, 25
- audits
  - accountability, 741–742
  - application-level events, 743
  - external, 842–843
  - internal, 840–842
  - overview, 838–840
  - physical security, 929
  - protecting, 744–745
  - reviewing, 743–744
  - software security, 1147
  - strategies, 813–816
  - system-level events, 742
  - third-party, 843–844
  - user-level events, 743
- AUPs (acceptable use policies)
  - software, 226
  - user accounts, 858
  - web proxies, 664
- authenticated encryption (AE), 604
- authenticated encryption with additional data (AEAD), 604
- authentication. *See also* authorization
  - access control and markup languages, 776–781
  - asymmetric key cryptography, 336
  - biometric. *See* biometric authentication
  - cryptosystems, 323
  - description, 716
  - Diameter, 794–795
  - 802.11, 580

- factors, 718–719
  - Internet of Things, 306
  - Kerberos, 785–788
  - knowledge-based, 720–723
  - network sockets, 703
  - ownership-based, 729–734
  - quorum, 34
  - race conditions, 717
  - VPNs, 697–699
  - Authentication Header (AH) in IPSec, 608
  - authenticators in Kerberos, 786–787
  - authenticity, 6
  - authoritative name servers in DNS, 525
  - authoritative system of record (ASOR), 739
  - authority
    - disaster recovery goals, 1054
    - URLs, 613
  - authorization. *See also* authentication
    - ABAC, 774
    - access control and markup languages, 776–781
    - cryptosystems, 324
    - DAC, 766–768
    - data loss prevention, 267, 271
    - description, 716
    - Diameter, 795
    - e-mail, 624
    - IP telephony, 692
    - Kerberos, 784–789
    - MAC, 768–771
    - OAuth, 782–783
    - OpenID Connect, 783–784
    - overview, 765–766
    - race conditions, 717
    - RB-RBAC, 774
    - risk-based access control, 775–776
    - Risk Management Framework, 176
    - role-based access control, 771–773
  - authorization code flow in OIDC, 784
  - authorization creep
    - description, 395
    - privileged accounts, 889
    - role changes, 799
    - user accounts, 859
  - authorization servers in OAuth, 782
  - auto iris lenses in CCTV systems, 915
  - automated risk analysis methods, 73
  - automated scanning of devices, 226
  - automated tests in software
    - development, 1091
  - automatic tunneling in IPv6, 514
  - automation
    - backups, 863
    - configuration management, 895
    - HMIs, 292
    - SOAR, 980
    - virtualization, 861
    - ZigBee, 571
  - autonomous systems (ASs), 533
  - availability
    - business continuity, 103
    - business continuity planning, 1067–1070
    - CIA triad, 7–8
    - disaster recovery, 1049–1053
    - fault tolerance and system resilience, 1051
    - high, 1050–1053
    - overview, 6
    - quality of service, 1050–1051
  - available bit rate (ABR) in ATM, 551
  - avalanche effect in symmetric key cryptography, 332
  - avoidance risk strategy
    - ISO/IEC 27005, 178
    - overview, 79
  - AVPs (attribute-value pairs) in RADIUS, 792
  - awareness programs
    - content reviews, 43
    - culture factors, 867
    - data protection, 867
    - disaster recovery plans, 1060–1061
    - effectiveness evaluation, 43–44
    - employees, 266
    - goals, 40
    - methods and techniques, 40–44
    - online safety, 866–867
    - overview, 863–864
    - personnel, 930–931
    - social engineering, 864–866
  - AXELOS, 196
- ## B
- B channels in ISDN, 686
  - B2B (business-to-business) transactions in SAML, 780
  - B2C (business-to-consumer) transactions in SAML, 780

- back doors in software development, 1091
- back-off algorithm in CSMA, 491
- background checks in candidate screening and hiring, 35–36
- background elements in reports, 873
- backup administrators, 1035
- backup lighting, 912
- backups
  - vs. archives, 239–240
  - business continuity planning, 1069–1070
  - data loss prevention, 269
  - digital asset management, 261–262
  - electric power, 448–450, 671
  - facilities, 1040–1041
  - hierarchical storage management, 898–899
  - overview, 1034–1037
  - protecting, 896–899
  - restoring, 1037, 1041–1042
  - strategies, 1037–1040
  - verification, 860–862
- BAI (Build, Acquire and Implement) domain in COBIT 2019, 189
- balanced security, 7–8
- bandwidth
  - ATM, 550
  - cable modems, 686–687
  - cabling, 654–655
  - coaxial cable, 649
  - dedicated links, 541–542
  - distribution facilities, 446
  - DSL, 683–684
  - frame relay, 547–548
  - ISDN, 685–686
  - optical carriers, 543
  - proxy servers, 664
  - PVCs, 549
  - QoS, 551–552, 1050
  - satellite communications, 588
  - server-based systems, 300
  - switches, 658
  - unmanaged patching threat, 904
  - VoIP, 688
  - WANs, 543
- barriers in physical security, 908
- BAS (breach and attack simulations), 828
- baseband transmission, 647–648
- Baseline Privacy Interface/Security (BPI/SEC) specifications, 687
- baselines, 31–32
  - anomaly-based IDS/IPS, 968
  - configuration management, 894
  - ISO/IEC 27004, 852
- Basic CIS controls, 187
- Basic Rate Interface (BRI) ISDN, 685–686
- bastion hosts, 965
- BC. *See* business continuity (BC)
- BCM (business continuity management), 102–105
  - enterprise security program, 106–108
  - Professional Practices for Business Continuity Management, 106
- BCP. *See* business continuity planning (BCP)
- beaconing in Token Ring, 496
- beamforming, 567
- behavior blocking in antimalware software, 970–971
- behavioral biometric authentication, 724
- behavioral model for software development design, 1084
- Bell, Alexander Graham, 681
- Bell-LaPadula model, 398–399, 403
- benches, 431
- Berners-Lee, Tim, 253
- best-effort protocols, 503
- best-effort service in QoS, 551
- best practices in business continuity, 104–106
- BGP (Border Gateway Protocol), 536–537
- BIA. *See* business impact analysis (BIA)
- Biba model, 399–400, 403
- big data, retaining, 235
- biometric authentication, 727
  - facial scans, 728
  - fingerprints, 726
  - hand geometry, 727
  - hand topography, 728–729
  - iris scans, 727
  - issues and concerns, 729
  - keystroke dynamics, 728
  - overview, 723–726
  - retina scans, 727
  - signature dynamics, 727–728
  - voice prints, 728
- birthday attacks, 353–354
- BISDN (Broadband ISDN), 685
- bitcoin, 307
- BitTorrent protocol, 149, 307

- black box testing, 826
- black holes, 535, 975
- blacklisting in IDS/IPS, 968–969
- blackouts, 451
- blind penetration testing, 825–826
- block ciphers, 330–333
- Bluejacking, 573
- blueprints in frameworks, 201–203
- Bluesnarfing, 573
- Bluetooth wireless technology, 572–573
- board members, risk reporting for, 94–95
- bollards, 429, 910–911
- BOOTP (Bootstrap Protocol), 519
- Border Gateway Protocol (BGP), 536–537
- botnets, 134
- bots, 134
- boundary conditions in interface testing, 837
- BPC (business process compromise attacks, 59–60
- BPI/SEC (Baseline Privacy Interface/Security) specifications, 687
- branches in tabletop exercises, 1063
- brand issues in disaster recovery, 1054
- BrandScope attacks, 257
- Brazil, General Personal Data Protection Law in, 144
- breach and attack simulations (BAS), 828
- breaches. *See* data breaches
- Brewer and Nash model, 402–403
- BRI (Basic Rate Interface) ISDN, 685–686
- bridges
  - characteristics, 665
  - forwarding tables, 656–657
  - overview, 656
  - vs. routers, 657
- bring your own devices (BYOD), 220
- Broadband ISDN (BISDN), 685
- broadband transmission vs. baseband, 647–648
- broadband wireless access, 569
- broadcast domains in medium access control, 492–494
- broadcast storms in bridges, 656
- broadcast transmission in local area networks, 499–500
- Broken Windows*, 433
- brownouts, 451
- brute-force attacks
  - cryptography, 325, 368
  - passwords, 721
- BSA (Business Software Alliance), 154, 226
- Budapest Convention, 139
- buffer overflows
  - description, 819
  - software development, 1089–1090
- buffers, emulation, 970
- Build, Acquire and Implement (BAI) domain in COBIT 2019, 189
- building codes, 436–437
- bulletproof doors, 440
- bump keys, 924
- bus encryption, 407–408
- bus topology, 487–488
- business continuity (BC)
  - BCP life cycle, 1065–1067
  - business impact analysis, 108–115
  - description, 1030
  - enterprise security program, 106–108
  - overview, 101–104, 867–869, 1065
  - standards and best practices, 104–106
- Business Continuity Institute, Good Practice Guidelines, 105–106
- business continuity management (BCM), 102–105
  - enterprise security program, 106–108
  - Professional Practices for Business Continuity Management, 106
- business continuity planning (BCP), 101–105
  - end-user environment, 1071
  - enterprise security program, 108
  - hardware backups, 1069–1070
  - information systems availability, 1067–1070
  - life cycle, 1065–1067
  - overview, 107, 1065
  - storing, 1042
  - teams, 1030
- business critical data in disaster recovery, 1032
- business enablement, 16
- business entry rule in evidence admissibility, 1014

- business impact analysis (BIA), 104–105
  - asset value, 112–115
  - disaster recovery, 1032
  - overview, 108–109
  - risk assessment, 109–112
  - steps, 112
- business process compromise (BPC) attacks, 59–60
- business process recovery, 1033–1034
- Business Software Alliance (BSA), 154, 226
- business strategy, aligning security to, 13–16
- business-to-business (B2B) transactions
  - in SAML, 780
- business-to-consumer (B2C) transactions
  - in SAML, 780
- business unit leads on incident response teams, 1001
- business units in incident notifications, 1004
- BYE messages in SIP, 689–690
- BYOD (bring your own devices), 220
- bytecode in Java programming language, 1122–1123

## C

- C programming language, 1121–1122
- cable modems, 686–687
- cable traps, 921
- cabling
  - bandwidth and throughput, 654–655
  - coaxial cable, 649
  - fiber-optic cable, 650–651
  - forensics field kits, 1015
  - overview, 648
  - problems, 651–653
  - twisted-pair cabling, 649–650
- CABs (change advisory boards)
  - policies for, 891
  - purpose, 93
  - software development tools, 1138
- cache poisoning, ARP table, 516–517
- Caesar, Julius, 318
- Caesar cipher, 318–319
- California Consumer Privacy Act (CCPA), 141–142
- call-processing managers, 688
- call trees in disaster recovery plans, 1056
- cameras in CCTV systems, 916
- CAN (Controller Area Network) bus, 627
- Canada, Personal Information Protection and Electronic Documents Act in, 147
- Capability Maturity Model (CMM), 197–199
- Capability Maturity Model Integration (CMMI), 1107–1109
- capacitance detectors, 927
- CAPTCHA data, 723
- card badge readers, 925
- care-of addresses in mobile IP, 793
- carrier sense multiple access (CSMA), 490–491
- carrier sense multiple access with collision avoidance (CSMA/CA), 491
- carrier sense multiple access with collision detection (CSMA/CD), 491
- carriers in steganography, 265
- CART acronym in threat intelligence, 941
- CAs (certificate authorities), 360–362
- CASBs (cloud access security brokers), 275–276
- cascading errors, 62
- CASE (computer-aided software engineering) tools, 1087
- catastrophes, 1043
- categorize step in Risk Management Framework, 174–175
- CBC-MAC (CCM), 578
- CBEST standard, 156
- CBKE (Certificate-Based Key Establishment) protocol, 572
- CBR (constant bit rate) in ATM, 551
- CCDs (charged-coupled devices), 914
- CCM (CBC-MAC), 578
- CCPA (California Consumer Privacy Act), 141–142
- CCTV (closed-circuit TV) systems, 913–916
- CD (continuous delivery) in software security, 1140–1141
- CDDI (Copper Distributed Data Interface), 497
- CDIs (constrained data items) in Clark-Wilson model, 400
- CDMA (code division multiple access), 584–585
- CDNs (content distribution networks), 308, 674

- ceilings
  - considerations, 437
  - dropped, 442
  - RFI issues, 450
- cell suppression in database systems, 288
- Center for Internet Security (CIS) framework
  - CIS Controls Measures and Metrics document, 92
  - security controls, 172, 185–187
- centralized patch management, 904–905
- Centripetal Networks, 151
- CEOs (chief executive officers), 19–21
- CER (crossover error rate) in biometric authentication, 724–725
- CERT (Computer Emergency Response Team), 993
- CERT Advisory for privacy issues, 1014
- CERT/CC (Computer Emergency Response Team Coordination Center), 901
- certificate authorities (CAs), 360–362
- Certificate-Based Key Establishment (CBKE) protocol, 572
- certificate revocation lists (CRLs), 361–362
- certificates in PKI, 359–360
- certifications, 40–41
- CFOs (chief financial officers), 19–20
- chain of custody for evidence, 1010–1011
- Challenge Handshake Authentication Protocol (CHAP), 698
- change
  - data loss prevention for, 270
  - digital asset management, 262
  - monitoring, 92–93
- change advisory boards (CABs)
  - policies for, 891
  - purpose, 93
  - software development tools, 1138
- change control analysts, 24
- change management, 891
  - vs. configuration management, 895
  - documentation, 893
  - practices, 891–892
  - runbooks, 1006
  - software development, 1092–1094
  - software security, 1145
- change management boards, 223
- channel service unit/data service unit (CSU/DSU), 543–545
- channels
  - access points, 565
  - for attacks, 474
- CHAP (Challenge Handshake Authentication Protocol), 698
- charged-coupled devices (CCDs), 914
- Check phase in Plan-Do-Check-Act loop, 875
- checkers, password, 722
- checklist tests in disaster recovery plans, 1062–1063
- chemical fire extinguishers, 459
- chests for data protection, 222
- Cheyenne Mountain complex, 436
- chief executive officers (CEOs), 19–21
- chief financial officers (CFOs), 19–20
- chief human resources officers (CHROs), 990
- chief information officers (CIOs), 19–21, 990
- chief information security officers (CISOs)
  - IMPs, 990
  - incident notifications, 1004
  - incident response teams, 1001
  - role, 22
- chief operations officers (COOs), 990
- chief privacy officers (CPOs), 21
- chief security officers (CSOs), 22
- Chinese Remainder Theorem (RSA-CRT), 372
- Chinese Wall model, 402–403
- chipping code in DSSS, 562
- chips in DSSS, 562
- chosen-ciphertext attacks, 369
- chosen-plaintext attacks, 368–369
- CHROs (chief human resources officers), 990
- CI (continuous integration) in software security, 1140–1141
- CIA triad, 7–8
- CIDR (classless interdomain routing), 512
- CIOs (chief information officers), 19–21, 990
- cipher locks, 920–921
- ciphers in cryptology, 318–321
- ciphertext-only attacks, 368
- CIR (committed information rate) in frame relay, 547–548
- circuit-level proxies, 953–957
- circuit switching in WANs, 545–547
- circumventing locks, 922–924

- CIS (Center for Internet Security) framework
  - CIS Controls Measures and Metrics document, 92
  - security controls, 172, 185–187
- Cisco Systems, 151
- CISOs. *See* chief information security officers (CISOs)
- civil investigations, 162
- civil law, 126–129
- Clark-Wilson model, 400, 403
- classes
  - IP addresses, 510
  - object-oriented programming, 1125–1127
- classification
  - artificial intelligence tools, 977
  - data retention, 236
  - incidents, 1002–1003
  - information, 215–219
- classless interdomain routing (CIDR), 512
- classless IP addresses, 512
- clean desk policy, 442–443
- cleanroom methodology in software development, 1105
- clearing media, 259
- client-based systems, 284
- client/server systems, 284
- clipping levels for failed logon attempts, 721
- close stage in change management, 892
- CLOSE-WAIT state in TCP connections, 951
- closed-circuit TV (CCTV) systems, 913–916
- CLOSING state in TCP connections, 951
- cloud access security brokers (CASBs), 275–276
- cloud-based systems
  - asset provisioning, 228
  - backups, 1038
  - deployment models, 305
  - FIM systems, 756
  - frame relay, 548
  - IaaS, 304
  - overview, 301–302
  - PaaS, 302–304
  - SaaS, 302–303
  - XaaS, 304–305
- clustered servers in quality of service, 1051
- clustering for artificial intelligence tools, 978
- CM. *See* configuration management (CM)
- CMDB (configuration management database), 895
- CMF (collection management framework)
  - forensics investigations, 1016–1017
  - logs, 978
  - threat intelligence, 942
- CMM (Capability Maturity Model), 197–199
- CMMI (Capability Maturity Model Integration), 1107–1109
- CO<sub>2</sub> fire suppression, 458
- coaxial cable, 649
- COBIT 2019 framework, 172, 187–189
- code and coding
  - bloat, 833
  - obfuscation, 905
  - repositories, 1143–1144
  - reviews, 833–834
  - secure practices, 1134–1136
  - testing, 834–835
- code division multiple access (CDMA), 584–585
- code law, 126
- Code of Ethics, 44–45
- Codecov platform, 1141
- CoE (Council of Europe), 139
- cognitive passwords, 723
- cohesion in software, 1130–1132
- COI (community of interest) as threat data source, 943
- cold sites in disaster recovery, 1045–1047
- collection
  - data, 231–232
  - evidence, 1010–1012
- Collection Limitation Principle in OECD, 142
- collection management framework (CMF)
  - forensics investigations, 1016–1017
  - logs, 978
  - threat intelligence, 942
- collision free hashing algorithms, 351–352
- collisions
  - CSMA, 490
  - hashing functions, 353
  - medium access control, 492–494
- collusion, 34
- COM domain in DNS, 527
- combi smart cards, 734
- combination locks, 920
- Command and Control
  - Cyber Kill Chain model, 388, 994
  - MITRE ATT&CK framework, 389



- commercial off-the-shelf (COTS) software
  - description, 153
  - security concerns, 1146
- committed information rate (CIR) in frame relay, 547–548
- common controls in Risk Management Framework, 175
- common law, 126–130
- Common Weakness Enumeration (CWE) initiative, 1088
- communication
  - audit results, 839–840
  - in disaster recovery plans, 1056–1057
  - employees, 266
  - object-oriented programming, 1126
- communications channels
  - chapter questions, 709–712
  - chapter review, 707–709
  - data, 702–704
  - multimedia collaboration, 693–696
  - overview, 681
  - remote access, 696–702
  - third-party connectivity, 705–706
  - virtualized networks, 704–705
  - voice. *See* voice communications
- community clouds, 305
- community of interest (COI) as threat data source, 943
- community strings in SNMP, 522–524
- comparability of security metrics, 854–855
- compartmentalizing information in forensics investigation interviews, 1019
- compensating controls in risk responses, 85, 87–88
- compiled code, software escrow for, 1143
- compilers, 1119–1122
- complete characteristic of threat intelligence, 941
- complexities in cybercrimes, 132–134
- compliance
  - audits, 844
  - chapter questions, 165–169
  - chapter review, 162–165
  - checks, 838
  - cybercrimes, 130–139
  - data breaches, 139–147
  - identity and access, 796–797
  - investigation requirements, 161–162
  - laws and regulations, 125–130
  - liability and ramifications, 158–161
  - licensing and intellectual property requirements, 147–154
  - monitoring, 93–94
  - overview, 125
  - policies, 39–40
  - requirements, 155–161
- compromise assessments, 17
- computer-aided software engineering (CASE) tools, 1087
- computer-assisted crimes, 130–131
- Computer Emergency Response Team (CERT), 993
- Computer Emergency Response Team Coordination Center (CERT/CC), 901
- Computer Ethics Institute, 45–46
- “computer is incidental” crimes, 130–131
- computer surveillance, 1020
- computer system connections, 479
- computer-targeted crimes, 130–131
- concentrators, 655
- concurrency management in software, 1142
- conference call bridges in H.323, 689
- confidential classification level, 216–217
- confidentiality
  - asymmetric key cryptography, 336
  - audit logs, 745
  - Bell-LaPadula model, 398
  - business continuity, 102–103
  - CIA triad, 8, 64
  - cryptosystems, 323–324, 330
  - customer relations, 174–175
  - DNS over HTTPS, 621
  - forensics investigation interviews, 1019
  - overview, 4–5
  - TLS, 602
  - VPNs, 605
- configuration management (CM)
  - automation, 895
  - baselining, 894
  - vs. change management, 895
  - identity and access, 799
  - overview, 893–894
  - preventive and detective measures, 944
  - provisioning, 894–895
  - secure software, 1142
  - unmanaged patching threat, 904



- configuration management database (CMDB), 895
- confusion in symmetric key cryptography, 331
- congestion
  - TCP vs. UDP, 503, 506
  - throughput, 654
- connection-oriented protocols
  - description, 479
  - TCP, 503–504
- connectionless protocols
  - description, 479
  - UDP, 503–504
- connections in TCP vs. UDP, 506
- connectivity for federated identity, 754–755
- consent provision in GDPR, 144–145
- consistency in ACID properties, 286
- constant bit rate (CBR) in ATM, 551
- constrained data items (CDIs) in Clark-Wilson model, 400
- construction issues, 436–439
- consultants, 39
- consumer-grade products for meeting applications, 694
- contact smart cards, 733
- contactless smart cards, 733–734
- containerization, 298–299
- content-dependent access control in database systems, 287
- content distribution networks (CDNs), 308, 674
- content reviews, periodic, 43
- context-dependent access control for database systems, 287–288
- context in ABAC, 774
- contingency category in PACE plans, 1057
- contingency strategies in business continuity, 104–105
- contingency suppliers in disaster recovery, 1046
- continuous delivery (CD) in software security, 1140–1141
- continuous improvement in risk management, 95–96
- continuous integration (CI) in software security, 1140–1141
- continuous lighting, 912
- continuous monitoring, 981–982
- contractors, 39
- contractual requirements compliance, 156–158
- control planes in SDNs, 633–634
- control zones, 803
- controlled unclassified data, 216–217
- Controller Area Network (CAN) bus, 627
- controllers, data, 244
- controls
  - assessments. *See* testing
  - CPTED, 430–431
  - data states, 254–258
  - defined, 9
  - digital asset management, 261–262
  - frameworks, 172, 183–189
  - overview, 253–254
  - preventive and detective measures, 944
  - scoping and tailoring, 258
  - standards, 258
  - threat modeling, 387
- controls for risk response
  - assessments, 88–91
  - selection, 82–83
  - types, 83–88
- controls for secure software
  - application testing, 1139–1140
  - code repositories, 1143–1144
  - continuous integration and delivery, 1140–1141
  - development platforms, 1137–1138
  - overview, 1136–1137
  - SOAR, 1141–1142
  - software configuration management, 1142
  - tool sets, 1138
- controls for site and facilities
  - data processing facilities, 443–446
  - distribution facilities, 446–447
  - environmental issues, 461
  - fire safety, 454–460
  - storage facilities, 447–448
  - utilities, 448–454
  - work area security, 441–443
- Convention on Cybercrime, 139
- converged protocols, 627–628
- cookies for web services, 613
- coordinators in WPANs, 570
- COOs (chief operations officers), 990
- copper cable, 649–650
- Copper Distributed Data Interface (CDDI), 497
- Copyright Directive, 155

