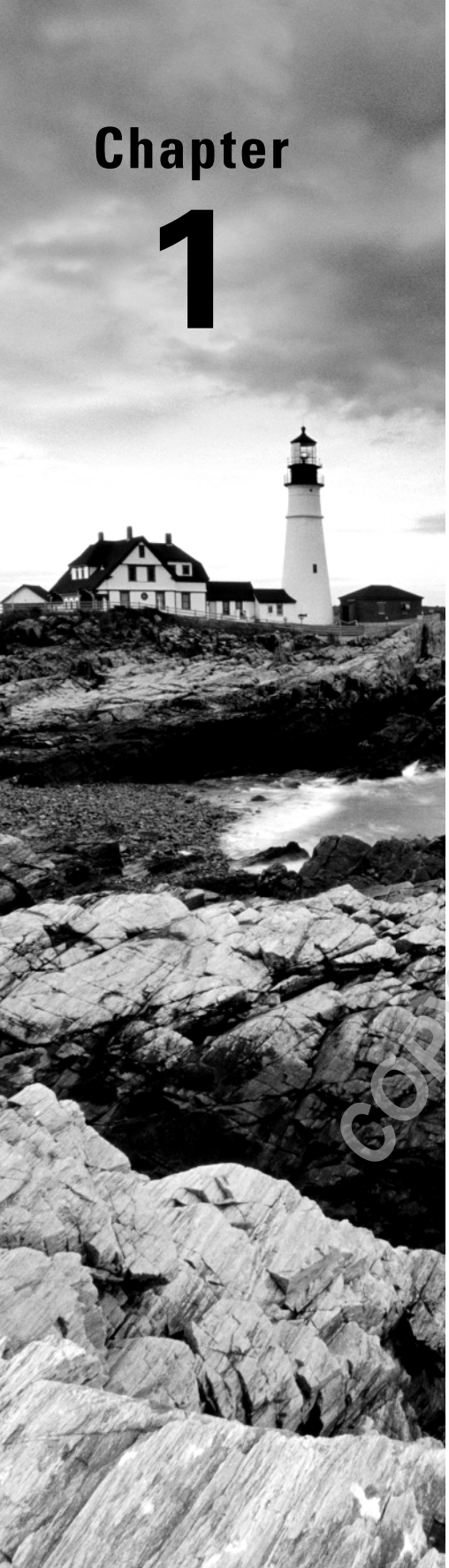

Chapter

1

Domain 1: Architectural Concepts and Design Requirements

Domain 1 of the CCSP CBK is an introductory section that touches on almost every other element of the CBK, so you'll find a wide breadth of content and subject matter ranging over many topics. The questions in this chapter will reflect that broad scope but will also get into some level of detail on certain aspects you'll find pertinent to the exam.

1. Alice is the CEO for a software company; she is considering migrating the operation from the current on-premises legacy environment into the cloud. Which cloud service model should she most likely consider for her company's purposes?
   - **A.** Platform as a service (PaaS)
   - **B.** Software as a service (SaaS)
   - **C.** Backup as a service (Baas)
   - **D.** Information as a service (IaaS)

2. Alice is the CEO for a software company; she is considering migrating the operation from the current on-premises legacy environment into the cloud. Which aspect of cloud computing should she be *most* concerned about, in terms of security issues?
   - **A.** Multitenancy
   - **B.** Metered service
   - **C.** Service-level agreement (SLA)
   - **D.** Remote access

3. Alice is the CEO for a software company; she is considering migrating the operation from the current on-premises legacy environment into the cloud. In order to protect her company's intellectual property, Alice might want to consider implementing all these techniques/solutions *except* _____.
   - **A.** Egress monitoring
   - **B.** Encryption
   - **C.** Turnstiles
   - **D.** Digital watermarking

4. Alice is the CEO for a software company; she is considering migrating the operation from the current on-premises legacy environment into the cloud. What is probably the biggest factor in her decision?
   - **A.** Network scalability
   - **B.** Offsite backup capability
   - **C.** Global accessibility
   - **D.** Reduced overall cost due to outsourcing administration

5. In which of the following situations does the data owner have to administer the OS?
   - **A.** IaaS
   - **B.** PaaS
   - **C.** Offsite archive
   - **D.** SaaS

6. You are setting up a cloud implementation for an online retailer who will accept credit card payments. According to the Payment Card Industry Data Security Standard (PCI DSS), what can you never store for any length of time?
   - **A.** Personal data of consumers
   - **B.** The credit card verification (CCV) number
   - **C.** The credit card number
   - **D.** Home address of the customer

7. The Payment Card Industry Data Security Standard (PCI DSS) distinguishes merchants by different tiers, based on _____.
   - **A.** Number of transactions per year
   - **B.** Dollar value of transactions per year
   - **C.** Geographic location
   - **D.** Jurisdiction

8. What is usually considered the difference between business continuity (BC) efforts and disaster recovery (DR) efforts?
   - **A.** BC involves a recovery time objective (RTO), and DR involves a recovery point objective (RPO).
   - **B.** BC is for events caused by humans (like arson or theft), while DR is for natural disasters.
   - **C.** BC is about maintaining critical functions during a disruption of normal operations, and DR is about recovering to normal operations after a disruption.
   - **D.** BC involves protecting human assets (personnel, staff, users), while DR is about protecting property (assets, data).