- copyrights, 149–150
- core RBAC, 772
- corrective controls in risk response, 85, 87
- cost approach in executive summaries, 874
- cost/benefit comparisons in risk assessment, 64, 82
- costs
  - outsourced security services, 974
  - smart cards, 734
- COTS (commercial off-the-shelf) software
  - description, 153
  - security concerns, 1146
- Council of Europe (CoE), 139
- Counter Mode Cipher Block Chaining Message Authentication Code Protocol, 578
- countermeasures
  - defined, 9
  - risk responses, 81–83
- coupling in software, 1130–1132
- coverage for backups, 863
- covert channels, 401
- covert timing channels, 401
- CPOs (chief privacy officers), 21
- CPTED. *See* Crime Prevention Through Environmental Design (CPTED)
- crackers for passwords, 722
- create, read, update, and delete (CRUD)
  - actions for database systems, 285–287
- credential management
  - accountability, 741–745
  - just-in-time access, 738
  - overview, 736
  - password managers, 736–737
  - password resets, 737–738
  - password synchronization, 737
  - profile updates, 740
  - registration and proofing of identity, 738–740
  - session management, 740–741
  - unmanaged patching threat, 904
- Crime Prevention Through Environmental Design (CPTED)
  - landscaping, 908
  - maintenance, 433
  - natural access control, 428–431
  - natural surveillance, 431
  - overview, 427–428
  - territorial reinforcement, 431–432
- crimes. *See also* incidents
  - crime scene control, 1010
  - detection goals, 424
  - evidence collection and handling, 1008
  - incident investigations, 1006–1008
  - incident response, 992
  - investigation requirements, 162
- criminal law system, 127, 129
- critical data backups, 1037
- criticality of data, 215
- criticality values in disaster recovery, 1032
- CRLs (certificate revocation lists), 361–362
- cross-certification, 361
- cross-sectional photoelectric cells, 927
- crossover error rate (CER) in biometric authentication, 724–725
- crosstalk in cabling, 653
- CRUD (create, read, update, and delete)
  - actions for database systems, 285–287
- cryptanalysis, 317
- cryptographic hash chaining, 831
- cryptology. *See also* encryption
  - asymmetric key, 335–342
  - attacks against, 367–375
  - chapter questions, 379–383
  - chapter review, 375–378
  - cryptosystems, 323–325
  - definitions and concepts, 321–323
  - ECC, 342–343
  - hardware vs. software systems, 602
  - history, 317–321
  - hybrid encryption methods, 346–350
  - integrity, 351–358
  - IP telephony, 692
  - Kerckhoffs' Principle, 324–325
  - life cycle, 328
  - methods overview, 328
  - one-time pads, 325–328
  - overview, 317
  - PKI, 359–367
  - quantum, 344–346
  - symmetric key, 329–335
- cryptoprocessors for bus encryption, 408
- cryptosystems
  - components, 323–324
  - description, 321
  - strength, 325

- cryptovariables, 322
- CSMA (carrier sense multiple access), 490–491
- CSMA/CA (carrier sense multiple access with collision avoidance), 491
- CSMA/CD (carrier sense multiple access with collision detection), 491
- CSOs (chief security officers), 22
- CSU/DSU (channel service unit/data service unit), 543–545
- culture
  - data prevention strategies, 269
  - DevOps, 1104
  - employee matches, 35
  - internal audits, 841
  - risk analysis teams, 76, 78
  - security awareness, 867
- current in electrical power, 670
- custodians, data, 244
- customary law system, 128
- customers
  - confidentiality for, 174–175
  - incident notifications to, 1004
- CWE (Common Weakness Enumeration) initiative, 1088
- Cyber Kill Chain framework, 387–389, 994–995
- cyber-physical systems, 306
- cybercrimes and data breaches
  - common schemes, 137
  - complexities, 132–134
  - evolution of attacks, 134–138
  - international issues, 138–139
  - overview, 130–132
- cybercriminals, 60
- cybersecurity analysts
  - incident response teams, 1001
  - tasks and responsibilities, 886
- Cybersecurity Framework, 172, 182
- cybersecurity governance
  - aligning security to business strategy, 13–16
  - authenticity, 6
  - availability, 6
  - balanced security, 7–8
  - baselines, 31–32
  - chapter questions, 48–52
  - chapter review, 46–48
  - concepts and terms, 4–10

- confidentiality, 5
- education and training, 40–44
- guidelines, 32
- implementation, 32–33
- integrity, 5–6
- miscellaneous terms, 8–10
- nonrepudiation, 6–7
- organizational processes, 17–18
- organizational roles and responsibilities, 18–25
- overview, 3–4
- personnel security, 33–40
- principles, 10–12
- procedures, 32
- professional ethics, 44–46
- security overview, 25–27
- security policies, 27–29
- standards, 29–31
- cyberthreat hunting, 943

## D

- D-AMPS (Digital AMPS), 584
- D channels in ISDN, 686
- DAC (discretionary access control)
  - challenges, 768
  - characteristics, 776
  - overview, 766–767
- DACs (dual-attached concentrators)
  - in FDDI, 498
- damage assessment in disaster recovery plans, 1058
- DASs (data acquisition servers)
  - in SCADA systems, 294
- DASs (dual-attachment stations)
  - in FDDI, 498
- DAST (dynamic application security testing), 1139
- data
  - acquisition, 230
  - archival, 239–240
  - backups, 861–862, 1034–1041
  - classification, 215–216
  - collection, 231–232
  - destruction, 240–244
  - roles, 244–245
  - sharing, 238–239
  - storage, 232–233
  - use, 237–238

- data acquisition servers (DASs) in SCADA systems, 294
- data analysts, 24
- data at rest
  - description, 59
  - overview, 254–255
- data breaches
  - Codecov, 1141
  - European Union Laws, 142–144
  - GDPR, 144
  - import/export controls, 145–146
  - overview, 139–141
  - PII, 140–141
  - privacy, 147
  - transborder data flow, 146–147
  - U.S. laws, 141–142
- data communications, 702
  - application layer, 474–475
  - data link layer, 480–483
  - functions and protocols, 483–485
  - layers together, 485–487
  - network layer, 480
  - network reference models, 470–471
  - network sockets, 703
  - overview, 469–470
  - physical layer, 483
  - presentation layer, 475–476
  - protocols, 471–474
  - remote procedure calls, 703–704
  - session layer, 477–478
  - transport layer, 479–480
- data controllers in GDPR, 143
- data custodians, 23
- data diodes, 293, 831
- Data Encryption Standard (DES), 321
- data flows in data loss prevention, 268–269
- data hiding in object-oriented programming, 1128
- data historians, 293
- data in motion/transit
  - description, 59
  - overview, 254–256
- data in use
  - description, 59
  - overview, 254, 256–258
- data leaks, 267
- data life cycle
  - data acquisition, 230
  - data archival, 239–240
  - data collection, 231–232
  - data destruction, 240–244
  - data loss prevention, 269
  - data retention, 233–236
  - data roles, 244–245
  - data sharing, 238–239
  - data storage, 232–233
  - data use, 237–238
  - e-discovery, 236–237
  - overview, 230
- data link layer
  - functions and protocols, 484–485
  - OSI model, 480–483
  - protocols, 646
- data localization laws, 146–147, 232
- data loss prevention (DLP)
  - approaches, 267
  - awareness programs, 867
  - data flows, 268–269
  - endpoint, 273–274
  - hybrid, 274
  - inventories, 267–268
  - network, 272–273
  - overview, 265–267
  - protection strategies, 269–271
  - SOAR, 1142
- Data-Over-Cable Service Interface Specifications (DOCSIS), 687
- data owners, 22–23
- data processing facilities, 443–446
- data processors in GDPR, 143
- Data Protection Directive (DPD), 143
- data protection methods
  - cloud access security brokers, 275–276
  - data loss prevention, 265–274
  - digital asset management, 261–263
  - Digital Rights Management, 263–265
  - overview, 258–261
- Data Protection Officers (DPOs)
  - in GDPR, 144
- Data Quality Principle in OECD, 142
- data retention
  - overview, 233
  - policies, 234–236

- data security
  - chapter questions, 277–279
  - chapter review, 276–277
  - controls, 253–258
  - overview, 253
  - protection methods. *See* data protection methods
  - supply chain risk management, 100
- data sovereignty laws, 232
- data states in controls, 254–258
- data structures in TCP, 509
- data subjects in GDPR, 143
- database management systems (DBMSs), 285–286
- database systems, 285
  - ACID properties, 286
  - backups, 861
  - directory services, 747
  - securing, 286–288
- dating evidence, 1010
- DBMSs (database management systems), 285–286
- DCs (domain controllers) in directory services, 747–748
- DCSs (distributed control systems), 290, 293
- DDoS (distributed denial-of-service) attacks
  - CDNs for, 674
  - DNS, 619–620
  - PaaS for, 303
- DDR (dial-on-demand routing), 686
- decision stage in forensics investigations, 1016–1017
- decommissioning assets, 229–230
- dedicated lines for WANs, 541–543, 552
- defaults
  - network, 598
  - secure, 396–397, 422
  - third-party connectivity, 706
  - web services, 611
- defects per KLOC, 395
- defense in depth
  - controls for, 84
  - design principle, 390–392
  - HTTPS, 614
  - network security, 598
  - physical security, 906
  - site and facility security, 419
  - third-party connectivity, 706
- deferred commitment in object-oriented programming, 1127
- defined level in CMMI, 1108
- degaussing media, 243, 261
- degrees, 40–41
- delay time for locks, 918, 920
- delayed loss risk, 63
- delaying mechanisms in site planning, 424
- Deliver, Service and Support (DSS) domain in COBIT 2019, 189
- delivery stage in Cyber Kill Chain model, 388, 994
- Delphi technique, 77
- deluge water sprinkler systems, 460
- DeMarco, Tom, 283
- demilitarized zones (DMZs) for firewalls
  - dual-homed, 959
  - functions, 945–946
  - screened subnet, 960
- denial-of-service (DoS) attacks
  - STRIDE model, 388
  - wireless communications, 578
- Denis Trojan, 389
- deny lists in IDS/IPS, 968–969
- Department of Defense Architecture Framework (DoDAF), 173, 195
- depositories, protecting, 222
- deprovisioning accounts, 800
- depth of field in CCTV systems, 915
- DES (Data Encryption Standard), 321
- design
  - assessments, 814–815
  - network security, 597–599
  - SDLC, 1080, 1083–1087
  - secure. *See* secure design principles
  - site and facility security, 417–418
  - software. *See* secure software; software development
- Design function in SAMM, 1109
- Design practice in Good Practice Guidelines, 106
- desktop virtualization, 699–701
- destroying data, 240–244
- detection
  - fire safety, 454–457
  - Framework Core, 182
  - incidents, 995–996

- detective controls in risk responses, 85, 87
- deterrent controls in risk responses, 85, 87
- deterrents in physical security, 908
- development platforms for software, 1137–1138
- development stage in SDLC, 1080, 1087–1089
- device locks, 922–923
- devices
  - access control, 802
  - industrial control systems, 291–293
  - IP telephony, 688
  - management software, 226
- DevOps, 1103–1104
- DevSecOps
  - software development, 1104
  - software security, 1144–1145
- DFS (Dynamic Frequency Selection), 574
- DGAs (domain generation algorithms) in DNS, 617–618
- DHCP (Dynamic Host Configuration Protocol)
  - IP addresses, 501
  - overview, 517–519
- DHCPACK packets, 518–519
- DHCPDISCOVER packets, 518–519
- DHCPOFFER packets, 518–519
- DHCPREQUEST packets, 518–519
- diagonal filters in QKD, 344
- diagrams, network, 668–670
- dial-on-demand routing (DDR), 686
- dial-up connections, 684
- dialog management, 477
- Diameter protocol, 793–795
- dictionary attacks on passwords, 721
- differential backups, 1035–1036
- differential cryptanalysis attacks, 369–370
- differential power analysis for smart cards, 735
- differentiated service in QoS, 551
- Diffie, Whitfield, 337–340
- Diffie-Hellman algorithm, 337–340
- diffusion in symmetric key cryptography, 331–332
- digital acquisition of evidence, 1012
- Digital AMPS (D-AMPS), 584
- digital certificates in PKI, 359–360
- digital forensics
  - artifacts, 1020–1021
  - field kits, 1015
  - interviews, 1018–1019
  - investigation techniques, 1016–1018
  - overview, 1015–1016
  - reporting and documenting, 1021–1022
  - surveillance, 1019–1020
  - undercover investigations, 1020
- Digital Millennium Copyright Act (DMCA), 154
- Digital Rights Management (DRM), 263–265
- Digital Signature Algorithm (DSA), 357–358
- Digital Signature Standard (DSS), 352, 357
- digital signatures for message verification, 356–358
- digital subscriber lines (DSLs), 648, 683–685
- digital transmission, 644–645
- digital video recording (DVR) systems, 913
- digital zoom in CCTV systems, 915
- dignitary wrongs category in civil law, 128
- diode lasers in fiber-optic cable, 651
- dips in electric power, 451
- direct-attached storage for backups, 1038
- direct sequence spread spectrum (DSSS), 562–563
- directors of security operations in incident response teams, 1001
- directory permissions, testing, 821
- directory roles in identity management, 748–750
- directory services, 747–748
- disassembly tools in forensics field kits, 1015
- disaster recovery (DR)
  - availability issues, 1049–1053
  - description, 101, 1029–1030
  - incident response, 992
  - overview, 867–869
  - process overview, 1053–1055
- disaster recovery plans (DRPs)
  - assessment, 1058
  - communications, 1056–1057
  - contents, 1055
  - description, 101
  - lessons learned, 1061
  - personnel, 1055–1056
  - responses, 1055
  - restoration, 1058–1060

- disaster recovery plans (DRPs) (*cont.*)
  - storing, 1042
  - testing, 1061–1065
  - training and awareness, 1060–1061
- disasters
  - business continuity, 1065–1071
  - business process recovery, 1033–1034
  - chapter questions, 1073–1076
  - chapter review, 1071–1073
  - data backups, 1034–1041
  - description, 1043
  - documentation, 1041–1042
  - human resources, 1042–1043
  - overview, 1029
  - reciprocal agreements, 1047–1048
  - recovery site strategies, 1043–1047
  - recovery strategies overview, 1029–1033
  - redundant sites, 1048–1049
- disc tumbler locks, 919
- discovery step in penetration testing, 824
- discrepancies in identity, 798–799
- discretionary access control (DAC)
  - challenges, 768
  - characteristics, 776
  - overview, 766–767
- disposal of digital asset management, 262
- disruption prevention in site planning, 424
- distance-vector routing protocols, 535
- distinguished names (DNs)
  - directory services, 747–748
  - LDAP, 749
- distributed control systems (DCSs), 290, 293
- distributed denial-of-service (DDoS) attacks
  - CDNs for, 674
  - DNS, 619–620
  - PaaS for, 303
- Distributed Network Protocol 3 (DNP3), 626–627
- distributed systems, 307–309
- distribution facilities, 446–447
- divestitures, 17–18
- DKIM (DomainKeys Identified Mail), 625
- DLP. *See* data loss prevention (DLP)
- DMARC (Domain-based Message Authentication, Reporting and Conformance) system, 625
- DMCA (Digital Millennium Copyright Act), 154
- DMZs (demilitarized zones) for firewalls
  - dual-homed, 959
  - functions, 945–946
  - screened subnet, 960
- DNP3 (Distributed Network Protocol 3), 626–627
- DNS. *See* Domain Name Service (DNS)
- DNs (distinguished names)
  - directory services, 747–748
  - LDAP, 749
- DNS over HTTPS (DoH), 621
- DNSSEC (DNS security)
  - overview, 620–621
  - threats, 529–531
- Do phase in Plan-Do-Check-Act loop, 875
- DOCSIS (Data-Over-Cable Service Interface Specifications), 687
- documentation
  - audits, 839–840
  - backups, 863
  - change management, 262, 893
  - digital forensics, 1021–1022
  - disaster recovery, 1041–1042
  - forensics field kits, 1015
  - incident response, 992
  - software vulnerability scans, 901
- DoDAF (Department of Defense Architecture Framework), 173, 195
- dogs, 929
- DoH (DNS over HTTPS), 621
- Domain-based Message Authentication, Reporting and Conformance (DMARC) system, 625
- domain controllers (DCs) in directory services, 747–748
- domain generation algorithms (DGAs)
  - in DNS, 617–618
- Domain Name Service (DNS)
  - attack prevention, 617–620
  - DNS over HTTPS, 621
  - DNSSEC, 620–621
  - domains, 526–527
  - filters, 621
  - MITRE ATT&CK framework, 389
  - overview, 524–526, 616
  - resolution components, 527–528
  - splitting, 530
  - threats, 529–531



- DomainKeys Identified Mail (DKIM), 625
  - domains
    - collision and broadcast, 492–494
    - DNS, 526–527
  - doors
    - considerations, 437
    - data processing facilities, 443
    - lock delay feature, 920
    - types, 440–441
  - DoS (denial-of-service) attacks
    - STRIDE model, 388
    - wireless communications, 578
  - double-blind penetration tests, 826
  - double tagging attacks on VLANs, 632
  - downstream liability, 39, 161
  - downstream suppliers in risk management, 98
  - downtime in high availability, 1050
  - DPD (Data Protection Directive), 143
  - DPOs (Data Protection Officers)
    - in GDPR, 144
  - DR. *See* disaster recovery (DR)
  - draft IEEE 802.11i, 576
  - DRI International Institute, Professional Practices for Business Continuity Management, 106
  - drive-by downloads, 865
  - drives, self-encrypting, 407
  - DRM (Digital Rights Management), 263–265
  - dropped ceilings, 442
  - DRPs. *See* disaster recovery plans (DRPs)
  - dry pipe water sprinkler systems, 460
  - DSA (Digital Signature Algorithm), 357–358
  - DSD (dynamic separation of duty)
    - relations, 773
  - DSLAMs (DSL access multiplexers), 683
  - DSLs (digital subscriber lines), 648, 683–685
  - DSS (Deliver, Service and Support) domain in COBIT 2019, 189
  - DSS (Digital Signature Standard), 352, 357
  - DSSS (direct sequence spread spectrum), 562–563
  - dual-attached concentrators (DACs)
    - in FDDI, 498
  - dual-attachment stations (DASs)
    - in FDDI, 498
  - dual control, 34
  - dual-homed firewalls, 959, 963
  - dual-use goods, 145
  - due care issues
    - disaster recovery plans, 1060
    - liability, 158–159
  - due diligence, 158–159
  - dumpster diving, 260–261
  - Dunn, Andy, 885
  - durability in ACID properties, 286
  - duress codes, 931–932
  - Dutch Data Protection Authority, 397
  - DVR (digital video recording)
    - systems, 913
  - Dyn attack, 307
  - dynamic analysis
    - antimalware software, 970
    - application security, 1139
  - dynamic application security testing (DAST), 1139
  - Dynamic Frequency Selection (DFS), 574
  - Dynamic Host Configuration Protocol (DHCP)
    - IP addresses, 501
    - overview, 517–519
  - dynamic mapping in NAT, 532
  - dynamic passwords, 729–732
  - dynamic ports, 507
  - dynamic routing protocols, 534–535
  - dynamic separation of duty (DSD)
    - relations, 773
  - Dyre Trojan, 604
- ## E
- E-carriers for WANs, 542
  - e-discovery, 236–237
  - e-mail
    - authorization, 624
    - DKIM, 625
    - DMARC, 625
    - gateways, 663
    - IMAP, 623–624
    - MIME, 625–626
    - overview, 621–622
    - phishing, 864
    - POP, 623
    - SPF, 624
    - threats, 623
  - E2EE (end-to-end encryption) vs. link encryption, 600–602
  - EAC (electronic access control) tokens, 925



- EAP (Extensible Authentication Protocol)
  - VPNs, 699
  - WPA Enterprise, 577
- EAP and Transport Layer Security (EAP-TLS), 580–581
- EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) authentication framework, 501
- EAP-Tunneled Transport Layer Security (EAP-TTLS), 580
- ECC (elliptic curve cryptography), 328, 342–343
- Economic Espionage Act, 141
- economic wrongs category in civil law, 128
- edge computing systems, 308–309
- EDI (electronic data interchange), 538
- EDLP (endpoint DLP), 273–274
- EDM (Evaluate, Direct and Monitor) domain in COBIT 2019, 189
- EDNS(0) technique in DNS, 620
- EDR. *See* endpoint detection and response (EDR)
- EDRM (Electronic Discovery Reference Model), 237
- EDU domain in DNS, 527
- education. *See* training
- EF (exposure factor), 74
- effectiveness monitoring for risk, 91–92
- egress
  - filtering, 948
  - monitoring, 981
- 80/20 Pareto principle, 179
- 802.1AE standard, 500–501
- 802.1AR standard, 501
- 802.1x standard, 579–581
- 802.11 standard, 565–566, 575–576
- 802.11a standard, 566–567
- 802.11ac standard, 567
- 802.11ax standard, 567–568
- 802.11b standard, 566
- 802.11e standard, 573
- 802.11f standard, 574
- 802.11g standard, 567
- 802.11h standard, 574
- 802.11i standard, 576–578
- 802.11j standard, 574
- 802.11n standard, 567
- 802.11w standard, 578
- 802.15.4 standard, 570–571
- 802.16 standard, 569
- EIGRP (Enhanced Interior Gateway Routing Protocol), 536
- EKs (endorsement keys) in Trusted Platform Modules, 405
- Elastic Stack product, 979
- electric power
  - backup, 448–450
  - considerations, 438
  - fallback plans, 448
  - issues, 450–452
  - overview, 670–672
  - protecting, 452–453
- electrical wires in transmission media, 643
- electromagnetic analysis for smart cards, 735
- electromagnetic interference (EMI)
  - coaxial cable, 649
  - electric power, 450
- electromechanical IDSs, 926
- electronic access control (EAC) tokens, 925
- electronic data interchange (EDI), 538
- Electronic Discovery Reference Model (EDRM), 237
- electronic monitoring of passwords, 721
- electronic vaulting for backups, 1038–1039
- electronically stored information (ESI), 236–237
- elevation of privilege category in STRIDE model, 388
- elliptic curve cryptography (ECC), 328, 342–343
- embedded systems, 306
- Embedding Business Continuity practice in Good Practice Guidelines, 105
- emergency category in PACE plans, 1057
- emergency changes, 892
- emergency management, 931
- emergency response groups, 1057
- emergency response procedures, 868–869
- EMI (electromagnetic interference)
  - coaxial cable, 649
  - electric power, 450
- Emotet Trojan, 604
- employees. *See* personnel safety and security
- emtocells in Li-Fi standard, 568
- emulating services in honeypots, 974
- emulation buffers in antimalware, 970