9. For business continuity and disaster recovery (BCDR) purposes, the contract between cloud provider and customer should include all of the following *except* _____.
   - **A.** Which party will be responsible for initiating a BCDR response activity
   - **B.** How a BCDR response will be initiated
   - **C.** How soon the customer's data can be ported to a new cloud provider in the event a disruptive event makes the current provider unable to continue service
   - **D.** How much a new cloud provider will charge the customer in the event data has to be ported from the current cloud provider because of a disruptive event

10. When the cloud customer requests modifications to the current contract or service-level agreement (SLA) between the cloud customer and provider for business continuity/disaster recovery (BD/DR) purposes, who should absorb the cost of modification?

A. The customer absorbs the cost.

B. The provider absorbs the cost.

C. The cost should be split equally.

D. Modifications don't cost anything.

11. Which of the following is *not* a factor an organization might use in the cost-benefit analysis when deciding whether to migrate to a cloud environment?

A. Pooled resources in the cloud

B. Shifting from capital expenditures to support IT investment to operational expenditures

C. The time savings and efficiencies offered by the cloud service

D. Branding associated with which cloud provider might be selected

12. Which of the following is the *least* important factor an organization might use in the cost-benefit analysis when deciding whether to migrate to a cloud environment?

A. Depreciation of IT assets

B. Shift in focus from IT dependencies to business process opportunities

C. The cloud provider's proximity to the organization's employees

D. Costs associated with utility consumption

13. Which of the following is an aspect of IT costs that should be reduced by moving into the cloud?

A. Number of users

B. Cost of software licensing

C. Number of applications

D. Number of clientele

14. Which of the following is an aspect of IT costs that should be reduced by moving into the cloud?

A. Utilities costs

B. Security costs

C. Landscaping costs

D. Travel costs

15. Which of the following is an aspect of IT costs that should be reduced by moving into the cloud?

A. Personnel training

B. Personnel turnover

C. Loss due to depreciation of IT assets

D. Loss due to an internal data breach

16. While cloud migration might offer significant cost savings for an organization, which of the following factors might reduce the actual financial benefit the organization realizes in a cloud environment?

A. Altitude of the cloud data center

B. Security controls and countermeasures

C. Loss of ownership of IT assets

D. Costs of Internet connectivity for remote users

17. What is the international standard that dictates creation of an organizational information security management system (ISMS)?

A. NIST SP 800-53

B. PCI DSS

C. ISO 27001

D. NIST SP 800-37

18. ISO 27001 favors which type of technology?

A. Open source

B. PC

C. Cloud based

D. None

19. Why might an organization choose to comply with the ISO 27001 standard?

A. Price

B. Ease of implementation

C. International acceptance

D. Speed

20. Why might an organization choose to comply with NIST SP 800-series standards?

A. Price

B. Ease of implementation

C. International acceptance

D. Speed

21. Which standard contains guidance for selecting, implementing, and managing information security controls mapped to an information security management system (ISMS) framework?

A. ISO 27002

B. Payment Card Industry Data Security Standard (PCI DSS)

C. NIST SP 800-37

D. Health Insurance Portability and Accountability Act (HIPAA)

22. The Statement on Auditing Standards (SAS) 70 , published by the American Institute of Certified Public Accountants (AICPA), was, for a long time, the definitive audit standard for data center customers. It was replaced in 2011 by the _____.

A. SABSA

B. SSAE 16

C. Biba

D. NIST SP 800-53

23. Which US federal law instigated the change from the SAS 70 audit standard to SSAE 16?

A. NIST 800-53

B. HIPAA

C. Sarbanes-Oxley Act (SOX)

D. Gramm-Leach-Bliley Act (GLBA)

24. The Statement on Standards for Attestation Engagements 16 (SSAE 16) Service Organization Control (SOC) reports are audit tools promulgated by the American Institute of Certified Public Accountants (AICPA). What kind of entities were SOC reports designed to audit?

A. US federal government

B. Privately held companies

C. Publicly traded corporations

D. Nonprofit organizations

25. The SSAE 16 Service Organization Control (SOC) reports are audit tools promulgated by the American Institute of Certified Public Accountants (AICPA). As an IT security professional, when reviewing SOC reports for a cloud provider, which report would you *most* like to see?

A. SOC 1

B. SOC 2, Type 1

C. SOC 2, Type 2

D. SOC 3

26. The SSAE 16 Service Organization Control (SOC) reports are audit tools promulgated by the American Institute of Certified Public Accountants (AICPA). As an investor, when reviewing SOC reports for a cloud provider, which report would you *most* like to see?

A. SOC 1

B. SOC 2, Type 1

C. SOC 2, Type 2

D. SOC 3

27. The SSAE 16 Service Organization Control (SOC) reports are audit tools promulgated by the American Institute of Certified Public Accountants (AICPA). You are an IT security professional working for an organization that is considering migrating from your on-premises environment into the cloud. Assuming some have passed SSAE 16 audits and some haven't, which SOC report might be best to use for your initial review of several different cloud providers, in order to narrow down the field of potential services in a fast, easy way?

A. SOC 1

B. SOC 2, Type 1

C. SOC 2, Type 2

D. SOC 3

28. Which of the following entities would *not* be covered by the Payment Card Industry Data Security Standard (PCI DSS)?

A. A bank issuing credit cards

B. A retailer accepting credit cards as payment

C. A business that processes credit card payments on behalf of a retailer

D. A company that offers credit card debt repayment counseling

29. What sort of legal enforcement may the Payment Card Industry (PCI) Security Standards Council *not* bring to bear against organizations that fail to comply with the Payment Card Industry Data Security Standard (PCI DSS)?

A. Fines

B. Jail time

C. Suspension of credit card processing privileges

D. Subject to increased audit frequency and scope

30. The Payment Card Industry Data Security Standard (PCI DSS) merchant levels are based on _____.

A. Dollar value of transactions over the course of a year

B. Number of transactions over the course of a year

C. Location of the merchant or processor

D. Dollar value and number of transactions over the course of a year

31. In terms of greatest stringency and requirements for security validation, which is the highest merchant level in the Payment Card Industry (PCI) standard?

A. 1

B. 2

C. 3

D. 4

32. The Payment Card Industry Data Security Standard (PCI DSS) requires _____ security requirements for entities involved in credit card payments and processing.

A. Technical

B. Nontechnical

C. Technical and nontechnical

D. Neither technical nor nontechnical

33. According to the Payment Card Industry Data Security Standard (PCI DSS), if a merchant is going to store credit cardholder information for any length of time, what type of security protection *must* be used?

A. Tokenization or masking

B. Obfuscation or tokenization

C. Masking or obfuscation

D. Tokenization or encryption

34. What element of credit cardholder information may *never* be stored for any length of time, according to the Payment Card Industry Data Security Standard (PCI DSS)?

A. The full credit card number

B. The card verification value (CVV)

C. The cardholder's mailing address

D. The cardholder's full name

35. When reviewing IT security products that have been subjected to common criteria certification, what does the Evaluation Assurance Level (EAL) tell you?

A. How secure the product is from an external attack

B. How thoroughly the product has been tested

C. The level of security the product delivers to an environment

D. The level of trustworthiness you can have if you deploy the product

36. Which Common Criteria Evaluation Assurance Level (EAL) is granted to those products that are functionally tested by their manufacturer/vendor?

A. 1

B. 3

C. 5

D. 7

37. Which Common Criteria Evaluation Assurance Level (EAL) is granted to those products that are formally verified in terms of design and tested by an independent third party?

A. 1

B. 3

C. 5

D. 7

38. Who pays for the Common Criteria certification of an IT product?

A. NIST

B. The vendor/manufacturer

C. The cloud customer

D. The end user

39. Who publishes the list of cryptographic modules validated according to the Federal Information Processing Standard (FIPS) 140-2?

A. The US Office of Management and Budget (OMB)

B. The International Standards Organization (ISO)

C. $(ISC)^2$

D. The National Institute of Standards and Technology (NIST)

40. Who performs the review process for hardware security modules (HSM) in accordance with FIPS 140-2?

A. The National Institute of Standards and Technology (NIST)

B. The National Security Agency (NSA)

C. Independent (private) laboratories

D. The European Union Agency for Network and Information Security (ENISA)

41. In terms of the amount of security functions offered, which is the highest Federal Information Processing Standard (FIPS) 140-2 security level a cryptographic module can achieve in certification?

A. 1

B. 2

C. 3

D. 4

42. What distinguishes the FIPS 140-2 security levels for cryptographic modules?

A. The level of sensitivity of data they can be used to protect

B. The amount of physical protection provided by the product, in terms of tamper resistance

C. The size of the IT environment the product can be used to protect

D. The geographic locations in which the product is permitted to be used

43. For US government agencies, what level of data sensitivity/classification may be processed by cryptographic modules certified according to the FIPS 140-2 criteria?

A. Controlled Unclassified Information (CUI)

B. Secret

C. Top Secret

D. Sensitive Compartmentalized Information (SCI)

44. Who pays for cryptographic modules to be certified in accordance with FIPS 140-2 criteria?

A. The US government

B. Module vendors

C. Certification laboratories

D. Module users

45. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. What is probably the single *most* important way of countering the highest number of items on the OWASP Top Ten (regardless of year)?

A. Social engineering training

B. Disciplined coding practices and processes

C. White-box source code testing

D. Physical controls at all locations at which the application is eventually used

46. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "injection." In most cases, what is the attacker trying to do with an injection attack?

A. Get the user to allow access for the attacker.

B. Insert malware onto the system.

C. Trick the application into running commands.

D. Penetrate the facility hosting the software.

47. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "injection." In most cases, what is the method for reducing the risk of an injection attack?