- Encapsulating Security Payload (ESP), 608
- encapsulation
  - multilayer protocols, 628
  - object-oriented programming, 1127–1128, 1130
  - OSI, 472–473
  - TCP, 509
- encryption. *See also* cryptology
  - bus, 407–408
  - code repositories, 1144
  - data at rest, 255
  - data in motion, 255–256
  - homomorphic, 258
  - hybrid methods, 346–350
  - Internet of Things, 307
  - Kerberos, 785–789
  - link vs. end-to-end encryption, 600–602
  - meeting applications, 694
  - mobile devices, 243
  - network sockets, 703
  - overview, 256–258
  - passwords, 722
- end-of-life (EOL) of assets, 229
- end-of-support (EOS) of assets, 229
- end-to-end encryption (E2EE) vs. link encryption, 600–602
- end-user environment in business continuity planning, 1071
- End User License Agreement (EULA), 153
- endorsement keys (EKs) in Trusted Platform Modules, 405
- endpoint detection and response (EDR)
  - breach attack simulations, 828
  - defense in depth, 391
  - effectiveness monitoring, 91–92
  - HIDSs, 968
  - security operations centers, 940
- endpoint DLP (EDLP), 273–274
- endpoint security, 673–674
- Enhanced Interior Gateway Routing Protocol (EIGRP), 536
- Enhanced Performance Architecture (EPA), 627
- Enigma machine, 320
- ENISA (European Union Agency for Cybersecurity), 106
- enrollment in biometric authentication, 725
- enterprise architecture frameworks
  - military-oriented, 195–196
  - models, 172–173
  - need for, 191–192
  - overview, 189–191
  - The Open Group Architecture Framework, 194–195
  - Zachman Framework, 192–194
- enterprise security architecture
  - description, 13
  - vs. ISMS, 26
- enterprise security program in business continuity management, 106–108
- entry points in physical security, 439–441
- enumeration step in penetration testing, 824
- environmental issues
  - business continuity planning, 1071
  - CPTED, 427–433
  - digital asset management, 262
  - disaster recovery, 1059
  - site and facilities, 461
- Environmental Protection Agency (EPA), 434
- EOL (end-of-life) of assets, 229
- EOS (end-of-support) of assets, 229
- EPA (Enhanced Performance Architecture), 627
- EPA (Environmental Protection Agency), 434
- ephemeral keys in TLS, 604
- ephemeral ports, 507
- equipment malfunction in risk management, 54
- equipment warranty, 672
- erasing media, 259
- escrow, software, 1070, 1143
- ESI (electronically stored information), 236–237
- ESMTP (Extended SMTP), 622
- ESP (Encapsulating Security Payload), 608
- ESTABLISHED state in TCP connections, 951
- Ethernet
  - data link layer, 481–482
  - layer 2 protocol, 494–495
  - local area networks, 499
  - Metro Ethernet, 539–540
  - Token Ring, 495–496

- ethics
    - professional, 44–46
    - vulnerability disclosures, 872
  - EULA (End User License Agreement), 153
  - European Union Agency for Cybersecurity (ENISA), 106
  - European Union Laws, 142–144
  - Evaluate, Direct and Monitor (EDM) domain in COBIT 2019, 189
  - evaluation
    - business impact analysis, 110–112
    - change management procedure, 891
    - framework steps, 201
    - program effectiveness, 43–44
  - Everything as a Service (XaaS), 304–305
  - evidence
    - acquiring, 1012
    - admissibility, 1013–1014
    - collecting, 1008–1012
    - identification guidelines, 1009–1010
    - incident investigations, 1006–1007
    - order of volatility, 1016
    - preserving, 1013
    - storage, 447–448
  - evolution of attacks, 134–138
  - evolutionary prototypes in software development, 1096
  - examination stage in forensics investigations, 1016–1017
  - exception handling, 871
  - executive succession planning, 1043
  - executive summaries in reports, 872–875
  - executives
    - incident notifications for, 1004
    - risk reporting for, 94–95
    - roles, 19–22
  - exercises for disaster recovery plans, 1061–1062
  - exigent circumstances, 1011
  - exploitation
    - Cyber Kill Chain model, 388, 994
    - penetration testing, 824
  - exploratory methodology in software development, 1104
  - exposure, defined, 9
  - exposure factor (EF), 74
  - extended detection and response (XDR)
    - platforms, 968
  - Extended SMTP (ESMTP), 622
  - Extended TACACS (XTACACS), 790–791
  - extended teams in incident response plans, 1000–1001
  - Extensible Access Control Markup Language (XACML), 781
  - Extensible Authentication Protocol (EAP)
    - VPNs, 699
    - WPA Enterprise, 577
  - Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) authentication framework, 501
  - Extensible Markup Language (XML), 615, 777
  - exterior lighting, 911–912
  - exterior routing protocols, 536–537
  - external audits, 842–843
  - external labeling in digital asset management, 263
  - external parties issues in data loss prevention, 267
  - external perimeter security
    - bollards, 910–911
    - fencing, 908–910
    - lighting, 911–912
    - overview, 906–908
    - surveillance devices, 913
    - visual recording devices, 913–916
  - extranets, 537–538
  - Extreme Programming (XP), 1102
- ## F
- Facebook breach, 20
  - facial scans, 728
  - Facilitated Risk Analysis Process (FRAP), 68
  - facilities. *See* site and facility security
  - facility safety officers, 434
  - Factor Analysis of Information Risk (FAIR)
    - framework, 172, 179
  - factors in ISO/IEC 27004, defined, 852
  - fail-safe devices, 931
  - fail safe systems for locks, 921
  - failed logon attempts, 721–723
  - failing securely
    - network security, 598
    - secure design, 396–397
    - site and facility security, 422
    - third-party connectivity, 706
    - web services, 612

- failover capability in quality of service, 1051
- Failure Modes and Effect Analysis (FMEA), 69–71
- FAIR (Factor Analysis of Information Risk) framework, 172, 179
- fairness issue in forensics investigation interviews, 1019
- false acceptance rate (FAR) in biometric authentication, 724–725
- false negatives in anomaly-based IDS/IPS, 967
- false positives in anomaly-based IDS/IPS, 967
- false rejection rate (FRR) in biometric authentication, 724–725
- FAR (false acceptance rate) in biometric authentication, 724–725
- FAST (Federation Against Software Theft), 154
- fault generation attacks on smart cards, 734
- fault injection attacks in cryptography, 372
- fault tolerance in availability, 1051
- fault tree analysis in risk assessment, 71–72
- FCoE (Fibre Channel over Ethernet) protocol, 628–629
- FCS (frame check sequence) numbers in WANs, 546
- FDDI (Fiber Distributed Data Interface) technology, 496–499
- FDDI rings in MANs, 538
- FDE (full-disk encryption), 407
- FDM (frequency-division multiplexing), 544
- FDMA (frequency division multiple access), 584
- Federal Copyright Act, 149–150
- Federal Emergency Management Agency (FEMA), 1054
- Federal Information Processing Standard (FIPS) 140-2, 406–407
- Federal Risk and Authorization Management Program (FedRAMP), 156, 1146
- Federal Rules of Evidence (FRE), 1014
- federated identity management (FIM) systems
  - overview, 752–754
  - with third-party service, 754–756
- Federation Against Software Theft (FAST), 154
- FedRAMP (Federal Risk and Authorization Management Program), 156, 1146
- Feistel, Horst, 332
- FEMA (Federal Emergency Management Agency), 1054
- fencing, 908–910
- FHSS (frequency hopping spread spectrum), 561–563
- Fiber Distributed Data Interface (FDDI) technology, 496–499
- fiber-optic cable, 650–651
- Fibre Channel over Ethernet (FCoE) protocol, 628–629
- field kits for digital forensics, 1015
- field of view in CCTV systems, 913, 915
- fifth-generation (5G) mobile wireless, 586–587
- fifth-generation programming languages, 1119–1120
- file descriptor attacks, 821
- file permissions, 821
- File Transfer Protocol (FTP)
  - application-level proxies, 954
  - sessions, 951
- filters
  - DNS, 621
  - firewalls. *See* firewalls
  - QKD, 344–345
- FIM (federated identity management) systems
  - overview, 752–754
  - with third-party service, 754–756
- FIN-WAIT-1 state in TCP connections, 951
- FIN-WAIT-2 state in TCP connections, 951
- findings in reports, 873
- finances for executive management, 20
- fingerprint detection in antimalware software, 969
- fingerprints, 726
- FIPS (Federal Information Processing Standard) 140-2, 406–407
- fire codes for door placement, 440
- fire detection considerations, 438
- fire extinguishers, 455
- fire prevention, 454
- fire rating for cabling, 653
- fire resistance ratings, 456
- fire-resistant material, 439
- fire safety
  - detection, 454–457
  - overview, 454

- fire sensors, 445
- fire suppression
  - considerations, 438
  - fire types, 458–459
  - heat-activated, 456–457
  - overview, 454, 457–459
  - smoke activated, 456
  - water sprinklers, 459–460
- firewalls
  - appliances, 958
  - architecture, 959–965
  - bastion hosts, 965
  - comparisons, 958
  - configuring, 965–966
  - demilitarized zones, 945–946
  - dual-homed, 959
  - next-generation, 957–958
  - overview, 945–946
  - packet-filtering, 946–949
  - proxy, 952–957
  - screened host, 959–960
  - screened subnet, 960–962
  - stateful, 949–952
  - virtual, 964
- first-generation (1G) mobile wireless, 585–586
- first-generation programming languages, 1118
- five nines availability, 1050
- fixed focal length in CCTV systems, 914–915
- fixed mounting cameras in CCTV systems, 916
- floods, SYN, 508
- flooring considerations, 438
- fluorescent lighting interference, 450
- FMEA (Failure Modes and Effect Analysis), 69–71
- foams for fire suppression, 459
- focal length in CCTV systems, 914–915
- foot-candles
  - CCTV systems, 916
  - lighting, 911
- footprints of satellites, 589
- forensics. *See* digital forensics
- Forrester report, 1134
- forward secrecy in TLS, 604
- forwarding planes in SDNs, 633–634
- forwarding proxies, 663–664
- forwarding tables for bridges, 656–657
- Foundational controls, 187
- Fourth Amendment issues, 1011
- fourth-generation (4G) mobile wireless, 586–587
- fourth-generation programming languages, 1119–1120
- fractional T lines, 542
- fragmentation in firewalls, 948, 965–966
- frame check sequence (FCS) numbers in WANs, 546
- frame relay for WANs, 547–548, 552
- frames
  - description, 483
  - packets, 509
  - TCP, 509
- Framework Core, 182–183
- Framework Profile in Cybersecurity Framework, 182
- frameworks
  - chapter questions, 205–209
  - chapter review, 203–205
  - CIS controls, 185–187
  - CMM, 197–199
  - COBIT 2019, 187–189
  - description, 15
  - enterprise architecture, 189–196
  - information security, 179–189
  - ITIL, 196–197
  - overview, 171–173
  - process steps, 199–203
  - risk, 172–179
  - security controls, 183–189
  - security programs, 180–183
  - Six Sigma, 197
- framing risk, 57
- Franklin, Benjamin, 317
- FRAP (Facilitated Risk Analysis Process), 68
- fraud
  - IP telephony, 692
  - PBX systems, 666
- FRE (Federal Rules of Evidence), 1014
- free space transmission media, 644
- freeware, 153
- frequency analysis attacks in cryptography, 370
- frequency division multiple access (FDMA), 584
- frequency-division multiplexing (FDM), 544

- frequency hopping spread spectrum (FHSS), 561–563
- frequency in wireless signals, 559
- FRR (false rejection rate) in biometric authentication, 724–725
- FTP (File Transfer Protocol)
  - application-level proxies, 954
  - sessions, 951
- full backups, 1035–1036
- full-disk encryption (FDE), 407
- full-duplex
  - session layer, 478
  - TCP, 508
- full-interruption tests in disaster recovery plans, 1064
- full knowledge in penetration testing, 825
- full RBAC, 773
- full tunnels in VPNs, 697
- functional analysis in BIA, 109
- functional model in software development design, 1084
- functional policies, 28
- functional requirements in software development, 1083
- fuzzing in application security testing, 1139–1140

## G

- G.fast standard, 684
- gamification, 42–43
- garbage collectors in programming languages, 1122
- gas lines, 438
- gatekeepers in H.323, 689
- gates, 910
- gateways
  - characteristics, 665
  - H.323, 689
- gauge for fencing, 909
- General Data Protection Regulation (GDPR)
  - compliance monitoring, 93
  - entities, 143–144
  - FIM systems, 754
  - legal systems, 126
  - privacy issues, 147, 158, 397
- general hierarchies in RBAC, 772
- General Personal Data Protection Law, 144
- Generalized Markup Language (GML), 776

- generators, 449–450
- Generic Routing Encapsulation (GRE), 606
- Geneva, Switzerland, QKD in, 346
- geosynchronous satellites, 588–590
- GET methods in HTTP, 614
- Get Out of Jail Free Cards, 824
- glare protection, 912
- glass in data processing facilities, 446
- Glenny, Misha, 939
- Global System for Mobile Communication (GSM), 584
- GML (Generalized Markup Language), 776
- goals
  - audits, 839
  - disaster recovery, 1053–1054
- GOC domain in DNS, 527
- Gold Masters, 225
- Good Practice Guidelines (GPG), 105–106
- Goodman, Marc, 597
- Google trademark case, 150
- governance committees, 18
- Governance function in SAMM, 1109
- governance objectives in COBIT 2019, 189
- governance, risk, and compliance (GRC)
  - programs, 155
- GPG (Good Practice Guidelines), 105–106
- grades of locks, 923
- Graham-Denning model, 402–403
- Gramm-Leach-Bliley Act, 141, 147
- gray box testing, 826
- GRC (governance, risk, and compliance)
  - programs, 155
- GRE (Generic Routing Encapsulation), 606
- Gretzky, Wayne, 997
- groups for separation of duties, 394
- GSM (Global System for Mobile Communication), 584
- guaranteed service in QoS, 551
- Guaranteed Time Slot (GTS) reservations in WPANs, 570
- guards, 928–929
- guests in virtualized systems, 296
- guidelines
  - coding, 1136
  - overview, 32
- Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 142–144

## H

- H.323 standard, 689
- HA (high availability), 1050–1053
- HaaS (Hacking as a Service), 135
- hacking mobile phones, 588
- hacktivists, 61
- Hadnagy, Chris, 902
- HAIPE (High Assurance Internet Protocol Encryptor), 609
- half-duplex mode in session layer, 478
- hand geometry, 727
- hand topography, 728–729
- handling evidence, 1008–1015
- handoffs in 802.11f standard, 574
- handouts for information access control, 801
- handshakes
  - RADIUS, 789
  - session keys, 350
  - SIP, 689–690
  - SSH, 700–701
  - TCP, 508, 949–951
  - TLS, 603
- hardware
  - backups in business continuity planning, 1069–1070
  - cryptography systems, 602
  - electrical power, 670–672
  - operation, 670–672
  - supply chain risk management, 98
  - tracking, 224
- hardware guard in MAC, 770
- hardware reverse engineering in cryptography, 371
- hardware security modules (HSMs), 406–407
- Harrison-Ruzzo-Ullman (HRU) model, 402–404
- hash chaining, 831
- hash MAC (HMAC), 355, 358
- hashing functions
  - algorithms, 351–352
  - attacks against, 353
  - overview, 351
  - passwords, 722
- HDLC (High-level Data Link Control) frames, 550
- headers
  - IPv6, 513–514
  - TCP, 950–951
- Health Information Technology for Economic and Clinical Health (HI-TECH) Act, 141
- Health Insurance Portability and Accountability Act (HIPAA), 147
- hearsay evidence, 1014
- Heartbleed security bug, 257, 370
- heat-activated fire suppression, 456–457
- heating, ventilation, and air conditioning (HVAC)
  - considerations, 438
  - data processing facilities, 446
  - fire suppression, 459
  - overview, 453–454
- heavy timber construction material, 439
- heavyweight methods in software development, 1101
- Hellman, Martin, 337–340
- Hello messages in TLS, 603
- help desk tasks and responsibilities, 886
- heuristic detection in antimalware software, 969, 971
- hexadecimal values, 1121
- HI-TECH (Health Information Technology for Economic and Clinical Health) Act, 141
- hiding data in steganography, 264–265
- HIDSs (host-based intrusion detection systems), 967
- hierarchical RBAC, 772–773
- hierarchical storage management (HSM) for backups, 898–899
- High Assurance Internet Protocol Encryptor (HAIPE), 609
- high availability (HA), 1050–1053
- high coupling in software, 1131–1132
- High-level Data Link Control (HDLC) frames, 550
- high-level languages, 1118–1121
- high-performance computing (HPC) systems, 288–289
- high privacy risk in software development, 1082
- High-Speed Serial Interface (HSSI), 552
- Hinckley, Gordon B., 171
- hints for passwords, 720
- HIPAA (Health Insurance Portability and Accountability Act), 147
- hiring candidates, 35–36
- history of changes, documenting, 262



- HMAC (hash MAC), 355, 358
  - HMI (human-machine interface), 291–294
  - holistic risk management, 54–55
  - hollow-core doors, 440
  - home IP address in mobile IP, 793
  - homomorphic encryption, 258
  - honeyclients, 975
  - honeynets, 975
  - honeypots, 974–976
  - hop devices, 601
  - hop sequences in FHSS, 561–563
  - Hopper, Grace, 851
  - hopping attacks in VLANs, 632
  - horizontal enactment for privacy, 147
  - host addresses in IP addresses, 510
  - host-based intrusion detection systems (HIDSs), 967
  - hostage alarm feature for combination locks, 920
  - HOSTS file in DNS, 528, 530
  - hosts in virtualized systems, 296
  - hot sites
    - disaster recovery, 1044–1046
    - vs. redundant sites, 1049
  - hot washes
    - event debriefing, 869
    - lessons learned, 1061
  - hotel key cards, 921
  - HPC (high-performance computing) systems, 288–289
  - HR (human resources)
    - disasters, 1042–1043
    - proofing of identity, 739
  - HRU (Harrison-Ruzzo-Ullman) model, 402–404
  - HSM (hierarchical storage management) for backups, 898–899
  - HSMs (hardware security modules), 406–407
  - HSSI (High-Speed Serial Interface), 552
  - HTML (Hypertext Markup Language), 776–777
  - HTTP (hypertext transfer protocol), 613–614
  - HTTPS (Hypertext Transfer Protocol Secure), 614
  - hubs, 655–656
  - human interaction in risk management, 54
  - human-machine interface (HMI), 291–294
  - human resource managers on incident response teams, 1001
  - human resources (HR)
    - disasters, 1042–1043
    - proofing of identity, 739
  - human sensors for incident detection, 995
  - human vulnerabilities, 902–903
  - humidity
    - data processing facilities, 446
    - HVAC systems, 453
    - hygrometers, 461
  - HVAC. *See* heating, ventilation, and air conditioning (HVAC)
  - hybrid clouds, 305
  - hybrid controls in Risk Management Framework, 175
  - hybrid data loss prevention, 274
  - hybrid encryption methods, 346
    - asymmetric and symmetric together, 346–349
    - session keys, 349–350
  - hybrid FIM systems, 756
  - hybrid flow in OIDC, 784
  - hybrid RBAC, 773
  - hybrid smart cards, 734
  - hybrid teams for incident response, 991
  - hygrometers, 461
  - Hypertext Markup Language (HTML), 776–777
  - hypertext transfer protocol (HTTP), 613–614
  - Hypertext Transfer Protocol Secure (HTTPS), 614
  - hypervisors in virtual machines, 296–298
- ## I
- IaaS (Infrastructure as a Service), 228, 302, 304
  - IAM (identity and access management), 745
  - ICMP. *See* Internet Control Message Protocol (ICMP)
  - ICSs. *See* industrial control systems (ICSs)
  - ICVs (Integrity Check Values), 501, 575–576
  - IDaaS (Identity as a Service), 754
  - IDC (International Data Corporation), 154
  - identification, 214
    - authentication. *See* authentication
    - credential management, 736–745
    - crime scenes, 1009–1010