A. User training

B. Hardening the OS

C. Input validation/bounds checking

D. Physical locks

48. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "broken authentication and session management." Which of the following is a good method for reducing the risk of broken authentication and session management?

A. Do not use custom authentication schemes.

B. Implement widespread training programs.

C. Ensure that strong input validation is in place.

D. Use X.400 protocol standards.

49. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "broken authentication and session management." Which of the following is *not* a practice/vulnerability that can lead to broken authentication and infringe on session management?

A. Session identification exposed in URLs

B. Unprotected stored credentials

C. Lack of session time-out

D. Failure to follow Health Insurance Portability and Accountability Act (HIPAA) guidance

50. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "broken authentication and session management." Which of the following is *not* a practice/vulnerability that can lead to broken authentication and infringe on session management?

A. Failure to rotate session IDs after a successful login

B. Easily guessed authentication credentials

C. Weak physical entry points in the data center

D. Credentials sent over unencrypted lines

51. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "cross-site scripting (XSS)." Which of the following is *not* a method for reducing the risk of XSS attacks?

A. Only put untrusted data in allowed slots of HTML documents.

B. HTML escape when including untrusted data in any HTML elements

C. Attribute escape when including untrusted data in attribute elements

D. Encrypting all HTML documents

52. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "cross-site scripting (XSS)." Which of the following is *not* a method for reducing the risk of XSS attacks?

A. Use an auto-escaping template system.

B. XML escape all identity assertions.

C. Sanitize HTML markup with a library designed for the purpose.

D. HTML escape JSON values in an HTML context and read the data with `JSON.parse`.

53. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "insecure direct object references." Which of these is an example of an insecure direct object reference?

A. `www.sybex.com/authoraccounts/benmalisow`

B. `10 ? "sybex accounts"; 20 goto 10`

C. `mysql -u [bmalisow] -p [database1];`

D. `bmalisow@sybex.com`

54. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "insecure direct object references." Which of these is a method to counter the risks of insecure direct object references?

A. Performing user security training

B. Check access each time a direct object reference is called by an untrusted source.

C. Install high-luminosity interior lighting throughout the facility.

D. Append each object with sufficient metadata to properly categorize and classify based on asset value and sensitivity.

55. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "security misconfiguration." Which of these is an example of a security misconfiguration?

A. Not providing encryption keys to untrusted users

B. Having a public-facing website

C. Leaving default accounts unchanged

D. Using turnstiles instead of mantraps

56. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "security misconfiguration." Which of these is an example of a security misconfiguration?

A. Having unpatched software in the production environment

B. Leaving unprotected portable media in the workplace

C. Letting data owners determine the classifications/categorizations of their data

D. Preventing users from accessing untrusted networks

57. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "security misconfiguration." Which of these is a technique to reduce the potential for a security misconfiguration?

A. Enforce strong user access control processes.

B. Have a repeatable hardening process for all systems/software.

C. Use encryption for all remote access.

D. Use encryption for all stored data.

58. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "security misconfiguration." Which of these is a technique to reduce the potential for a security misconfiguration?

A. Broad user training that includes initial, recurring, and refresher sessions

B. Deeper personnel screening procedures for privileged users than is used for regular users

C. A repeatable patching process that includes updating libraries as well as software

D. Randomly auditing all user activity, with additional focus on privileged users

59. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "security misconfiguration." Which of these is a technique to reduce the potential for a security misconfiguration?

A. Purchase only trusted devices/components.

B. Follow a published, known industry standard for baseline configurations.

C. Hire only screened, vetted candidates for all positions.

D. Update policy on a regular basis, according to a proven process.

60. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "security misconfiguration." Which of these is a technique to reduce the potential for a security misconfiguration?

A. Get regulatory approval for major configuration modifications.

B. Update the BCDR plan on a timely basis.

C. Train all users on proper security procedures.

D. Perform periodic scans and audits of the environment.

61. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "sensitive data exposure." Which of these is a technique to reduce the potential for a sensitive data exposure?

A. Extensive user training on proper data handling techniques

B. Advanced firewalls inspecting all inbound traffic, to include content-based screening

C. Ensuring the use of utility backup power supplies

D. Roving security guards

62. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "sensitive data exposure." Which of these is *not* a technique to reduce the potential for a sensitive data exposure?

A. Destroy sensitive data as soon as possible.

B. Avoid categorizing data as sensitive.

C. Use proper key management when encrypting sensitive data.

D. Disable autocomplete on forms that collect sensitive data.

63. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "missing function level access control." Which of these is a technique to reduce the potential for a missing function level access control?

A. Set default to deny all access to functions, and require authentication/authorization for each access request.

B. HTML escape all HTML attributes.

C. Restrict permissions based on an access control list (ACL).

D. Refrain from including direct access information in URLs.

64. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "missing function level access control." Which of these is a technique to reduce the potential for a missing function level access control?

A. Run a process as both user and privileged user, and determine similarity.

B. Run automated monitoring and audit scripts.

C. Include browser buttons/navigation elements to secure functions.

D. Enhance user training to include management personnel.

65. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "cross-site request forgery" (CSRF). Which of these is a technique to reduce the potential for a CSRF?