- identification (*cont.*)
  - description, 716
  - directory services, 747–750
  - FIM systems, 752–754
  - forensics investigations, 1016–1017
  - identity management, 745–754
  - life cycle of assets, 222–223
  - proofing, 738–740
  - single sign-on, 750–752
- identify function in Framework Core, 182
- identities and access fundamentals
  - access control and markup languages, 776–781
  - authorization. *See* authorization
  - chapter questions, 759–763
  - chapter review, 756–758
  - overview, 715–717
  - remote access control, 789–795
- identity and access management (IAM), 745
  - attribute-based access control, 774
  - authorization. *See* authorization
  - chapter questions, 805–809
  - chapter review, 804–805
  - discretionary access control, 766–768
  - life cycle management, 795–800
  - mandatory access control, 768–771
  - overview, 765
  - physical and logical access, 801–803
  - provisioning life cycle, 795–800
  - risk-based access control, 775–776
  - role-based access control, 771–773
  - rule-based access control, 774
- Identity as a Service (IDaaS), 754
- identity-based access control, 767
- identity management (IdM)
  - directory roles, 748–750
  - directory services, 747–748
  - federated identity management systems, 752–754
  - federated identity with third-party services, 754–756
  - overview, 745–747
  - single sign-on, 750–752
- identity providers (IdPs)
  - OpenID Connect, 783
  - SAML, 780
- identity repositories, 739
- identity stores, 748
- IDEs (integrated development environments)
  - in software development, 1137
- iDevIDs (initial device identities), 501
- IDFs (intermediate distribution facilities), 446–447
- IdPs (identity providers)
  - OpenID Connect, 783
  - SAML, 780
- IDSs. *See* intrusion detection systems (IDSs)
- IEC (International Electrotechnical Commission) 27000 Series, 180–182
- IETF (Internet Engineering Task Force) RFC 4987, SYN flood attacks, 508
- if this, then that (IFTTT) programming rules, 774
- IGMP (Internet Group Management Protocol), 500
- IGP (Interior Gateway Protocol), 533
- IGRP (Interior Gateway Routing Protocol), 536
- IGs (implementation groups) in CIS controls, 187
- IIoT (Industrial Internet of Things) devices, 570
- IKE (Internet Key Exchange), 608
- illogical processing, 62
- illumination in CCTV systems, 913, 916
- images
  - evidence, 1012–1013
  - system, 896
- IMAP (Internet Message Access Protocol), 623–624
- impact in incidents classification, 1002
- implementation
  - change management, 892
  - cybersecurity governance, 32–33
  - data loss prevention, 270–271
  - disaster recovery goals, 1054
  - frameworks, 200
  - Good Practice Guidelines, 106
  - Risk Management Framework, 175–176
  - SAMM, 1109
  - software, 1133
- implementation attacks in cryptography, 370–372
- implementation groups (IGs) in CIS controls, 187
- Implementation Tiers in Cybersecurity Framework, 182

- implicit denies in firewalls, 965
- implicit flow in OIDC, 784
- import/export controls for data breaches, 145–146
- IMPs (incident management policies), 990, 1000
- IMSI (International Mobile Subscriber Identity) catchers, 588
- in-rush current for electric power, 451
- inactivity, session termination from, 741
- incident assessment in site planning, 424
- incident investigations
  - chapter questions, 1024–1027
  - chapter review, 1022–1024
  - digital forensics, 1015–1022
  - evidence collection and handling, 1008–1015
  - law enforcement involvement, 1007
  - motive, opportunity, and means, 1007–1008
  - overview, 1006–1007
  - privacy issues, 1014
- incident management in business continuity, 1066
- incident management policies (IMPs), 990, 1000
- incident responders, tasks and responsibilities, 886
- incident response plans (IRPs)
  - classifications, 1002–1003
  - notifications, 1003–1004
  - operational tasks, 1004–1005
  - overview, 1000
  - roles and responsibilities, 1000–1002
  - runbooks, 1006
- incidents
  - classification, 1002–1003
  - Cyber Kill Chain framework, 994–995
  - detection, 995–996
  - investigations. *See* incident investigations
  - lessons learned, 999–1000
  - management overview, 989–994
  - mitigating, 996–997
  - notifications, 1003–1004
  - operational tasks, 1004–1005
  - overview, 989
  - recovery, 998
  - remediating, 999
  - reporting, 997–998
  - response plans, 1000–1006
  - response teams, 991
  - responses, 996
  - runbooks, 1006
  - supply chain risk management, 100
- incombustible material, 439
- income approach for executive summaries, 874
- incomplete level in CMMI, 1107
- incremental backups, 1036–1037
- Incremental software development, 1096–1097
- incremental testing for federated identity, 755
- indexing for data retention, 236
- indicators in ISO/IEC 27004, 852
- indicators of attack (IOAs), 999
- indicators of compromise (IOCs)
  - incident remediation, 999
  - threat data sources, 942
- Individual Participation Principle in OECD, 142
- industrial control systems (ICSs)
  - devices, 291–293
  - distributed control systems, 293
  - overview, 289–290
  - SCADA systems, 294
  - security, 294–295
- Industrial Internet of Things (IIoT) devices, 570
- industrial, scientific, and medical (ISM) bands, 565–566
- industry standards, compliance with, 156–158
- inference in database systems, 287
- information disclosure category in STRIDE model, 388
- information security
  - access control, 801
  - bus encryption, 407–408
  - classification, 215–219
  - frameworks, 179–189
  - hardware security modules, 406–407
  - identification, 215–219
  - overview, 214, 404
  - secure processing, 408
  - self-encrypting drives, 407
  - trusted execution environments, 408–410
  - Trusted Platform Modules, 404–406
  - vulnerabilities, 59

- Information Security Continuous Monitoring (ISCM), 981–982
- information security management systems (ISMSs)
  - commercial software certifications, 1146
  - description, 12
  - vs. enterprise security architecture, 26
  - ISO/IEC 27000 series, 180
  - security operations centers, 939
- Information Systems Audit and Control Association (ISACA), 187
- information systems availability in business continuity planning, 1067–1070
- information systems risk management (ISRM) policies, 56
- information systems view (Tier 3) in risk management, 55
- Information Technology Infrastructure Library (ITIL), 196–197
- informational model in software development design, 1084
- informative policies, 30
- Infrastructure as a Service (IaaS), 228, 302, 304
- infrastructure WLANs, 565
- ingress filtering, 948
- initial level in CMMI, 1107
- initial device identities (iDevIDs), 501
- initialization vectors (IVs)
  - 802.11 standard, 575–576
  - symmetric key cryptography, 334–335
- inputs, reviewing, 876–877
- inside attacks in risk management, 54
- installation stage in Cyber Kill Chain model, 388, 994
- instantiation in object-oriented programming, 1125
- INT domain in DNS, 527
- integrated development environments (IDEs)
  - in software development, 1137
- integrated product teams (IPTs), 1105
- Integrated Services Digital Network (ISDN), 685–686
- integration issues in federated identity, 754–755
- integration testing in software development, 1091
- integrity
  - Biba model, 399
  - CIA triad, 8
  - in cryptography, hashing functions, 351–354
  - in cryptography, message verification, 354–358
  - in cryptography, overview, 351
  - cryptosystems, 323
  - overview, 5–6
- Integrity Check Values (ICVs), 501, 575–576
- integrity verification procedures (IVPs) in Clark-Wilson model, 400
- Intel trade secrets theft, 149
- intellectual property (IP)
  - data breaches, 139
  - internal protection, 152–153
  - requirements. *See* licensing and intellectual property requirements
- intelligence cycle in threat intelligence, 941–942
- intentional category in civil law, 127
- interface testing, 837
- interference
  - coaxial cable, 649
  - electric power, 450–451
  - twisted-pair cabling, 649–650
- Interior Gateway Protocol (IGP), 533
- Interior Gateway Routing Protocol (IGRP), 536
- interior routing protocols, 535–536
- intermediate distribution facilities (IDFs), 446–447
- Intermediate System to Intermediate System (IS-IS), 536
- internal actors, 61–62
- internal audits, 840–842
- internal labeling in digital asset management, 263
- internal partitions, 442
- internal protection of intellectual property, 152–153
- internal security controls, 924
- internal sources of threat data, 942–943
- International Data Corporation (IDC), 154
- International Electrotechnical Commission (IEC) 27000 Series, 180–182
- international issues in cybercrimes, 138–139

- International Mobile Subscriber Identity (IMSI) catchers, 588
- International Organization for Standardization (ISO)
  - ISO 7498-1, 472
  - ISO 22301:2019, 105–106
  - ISO 28000:2007, 224
  - ISO/IEC 14443, 735
  - ISO/IEC 27000 series, 172, 180–182
  - ISO/IEC 27001, 1146
  - ISO/IEC 27004, 852
  - ISO/IEC 27005, 177–179
  - ISO/IEC 27031:2011, 105–106
  - ISO/IEC 27034, 1146
  - ISO/IEC 27037, 1009
  - network reference model, 470
- Internet Control Message Protocol (ICMP)
  - attacks using, 520–522, 537
  - message types, 520–521
  - overview, 520
  - stateful firewalls, 952
- Internet Engineering Task Force (IETF) RFC 4987, SYN flood attacks, 508
- Internet Group Management Protocol (IGMP), 500
- Internet growth, increase of attacks from, 134
- Internet Key Exchange (IKE), 608
- Internet Message Access Protocol (IMAP), 623–624
- Internet of Things (IoT)
  - devices, 570
  - issues, 306–307
- Internet Protocol (IP)
  - addresses. *See* IP addresses
  - L2TP, 606–607
- Internet protocol networking
  - ARP, 515–517
  - DHCP, 517–519
  - DNS, 524–531
  - ICMP, 520–522
  - IP addresses, 510–515
  - NAT, 531–533
  - overview, 502–503
  - routing protocols, 533–537
  - SNMP, 522–524
  - TCP, 503–509
- Internet Protocol Security (IPSec)
  - transport adjacency, 609
  - VPNs, 607–609
- Internet Protocol telephony, 687–688
  - H.323, 689
  - issues, 692
  - SIP, 689–691
- Internet Security Association and Key Management Protocol (ISAKMP), 608
- Internet Small Computer Systems Interface (iSCSI), 629
- internetworks, 657
- interoperability
  - data loss prevention, 270
  - ISO/IEC 14443, 735
- interpreters, 1119–1122
- interviews in forensics investigations, 1018–1019
- Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), 514
- intranets, 537–538
- intraorganizational configuration in SIP, 691
- intrasite tunneling mechanisms, 514
- intrusion detection systems (IDSs)
  - anomaly-based, 967–968
  - audits, 743
  - characteristics, 928
  - dogs, 929
  - overview, 925–928, 967
  - patrol forces and guards, 928–929
  - physical security, 908
  - rule-based, 967
  - whitelisting and blacklisting, 968–969
- intrusion prevention systems (IPSs)
  - anomaly-based, 967–968
  - overview, 967
  - rule-based, 967
  - whitelisting and blacklisting, 968–969
- inventories
  - data loss prevention, 267–268
  - digital asset management, 262
  - hardware, 224
  - software, 224–227
- investigations
  - incidents. *See* incident investigations
  - requirements, 161–162
- INVITE messages in SIP, 689–690
- invocation property in Biba model, 399
- IOAs (indicators of attack), 999

- IOCs (indicators of compromise)
    - incident remediation, 999
    - threat data sources, 942
  - IoT (Internet of Things)
    - devices, 570
    - issues, 306–307
  - IP addresses
    - DHCP, 501
    - DNS, 524–531
    - multicasting, 500
    - NAT, 531–533
    - overview, 510–512
    - packet-filtering firewalls, 948
    - three-way-handshake process, 951
  - IP convergence, 628
  - IP (intellectual property)
    - data breaches, 139
    - internal protection, 152–153
    - requirements. *See* licensing and intellectual property requirements
  - IP (Internet Protocol)
    - addresses. *See* IP addresses
    - L2TP, 606–607
    - networking, 502–503
  - IP version 4 (IPv4), 510
  - IP version 6 (IPv6), 510, 512–514
  - IPSec (Internet Protocol Security)
    - transport adjacency, 609
    - VPNs, 607–609
  - IPTs (integrated product teams), 1105
  - IPv4 (IP version 4), 510
  - IPv6 (IP version 6), 510, 512–514
  - iris lenses in CCTV systems, 915–916
  - iris scans, 727
  - IRPs. *See* incident response plans (IRPs)
  - IS-IS (Intermediate System to Intermediate System), 536
  - ISACA (Information Systems Audit and Control Association), 187
  - ISAKMP (Internet Security Association and Key Management Protocol), 608
  - ISATAP (Intra-Site Automatic Tunnel Addressing Protocol), 514
  - (ISC)<sup>2</sup> Code of Ethics, 44–45
  - ISCM (Information Security Continuous Monitoring), 981–982
  - iSCSI (Internet Small Computer Systems Interface), 629
  - ISDN (Integrated Services Digital Network), 685–686
  - island-hopping attacks, 133
  - ISM (industrial, scientific, and medical)
    - bands, 565–566
  - ISMSs. *See* information security management systems (ISMSs)
  - ISO. *See* International Organization for Standardization (ISO)
  - isochronous networks, 687
  - isolation in ACID properties, 286
  - ISRM (information systems risk management)
    - policies, 56
  - issue-specific policies, 28
  - IT engineers, tasks and responsibilities, 886
  - IT Governance Institute (ITGI), 187
  - IT support specialists on incident response teams, 1001
  - iterated tunneling in IPSec, 609
  - ITGI (IT Governance Institute), 187
  - ITIL (Information Technology Infrastructure Library), 196–197
  - IVPs (integrity verification procedures) in Clark-Wilson model, 400
  - IVs (initialization vectors)
    - 802.11 standard, 575–576
    - symmetric key cryptography, 334–335
- ## J
- JAD (Joint Application Development), 1104–1105
  - Java programming language, 1121–1122
    - bytecode, 1122–1123
    - protection mechanisms, 1123–1124
  - Java Virtual Machine (JVM), 1122–1123
  - JavaScript Object Notation (JSON), 615
  - JavaScript programming language, 1121
  - Jigsaw ransomware, 604
  - JIT (just-in-time) access, 738
  - jitter in IP telephony, 687–688
  - job rotation, 34, 889–890
  - Joint Application Development (JAD), 1104–1105
  - journaling, remote, 1039
  - JSON (JavaScript Object Notation), 615
  - jumbograms in IPv6, 514
  - jump boxes, 700

jurisdiction in incident response, 993  
just-in-time (JIT) access, 738  
JVM (Java Virtual Machine), 1122–1123

## K

k-means clustering, 978  
k-nearest neighbors (KNN), 977  
Kanban development methodology,  
1102–1103  
KBA (knowledge-based authentication)  
description, 718  
passwords, 720–723  
KDCs (Key Distribution Centers)  
Kerberos, 785–788  
PKI, 365  
Kelling, George L., 433  
Kerberos protocol  
authentication process, 785–788  
components, 785  
key management, 365  
overview, 784–785  
passwords, 789  
weaknesses, 788–789  
Kerckhoffs, Auguste, 324–325  
Kerckhoffs' principle, 324–325  
kernel flaws in cryptography, 819  
key distillation in quantum  
cryptography, 344  
Key Distribution Centers (KDCs)  
Kerberos, 785–788  
PKI, 365  
key escrow in PKI, 366  
key exchange protocol in RSA, 340  
key management in PKI, 364–367  
key override feature for combination  
locks, 920  
key performance indicators (KPIs),  
155, 856–857  
key risk indicators (KRIs), 855–857  
keycard entry systems, 442  
keys  
asymmetric key cryptography, 335  
cryptography, 322–323, 367–370  
Diffie-Hellman algorithm, 337–338  
hybrid methods, 347–348  
RSA, 340–341  
session, 349–350  
symmetric key cryptography, 329

TLS, 604  
ZigBee, 572  
keyspaces for cryptology, 322  
keystream generators in symmetric key  
cryptography, 333  
keystroke dynamics, 728  
kill chains in threat modeling, 386  
kill switches in VPNs, 697  
knowledge-based authentication (KBA)  
description, 718  
passwords, 720–723  
known-plaintext attacks in cryptography, 368  
Koolhaas, Rem, 417  
KPIs (key performance indicators), 155,  
856–857  
KRIs (key risk indicators), 855–857

## L

L2F (Layer 2 Forwarding) protocol, 606  
L2TP (Layer 2 Tunneling Protocol),  
606–607  
labels  
digital asset management, 263  
evidence, 1010  
IPv6, 514  
MAC, 768–769  
laminated windows, 441  
landscaping, 908  
language in reports, 871  
LANs. *See* local area networks (LANs)  
LAST-ACK state in TCP connections, 951  
last full backups, 1035–1036  
latency in cabling, 654  
law enforcement involvement in incident  
investigations, 1007  
laws and regulations  
data breaches, European Union, 142–144  
data breaches, U.S., 141–142  
legal systems, 126–130  
overview, 125–126  
security programs, 434  
layer 2  
local area networks, 494–499  
security standards, 500–502  
Layer 2 Forwarding (L2F) protocol, 606  
Layer 2 Tunneling Protocol (L2TP),  
606–607  
layer 3 and 4 switches, 659

- layers
  - encryption, 600–601
  - OSI reference model. *See* Open Systems Interconnection (OSI) reference model
- LDAP (Lightweight Directory Access Protocol), 747, 749
- LEAP (Lightweight Extensible Authentication Protocol), 580
- leased lines for WANs, 541–543
- least privilege principle
  - configuration management, 799
  - description, 888
  - endpoint security, 673
  - network security, 598
  - overview, 394–395
  - privileged accounts, 889
  - site and facility security, 421
  - software tracking, 225
  - third parties, 705–706
  - web services, 611
- least significant bits (LSBs) in steganography, 265
- LEDs (light-emitting diodes) in fiber-optic cable, 651
- legacy systems for federated identity, 755
- legal counsels in incident response teams, 1001
- legal departments, advice from, 157
- legal requirements
  - compliance, 156–158
  - physical security programs, 434
  - site planning, 427
- legal systems
  - civil law, 126, 129
  - common law, 126–130
  - customary law system, 128
  - mixed law system, 128–129
  - religious law system, 128
- legality issues in evidence admissibility, 1013–1014
- legally recognized obligations, 161
- Lei Geral de Proteção de Dados (LGPD), 144
- length of passwords, 720
- lenses in CCTV systems, 915–916
- LEO (low Earth orbit) satellites, 588–590
- lessons learned
  - disaster recovery plans, 1061
  - incidents, 999–1000
- levels
  - classification, 216–219
  - CMMI, 1107–1108
  - programming languages, 1120
- LGPD (Lei Geral de Proteção de Dados), 144
- Li-Fi standard, 568
- liability
  - civil law, 129
  - compliance, 158–161
  - outsourced security services, 974
- libraries
  - object-oriented programming, 1129–1130
  - software, 1132–1133
- licensing and intellectual property
  - requirements
    - copyrights, 149–150
    - internal protection of intellectual property, 152–153
    - overview, 147–148
    - patents, 151–152
    - software, 225–226
    - software piracy, 153–154
    - trade secrets, 148–149
    - trademarks, 150
- life cycle
  - business continuity planning, 1065–1067
  - cryptology, 328
  - data. *See* data life cycle
- life cycle of assets
  - decommissioning, 229–230
  - inventories, 224–227
  - overview, 222–223
  - ownership, 223
  - provisioning, 227–228
  - retention, 228–230
- life safety goals in site planning, 423
- light detectors in fiber-optic cable, 651
- light-emitting diodes (LEDs) in fiber-optic cable, 651
- light frame construction material, 438
- light sources for fiber-optic cable, 651
- lighting
  - CCTV systems, 916
  - EMI, 450
  - photoelectric IDSs, 926–927
  - physical security, 911–912
- Lightweight Directory Access Protocol (LDAP), 747, 749



- Lightweight Extensible Authentication Protocol (LEAP), 580
  - lightweight methods in software development, 1101
  - limited RBAC, 772–773
  - Linder, Doug, 1117
  - line conditioners for electric power, 451
  - line noise
    - cabling, 652
    - electric power, 450
  - line-of-succession plans, 1043
  - linear bus topology, 488
  - link encryption vs. end-to-end encryption, 600–602
  - link keys in ZigBee, 572
  - link-state routing protocols, 535
  - LISTEN state in TCP connections, 951
  - LLC (Logical Link Control), 481–482
  - loads, construction, 436
  - local area networks (LANs)
    - Ethernet, 494–495
    - FDDI, 496–498
    - medium access control, 489–494
    - protocols summary, 498–499
    - security standards, 500–502
    - Token Ring, 495–496
    - topologies, 487–490
    - transmission methods, 499–500
  - Local Security Authority Subsystem Service (LSASS), 372–374
  - Locard, Edmond, 1020
  - Locard's exchange principle, 1020–1021
  - lock bumping, 924
  - Lockheed Martin Cyber Kill Chain, 387–389
  - locks
    - administrative responsibilities, 922
    - circumventing, 922–924
    - grades, 923
    - mechanical, 918–922
    - overview, 917–918
  - Lucky ransomware, 604
  - logical access, 717, 801–803
  - logical acquisition of evidence, 1012
  - Logical Link Control (LLC), 481–482
  - logon attempts, failed, 721–723
  - logs
    - aggregating for microservices, 299
    - backups, 1039
    - evidence, 1014
    - managing, 978–979
    - protecting, 744–745
    - requirements factor, 978–979
    - reviews, 828–831
    - SIEM, 744, 979–980
    - standards, 979
    - tampering, 831
  - Long-Term Evolution (LTE), 587
  - loose coupling in software, 1131
  - loosely coupled microservices, 299
  - loss issues in risk management, 54, 63
  - low coupling in software, 1131
  - low Earth orbit (LEO) satellites, 588–590
  - low privacy risk in software development, 1083
  - LSASS (Local Security Authority Subsystem Service), 372–374
  - LSBs (least significant bits)
    - in steganography, 265
  - LTE (Long-Term Evolution), 587
  - Lucifer project, 321
  - lux values in CCTV systems, 916
- ## M
- m of n control
    - description, 34
    - PKI, 366–367
  - MAC (mandatory access control) model
    - characteristics, 776
    - overview, 768–771
  - MAC Security (MACSec) standard, 500–501
  - machine language, 1118, 1121
  - machine learning (ML), 977
  - MACSec Security Entity (SecY), 501
  - Madrid Agreement, 150
  - magnetic tapes for backups, 860
  - mail transfer agents (MTAs), 622
  - mailbox data, backups for, 862
  - main distribution facilities (MDFs), 446
  - maintenance
    - CPTED, 433
    - data, 238
    - frameworks, 201
  - maintenance hooks in software development, 1091
  - malicious code in advanced persistent threats, 136
  - malicious insiders, 61