A. Train users to detect forged HTTP requests.

B. Have users remove all browsers from their devices.

C. Don't allow links to or from other websites.

D. Include a CAPTCHA code as part of the user resource request process.

66. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "cross-site request forgery" (CSRF). A CSRF attack might be used for all the following malicious actions *except* _____.

A. The attacker could have the user log in to one of the user's online accounts

B. The attacker could collect the user's online account login credentials, to be used by the attacker later

C. The attacker could have the user perform an action in one of the user's online accounts

D. The attacker could trick the user into calling a fraudulent customer service number hosted by the attacker and talk the user into disclosing personal information

67. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "cross-site request forgery" (CSRF). Which of the following is a good way to deter CSRF attacks?

A. Have your website refuse all HTTP resource requests.

B. Ensure that all HTTP resource requests include a unique, unpredictable token.

C. Don't allow e-commerce on your website.

D. Process all user requests with only one brand of browser, and refuse all resource requests from other browsers.

68. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "using components with known vulnerabilities." Which of the following is a good way to protect against this problem?

A. Use only components your organization has written.

B. Update to current versions of component libraries as soon as possible.

C. Never use anyone else's component library.

D. Apply patches to old component libraries.

69. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "using components with known vulnerabilities." Why would an organization ever use components with known vulnerabilities to create software?

A. The organization is insured.

B. The particular vulnerabilities only exist in a context not being used by developers.

C. Some vulnerabilities only exist in foreign countries.

D. A component might have a hidden vulnerability.

70. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "using components with known vulnerabilities." Which of the following is a good way to protect against this problem?

A. Use only standard libraries.

B. Review all updates/lists/notifications for components your organization uses.

C. Be sure to HTML escape all attribute elements.

D. Increase the user training budget.

71. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "unvalidated redirects and forwards." Which of the following is a good way to protect against this problem?

A. HTML escape all HTML attributes.

B. Train users to recognize unvalidated links.

C. Block all inbound resource requests.

D. Implement audit logging.

72. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "unvalidated redirects and forwards." Which of the following is a good way to protect against this problem?

A. Don't use redirects/forwards in your applications.

B. Refrain from storing credentials long term.

C. Implement security incident/event monitoring (security information and event management (SIEM)/security information management (SIM)/security event management (SEM)) solutions.

D. Implement digital rights management (DRM) solutions.

73. You are the security subject matter expert (SME) for an organization considering a transition from the legacy environment into a hosted cloud provider's data center. One of the challenges you're facing is whether your current applications in the on-premises environment will function properly with the provider's hosted systems and tools. This is a(n) _____ issue.

A. Interoperability

B. Portability

C. Availability

D. Security

74. You are the security subject matter expert (SME) for an organization considering a transition from the legacy environment into a hosted cloud provider's data center. One of the challenges you're facing is whether the provider will have undue control over your data once it is within the provider's data center; will the provider be able to hold your organization hostage because they have your data? This is a(n) _____ issue.

A. Interoperability

B. Portability

C. Availability

D. Security

75. You are the security subject matter expert (SME) for an organization considering a transition from the legacy environment into a hosted cloud provider's data center. One of the challenges you're facing is whether the cloud provider will be able to comply with the existing legislative and contractual frameworks your organization is required to follow. This is a _____ issue.

A. Resiliency

B. Privacy

C. Performance

D. Regulatory

76. You are the security subject matter expert (SME) for an organization considering a transition from the legacy environment into a hosted cloud provider's data center. One of the challenges you're facing is whether the cloud provider will be able to allow your organization to substantiate and determine with some assurance that all of the contract terms are being met. This is a(n) _____ issue.

A. Regulatory

B. Privacy

C. Resiliency

D. Auditability

77. Encryption is an essential tool for affording security to cloud-based operations. While it is possible to encrypt every system, piece of data, and transaction that takes place on the cloud, why might that not be the optimum choice for an organization?

A. Key length variances don't provide any actual additional security.

B. It would cause additional processing overhead and time delay.

C. It might result in vendor lockout.

D. The data subjects might be upset by this.

78. Encryption is an essential tool for affording security to cloud-based operations. While it is possible to encrypt every system, piece of data, and transaction that takes place on the cloud, why might that not be the optimum choice for an organization?

A. It could increase the possibility of physical theft.

B. Encryption won't work throughout the environment.

C. The protection might be disproportionate to the value of the asset(s).

D. Users will be able to see everything within the organization.

79. Which of the following is *not* an element of the identification component of identity and access management (IAM)?

A. Provisioning

B. Management

C. Discretion

D. Deprovisioning

80. Which of the following entities is *most* likely to play a vital role in the identity provisioning aspect of a user's experience in an organization?

A. The accounting department

B. The human resources (HR) office

C. The maintenance team

D. The purchasing office

81. Why is the deprovisioning element of the identification component of identity and access management (IAM) so important?

A. Extra accounts cost so much extra money.

B. Open but unassigned accounts are vulnerabilities.

C. User tracking is essential to performance.

D. Encryption has to be maintained.

82. All of the following are reasons to perform review and maintenance actions on user accounts *except* _____.

A. To determine whether the user still needs the same access

B. To determine whether the user is still with the organization

C. To determine whether the data set is still applicable to the user's role

D. To determine whether the user is still performing well

83. Who should be involved in review and maintenance of user accounts/access?

A. The user's manager

B. The security manager

C. The accounting department

D. The incident response team

84. Which of the following protocols is *most* applicable to the identification process aspect of identity and access management (IAM)?

A. Secure Sockets Layer (SSL)

B. Internet Protocol security (IPsec)

C. Lightweight Directory Access Protocol (LDAP)

D. Amorphous ancillary data transmission (AADT)

85. Privileged user (administrators, managers, and so forth) accounts need to be reviewed more closely than basic user accounts. Why is this?

A. Privileged users have more encryption keys.

B. Regular users are more trustworthy.

C. There are extra controls on privileged user accounts.

D. Privileged users can cause more damage to the organization.

86. The additional review activities that might be performed for privileged user accounts could include all of the following *except* _____.

A. Deeper personnel background checks

B. Review of personal financial accounts for privileged users

C. More frequent reviews of the necessity for access

D. Pat-down checks of privileged users to deter against physical theft

87. If personal financial account reviews are performed as an additional review control for privileged users, which of the following characteristics is *least* likely to be a useful indicator for review purposes?

A. Too much money in the account

B. Too little money in the account

C. The bank branch being used by the privileged user

D. Specific senders/recipients

88. How often should the accounts of privileged users be reviewed?

A. Annually

B. Twice a year

C. Monthly

D. More often than regular user account reviews

89. Privileged user account access should be _____.

A. Temporary

B. Pervasive

C. Thorough

D. Granular

90. The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing. According to the CSA's Notorious Nine list, data breaches can be _____.

A. Overt or covert

B. International or subterranean

C. From internal or external sources

D. Voluminous or specific

91. The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing. According to the CSA, an organization that operates in the cloud environment and suffers a data breach may be required to _____.

A. Notify affected users

B. Reapply for cloud service

C. Scrub all affected physical memory

D. Change regulatory frameworks

92. The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing. According to the CSA, an organization that suffers a data breach might suffer all of the following negative effects *except* _____.

A. Cost of compliance with notification laws

B. Loss of public perception/goodwill

C. Loss of market share

D. Cost of detection

93. The Cloud Security Alliance (CSA) publishes, the Notorious Nine, a list of common threats to organizations participating in cloud computing. According to the CSA, in the event of a data breach, a cloud customer will likely need to comply with all the following data breach notification requirements *except* _____.

A. Multiple state laws

B. Contractual notification requirements

C. All standards-based notification schemes

D. Any applicable federal regulations

94. The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing. According to the CSA, data loss can be suffered as a result of _____ activity.

A. Malicious or inadvertent

B. Casual or explicit

C. Web-based or stand-alone

D. Managed or independent

95. The Cloud Security Alliance (CSA) publishes, the Notorious Nine, a list of common threats to organizations participating in cloud computing. According to the CSA, all of the following activity can result in data loss *except* _____.

A. Misplaced crypto keys

B. Improper policy

C. Ineffectual backup procedures

D. Accidental overwrite

96. The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing. According to the CSA, service traffic highjacking can affect all of the following portions of the CIA triad *except* _____.

A. Confidentiality

B. Integrity

C. Availability

D. None. Service traffic highjacking can't affect any portion of the CIA triad.

97. The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing. The CSA recommends the prohibition of _____ in order to diminish the likelihood of account/service traffic highjacking.

A. All user activity

B. Sharing account credentials between users and services

C. Multifactor authentication

D. Interstate commerce

98. The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing. According to the CSA, which aspect of cloud computing makes it particularly susceptible to account/service traffic highjacking?

A. Scalability

B. Metered service

C. Remote access

D. Pooled resources

99. The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing. According to the CSA, what is one reason the threat of insecure interfaces and APIs is so prevalent in cloud computing?

A. Most of the cloud customer's interaction with resources will be performed through APIs.

B. APIs are inherently insecure.

C. Attackers have already published vulnerabilities for all known APIs.

D. APIs are known carcinogens.

100. The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing. According to the CSA, what is one reason the threat of insecure interfaces and APIs is so prevalent in cloud computing?

A. Cloud customers and third parties are continually enhancing and modifying APIs.

B. APIs can have automated settings.

C. It is impossible to uninstall APIs.

D. APIs are a form of malware.

101. The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing. According to the CSA, what is one reason the threat of insecure interfaces and APIs is so prevalent in cloud computing?

A. APIs are always used for administrative access.

B. Customers perform many high-value tasks via APIs.

C. APIs are cursed.

D. It is impossible to securely code APIs.

102. The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing. According to the CSA, why are denial of service (DoS) attacks such a significant threat to cloud operations?