- man-in-the-middle (MitM) attacks
  - cryptography, 374–375
  - data in motion, 59, 256
  - Diffie-Hellman algorithm, 338–339
- managed level in CMMI, 1107
- managed security services providers (MSSPs), 973–974
- managed service accounts (MSAs), 800
- managed services in software security, 1148
- Management Frame Protection (MFP), 578
- Management Information Base (MIB) in SNMP, 522–524
- management objectives in COBIT 2019, 189
- management review and approval, 875–877
- managers, risk reporting for, 95
- mandatory access control (MAC) model
  - characteristics, 776
  - overview, 768–771
- mandatory vacations, 35, 890
- manmade threats in site planning, 423
- MANs (metropolitan area networks), 538–540
- mantraps, 441
- manual iris lenses in CCTV systems, 915
- manual penetration tests (MPTs), 1140
- manual tests in software development, 1091
- market approach in executive
  - summaries, 874
- markup languages, 776–778
- Mary, Queen of Scots, 319
- masks in IP addresses, 511–512
- masquerading firewalls, 965
- master keying feature for combination
  - locks, 920
- master keys in ZigBee, 572
- matrices
  - access control, 766–767
  - classification, 1002–1003
  - notification, 1003–1004
  - qualitative risk, 76–77
  - role, 799
- Mattermost service, 1057
- maturity models for risk, 96
- maturity software development models
  - CMMI, 1107–1109
  - overview, 1106
  - SAMM, 1109–1110
- MAUs (Multistation Access Units), 495
- maximum tolerable downtime (MTD)
  - BIA, 113–114
  - disaster recovery, 1030–1033
  - spare servers for, 672
- maximum tolerable period of disruption (MTPD), 113
- maximum transmission units (MTUs)
  - MAC mechanisms, 489–494
  - routers, 661
- “McAfee 2019 Cloud Adoption and Risk Report,” 303
- McNulty, Paul, 125
- MCUs (multipoint control units)
  - in H.323, 689
- MD5 (Message Digest 5)
  - description, 352
  - passwords, 722
- MDFs (main distribution facilities), 446
- MEA (Monitor, Evaluate and Assess) domain
  - in COBIT 2019, 189
- means in criminal investigations, 1008
- measurements in ISO/IEC 27004, 852
- measuring security, 851
  - account management, 858–860
  - backup verification, 860–862
  - chapter questions, 879–881
  - chapter review, 877–879
  - disaster recovery and business continuity, 867–869
  - key performance and risk indicators, 855–857
  - management review and approval, 875–877
  - metrics, 852–855
  - process data overview, 857–858
  - quantifying, 851–853
  - reporting, 869–875
  - training, 863–867
- mechanical locks, 918–922
- Media Access Control (MAC) addresses
  - ARP, 515–517
  - bridges, 656
  - DHCP, 519
  - switches, 658–659
- Media Access Control (MAC) in data link layer, 481–482
- media for storage, 447

- medium access control (MAC)
  - collision and broadcast domains, 492–494
  - CSMA, 490–491
  - overview, 489–490
  - polling, 494
  - token passing, 491–492
- meeting applications, 694–695
- Meltdown attacks, 257, 372
- members in object-oriented programming, 1125
- memory cards in ownership-based authentication, 732–733
- memory for Trusted Platform Modules, 405–406
- mergers and acquisitions (M&A), 17
- mesh size for fencing, 909
- mesh topology for local area networks, 488–489
- message authentication code (MAC), 355–356, 603–604
- Message Digest 5 (MD5)
  - description, 352
  - passwords, 722
- message digests, 354–355
- messages
  - ICMP, 520–521
  - integrity verification, 354–358
  - object-oriented programming, 1127–1128
  - TCP, 509
- meta-directories, 748
- methodologies
  - description, 15
  - reports, 873
- methods in object-oriented programming, 1127
- Metro Ethernet, 539–540
- metropolitan area networks (MANs), 538–540
- Metropolitan Transit Authority (MTA), 433
- MFA (multifactor authentication)
  - strong authentication, 719
  - VPNs, 697
- MFP (Management Frame Protection), 578
- MIB (Management Information Base) in SNMP, 522–524
- micro-segmentation, 629
- microcontrollers in embedded systems, 306
- microprobing attacks on smart cards, 735
- microservices, 299–301
- middle management, awareness
  - programs for, 42
- MIL domain in DNS, 527
- military-oriented architecture frameworks, 195–196
- Miller, Charlie, 627
- MIME (Multipurpose Internet Mail Extensions), 625–626
- MIMO (multiple input, multiple output)
  - standard, 567, 585
- Mirai botnet, 307
- mission/business process view (Tier 2) in risk management, 55
- mission critical data in disaster recovery, 1032
- misuse cases
  - data loss prevention, 271
  - testing, 835–836
- misuse of data in risk management, 54
- Mitchell, Joni, 213
- mitigation
  - incidents, 996–997
  - software security, 1144–1145
- mitigation risk strategy
  - ISO/IEC 27005, 178
  - overview, 79
- MitM (man-in-the-middle) attacks
  - cryptography, 374–375
  - data in motion, 59, 256
  - Diffie-Hellman algorithm, 338–339
- MITRE corporation
  - ATT&CK framework, 389–390
  - Common Weakness Enumeration initiative, 1088
- mixed law systems, 128–129
- ML (machine learning), 977
- MLS (multilevel security) systems
  - Bell-LaPadula, 398
  - description, 769
- MO (modus operandi) in criminal investigations, 1008
- mobile devices and communications
  - disaster recovery plans, 1062
  - endpoint security, 673–674
  - forensics investigations, 1021
  - generations, 585–587
  - hacking, 588

- ul style="list-style-type: none;">
- mobile devices and communications (*cont.*)
  - multiple access technologies, 584–585
  - overview, 582–583
  - protecting, 220–221
- mobile hot sites in disaster recovery, 1049
- mobile IP, 793
- Modbus system, 627
- modems, cable, 686–687
- moderate privacy risk in software development, 1082
- modularity in object-oriented programming, 1127–1128
- modus operandi (MO) in criminal investigations, 1008
- MOM (motive, opportunity, and means) in incident investigations, 1007–1008
- Monitor, Evaluate and Assess (MEA) domain in COBIT 2019, 189
- monitoring
  - continuous, 981–982
  - egress, 981
  - frameworks, 201
  - ingress, 948
  - passwords, 721
  - Risk Management Framework, 176–177
  - UEBA, 981
- monitoring risk
  - change, 92–93
  - compliance, 93–94
  - continuous improvement, 95–96
  - description, 58
  - effectiveness, 91–92
  - maturity models, 96
  - reporting, 94–95
- monitors in Token Ring, 496
- monoalphabetic substitution ciphers, 318
- monoammonium phosphate for fire suppression, 458
- motion detectors, 927
- motive, opportunity, and means (MOM) in incident investigations, 1007–1008
- MPLS (Multiprotocol Label Switching)
  - Metro Ethernet, 540
  - routing tags and labels, 659
- MPTs (manual penetration tests), 1140
- MSAs (managed service accounts), 800
- MSSPs (managed security services providers), 973–974
- MTA (Metropolitan Transit Authority), 433
- MTAs (mail transfer agents), 622
- MTD (maximum tolerable downtime)
  - BIA, 113–114
  - disaster recovery, 1030–1033
  - spare servers for, 672
- MTPD (maximum tolerable period of disruption), 113
- MTUs (maximum transmission units)
  - MAC mechanisms, 489–494
  - routers, 661
- multi-user MIMO (MU-MIMO) technology, 567–568
- multicast transmission method, 499
- multifactor authentication (MFA)
  - strong authentication, 719
  - VPNs, 697
- multihomed devices, 959
- multilayer protocols, 626–627
- multilayered switches, 658
- multilevel security (MLS) systems
  - Bell-LaPadula, 398
  - description, 769
- multimedia collaboration, 693–694
  - meeting applications, 694–695
  - unified communications, 695–696
- multimode fiber-optic cable, 651
- multiparty key recovery in PKI, 366
- multiple access technologies in mobile communications, 584–585
- multiple input, multiple output (MIMO)
  - standard, 567, 585
- multiple processing sites in disasters
  - recovery, 1049
- multiplexing functionalities, 544
- multipoint control units (MCUs) in H.323, 689
- Multiprotocol Label Switching (MPLS)
  - Metro Ethernet, 540
  - routing tags and labels, 659
- Multipurpose Internet Mail Extensions (MIME), 625–626
- Multistation Access Units (MAUs), 495
- muscle memory in disaster recovery, 1060
- mutual aid agreements in disasters
  - recovery, 1047
- mutual authentication
  - description, 719
  - 802.11, 580

## N

## NAC (network access control)

- devices, 667–668

- importance, 697

## namespaces

- directory services, 747

- DNS, 525

- LDAP, 749

Nappo, Stephane, 989

## NAS (network-attached storage) for

- backups, 1038

## NAT (network address translation),

- 512–513, 531–533

nation-state actors, 60–61

## National Institute of Standards and Technology (NIST)

- Cybersecurity Framework, 182

- Digital Signature Standard, 357

- enterprise architecture frameworks, 190–191

- passwords, 720–721

- Risk Management Framework, 172–177

- SHA, 352

- SP 800-30, 67–68, 173

- SP 800-34, 104–105, 1059

- SP 800-37, 173

- SP 800-39, 55, 173

- SP 800-53, 172, 175, 183–185

- SP 800-57, 367

- SP 800-60, 174

- SP 800-63B, 720–721

- SP 800-82, 290, 294

- SP 800-88, 240

- SP 800-111, 255

- SP 800-137, 981–982

- SP 800-161, 97

- SP 800-190, 298–299

## National Security Agency (NSA)

- DES standard, 321

- HAIPE, 609

natural access control in CPTED, 428–431

natural environmental threats in site

- planning, 423

natural languages, 1119–1120

natural surveillance in CPTED, 431–432

natural threats, 62

naturalness in object-oriented

- programming, 1127

## NDAs (nondisclosure agreements)

- incident response teams, 1001

- trade secrets, 148

## NDLP (network DLP), 272–273

## NDR (network detection and response)

- products

- forensics investigations, 1021

- HIDSs, 968

- security operations centers, 940

## Near Field Communication (NFC) with

- smart cards, 735

near-line devices for backups, 898–899

## need-to-know principle

- description, 394

- overview, 888

## negligence

- breaches from, 266

- civil law category, 127

## negligent insiders, 61

## NET domain in DNS, 527

## network access control (NAC)

- devices, 667–668

- importance, 697

## network address translation (NAT),

- 512–513, 531–533

## network administrators, tasks and

- responsibilities, 886

## network-attached storage (NAS) for

- backups, 1038

## network-based intrusion detection systems (NIDSs), 967

## network components, 643

- CDNs, 674

- chapter questions, 677–679

- chapter review, 674–676

- devices. *See* network devices

- endpoint security, 673–674

- transmission media, 643–655

## network detection and response (NDR)

- products

- forensics investigations, 1021

- HIDSs, 968

- security operations centers, 940

## network devices

- bridges, 656–657

- gateways, 662–663

- hardware operation, 670–672

- NACs, 667–668

- network diagramming, 668–670

- network devices (*cont.*)
  - overview, 655
  - PBXs, 665–667
  - proxy servers, 663–664
  - repeaters, 655–656
  - routers, 660–662
  - switches, 657–660
- network DLP (NDLP), 272–273
- network forensics, 1021
- network keys in ZigBee, 572
- network layer
  - functions and protocols, 484
  - OSI model, 480
- network reference models, 470–471
- network security
  - chapter questions, 638–641
  - chapter review, 635–638
  - design principles, 597–599
  - DNS, 616–621
  - e-mail, 621–626
  - link encryption vs. end-to-end encryption, 600–602
  - multilayer protocols, 626–627
  - overview, 597
  - protocol overview, 611
  - segmentation. *See* network segmentation
  - TLS, 602–605
  - VPNs, 605–611
  - web services, 611–616
- network segmentation
  - overview, 629
  - risk mitigation, 295
  - SD-WANs, 635
  - SDNs, 632–635
  - VLANs, 630–632
  - VxLANs, 632
- network sockets, 703
- Network Time Protocol (NTP), 829–830
- networking fundamentals
  - chapter questions, 555–558
  - chapter review, 552–555
  - data communications. *See* data communications
  - Internet protocol networking. *See* Internet protocol networking
  - intranets and extranets, 537–538
  - local area networks. *See* local area networks (LANs)
  - MANs, 538–540
  - overview, 469
  - WANs, 540–552
- networks
  - diagramming, 668–670
  - testing, 818
  - virtualized, 704–705
- New Zealand, Privacy Act in, 147
- newly observed domains (NODs) as threat data source, 943
- next-generation firewalls (NGFWs), 957–958
- NFC (Near Field Communication) with smart cards, 735
- NGFWs (next-generation firewalls), 957–958
- NIDSs (network-based intrusion detection systems), 967
- NIST. *See* National Institute of Standards and Technology (NIST)
- NMT (Nordic Mobile Telephone), 584
- NODs (newly observed domains) as threat data source, 943
- noise
  - cabling, 652
  - database systems, 288
  - digital transmission, 645
  - electric power, 450
- non-symbolic AI approach, 976–978
- nonces for one-time passwords, 731
- nondisasters
  - availability, 1049–1053
  - description, 1043
- nondisclosure agreements (NDAs)
  - incident response teams, 1001
  - trade secrets, 148
- nonfunctional requirements in software development, 1083
- noninterference model, 400–401, 403
- nonpersistent VDI, 701
- nonplenum cables, 653
- nonpracticing entities (NPEs), 152
- nonrecursive queries in DNS, 527
- nonrepudiation
  - cryptosystems, 324
  - overview, 6–7
- nonvolatile RAM (NVRAM) in Trusted Platform Modules, 405
- NORAD (North American Aerospace Defense Command), 436

- Nordic Mobile Telephone (NMT), 584
- normal changes, 892
- normal management in business
  - continuity, 1066
- normalization in data retention, 236
- North American Aerospace Defense Command (NORAD), 436
- notifications for incidents, 1003–1004
- Novell Red color, 150
- NPEs (nonpracticing entities), 152
- NSA (National Security Agency)
  - DES standard, 321
  - HAIPE, 609
- NTP (Network Time Protocol), 829–830
- nuisance category in civil law, 127
- NVRAM (nonvolatile RAM) in Trusted Platform Modules, 405
- O**
- O&M (operation and maintenance) in life cycle of assets, 223
- OASIS (Organization for the Advancement of Structured Information Standards), 781
- OAuth standard, 782–783
- Obama, Barack, 182
- object-oriented programming (OOP)
  - abstraction, 1129
  - benefits, 1127
  - classes and objects, 1125–1127
  - encapsulation, 1130
  - libraries, 1129–1130
  - messages, 1127–1128
  - overview, 1124–1125
  - vs. procedural programming, 1125–1126
  - relationships, 1128
- objectives in Spiral methodology, 1098
- objectivity in forensics investigation
  - interviews, 1019
- objects in ABAC, 774
- obligations, legally recognized, 161
- occupant emergency plans (OEPs), 931
- Occupational Safety and Health Administration (OSHA), 434
- OceanLotus attack, 389–390
- OCs (optical carriers) for WANs, 543
- OCSP (Online Certificate Status Protocol), 362
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) framework, 68, 172, 178–179
- OECD (Organisation for Economic Co-operation and Development), 142–144
- OEMs (original equipment manufacturers), 229
- OEPs (occupant emergency plans), 931
- OFDM (orthogonal frequency division multiplexing), 561, 563–564
- OFDMA (orthogonal frequency division multiple access), 585
- Office of Management and Budget, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information,” 140
- offline media for backups, 1038
- offsite backups, 1037
- offsite locations in disasters recovery, 1047
- OIDC (OpenID Connect), 783–784
- on-premise FIM systems, 755–756
- onboarding personnel security, 37–38
- ONC (Open Network Computing), 703
- one-time pads in cryptology, 325–328
- one-time passwords (OTPs), 729–732
- one-to-many identification, 718
- one-to-one identification, 718
- one-way hashing functions, attacks against, 353–354
- one-way RSA functions, 341–342
- ONF (Open Networking Foundation), 634–635
- online backups, 1035
- Online Certificate Status Protocol (OCSP), 362
- online encryption vs. end-to-end encryption, 600–602
- online safety, 866–867
- online UPS systems, 452–453
- onsite backups, 1037
- Ontario Information Commissioner, 397
- OOP. *See* object-oriented programming (OOP)
- open message format in asymmetric key cryptography, 336
- open network architectures, 472
- Open Network Computing (ONC), 703
- Open Networking Foundation (ONF), 634–635
- open proxies, 663

- Open Shortest Path First (OSPF) protocol, 535–536
- open-source intelligence (OSINT)
  - social engineering, 903
  - threat data sources, 942
- open-source software, securing, 1146–1147
- open system authentication (OSA), 575
- open systems, 474
- Open Systems Interconnection (OSI)
  - reference model, 470–471, 648
    - application layer, 474–475
    - attacks, 474
    - data link layer, 480–483
    - functions and protocols, 483–485
    - layers together, 485–487
    - network layer, 480
    - physical layer, 483
    - presentation layer, 475–476
    - protocols, 471–474
    - session layer, 477–478
    - transport layer, 479–480
- open trust model in ZigBee, 572
- Open Web Application Security Project (OWASP)
  - SAMM, 1109–1110
  - Threat Dragon, 1087
  - web applications, 1134–1135
- OpenFlow interface, 634–635
- OpenID Connect (OIDC), 783–784
- Openness Principle in OECD, 142
- operate steps in frameworks, 201
- operation and maintenance (O&M) in life cycle of assets, 223
- operational prototypes in software development, 1096
- operational tasks in incident handling, 1004–1005
- operational technology (OT), 290, 292–293, 295
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
  - framework, 68, 172, 178–179
- operations and maintenance phase
  - change control, 1092–1094
  - change management, 1092
  - SDLC, 1080, 1091–1094
- Operations function in SAMM, 1109
- operations management. *See* security operations; security operations management
- opportunity in criminal investigations, 1008
- optical carriers (OCs) for WANs, 543
- optical discs for logs, 745
- optical fiber
  - fiber-optic cable, 651
  - transmission media, 643
- optical zoom in CCTV systems, 915
- optimizing level in CMMI, 1108
- orchestration in SOAR, 980
- order of volatility for evidence, 1016
- ORG domain in DNS, 527
- Organisation for Economic Co-operation and Development (OECD), 142–144
- Organization for the Advancement of Structured Information Standards (OASIS), 781
- organization view (Tier 1) in risk management, 55
- organizational change, data loss prevention in, 270
- organizational CIS controls, 187
- organizational code of ethics, 45
- organizational processes, 17–18
- organizational roles and responsibilities, 18–19
  - auditors, 25
  - change control analysts, 24
  - data analysts, 24
  - data custodians, 23
  - data owners, 22–23
  - executive management, 19–22
  - security administrators, 24
  - system owners, 23–24
  - users, 25
- organizational security policies, 27–29
- organizational units (OUs) in LDAP, 749
- organized cybercrime gangs, 134
- organizing steps for frameworks, 200
- original equipment manufacturers (OEMs), 229
- orthogonal frequency division multiple access (OFDMA), 585
- orthogonal frequency division multiplexing (OFDM), 561, 563–564
- OSA (open system authentication), 575
- OSHA (Occupational Safety and Health Administration), 434



OSI model. *See* Open Systems  
Interconnection (OSI) reference model  
OSINT (open-source intelligence)  
    social engineering, 903  
    threat data sources, 942  
OSPF (Open Shortest Path First) protocol,  
    535–536  
OT (operational technology), 290,  
    292–293, 295  
OTPs (one-time passwords), 729–732  
OUs (organizational units) in LDAP, 749  
out-of-band method in symmetric key  
    cryptography, 330  
outside attacks in risk management, 54  
outsourced security services, 973–974  
outsourced software, 1147  
outsourcing business continuity  
    planning, 1068  
overflows  
    description, 819  
    software development, 1089–1090  
overlays in SDNs, 635  
overwriting  
    data, 243  
    media, 259–260  
OWASP (Open Web Application  
    Security Project)  
    SAMM, 1109–1110  
    Threat Dragon, 1087  
    web applications, 1134–1135  
owners  
    assets, 223  
    data, 244  
    OAuth, 782  
    risk reporting for, 95  
ownership-based authentication  
    cryptographic keys, 732  
    memory cards, 732–733  
    one-time passwords, 729–732  
    overview, 729  
    smart cards, 733–735

## P

PaaS (Platform as a Service), 228, 302–304  
PACE (Primary, Alternate, Contingency, and  
    Emergency) communications plans, 1057  
package supplies in forensics field kits, 1015  
packet-filtering firewalls, 946–949  
packet jitter, 681  
packet switching in WANs, 546–547  
packets  
    firewalls, 945  
    TCP, 509  
    TCP vs. UDP, 506  
Padding Oracle On Downgraded Legacy  
    Encryption (POODLE) attacks, 602  
padlocks, 917  
pair programming in Extreme  
    Programming, 1102  
palm scans, 727  
PAM (privileged account management), 889  
pan, tilt, or zoom (PTZ) capabilities in CCTV  
    systems, 916  
panic bars, 440  
panic buttons, 931  
PanOptis lawsuit, 151  
PAP (Password Authentication Protocol),  
    697–698  
paper records, protecting, 221  
parallel tests in disaster recovery plans, 1064  
parameter validations in APIs, 1132  
Pareto principle, 179  
Paris Convention, 150  
partial knowledge in penetration  
    testing, 825  
partitions  
    database systems, 288  
    physical security, 442  
pass the hash attacks, 372  
passive infrared (PIR) IDSs, 927  
passive patch management, 904  
passive relocking function for safes, 222  
Password Authentication Protocol (PAP),  
    697–698  
password-guessing attacks, 789  
password managers, 736–737  
passwords  
    checkers, 722  
    cognitive, 723  
    failed logon attempts, 721–723  
    hashing and encrypting, 722  
    Kerberos protocol, 789  
    knowledge-based authentication, 720  
    one-time, 729–732  
    passphrases, 723  
    PBX systems, 666