A. DoS attackers operate internationally.

B. There are no laws against DoS attacks, so they are impossible to prosecute.

C. Availability issues prevent productivity in the cloud.

D. DoS attacks that can affect cloud providers are easy to launch.

103. The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing. According to the CSA, what do we call denial of service (DoS) attacks staged from multiple machines against a specific target?

A. Invasive denial of service (IDoS)

B. Pervasive denial of service (PDoS)

C. Massive denial of service (MDoS)

D. Distributed denial of service (DDoS)

104. The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing. According to the CSA, what aspect of managed cloud services makes the threat of malicious insiders so alarming?

A. Scalability

B. Multitenancy

C. Metered service

D. Flexibility

105. The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing. According to the CSA, what aspect of managed cloud services makes the threat of abuse of cloud services so alarming, from a management perspective?

A. Scalability

B. Multitenancy

C. Resiliency

D. Broadband connections

106. The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing. According to the CSA, which of the following is *not* an aspect of due diligence that the cloud customer should be concerned with when considering a migration to a cloud provider?

A. Ensuring that any legacy applications are not dependent on internal security controls before moving them to the cloud environment

B. Reviewing all contractual elements to appropriately define each party's roles, responsibilities, and requirements

C. Assessing the provider's financial standing and soundness

D. Vetting the cloud provider's administrators and personnel to ensure the same level of trust as the legacy environment

107. The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing. A cloud customer that does not perform sufficient due diligence can suffer harm if the cloud provider they've selected goes out of business. What do we call this problem?

A. Vendor lock-in

B. Vendor lock-out

C. Vendor incapacity

D. Unscaled

108. Which of the following is *not* a method for creating logical segmentation in a cloud data center?

A. Virtual local area networks (VLANs)

B. Network address translation (NAT)

C. Bridging

D. Hubs

109. According to the (ISC)^2 CBK, the lack/ambiguity of physical endpoints as individual network components in the cloud environment creates what kind of threat/concern?

A. The lack of defined endpoints makes it difficult to uniformly define, manage, and protect IT assets.

B. Without physical endpoints, it is impossible to apply security controls to an environment.

C. Without physical endpoints, it is impossible to track user activity.

D. The lack of physical endpoints increases the opportunity for physical theft/damage.

110. When should cloud providers allow PaaS customers shell access to the servers running their instances?

A. Never

B. Weekly

C. Only when the contract stipulates that requirement

D. Always

111. In a PaaS implementation, each instance should have its own user-level permissions; when instances share common policies/controls, the cloud security professional should be careful to reduce the possibility of _____ and _____ over time.

A. Denial of service (DoS)/physical theft

B. Authorization creep/inheritance

C. Sprawl/hashing

D. Intercession/side-channel attacks

112. In a PaaS environment, user access management often requires that data about user activity be collected, analyzed, audited, and reported against rule-based criteria. These criteria are usually based on _____.

A. International standards

B. Federal regulations

C. Organizational policies

D. Federation directives

113. An essential element of access management, _____ is the practice of confirming that an individual is who they claim to be.

A. Authentication

B. Authorization

C. Nonrepudiation

D. Regression

114. An essential element of access management, _____ is the practice of granting permissions based on validated identification.

A. Authentication

B. Authorization

C. Nonrepudiation

D. Regression

115. What is the usual order of an access management process?

A. Access-authorization-authentication

B. Authentication-authorization-access

C. Authorization-authentication-access

D. Authentication-access-authorization

116. Why are PaaS environments at a higher likelihood of suffering backdoor vulnerabilities?

A. They rely on virtualization.

B. They are often used for software development.

C. They have multitenancy.

D. They are scalable.

117. Backdoors are sometimes left in software by developers _____.

A. In lieu of other security controls

B. As a means to counter DoS attacks

C. Inadvertently or on purpose

D. As a way to distract attackers

118. Alice is staging an attack against Bob's website. She is able to introduce a string of command code into a database Bob is running, simply by entering the command string into a data field. This is an example of which type of attack?

A. Insecure direct object reference

B. Buffer overflow

C. SQL injection

D. Denial of service

119. Bob is staging an attack against Alice's website. He is able to embed a link on her site that will execute malicious code on a visitor's machine, if the visitor clicks on the link. This is an example of which type of attack?

A. Cross-site scripting

B. Broken authentication/session management

C. Security misconfiguration

D. Insecure cryptographic storage

120. Alice is staging an attack against Bob's website. She has discovered that Bob has been storing cryptographic keys on a server with a default admin password and is able to get access to those keys and violate confidentiality and access controls. This is an example of which type of attack?

A. SQL injection

B. Buffer overflow

C. Using components with known vulnerabilities

D. Security misconfiguration

121. Which of the following is a new management risk that organizations operating in the cloud will have to address?

A. Insider threat

B. Virtual sprawl

C. Distributed denial of service attacks (DDoS)

D. Natural disasters

122. Which kind of hypervisor is the preferred target of attackers, and why?

A. Type 1, because it is more straightforward

B. Type 1, because it has a greater attack surface

C. Type 2, because it is less protected

D. Type 2, because it has a greater attack surface

123. Which of the following would make a good provision to include in the service-level agreement (SLA) between cloud customer and provider?