- passwords (*cont.*)
  - policies, 720–722
  - resets, 737–738
  - synchronization, 737
  - TACACS, 791
  - vulnerabilities, 60
- PAT (port address translation), 532
- patch management, 903
  - centralized, 904–905
  - reverse engineering patches, 905
  - unmanaged patching, 904
- patent trolls, 152
- patents, 151–152
- paths in URLs, 614
- patrol forces, 928–929
- payloads
  - IPv6, 514
  - steganography, 265
- PBXs (Private Branch Exchanges), 665–667
- PCI DSS (Payment Card Industry Data Security Standard), 156
- PCRs (platform configuration registers) in Trusted Platform Modules, 406
- PDC (Personal Digital Cellular), 584
- PDPA (Personal Data Protection Act), 144
- PDU (protocol data units)
  - description, 473
  - TCP, 509
- PEAP (Protected EAP), 580
- peer-to-peer systems, 307
- Peltier, Thomas, 68
- penetration tests
  - application security, 1140
  - knowledge of targets, 825–826
  - overview, 822–824
  - process, 824–825
  - red team exercises, 902
  - software development, 1090
  - vs. vulnerability tests, 826–827
- people as vulnerabilities, 60
- perfect forward secrecy in TLS, 604
- performance-based approach in site planning, 424
- performance metrics, 854
- Perimeter Intrusion Detection and Assessment System (PIDAS), 910
- perimeter security, 803
- periodic content reviews, 43
- peripheral switch controls for device locks, 921
- Perl programming language, 1121
- permanent teams for incident response, 991
- permanent virtual circuits (PVCs), 549
- permissions
  - DAC, 767
  - setting, 739
  - testing, 821
- persistent memory in Trusted Platform Modules, 405
- persistent VDI, 701
- Personal Data Protection Act (PDPA), 144
- Personal Digital Cellular (PDC), 584
- personal health information (PHI)
  - breaches, 255
- Personal Information Protection and Electronic Documents Act, 147
- personal liability of executive management, 20
- personally identifiable information (PII)
  - components, 140–141
  - U.S. laws, 141
- personnel
  - disaster recovery plans, 1055–1056
  - testing, 818
- personnel safety and security
  - access controls, 924–925
  - breaches from, 266
  - candidate screening and hiring, 35–36
  - compliance policies, 39–40
  - duress, 931–932
  - emergency management, 931
  - employment agreements and policies, 36–37
  - incident response, 993
  - onboarding, transfers, and termination processes, 37–38
  - overview, 33–35, 929–930
  - privacy policies, 40
  - threats, 138
  - training and awareness, 930–931
  - travel, 930
  - vendors, consultants, and contractors, 39
- perturbation in database systems, 288
- pervasive systems
  - embedded, 306
  - Internet of Things, 306–307
  - overview, 305

- Petya ransomware, 604
- PGP (Pretty Good Privacy), 367
- PHI (personal health information)
  - breaches, 255
- phishing awareness programs, 42, 864–865
- phone calls in PBXs, 665–667
- photoelectric IDS systems, 926–927
- phreakers, 666
- physical damage in risk management, 54
- physical destruction of data, 244
- physical layer
  - functions and protocols, 485
  - OSI model, 483
- physical security and controls
  - auditing, 929
  - data loss prevention, 269
  - devices, 802
  - digital asset management, 261
  - external perimeter, 906–916
  - facilities, 802–803, 916–924
  - information access, 801
  - internal controls, 924
  - intrusion detection systems, 925–929
  - mobile devices, 220–221
  - overview, 220, 801, 906
  - paper records, 221
  - personnel access controls, 924–925
  - risk responses, 83–84, 86–87
  - safes, 221–222
- physical security programs
  - construction, 436–439
  - design overview, 433–435
  - entry points, 439–441
  - facilities, 435–436
- physical surveillance in digital forensics, 1019–1020
- physical testing, 818
- physiological biometric authentication, 724
- PIDAS (Perimeter Intrusion Detection and Assessment System), 910
- piggybacking, 925
- PII (personally identifiable information)
  - components, 140–141
  - U.S. laws, 141
- pin tumbler locks, 918
- PINs
  - memory cards, 732
  - smart cards, 733
- PIR (passive infrared) IDSs, 927
- piracy, software, 153–154
- pirated software, dangers in, 225
- PKCS (Public Key Cryptography Standards), 626
- PKI. *See* public key infrastructure (PKI)
- plaintext, 321
- Plan-Do-Check-Act loop, 875
- plans
  - audits, 839
  - backups, 863
  - business continuity, 104–105
  - change management, 891
  - forensics investigation interviews, 1019
  - frameworks, 200
  - incident response, 1000–1006
  - OEPs, 931
  - Plan-Do-Check-Act loop, 875
  - Spiral methodology, 1098
- Platform as a Service (PaaS), 228, 302–304
- platform configuration registers (PCRs) in Trusted Platform Modules, 406
- platforms for secure software, 1137–1138
- PLCs (programmable logic controllers), 290–291
- plenum areas
  - cabling, 653
  - fire suppression, 459
- PMs (project managers) in software development, 1080
- point-to-point links in WANs, 541–543
- Point-to-Point Tunneling Protocol (PPTP), 606
- poisoning of ARP cache tables, 516–517
- polarized filters in QKD, 344–345
- policies
  - acceptable use, 226, 664, 858
  - compliance, 39–40
  - data retention, 234–236
  - employment, 36–37
  - IMPs, 990, 1000
  - passwords, 720–722
  - privacy, 40
  - security, 27–29
  - security operations centers, 940
  - types, 30

- Policy and Program Management
  - practice, 105
- policy engines for data loss prevention, 270
- polling, MAC, 494
- polyalphabetic substitution ciphers, 318–320
- polyvinyl chloride (PVC) jacket covering, 653
- POODLE (Padding Oracle On Downgraded Legacy Encryption) attacks, 602
- POP (Post Office Protocol), 623
- port address translation (PAT), 532
- portable code, 1122
- portable fire extinguishers, 455
- portals, TLS, 610
- portlets for web portal functions, 753–754
- ports
  - device locks, 921
  - packet-filtering firewalls, 948
  - TCP, 504
  - three-way-handshake process, 951
  - types, 507
- positive drains, 448
- POST methods in HTTP, 614
- Post Office Protocol (POP), 623
- powders for fire suppression, 458
- power, electrical. *See* electric power
- power supplies
  - considerations, 438
  - data processing facilities, 446
- PP (Professional Practices) in Good Practice Guidelines, 105–106
- PPTP (Point-to-Point Tunneling Protocol), 606
- preaction water sprinkler systems, 460
- prediction with artificial intelligence tools, 977
- prefabricated buildings in disasters
  - recovery, 1049
- preparation step
  - Risk Management Framework, 174
  - software vulnerability scans, 901
- preparedness metrics, 855
- presence information in unified communications, 695
- presentation layer
  - functions and protocols, 483–484
  - OSI model, 475–476
- presentation stage in forensics investigations, 1016–1018
- preservation
  - evidence, 1013
  - forensics investigations, 1016–1017
- preset locks, 917
- preshared keys (PSKs) in 802.11 standard, 575
- pressurized conduits for cabling, 653
- pretexting, 865
- Pretty Good Privacy (PGP), 367
- preventive and detective measures
  - anomaly-based intrusion detection and prevention, 967–968
  - antimalware software, 969–972
  - artificial intelligence tools, 976–978
  - firewalls. *See* firewalls
  - intrusion detection and prevention systems
    - overview, 967
  - outsourced security services, 973–974
  - process, 944–945
  - vs. recovery strategies, 1033
  - rule-based intrusion detection and prevention, 967
  - sandboxes, 972–973
  - whitelisting and blacklisting, 968–969
- preventive controls
  - business continuity, 104–105
  - risk responses, 85–87
- PRI (Primary Rate Interface) ISDN, 685–686
- Primary, Alternate, Contingency, and Emergency (PACE) communications plans, 1057
- primary category in PACE plans, 1057
- primary images for evidence, 1012
- Primary Rate Interface (PRI) ISDN, 685–686
- principals in KDC, 785
- principle of least privilege. *See* least privilege principle
- principles in SAML, 780
- priorities in disaster recovery goals, 1054
- privacy
  - classification level, 216–217
  - compliance issues, 147
  - control assessments, 90–91
  - data loss prevention, 270
  - incident investigations, 1014
  - policies, 40
  - requirements, 158
  - retina scan issues, 727
  - SDLC assessments, 1082
  - vs. security, 21

- privacy by design, 397
  - network security, 599
  - site and facility security, 423
  - third-party connectivity, 706
  - web services, 612
- Privacy by Design: Delivering the Promises* report, 397
- Private Branch Exchanges (PBXs), 665–667
- private clouds, 301, 305
- private keys
  - asymmetric key cryptography, 335
  - hybrid methods, 347
  - RSA, 340–341
- private portions in objects, 1128
- privilege escalation
  - identity and access, 799–800
  - software development, 1089
- privileged account management (PAM), 889
- PRNGs (pseudorandom number generators), 327, 370
- proactive searching in threat hunting, 943
- probationary periods in employment, 37
- procedural programming vs. object-oriented programming, 1125–1126
- procedures, 32
- process enhancement, 16
- process reengineering, 16
- processes
  - organizational, 17–18
  - race conditions, 717
  - vulnerabilities, 59–60, 902
- processing speed in biometric authentication, 726
- processors
  - data, 244–245
  - security extensions, 410
- professional ethics, 44–46
- Professional Practices for Business Continuity Management, 106
- Professional Practices (PP) in Good Practice Guidelines, 105–106
- profile updates, 740
- program effectiveness evaluation, 43–44
- programmable locks, 920
- programmable logic controllers (PLCs), 290–291
- programming languages and concepts.
  - See also* software development
  - assemblers, compilers, and interpreters, 1120–1122
  - levels, 1120
  - object-oriented programming, 1124–1130
  - overview, 1117–1120
  - runtime environments, 1122–1124
- Project Athena, 784
- project management in SDLC, 1081
- project managers (PMs) in software development, 1080
- project sizing factor in risk assessment, 64
- proofing of identity, 738–740
- protect function in Framework Core, 182
- Protected EAP (PEAP), 580
- protocol data units (PDUs)
  - description, 473
  - TCP, 509
- prototypes in software development, 1096
- provisioning
  - assets, 227–228
  - configuration management, 894–895
  - identity and access, 796
  - users, 739
- Provisioning Service Provider (PSP)
  - in SPML, 778
- Provisioning Service Target (PST)
  - in SPML, 778
- proximate causes, 161
- proximity detectors, 927
- proxy firewalls
  - application-level, 954–955, 957
  - circuit-level, 954–956
  - overview, 952–953
- proxy servers
  - characteristics, 665
  - overview, 663–664
  - SIP, 690
- pseudorandom number generators (PRNGs), 327, 370
- PSKs (preshared keys) in 802.11
  - standard, 575
- PSP (Provisioning Service Provider)
  - in SPML, 778
- PST (Provisioning Service Target)
  - in SPML, 778

- PSTNs (public switched telephone networks), 582–583, 682–683
- PTZ (pan, tilt, or zoom) capabilities in CCTV systems, 916
- public algorithms vs. secret, 369
- public classification level, 216–217
- public clouds, 301, 305
- public disclosure in incident response, 993
- public key cryptography, 328
- Public Key Cryptography Standards (PKCS), 626
- public key infrastructure (PKI)
  - certificate authorities, 360–362
  - code repositories, 1144
  - digital certificates, 359–360
  - key management, 364–367
  - overview, 359
  - registration authorities, 362
  - steps, 362–364
- public keys
  - asymmetric key cryptography, 335
  - hybrid methods, 347–348
  - RSA, 340–341
- public relations factor in incident response teams, 1001
- public switched telephone networks (PSTNs), 582–583, 682–683
- Purpose Specification Principle in OECD, 142
- PVC (polyvinyl chloride) jacket covering, 653
- PVCs (permanent virtual circuits), 549
- Python programming language, 1121–1122

## Q

- QA (quality assurance) in software development, 1080
- QKD (quantum key distribution), 344
- QoS (Quality of Service)
  - ATM, 551–552
  - availability, 1050–1051
- qualitative risk analysis
  - description, 72
  - overview, 76–78
- quality, defined, 1117
- quality assurance (QA) in software development, 1080
- Quality of Service (QoS)
  - ATM, 551–552
  - availability, 1050–1051
- quantifiability of security metrics, 854
- quantifying security, 851–853
- quantitative risk analysis
  - description, 72
  - vs. qualitative, 78–79
  - results, 75–76
  - steps, 73–75
- quantitatively managed level in CMMI, 1108
- quantum cryptography, 344–346
- quantum key distribution (QKD), 344
- queries
  - DNS, 527–528, 616
  - URLs, 615
- quorum authentication
  - description, 34
  - PKI, 366–367

## R

- RA (Requesting Authority) in SPML, 778
- race conditions
  - description, 821
  - processes, 717
- RAD (Rapid Application Development)
  - methodology, 1099–1100
- radio frequency interference (RFI)
  - electric power, 450
  - twisted-pair cabling, 649–650
- RADIUS (Remote Authentication Dial-In User Service)
  - network devices, 501
  - overview, 789–790
  - vs. TACACS, 791–793
- rainbow tables for passwords, 721–722
- raking locks, 922–923
- ramifications with compliance, 158–161
- random access memory (RAM) for Trusted Platform Modules, 405
- random numbers in cryptology, 327
- random password generation, 736
- random values in quantum cryptography, 345
- ransomware
  - cryptography, 375
  - protecting backups from, 897–898
  - TLS, 604
- Rapid Application Development (RAD)
  - methodology, 1099–1100
- rapid prototyping in software development, 1096

- RARP (Reverse Address Resolution Protocol), 519
- RAs (registration authorities), 360, 362
- RB-RBAC (rule-based access control), 774
- RBAC (role-based access control) model, 771
  - characteristics, 776
  - core, 772
  - hierarchical, 772–773
- RDP (Remote Desktop Protocol)
  - overview, 700
  - threat intelligence, 943
- RDS (Remote Desktop Services), 943
- reactive searching in threat hunting, 943
- real power, 671
- Real-time Transport Protocol (RTP), 689, 691
- real user monitoring (RUM) vs. synthetic transactions, 832
- realms in Kerberos, 785
- rebar, 439
- reciprocal agreements in disasters recovery, 1047–1048
- recommendations in reports, 873
- reconnaissance stage in Cyber Kill Chain model, 387, 994
- recording forensics investigation
  - interviews, 1019
- recover function in Framework Core, 182
- recovery
  - data loss prevention, 269
  - incidents, 998
  - risk responses, 85, 87
- recovery point objective (RPO)
  - disaster recovery, 1031–1032
  - high availability, 1052
- recovery strategies
  - availability, 1049–1053
  - business process recovery, 1033–1034
  - data backups, 1034–1041
  - documentation, 1041–1042
  - overview, 1029–1033
  - vs. preventive measures, 1033
  - reciprocal agreements, 1047–1048
  - recovery site strategies, 1043–1047
  - redundant sites, 1048–1049
- recovery teams in disaster recovery plans, 1056
- recovery time objective (RTO)
  - disaster recovery, 1031–1033
  - high availability, 1052
- rectilinear filters in QKD, 344
- recursive queries in DNS, 527, 616
- red teaming
  - exercises, 902
  - penetration tests, 827–828
- redirect servers in SIP, 691
- reduced-function devices (RFDs), 570
- reduction analysis in threat modeling, 386–387
- redundancy for quality of service, 1050–1051
- redundant lighting, 912
- redundant sites, 1048–1049
- REEs (rich execution environments), 408–409
- reference monitors, 766
- references for candidates, 37
- reflection attacks in DNS, 620
- registered ports, 507
- registered trademarks, 150
- registrar servers in SIP, 689–690
- registration authorities (RAs), 360, 362
- registration of accounts, 738–740
- regression analysis in artificial intelligence tools, 977
- regression testing in software development, 1091
- regulations. *See* laws and regulations
- regulatory investigation requirements, 162
- regulatory policies, 30
- reinforcing bar, 439
- relevance
  - evidence admissibility, 1013
  - security metrics, 854
- relevant characteristic in threat intelligence, 941
- reliability
  - disaster recovery, 1051–1052
  - evidence admissibility, 1013–1014
  - TCP vs. UDP, 506
- religious law system, 128
- relocation teams in disaster recovery plans, 1056
- relocking function for safes, 222
- remanence, data, 240–244
- remediate phase in software vulnerability scans, 901
- remediation
  - incidents, 999
  - vulnerabilities, 871

- remote access
  - desktop virtualization, 699–701
  - Diameter, 793–795
  - overview, 696, 789
  - RADIUS, 789–790
  - TACACS, 790–793
  - VPNs, 697–699
- Remote Authentication Dial-In User Service (RADIUS)
  - network devices, 501
  - overview, 789–790
  - vs. TACACS, 791–793
- Remote Desktop Protocol (RDP)
  - overview, 700
  - threat intelligence, 943
- Remote Desktop Services (RDS), 943
- remote desktops, 700
- remote journaling for backups, 1039
- remote logging, 831
- remote procedure calls (RPCs), 703–704
- remote terminal units (RTUs)
  - DNP3, 626
  - industrial controls, 290
  - SCADA systems, 294
- removal tools in forensics field kits, 1015
- repeaters
  - characteristics, 665
  - description, 655–656
- replay attacks
  - cryptography, 372–374
  - description, 787
- replication
  - backups, 1039–1040
  - logs, 831
- reports
  - digital forensics, 1021–1022
  - executive summaries, 872–875
  - incident response, 993
  - incidents, 997–998
  - overview, 869–870
  - penetration testing, 825
  - risk, 94–95
  - security results, 870–872
  - technical, 872–873
- repositories
  - backups, 1039
  - code, 1143–1144
  - identity, 739
- Representational State Transfer (REST), 615–616
- repudiation category in STRIDE model, 388
- reputation-based protection for antimalware software, 971
- reputation factor
  - disaster recovery, 1054
  - outsourced security services, 974
- request methods in HTTP, 614
- Requesting Authority (RA) in SPML, 778
- requests in change management, 891
- requirements gathering in SDLC, 1080, 1082–1083
- resets for passwords, 737–738
- residual risk vs. total risk, 81
- resilience
  - data loss prevention, 272
  - system, 1051
- resolvers in DNS, 527–528
- resource owners in OAuth, 782
- resource protection
  - backups, 896–899
  - overview, 895–896
  - source files, 896
  - system images, 896
- resource records in DNS, 525
- resource servers in OAuth, 782
- respond function in Framework Core, 182
- responses
  - disaster recovery plans, 1055
  - incidents, 996
  - physical security, 908
  - risk. *See* risk responses
  - site planning, 424
  - SOAR, 980
- responsibility
  - description, 161
  - disaster recovery goals, 1053
  - organizational. *See* organizational roles and responsibilities
- responsive area illumination, 912
- REST (Representational State Transfer), 615–616
- restoration
  - backups, 1037, 1041–1042
  - disaster recovery plans, 1058–1060
- restoration teams in disaster recovery plans, 1056



- restricted areas, 443
- results, analyzing, 870–872
- retention
  - assets, 228–230
  - data, 233–236
- retina scans, 727
- reusability in object-oriented programming, 1127
- reuse methodology in software development, 1105
- Reverse Address Resolution Protocol (RARP), 519
- reverse engineering attacks
  - in cryptography, 371
- reverse engineering patches, 905
- reverse proxies, 664
- reviews
  - audits, 743–744
  - change management, 892
- RFIDs (reduced-function devices), 570
- RFI (radio frequency interference)
  - electric power, 450
  - twisted-pair cabling, 649–650
- rich execution environments (REEs), 408–409
- right to be forgotten provision in GDPR, 144
- right to be informed provision in GDPR, 144
- right to restrict processing provision in GDPR, 144
- ring topology, 489
- RIP (Routing Information Protocol), 535
- risk
  - defined, 9
  - FAIR, 179
  - frameworks, 172–179
  - ISO/IEC 27005, 177–179
  - metrics, 854
  - OCTAVE, 178–179
  - Spiral methodology, 1098–1099
- risk analysis
  - qualitative, 72, 76–78
  - quantitative, 72–76, 78–79
  - software security, 1144–1145
- risk assessment
  - approaches, 72–76
  - asset valuation, 65–66
  - business impact analysis, 109–112
  - methodologies, 67–72
  - monitoring risk, 91–96
  - overview, 63–64
  - preventive and detective measures, 944
  - responses. *See* risk responses
  - SDLC, 1082–1083
  - teams, 66–67
- risk-based access control, 775–776
- risk-level acceptance in SDLC, 1082
- risk management
  - assessment. *See* risk assessment
  - business continuity. *See* business continuity (BC)
  - chapter questions, 118–123
  - chapter review, 116–118
  - concepts, 53–54
  - holistic, 54–55
  - information systems risk management
    - policy, 56
  - overview, 53
  - process, 57–58
  - risk analysis, 72–79
  - supply chain, 96–101
  - teams, 56–57
  - threats, 60–63
  - vulnerabilities, 58–60, 62–63
- Risk Management Framework, 172–177
- risk responses
  - control assessments, 88–91
  - control types, 83–88
  - countermeasure selection and implementation, 81–83
  - overview, 79–80
  - risk management response, 57
  - total risk vs. residual risk, 81
- Rivest, Ron, 340, 352
- roaming 802.11f standard, 574
- robustness of security metrics, 854
- role-based access control (RBAC) model, 771
  - characteristics, 776
  - core, 772
  - hierarchical, 772–773
- roles and responsibilities
  - data, 244–245
  - definitions, 799
  - incident response plans, 1000–1002
  - organizational. *See* organizational roles and responsibilities
  - separation of duties, 394
  - software development, 1080
  - tasks and responsibilities, 886



- rollback plans, 905
- rolling hot sites, 1049
- root account, 859
- round-trip time (RTT) in latency, 654
- route flapping, 535
- routers
  - vs. bridges, 657
  - characteristics, 665
  - overview, 660–662
- Routing Information Protocol (RIP), 535
- routing policies in BGP, 537
- routing protocols
  - attacks, 537
  - autonomous systems, 533–534
  - distance-vector vs. link-state, 535
  - dynamic vs. static, 534–535
  - exterior, 536–537
  - interior, 535–536
- RPC security (RPCSEC), 704
- RPCs (remote procedure calls), 703–704
- RPO (recovery point objective)
  - disaster recovery, 1031–1032
  - high availability, 1052
- RSA algorithm, 340–342
- RSA-CRT (Chinese Remainder Theorem), 372
- RSA SecurID, 730–732
- RTCP (RTP Control Protocol), 691
- RTEs (runtime environments), 1122–1124
- RTO (recovery time objective)
  - disaster recovery, 1031–1033
  - high availability, 1052
- RTP Control Protocol (RTCP), 691
- RTP (Real-time Transport Protocol), 689, 691
- RTT (round-trip time) in latency, 654
- RTUs (remote terminal units)
  - DNP3, 626
  - industrial controls, 290
  - SCADA systems, 294
- Ruff, Howard, 1029
- rule-based access control (RB-RBAC), 774
- rule-based IDS/IPS, 967
- rules in PKI key management, 366–367
- RUM (real user monitoring) vs. synthetic transactions, 832
- runbooks for incidents, 1006
- runtime environments (RTEs), 1122–1124