A. Location of the data center

B. Amount of data uploaded/downloaded during a pay period

C. Type of personnel security controls for network administrators

D. Physical security barriers on the perimeter of the data center campus

124. What is the *most* significant aspect of the service-level agreement (SLA) that incentivizes the cloud provider to perform?

A. The thoroughness with which it details all aspect of cloud processing

B. The financial penalty for not meeting service-levels

C. The legal liability for violating data breach notification requirements

D. The risk exposure to the cloud provider

125. From a customer perspective, all of the following are benefits of IaaS cloud services *except* _____.

A. Reduced cost of ownership

B. Reduced energy costs

C. Metered usage

D. Reduced cost of administering the operating system (OS) in the cloud environment

126. From an academic perspective, what is the main distinction between an event and an incident?

A. Incidents can last for extended periods (days or weeks), while an event is momentary.

B. Incidents can happen at the network level, while events are restricted to the system level.

C. Events are anything that can occur in the IT environment, while incidents are unscheduled events.

D. Events only occur during processing, while incidents can occur at any time.

127. The cloud computing characteristic of elasticity promotes which aspect of the CIA triad?

A. Confidentiality

B. Integrity

C. Availability

D. None

128. A hosted cloud environment is a great place for an organization to use as _____.

A. Storage of physical assets

B. A testbed/sandbox

C. A platform for managing unsecured production data

D. A cost-free service for meeting all user needs

129. What is the entity that created the Statement on Standards for Attestation Engagements (SSAE) auditing standard and certifies auditors for that standard?

A. NIST

B. ENISA

C. GDPR

D. AICPA

130. The current American Institute of Certified Public Accountants (AICPA) standard codifies certain audit reporting mechanisms. What are these called?

A. Sarbanes-Oxley Act (SOX) reports

B. Secure Sockets Layer (SSL) audits

C. Sherwood Applied Business Structure Architecture (SABSA)

D. System and Organization Controls (SOC) reports

131. Which of the following is *not* a report used to assess the design and selection of security controls within an organization?

A. Consensus Assessments Initiative Questionnaire (CAIQ)

B. Cloud Security Alliance Cloud Controls Matrix (CSA CCM)

C. SOC 1

D. SOC 2 Type 1

132. Which of the following is a report used to assess the implementation and effectiveness of security controls within an organization?

A. SOC 1

B. SOC 2 Type 1

C. SOC 2 Type 2

D. SOC 3

133. _____ is an example of due care, and _____ is an example of due diligence.

A. Privacy data security policy; auditing the controls dictated by the privacy data security policy

B. The EU Data Directive; the Gramm-Leach-Bliley Act (GLBA)

C. Locks on doors; turnstiles

D. Perimeter defenses; internal defenses

134. In a Lightweight Directory Access Protocol (LDAP) environment, each entry in a directory server is identified by a _____.

A. Domain name (DN)

B. Distinguished name (DN)

C. Directory name (DN)

D. Default name (DN)

135. Each of the following is an element of the Identification phase of the identity and access management (IAM) process *except* _____.

A. Provisioning

B. Inversion

C. Management

D. Deprovisioning

136. Which of the following is true about two-person integrity?

A. It forces all employees to distrust each other.

B. It requires two different identity and access management matrices (IAM).

C. It forces collusion for unauthorized access.

D. It enables more thieves to gain access to the facility.

137. All of the following are statutory regulations *except* _____.

A. Gramm-Leach-Bliley Act (GLBA)

B. Health Information Portability and Accountability Act (HIPAA)

C. Federal Information Systems Management Act (FISMA)

D. Payment Card Industry Data Security Standard (PCI DSS)

138. A cloud data encryption situation where the cloud customer retains control of the encryption keys and the cloud provider only processes and stores the data could be considered a _____.

A. Threat

B. Risk

C. Hybrid cloud deployment model

D. Case of infringing on the rights of the provider

139. Which of the following is one of the benefits of a private cloud deployment?

A. Less cost

B. Higher performance

C. Retaining control of governance

D. Reduction in need for maintenance capability on the customer side

140. What are the two general delivery modes for the SaaS model?

A. Ranked and free

B. Hosted application management and software on demand

C. Intrinsic motivation complex and undulating perspective details

D. Framed and modular

141. Your organization has migrated into a PaaS configuration. A network administrator within the cloud provider has accessed your data and sold a list of your users to a competitor. Who is required to make data breach notifications in accordance with all applicable laws?

A. The network admin responsible

B. The cloud provider

C. The regulators overseeing your deployment

D. Your organization

142. If an organization wants to retain the *most* control of their assets in the cloud, which service and deployment model combination should they choose?

A. PaaS, community

B. IaaS, hybrid

C. SaaS, public

D. IaaS, private

143. If an organization wants to realize the *most* cost savings by reducing administrative overhead, which service and deployment model combination should they choose?

A. PaaS, community

B. IaaS, hybrid

C. SaaS, public

D. IaaS, private