## S

- S/MIME (Secure MIME), 626
- SaaS (Software as a Service), 228, 302–303
- SABSA (Sherwood Applied Business Security Architecture), 14–15, 173
- SACs (single-attached concentrators) in FDDI, 498
- Safe Harbor Privacy Principles, 143
- “Safeguarding Against and Responding to the Breach of Personally Identifiable Information,” 140
- safes, 221–222
- safety issues
  - disaster recovery, 1059
  - fires, 454–457
  - personnel. *See* personnel safety and security
- sags in electric power, 451
- salvage teams in disaster recovery plans, 1056
- SAML (Security Assertion Markup Language), 779–780
- SAMM (Software Assurance Maturity Model), 1109–1110
- sandboxes
  - antimalware, 969–970, 972–973
  - Java Virtual Machine, 1123
- sanitized media, 259
- Sarbanes-Oxley Act (SOX), 20
- SAs (security associations) in IPSec, 608
- SASL (Simple Authentication and Security Layer), 624
- SASs (single-attachment stations) in FDDI, 498
- SAST (static application security testing), 1139
- satellite communications, 589–590
- SCADA (supervisory control and data acquisition) systems, 290, 294
- scalability
  - Kerberos, 785
  - packet-filtering firewalls, 948
  - stateful firewalls, 952
- scans
  - devices, 226
  - facial, 728
  - iris, 727
  - palm, 727
  - retina, 727
  - software vulnerabilities, 901

- scenarios for backups, 863
- schemes in URLs, 613
- Schneier, Bruce, 385
- Scientific Working Group on Digital Evidence (SWGDE), 1009
- SCIFs (sensitive compartmented information facilities), 443
- SCM (software configuration management), 1142
- scope creep in project management, 1081
- scope of audits, 839
- scope values in OIDS, 784
- scoping controls, 258
- SCPs (service control points), 683
- screen sharing in meeting applications, 694
- screened host firewalls, 959–960, 963
- screened subnet firewalls, 960–962
- screening candidates, 35–36
- screens in information access control, 801
- script kiddies, 60, 135
- scrubbing logs, 744
- Scrum methodology, 1101–1102
- scytale ciphers, 318
- SD-WAN (software-defined wide area networking), 635
- SDLC. *See* software development life cycle (SDLC)
- SDN. *See* software-defined networking (SDN)
- sealing systems, 405
- second-generation (2G) mobile wireless, 585–586
- second-generation programming languages, 1118
- secondary storage in information access control, 801
- SecOps, 887
- secret algorithms vs. public, 369
- secret classification level, 216–218
- secret keys
  - hybrid methods, 348
  - RSA, 340–341
  - symmetric key cryptography, 329
- secure defaults
  - network security, 598
  - third-party connectivity, 706
  - web services, 611
- secure design principles, 390
  - defaults, 396
  - defense in depth, 390–391
  - failing securely, 396–397
  - least privilege, 394–395
  - privacy by design, 397
  - separation of duties, 393–394
  - shared responsibility, 392–393
  - simplicity, 395–396
  - trust but verify, 392
  - zero trust, 392
- secure enclaves in trusted execution environments, 408
- Secure Hash Algorithm (SHA)
  - description, 352
  - passwords, 722
- Secure MIME (S/MIME), 626
- Secure Shell (SSH)
  - code repositories, 1144
  - communications channels, 701–702
- secure software
  - acquired software, 1145–1148
  - APIs, 1132
  - application security testing, 1139–1140
  - assemblers, compilers, and interpreters, 1120–1122
  - assessments, 1144–1145
  - change management, 1145
  - chapter questions, 1150–1153
  - chapter review, 1148–1150
  - code repositories, 1143–1144
  - cohesion and coupling, 1130–1132
  - configuration management, 1142
  - continuous integration and delivery, 1140–1141
  - controls, 1136–1144
  - development platforms, 1137–1138
  - libraries, 1132–1133
  - object-oriented programming, 1124–1130
  - overview, 1117
  - programming languages and concepts, 1117–1120
  - risk analysis and mitigation, 1144–1145
  - runtime environments, 1122–1124
  - secure coding practices, 1134–1136
  - SOAR, 1141–1142
  - source code vulnerabilities, 1133–1134
  - tool sets, 1138

- security
  - aligning to business strategy, 13–16
  - assessments. *See* assessments
  - endpoint, 673–674
  - network. *See* network security
  - policies, 27–29
  - vs. privacy, 21
- security administrators, 24
- security architects, tasks and responsibilities, 886
- security architectures, 385
  - chapter questions, 413–416
  - chapter review, 411–413
  - encryption locations, 411
  - information systems, 404–410
  - secure design principles, 390–397
  - security models, 397–404
  - security requirements, 404
  - threat modeling, 385–390
- Security Assertion Markup Language (SAML), 779–780
- security associations (SAs) in IPSec, 608
- security champions, 43
- security controls. *See* controls
- security directors, tasks and responsibilities, 886
- security effectiveness in control
  - assessments, 90–91
- security film windows, 441
- security information and event management (SIEM) systems
  - event data, 831
  - forensics investigations, 1021
  - incidents, 990–991
  - logs, 744, 979–980
  - security operations centers, 940
- security managers, tasks and responsibilities, 886
- security models
  - Bell-LaPadula, 398–399
  - Biba, 399–400
  - Brewer and Nash, 402
  - Clark-Wilson, 400
  - Graham-Denning, 402
  - Harrison-Ruzzo-Ullman, 402–404
  - noninterference, 400–401
  - overview, 397–398
  - summary, 403
- security operations, 939
  - antimalware software, 969–972
  - artificial intelligence tools, 976–978
  - chapter questions, 984–988
  - chapter review, 982–984
  - firewalls. *See* firewalls
  - honeypots and honeynets, 974–976
  - intrusion detection and prevention systems
    - overview, 967–969
  - logging and monitoring, 978–982
  - outsourced security services, 973–974
  - preventive and detective measures overview, 944–945
  - sandboxes, 972–973
  - security operations centers, 939–943
- security operations centers (SOCs)
  - cyberthreat hunting, 943
  - elements, 940–941
  - overview, 939
  - threat data sources, 942–943
  - threat intelligence, 941–942
- security operations management, 885
  - accountability, 887–888
  - change management, 891–893
  - chapter questions, 934–938
  - chapter review, 932–934
  - configuration management, 893–895
  - foundational concepts overview, 885–887
  - job rotation, 889–890
  - need-to-know and least privilege, 888
  - patch management, 903–906
  - personnel safety and security, 929–932
  - physical security. *See* physical security and controls
  - privileged account management, 889
  - resource protection, 895–899
  - separation of duties and responsibilities, 888–889
  - service level agreements, 890
  - vulnerability management, 900–903
- security orchestration, automation, and response (SOAR) platform
  - components, 980
  - secure software, 1141–1142
- security programs in frameworks, 172, 180–183
- Security Safeguards Principle in OECD, 142
- security zones in CPTED, 429–430

- SecY (MACSec Security Entity), 501
- SEDs (self-encrypting drives), 407
- segmentation, network, 295, 703
- segments in TCP, 509
- SEI (Software Engineering Institute), 993
- select step in Risk Management Framework, 175
- self-encrypting drives (SEDs), 407
- self-healing SONEts, 539
- self-service
  - password resets, 737
  - profile updates, 740
- Sender Policy Framework (SPF), 624
- senior management, awareness
  - programs for, 41–42
- sensitive classification level, 216–217
- sensitive compartmented information facilities (SCIFs), 443
- sensitive data
  - classification, 215
  - data loss prevention, 266, 270
- sensors in incident detection, 995–996
- separation of duties (SoD) principle
  - network security, 599
  - overview, 888–889
  - purpose, 34
  - role-based access control, 773
  - security architectures, 393–394
  - site and facility security, 421
  - software development, 1090
  - third-party connectivity, 706
  - web services, 612
- sequels for tabletop exercises, 1063
- sequence numbers in TCP, 508
- server-based systems, 284–285
- serverless systems, 299–301
- servers
  - clustered, 1051
  - OAuth, 782
  - proxy, 663–664
- service availability risk from unmanaged patching threats, 904
- service bureaus in disaster recovery, 1045
- service control points (SCPs), 683
- service level agreements (SLAs)
  - high availability, 1050
  - overview, 890
  - supply chain risk management, 101
- service-oriented architecture (SOA)
  - description, 780–781
  - web services, 612–613
- Service Provisioning Markup Language (SPML), 777–779
- Service Set IDs (SSIDs), 565
- services in supply chain risk management, 99
- Session Initiation Protocol (SIP), 689–691
- session keys, 349–350
- session layer
  - functions and protocols, 484
  - OSI model, 477–478
- session management, 740–741
- severity levels for incidents, 1003
- SGML (Standard Generalized Markup Language), 776
- SHA (Secure Hash Algorithm)
  - description, 352
  - passwords, 722
- shallow depth of focus in CCTV systems, 915
- Shamir, Adi, 340
- Shannon, Claude, 332
- shared key authentication (SKA), 575
- shared portions in objects, 1128
- shared responsibility principle
  - network security, 599
  - security design, 392–393
  - site and facility security, 420–421
  - third-party connectivity, 706
  - web services, 612
- shareware, 153
- sharing data, 238–239
- Shedd, William G.T., 53
- Sherwood Applied Business Security Architecture (SABSA), 14–15, 173
- shielded twisted pair (STP) cable, 649
- Shkreli, Martin, 20
- Shortest Path Bridging (SPB) protocol, 657
- shoulder surfing, 5
- side-channel attacks
  - cryptography, 371–372
  - description, 257
  - smart cards, 734–735
- SIEM systems. *See* security information and event management (SIEM) systems
- signal switching points (SSPs), 682
- signal transfer points (STPs), 683
- Signaling System 7 (SS7) protocol, 682

- signature-based detection in antimalware software, 969, 971
- signature dynamics, 727–728
- signatures in antimalware software, 969
- Simple Authentication and Security Layer (SASL), 624
- simple integrity axiom in Biba model, 399
- Simple Mail Transfer Protocol (SMTP), 622
- Simple Network Management Protocol (SNMP), 522–524
- Simple Object Access Protocol (SOAP), 614–615, 780
- simple security rule in Bell-LaPadula, 398
- simplex communication, 831
- simplex mode in session layer, 478
- simplicity
  - network security, 599
  - secure design principles, 395–396
  - security metrics, 854
  - site and facility security, 422
  - third-party connectivity, 706
- Simpson, O.J., 129–130
- simulation tests in disaster recovery plans, 1064
- simulations for breach attacks, 828
- single-attached concentrators (SACs) in FDDI, 498
- single-attachment stations (SASs) in FDDI, 498
- single loss expectancy (SLE)
  - key risk indicators, 857
  - quantitative risk analysis, 73–75
- single mode in fiber-optic cable, 651
- single sign-on (SSO)
  - identity management, 750–752
  - replay attacks, 372–373
- SIP (Session Initiation Protocol), 689–691
- site and facility security
  - access control, 802–803
  - backups, 1040–1041
  - chapter questions, 463–465
  - chapter review, 461–462
  - controls. *See* controls for site and facilities
  - CPTED, 427–433
  - defaults, 422
  - defense in depth, 419
  - design overview, 417–418
  - least privilege, 421
  - locks, 917–923
  - overview, 417, 916–917
  - physical security programs, 433–441
  - planning steps, 423–427
  - principles, 418–423
  - privacy by design, 423
  - separation of duties, 421
  - shared responsibility, 420–421
  - simplicity, 422
  - threat modeling, 418–419
  - trust but verify, 420
  - zero trust, 419–420
- Site Security Design Guide*, 906
- situational awareness, 744
- 6to4 tunneling method, 514
- Six Sigma methodology, 197
- SKA (shared key authentication), 575
- Slack service, 1057
- SLAs (service level agreements)
  - high availability, 1050
  - overview, 890
  - supply chain risk management, 101
- SLE (single loss expectancy)
  - key risk indicators, 857
  - quantitative risk analysis, 73–75
- slot locks, 921
- smart cards
  - access codes, 921
  - attacks on, 734–735
  - ownership-based authentication, 733–735
- smart phones, 688
- smoke-activated fire suppression, 456
- smoke detectors, 445
- SMTP (Simple Mail Transfer Protocol), 622
- Smyth, Robin, 20
- SNMP (Simple Network Management Protocol), 522–524
- snooping in DHCP, 519
- Snowden, Edward, 62
- SOA (service-oriented architecture)
  - description, 780–781
  - web services, 612–613
- SOAP (Simple Object Access Protocol), 614–615, 780
- SOAR (security orchestration, automation, and response) platform
  - components, 980
  - secure software, 1141–1142

- social engineering
  - awareness programs, 42
  - cryptography attacks, 375
  - description, 5, 60
  - human vulnerabilities, 902–903
  - passwords, 721
  - training, 864–865
- social network vulnerabilities, 60
- sockets
  - description, 504
  - network, 703
- SOCKS proxy firewalls, 956
- SOCs. *See* security operations centers (SOCs)
- SoD principle. *See* separation of duties (SoD) principle
- soft controls for risk responses, 83
- soft tokens in one-time passwords, 732
- software
  - antimalware, 969–972
  - backups in business continuity planning, 1070
  - cryptography systems, 602
  - escrow, 1070, 1143
  - licensing, 226
  - meeting applications, 695
  - piracy, 153–154
  - secure. *See* secure software
  - smart card attacks, 735
  - supply chain risk management, 99
  - tracking, 224–227
  - vulnerabilities, 901
- Software as a Service (SaaS), 228, 302–303
- Software Assurance Maturity Model (SAMM), 1109–1110
- software configuration
  - management (SCM), 1142
- software-defined networking (SDN)
  - approaches, 634–635
  - control and forwarding planes, 633–634
  - overview, 632–633
  - secure software, 1136
- software-defined security (SDS), 1136
- software-defined wide area networking (SD-WAN), 635
- software developers, tasks and responsibilities, 886
- software development
  - Agile methodologies, 1100–1103
  - chapter questions, 1112–1116
  - chapter review, 1110–1111
  - cleanroom methodology, 1105
  - DevOps, 1103–1104
  - DevSecOps, 1104
  - exploratory methodology, 1104
  - Incremental methodology, 1096–1097
  - Joint Application Development
    - methodology, 1104
  - maturity models, 1106–1110
  - methodologies overview, 1095
  - methodologies summary, 1106
  - overview, 1079
  - prototypes, 1096
  - Rapid Application Development
    - methodology, 1099–1100
  - reuse methodology, 1105
  - roles, 1080
  - SDLC. *See* software development life cycle (SDLC)
  - Spiral methodology, 1098–1099
  - Waterfall methodology, 1095–1096
- software development life cycle (SDLC)
  - design phase, 1083–1087
  - development phase, 1087–1089
  - operations and maintenance phase, 1091–1094
  - overview, 1079–1080
  - phases summary, 1094
  - project management, 1081
  - requirements gathering phase, 1082–1083
  - testing phase, 1089–1091
- Software Engineering Institute (SEI), 993
- software engineers, 1080
- software guard in MAC, 770
- Software Requirements Specification (SRS), 1083
- solar window film windows, 441
- solid-core doors, 440
- something a person does authentication factor, 718
- something a person has authentication factor, 718–719
- something a person is authentication factor, 718
- something a person knows authentication factor, 718

- somewhere a person is authentication factor, 718
- SONETs (Synchronous Optical Networks), 538–539
- source code analysis attacks
  - in cryptography, 370
- source code vulnerabilities, 1133–1134
- source files, protecting, 896
- source routing in firewalls, 966
- Soviet Union collapse, increase of attacks from, 134
- SOW (statements of work) in project management, 1081
- SOX (Sarbanes-Oxley Act), 20
- Spafford, Eugene H., 3
- spaghetti code, 1126
- Spanning Tree Protocol (STP), 657
- SPB (Shortest Path Bridging) protocol, 657
- spearphishing, 865
- Specht, Paul, 150
- special characters in passwords, 720
- Spectre attacks, 257, 372
- speed
  - biometric authentication, 726
  - TCP vs. UDP, 506
- SPF (Sender Policy Framework), 624
- spikes in electric power, 451
- Spiral methodology for software development, 1098–1099
- split knowledge, 34
- split tunnels in VPNs, 697
- splitting DNS, 530
- Splunk product, 979
- SPML (Service Provisioning Markup Language), 777–779
- spoofing
  - e-mail, 623
  - firewalls, 965
  - STRIDE model, 388
- spread spectrum wireless communications, 561–563
- sprinklers, 459–460
- sprints in Scrum methodology, 1102
- SRKs (storage root keys) in Trusted Platform Modules, 405
- SRS (Software Requirements Specification), 1083
- SS7 (Signaling System 7) protocol, 682
- SSD (static separation of duty) relations in RBAC, 773
- SSH (Secure Shell)
  - code repositories, 1144
  - communications channels, 701–702
- SSIDs (Service Set IDs), 565
- SSO (single sign-on)
  - identity management, 750–752
  - replay attacks, 372–373
- SSPs (signal switching points), 682
- staff, awareness programs for, 42
- stakeholders
  - enterprise architecture frameworks, 190
  - incident notifications, 1004
- standalone mode in WLANs, 565
- standard changes, 892
- Standard Generalized Markup Language (SGML), 776
- standard windows, 441
- standards
  - business continuity, 104–106
  - coding, 1135–1136
  - controls, 258
  - industry, 156–158
  - logs, 979
  - organizational, 29–31
  - WLANs, 565–574
- standby lighting, 912
- standby UPS systems, 453
- star integrity axiom in Biba model, 399
- star property rule in Bell-LaPadula, 398
- star topology, 488
- start bits, 646
- state actors, 60–61
- state tables
  - stateful firewalls, 949, 952
  - three-way-handshake process, 951
- stateful firewalls, 949–952
- stateful NAT, 533
- stateless inspection in packet-filtering firewalls, 948
- statements of work (SOW) in project management, 1081
- states
  - controls, 254–258
  - TCP connections, 951
- static analysis
  - antimalware software, 970
  - application security, 1139



- static application security
  - testing (SAST), 1139
- static electricity, 454
- static mapping in NAT, 532
- static routing protocols, 534–535
- static separation of duty (SSD) relations
  - in RBAC, 773
- statistical attacks in cryptography, 370
- statistical time-division multiplexing (STDM), 544
- steganography, 264–265
- stegomedium, 265
- Stevens, Ted, 469
- sticky notes in Kanban methodology, 1102–1103
- Stoll, Clifford, 643
- stop bits, 646
- storage, data, 232–233, 259–260
- storage facilities, 447–448
- storage keys in Trusted Platform Modules, 406
- storage root keys (SRKs) in Trusted Platform Modules, 405
- STP (shielded twisted pair) cable, 649
- STP (Spanning Tree Protocol), 657
- STPs (signal transfer points), 683
- strata in NTP, 831
- strategic alignment, 15–16
- stream ciphers in symmetric key cryptography, 333–334
- stream-symmetric ciphers, 575
- streaming protocols, 691
- strict liability category in civil law, 128
- STRIDE model, 387–388
- strong authentication, 718–719
- strong star property rule in Bell-LaPadula, 398
- structured walkthrough tests in disaster recovery plans, 1063
- subjects
  - ABAC, 774
  - data, 245
- subnet masks in IP addresses, 511–512
- subnets in IP addresses, 510–512
- substitution ciphers, 318
- sub-techniques in MITRE ATT&CK framework, 389
- succession planning, 1043
- Sullivan, Joseph, 20
- supernetting IP addresses, 512
- supervisor role, 24
- supervisory control and data acquisition (SCADA) systems, 290, 294
- supply chain risk management
  - attacks, 133
  - hardware, 98
  - minimum security requirements, 100
  - overview, 96–98
  - risk sources, 99–100
  - service level agreements, 101
  - services, 99
  - software, 99
  - upstream and downstream, 98
- supply system threats in site planning, 423
- support agreements, 672
- support staff, tasks and responsibilities, 886
- surges in electric power, 451
- surveillance
  - CPTED, 431–432
  - description, 913
  - digital forensics, 1019–1020
- suspending accounts, 860
- sustain stage in change management, 892
- Sutter Health of California breach, 255
- SVCs (switched virtual circuits), 549
- SWGDE (Scientific Working Group on Digital Evidence), 1009
- swipe cards for ownership-based authentication, 732–733
- switch controls in device locks, 921
- switch spoofing attacks, 632
- switched virtual circuits (SVCs), 549
- switches
  - characteristics, 665
  - layer 3 and 4, 659
  - overview, 657–658
  - VLANs, 630
- switching WANs, 545–547
- symbolic AI approach, 976–978
- symbolic links, 819, 821
- symmetric key cryptography
  - with asymmetric, 346–349
  - block ciphers, 330–333
  - description, 328
  - initialization vectors, 334–335
  - overview, 329–330
  - stream ciphers, 333–334
  - summary, 330



- symmetric services in DSL, 684
- SYN/ACK packets, 508
- SYN floods, 508
- SYN packets, 508, 949–951
- SYN-RECEIVED state in TCP connections, 951
- SYN-SENT state in TCP connections, 951
- synchronization
  - NTP, 830
  - passwords, 737
- Synchronous Optical Networks (SONETs), 538–539
- synchronous replication, 1039
- synchronous token devices for one-time passwords, 730–731
- synchronous transmission, 645–647
- synthetic transactions, 832
- system access control, 802
- system account access review, 798
- system administrators, tasks and responsibilities, 886
- system architectures
  - chapter questions, 311–315
  - chapter review, 310–311
  - client-based, 284
  - cloud-based, 301–305
  - database, 285–286
  - distributed, 307–309
  - high-performance computing, 288–289
  - industrial control systems, 289–296
  - overview, 283
  - pervasive, 305–307
  - server-based, 284–285
  - virtualized systems, 296–301
- system authentication, 579
- system images, 896
- system-level event audits, 742
- system owners, 23–24
- system resilience in availability, 1051
- system sensing access control readers, 925
- system-specific controls in Risk Management Framework, 175
- system-specific policies, 29
- system testing, 818

## T

- T-carriers for WANs, 541–542
- tables
  - forwarding, 656–657
  - rainbow, 721–722

- stateful firewalls, 949, 952
- three-way-handshake process, 951
- tabletop exercises (TTXs) in disaster recovery plans, 1063–1064
- TACACS (Terminal Access Controller Access Control System), 790–793
- TACS (Total Access Communication System), 584
- tactics in MITRE ATT&CK framework, 389
- tailoring controls, 258
- tamper-resistant property in reference monitors, 766
- tampering category in STRIDE model, 388
- tape vaulting for backups, 1039
- tapes for backups, 860
- Target company breach, 96–97
- target hardening vs. CPTED, 428
- targeted penetration tests, 826–827
- targets of attacks, 474
- tar pits, 976
- taxonomies in data retention, 236
- TCG (Trusted Computing Group), 404
- TCP. *See* Transmission Control Protocol (TCP)
- TCP/IP (Transmission Control Protocol/Internet Protocol) suite, 471, 502–503
- TDF (transborder data flow), 146–147
- TDM (time-division multiplexing), 541–542
- TDMA (time division multiple access)
  - GTS, 570
  - mobile communications, 584
- teams
  - backup administrators, 1035
  - business continuity planning, 1030
  - disaster recovery plans, 1056
  - incident response, 991, 1000–1001
  - risk analysis, 76, 78
  - risk assessment, 66–67
  - risk management, 56–57
  - software development, 1080
- technical controls
  - assessments. *See* testing
  - risk responses, 83, 86–87
- technical reports, 872–873
- technical sensors in incident detection, 995
- technological communication protocols, 646
- TEEs (trusted execution environments), 408–411
- telephone calls in PBXs, 665–667

- Telephone Records and Privacy Protection Act, 865
- telephones in disaster recovery plans, 1062
- telepresence in meeting applications, 695
- temperature
  - data processing facilities, 446
  - HVAC systems, 453–454
- tempered windows, 441
- templates for disaster recovery plans, 1059
- Temporal Key Integrity Protocol (TKIP), 577–578
- Teredo tunneling, 514
- Terminal Access Controller Access Control System (TACACS), 790–793
- terminals in H.323, 689
- termination processes in personnel security, 37–38
- territorial reinforcement in CPTED, 431–432
- tertiary sites in disaster recovery, 1046
- Tesla, Nikola, 559
- test coverage, 837
- test-driven development
  - Extreme Programming, 1102
  - software development, 1089
- testing
  - application security, 1139–1140
  - backups, 863
  - code reviews, 833–834
  - code testing, 834–835
  - compliance checks, 838
  - data loss prevention, 270–271
  - disaster recovery goals, 1054
  - disaster recovery plans, 1061–1065
  - federated identity, 755
  - interface, 837
  - log reviews, 828–831
  - misuse cases, 835–836
  - overview, 817
  - penetration, 822–827
  - red teaming, 827–828
  - SDLC, 1080, 1089–1091
  - Spiral methodology, 1098
  - strategies, 813–816
  - synthetic transactions, 832
  - test coverage, 837
  - vulnerabilities, 817–822
- testing mode in anomaly-based IDS/IPS, 967
- text messages in disaster recovery plans, 1056
- TGSs (ticket granting services) in KDC, 785–786
- Thailand, Personal Data Protection Act in, 144
- The Onion Router (TOR), 307
- The Open Group Architecture Framework (TOGAF), 172, 194–195
- The Silk Road, 665
- thermal relocking function in safes, 222
- third-generation (3G) mobile wireless, 585–586
- Third Generation Partnership Project (3GPP), 586
- third-generation programming languages, 1118–1119
- third parties
  - audits, 843–844
  - business continuity planning, 1068
  - connectivity, 705–706
  - dealing with, 39
  - security provided by, 973–974
  - software escrow, 1143
  - software security, 1147
- third-party sensors in incident detection, 995
- third-party services, federated identity with, 754–756
- threat data sources for security operations
  - centers, 942–943
- Threat Dragon, 1087
- threat hunters, tasks and responsibilities, 886
- threat hunting in security operations
  - centers, 943
- threat intelligence analysts on incident response teams, 1001
- threat intelligence in security operations
  - centers, 941–942
- threat modeling
  - attack trees, 386–387
  - Cyber Kill Chain, 387–389
  - importance, 389–390
  - MITRE ATT&CK framework, 389
  - network security, 598
  - overview, 385
  - site and facility security, 418–419
  - software development design, 1086
  - STRIDE, 387–388
  - third-party connectivity, 705
- threat trees in software development
  - design, 1086
- threat working group (TWG), 92

- threats
  - cybercriminals, 60
  - defined, 8
  - duress, 931–932
  - hacktivists, 61
  - identifying, 62–63
  - internal actors, 61–62
  - nation-state actors, 60–61
  - nature, 62
  - overview, 58
  - site planning, 423
- three-factor authentication, 719
- three-way-handshake process
  - SIP, 689
  - TCP, 949–951
- throughput in cabling, 654–655
- thunking, 296
- ticket granting services (TGSs) in KDC, 785–786
- tickets in KDC, 785–788
- Tier 1 (organization view) in risk management, 55
- Tier 2 (mission/business process view) in risk management, 55
- tiers
  - Cybersecurity Framework, 182
  - risk management, 55
- tight coupling software, 1131–1132
- time division multiple access (TDMA)
  - GTS, 570
  - mobile communications, 584
- time-division multiplexing (TDM), 541–542
- time-limited trials for third-party software, 1147
- time-of-check to time-of-use (TOC/TOU)
  - in atomic execution, 410
- time to first byte (TTFB) in latency, 654
- Time to Live (TTL) values in packets, 512
- TIME-WAIT state in TCP connections, 951
- timely characteristic in threat intelligence, 941
- timeouts in session termination, 741
- timing attacks in cryptography, 371–372
- timing smart cards, 735
- TKIP (Temporal Key Integrity Protocol), 577–578
- TLS. *See* Transport Layer Security (TLS)
- TOC/TOU (time-of-check to time-of-use)
  - in atomic execution, 410
- TOGAF (The Open Group Architecture Framework), 172, 194–195
- token passing, 491–492
- Token Ring, 495–496, 499
- tokens
  - electronic access control, 925
  - one-time passwords, 730
- toll fraud
  - IP telephony, 692
  - PBX systems, 666
- tool sets for secure software, 1138
- top-down approach in security programs, 199
- top-level domains in DNS, 527
- top secret classification level, 216–218
- topologies for local area networks, 487–490
- Tor network, 665
- TOR (The Onion Router), 307
- tort law system, 127–129
- Total Access Communication System (TACS), 584
- total risk vs. residual risk, 81
- TPC (Transmit Power Control), 574
- TPMs (Trusted Platform Modules), 404–406
- TPs (transformation procedures)
  - in Clark-Wilson model, 400
- Traceroute tool, 520–522
- tracking
  - digital asset management, 261–262
  - hardware, 224
  - software, 224–227
- trade secrets, 148–149
- trademarks, 150
- traffic direction in packet-filtering firewalls, 948
- traffic-flow security, 601
- traffic shaping in QoS, 551
- trailer hot sites, 1049
- training, 40
  - artificial intelligence tools, 977–978
  - content reviews, 43
  - degrees and certifications, 40–41
  - disaster recovery communications, 1057
  - disaster recovery plans, 1060–1061, 1064–1065
  - evaluating, 43–44
  - incident response, 993
  - measuring security, 863–867
  - methods and techniques, 41–43
  - personnel, 930–931

- training mode in anomaly-based IDS/IPS, 967
  - transactions, synthetic, 832
  - transborder data flow (TDF), 146–147
  - transfer risk strategy
    - ISO/IEC 27005, 178
    - overview, 79
  - transfers in personnel security, 37–38
  - transformation procedures (TPs)
    - in Clark-Wilson model, 400
  - Transmission Control Protocol (TCP)
    - connection-oriented protocol, 479
    - data structures, 509
    - handshakes, 508, 949–951
    - transport layer, 479, 503
    - vs. UDP, 503–506
  - Transmission Control Protocol/Internet Protocol (TCP/IP) suite, 471, 502–503
  - transmission media
    - cabling, 648–655
    - overview, 643–644
    - types, 644–648
  - transmission methods for local area networks, 499–500
  - Transmit Power Control (TPC), 574
  - transparent bridging, 656–657
  - transponders, 925
  - transport adjacency in IPSec, 609
  - transport layer
    - functions and protocols, 484
    - OSI model, 479–480
  - Transport Layer Security (TLS)
    - data in motion, 255–256
    - malware using, 604–605
    - network security, 602–605
    - suites, 603–604
    - types, 610–611
  - transport supplies in forensics field kits, 1015
  - transposition ciphers, 318
  - travel safety, 930
  - tree topology, 488
  - trials for third-party software, 1147
  - trialware, 153
  - TrickBot Trojan, 604, 969
  - Trojans in TLS, 604
  - trust but verify principle
    - network security, 599
    - secure architectures, 392
    - site and facility security, 420
    - third-party connectivity, 706
    - web services, 612
  - Trust Centers for mobile communications, 572
  - trust in federated identity, 755
  - Trusted Computing Group (TCG), 404
  - trusted execution environments (TEEs), 408–411
  - Trusted Platform Modules (TPMs), 404–406
  - TTFB (time to first byte) in latency, 654
  - TTL (Time to Live) values in packets, 512
  - TTXs (tabletop exercises) in disaster recovery plans, 1063–1064
  - tumbler locks, 918
  - tuning data loss prevention, 270–271
  - tunnels
    - DNS, 619
    - ICMP, 520
    - IPv6, 514–515
    - TLS, 610
  - turnstiles, 441
  - Tuzman, Kaleil Isaza, 20
  - TWG (threat working group), 92
  - twisted-pair cabling, 649–650
  - two-factor authentication (2FA), 719
  - type 1 hypervisors in virtual machines, 297
  - type 2 hypervisors in virtual machines, 297
  - Type I errors in biometric authentication, 724–725
  - Type II errors in biometric authentication, 724–725
  - types in incidents classification, 1002
- ## U
- U.S. Patent and Trademark Office (USPTO), 150
  - UAC (User Agent Client) in SIP, 689
  - UAS (User Agent Server) in SIP, 689
  - ubiquitous computing, 305
  - UBR (unspecified bit rate) in ATM, 551
  - UC (unified communications), 695–696
  - UCDs (use case diagrams) in software development, 1083
  - UDIs (unconstrained data items) in Clark-Wilson model, 400
  - UDP. *See* User Datagram Protocol (UDP)
  - UEBA (user and entity behavior analytics), 981

- UEM (unified endpoint management) systems, 226
  - UML (Unified Modeling Language)
    - software development, 1083
    - use case diagrams, 835–836
  - uncertainty in risk assessment, 74
  - unclassified classification level, 216–218
  - unconstrained data items (UDIs)
    - in Clark-Wilson model, 400
  - undercover investigations in digital forensics, 1020
  - understanding factor in outsourced security services, 974
  - unicast transmission method, 499
  - unified communications (UC), 695–696
  - unified endpoint management (UEM) systems, 226
  - Unified Modeling Language (UML)
    - software development, 1083
    - use case diagrams, 835–836
  - uniform resource identifiers (URIs) for web services, 613–614
  - uniform resource locators (URLs) in DNS, 524, 531
  - uninterruptible power supplies (UPSs)
    - data processing facilities, 446
    - online, 452–453
    - standby, 453
  - unit testing in software development, 1089, 1091
  - United States laws for data breaches, 141–142
  - unmanaged patching, 904–905
  - unshielded twisted pair (UTP) cable, 649–650
  - unspecified bit rate (UBR) in ATM, 551
  - updates
    - Internet of Things, 307
    - profiles, 740
  - UPS Brown color, 150
  - UPSs (uninterruptible power supplies)
    - data processing facilities, 446
    - online, 452–453
    - standby, 453
  - upstream suppliers in risk management, 98
  - uptime in high availability, 1050
  - urgency in incidents classification, 1002
  - URIs (uniform resource identifiers) for web services, 613–614
  - URLs (uniform resource locators) in DNS, 524, 531
  - usage in TCP vs. UDP, 506
  - use case diagrams (UCDs) in software development, 1083
  - use cases
    - data loss prevention, 271
    - misuse case testing, 835–836
  - Use Limitation Principle in OECD, 142
  - user access review for identity and access, 797
  - user-activated readers, 925
  - User Agent Client (UAC) in SIP, 689
  - User Agent Server (UAS) in SIP, 689
  - user and entity behavior analytics (UEBA), 981
  - user data file backups, 861
  - User Datagram Protocol (UDP)
    - connectionless protocol, 479
    - connections, 951–952
    - vs. TCP, 503–506
    - transport layer, 479
  - user-level event audits, 743
  - user managers, 24
  - user stories in Agile methodologies, 1101
  - users
    - Clark-Wilson model, 400
    - description, 25
    - provisioning, 739
  - USPTO (U.S. Patent and Trademark Office), 150
  - utilities
    - electric power, 448–453
    - HVAC, 453–454
    - water and wastewater, 448–450
  - utility tunnels in physical security, 439
  - UTP (unshielded twisted pair) cable, 649–650
- ## V
- vacations, mandatory, 35, 890
  - Valasek, Chris, 627
  - validation
    - assessments, 815–816
    - parameters, 1132
    - risk controls, 90
    - software development, 1090
  - Validation practice in Good Practice Guidelines, 106
  - valuation of assets, 65–66
  - variable bit rate (VBR) in ATM, 551
  - vaulting for backups, 1038–1039
  - vaults, protecting, 222

- VBR (variable bit rate) in ATM, 551
- VDI (virtual desktop infrastructure), 700–701
- VDSL (very high-data-rate DSL), 684
- vendors, 39
- ventilation ducts in physical security, 439
- Veracode report, 1133
- verifiable property for reference monitors, 766
- verification
  - backups, 860–862
  - message integrity, 354–358
  - risk controls, 90
  - software development, 1090
  - supply chain risk management, 100
- verification 1:1, 718
- Verification function in SAMM, 1109
- Vernam, Gilbert, 325
- Vernam cipher, 325–328
- versatile memory in Trusted Platform Modules, 406
- versioning software, 1142–1144
- vertical enactment for privacy, 147
- very high-data-rate DSL (VDSL), 684
- very high-level programming languages, 1119–1120
- very small aperture terminals (VSATs), 589–590
- vibration detectors, 927
- VIDs (VLAN identifiers), 631
- views in enterprise architecture frameworks, 190, 192
- Vigenère, Blaise de, 319
- Vigenère cipher, 319
- violence, threats of, 931–932
- virtual circuits in WANs, 548–549
- virtual desktop infrastructure (VDI), 700–701
- virtual directories, 750
- Virtual eXtensible Local Area Networks (VxLANs), 632
- virtual firewalls, 964
- virtual local area networks (VLANs)
  - latency, 654
  - overview, 630–632
- virtual machines (VMs), 296, 704–705
  - antimalware, 969–970
  - benefits, 297–298
  - hypervisors, 297
  - third-party connectivity, 705
- Virtual Network Computing (VNC), 700
- virtual NICs (vNICs), 704–705
- virtual passwords, 723
- virtual private clouds (VPCs), 301
- virtual private networks (VPNs)
  - authentication protocols, 697–699
  - data in motion, 256
  - IPSec, 607–609
  - L2TP, 606–607
  - overview, 605, 697
  - PPTP, 606
  - TLS, 610
- Virtual Router Redundancy Protocol (VRRP), 536
- virtual teams in incident response, 991
- virtual tunnel end points (VTEPs), 632
- virtualization
  - backups, 861
  - desktop, 699–701
- virtualized systems
  - containerization, 298–299
  - networks, 704–705
  - overview, 296
  - serverless, 299–301
  - virtual machines, 296–298
- visual recording devices, 913–916
- VLAN identifiers (VIDs), 631
- VLANs (virtual local area networks)
  - latency, 654
  - overview, 630–632
- VMs. *See* virtual machines (VMs)
- VNC (Virtual Network Computing), 700
- vNICs (virtual NICs), 704–705
- voice communications, 682
  - cable modems, 686–687
  - DSL, 683–685
  - IP telephony, 687–692
  - ISDN, 685–686
  - PSTN, 682–683
- voice gateways, 688
- voice over IP (VoIP) networks
  - business continuity planning, 1069
  - vs. IP telephony, 688
  - overview, 687–688
  - security, 693
- voice prints, 728
- voicemail systems, 688
- voices in information access control, 801

- voltage in electrical power, 670
- voltage regulators for electric power, 451
- volumetric IDSs, 926
- VPCs (virtual private clouds), 301
- VPNs. *See* virtual private networks (VPNs)
- VRRP (Virtual Router Redundancy Protocol), 536
- VSATs (very small aperture terminals), 589–590
- VTEPs (virtual tunnel end points), 632
- vulnerabilities
  - defined, 8
  - emergency situations, 869
  - exception handling, 871
  - human, 902–903
  - identifying, 62–63
  - information, 59
  - managing, 900–903
  - overview, 58
  - people, 60
  - processes, 59–60, 902
  - remediation, 871
  - software, 901, 1133–1134
  - testing, 817–822
- vulnerability mapping step in penetration testing, 824
- vulnerability testing vs. penetration tests, 827
- VxLANs (Virtual eXtensible Local Area Networks), 632

## W

- wafer tumbler locks, 919
- waiting room feature for meeting applications, 694
- walkthrough tests in disaster recovery plans, 1063
- walls
  - considerations, 437
  - data processing facilities, 446
- WANs. *See* wide area networks (WANs)
- WAPs (wireless access points), 564–565
- warded locks, 918
- warez sites, 149–150
- warm sites, 1045–1047
- Wassenaar Arrangement, 145–146
- water and wastewater, 448–450
- water detectors, 445
- water lines, 438
- water sprinklers, 459–460
- Waterfall software development, 1095–1096
- watts
  - electrical power, 670–672
  - radio signals, 560
- wave-division multiplexing (WDM), 544
- wave-pattern motion detectors, 927
- WBSs (work breakdown structures) in project management, 1081
- WDM (wave-division multiplexing), 544
- weaponization in Cyber Kill Chain model, 387, 994
- web application security risks, 1134
- web of trust, 367
- web portal functions in FIM systems, 753–754
- web proxies, 665
- web services
  - HTTP, 613–614
  - overview, 611–612
  - REST, 615–616
  - SOAP, 614–615
- Web Services Security (WS-Security or WSS) specification, 615
- well-formed transactions in Clark-Wilson model, 400
- well-known ports, 507
- WEP (Wired Equivalent Privacy), 575–576
- wet chemical fire extinguishers, 459
- wet pipe water sprinkler systems, 460
- whaling, 865
- White, Joe, 20
- white box testing, 826
- whitelisting
  - applications, 225
  - intrusion detection and prevention systems, 968–969
- whole-disk encryption, 255
- Wi-Fi Protected Access 2 (WPA2), 576–578
- wide-angle lenses in CCTV systems, 915
- wide area networks (WANs)
  - ATM, 550–552
  - CSU/DSU, 543–545
  - dedicated links, 541–543
  - frame relay, 547–548
  - HSSI, 552
  - overview, 540
  - switching, 545–547
  - virtual circuits, 548–549
  - X.25, 549–550



- WIDSs (wireless intrusion detection systems), 967
  - WiMAX standard, 569, 587
  - windows
    - considerations, 437
    - types, 441
  - WIPO (World Intellectual Property Organization), 150
  - Wired Equivalent Privacy (WEP), 575–576
  - wired windows, 441
  - wireless access points (WAPs), 564–565
  - wireless intrusion detection systems (WIDSs), 967
  - wireless LANs (WLANs)
    - best practices, 582
    - components, 564–565
    - security, 575–582
    - standards, 565–574
  - wireless networking
    - chapter questions, 592–595
    - chapter review, 590–592
    - communication techniques overview, 559–561
    - mobile communications, 582–588
    - OFDM, 563–564
    - overview, 559
    - satellites, 589–590
    - spread spectrum, 561–563
    - WLAN components, 564–565
    - WLAN security, 575–582
    - WLAN standards, 565–574
  - wireless personal area networks (WPANs), 570
  - wiring closets, 446
  - WLANs. *See* wireless LANs (WLANs)
  - Woods, John F., 1079
  - work area security, 441–443
  - work area separation, 803
  - work breakdown structures (WBSs)
    - in project management, 1081
  - work factor
    - cryptosystems, 325
    - electrical power, 671
  - work factor in RSA, 342
  - work recovery time (WRT) in disaster recovery, 1031–1032
  - working images for evidence, 1012
  - World Intellectual Property Organization (WIPO), 150
  - World Wide Web (WWW), 777
  - WPA Enterprise, 577
  - WPA2 (Wi-Fi Protected Access 2), 576–578
  - WPA3, 578–579
  - WPANs (wireless personal area networks), 570
  - write-once media for logs, 745, 831
  - wrongs against a person category
    - in civil law, 127
  - wrongs against property category
    - in civil law, 127
  - WRT (work recovery time) in disaster recovery, 1031–1032
  - WS-Security specification, 615
  - WSS (Web Services Security) specification, 615
  - WWW (World Wide Web), 777
- ## X
- X.25 protocol, 549–550, 552
  - X.509 certificates, 359
  - XaaS (Everything as a Service), 304–305
  - XACML (Extensible Access Control Markup Language), 781
  - XDR (extended detection and response)
    - platforms, 968
  - XML (Extensible Markup Language), 615, 777
  - XOR operation
    - one-time pads, 326–327
    - stream ciphers, 333
  - XTACACS (Extended TACACS), 790–791
  - YAML Ain't Markup Language (YAML), 615
- ## Y
- Ying, Jun, 20
- ## Z
- Zachman, John, 172, 192
  - Zachman Framework, 172, 192–194
  - zero-day attacks, 971
  - zero knowledge in penetration testing, 825
  - zero trust principle
    - network security, 599
    - secure design, 392
    - site and facility security, 419–420
    - third-party connectivity, 706
    - web services, 612
  - ZigBee standard, 571–572
  - Zimmermann, Phil, 367
  - zombies, 965



zone transfers in DNS, 525

zones

access control, 803

CPTED, 429–430

DNS, 525

lighting, 911

Zoom-bombing, 694

zoom in CCTV systems, 914–915