CCSP®

Official (ISC)²® Practice Tests

CCSP®

Official (ISC)²® Practice Tests

Ben Malisow

SYBEX®
A Wiley Brand

Senior Acquisitions Editor: Ken Brown
Development Editor: Kelly Talbot
Technical Editor: Bill Burke, Trevor L. Chandler, Aaron Kraus, Valerie Michelle Nelson, Brian T. O'Hara, Jordan Pike
Production Manager: Kathleen Wisor
Copy Editor: Judy Flynn
Editorial Manager: Mary Beth Wakefield
Executive Editor: Jim Minatel
Book Designers: Judy Fung and Bill Gibson
Proofreader: Nancy Carrasco
Indexer: John Sleeva
Project Coordinator, Cover: Brent Savage
Cover Designer: Wiley
Cover Image: ©Jeremy Woodhouse/Getty Images, Inc.

Published simultaneously in Canada

ISBN: 978-1-119-44922-5

ISBN: 978-1-119-48038-9 (ebk.)

ISBN: 978-1-119-48039-6 (ebk.)

Manufactured in the United States of America

Library of Congress Control Number: 2017962410

10 9 8 7 6 5 4 3 2 1

For Robin, again, for making this year possible

Acknowledgments

The author would like to thank various biological entities for their assistance in bringing this work to completion. First, Jim Minatel, perhaps the best editor anyone could ever have. Jim has ridiculous thresholds of patience and encouragement, a perfectly dry wit, and professional experience and knowledge that should make other editors whimper and hide in the dark places they belong. Kelly Talbot has similar amounts of patience, which have served to make him the finest of editors. He had to endure completely outrageous treatment in the form of writer behavior bordering on assault and prose that is perhaps only as interesting to someone outside the information security realm as paint thinner (and even paint thinner fumes have arguably medicinal qualities, which this book sorely lacks). Judy Flynn is a wickedly sharp editor and may, in fact, be a cyborg programmed with thesaurus capabilities. The amount of fixing she had to do to make this book readable is extraordinary, and she cannot be thanked enough. Katie Wisor's technological support efforts were unparalled, and her whimsical tolerance for the author's capricious attitude toward the editing process cannot be appreciated enough. The technical reviewers Bill Burke, Trevor Chandler, Aaron Kraus, Valerie Michelle Nelson, Brian O'Hara, and Jordan Pike were utterly amazing. They caught mistakes and pointed out pitfalls that caused the author to blush and cringe. More important, they made suggestions that have improved this work beyond measure, for which the author is humbled and utterly grateful. Finally, the author's partner, Robin (getting a doubleplusgood nod to go with the dedication of this book), for her own efforts to mollify and assuage the author as necessary during production, and the dog, Jake, who may have often expressed discontent when the author sat down at the keyboard but was just as pleased to jump up in delight when the author arose again.

About the Author

Ben Malisow, CISSP, CISM, CCSP, Security+, has been involved in INFOSEC and education for more than 20 years. At Carnegie Mellon University, he crafted and delivered the CISSP prep course for CMU's CERT/SEU. Malisow was the ISSM for the FBI's most highly classified counterterror intelligence-sharing network, served as a United States Air Force officer, and taught grades 6–12 at a reform school in the Las Vegas public school district (probably his most dangerous employment to date). His latest work has included the *CCSP (ISC)^2 Certified Cloud Security Professional Official Study Guide*, also from Sybex/Wiley, and *How to Pass Your INFOSEC Certification Test: A Guide to Passing the CISSP, CISA, CISM, Network+, Security+, and CCSP*, available from Amazon Direct. In addition to other consulting and teaching, Ben is a certified instructor for (ISC)^2, delivering CISSP and CCSP courses. You can reach him at: `www.benmalisow.com`.

About the Technical Editors

Bill Burke (CISSP, CCSP, CISM, CRISC, CEH, ITIL, Oracle ACE, OCP) is a 25+ year veteran in Information Technology and Cyber Security. He has worked for numerous financial services organizations, one of the most recognized being Visa where he served as a Chief Enterprise Security Architect. At Oracle, he was a leader in Advanced Technical Services where he served as a Consulting Technical Director to Oracle's strategic clients in Advanced Security Configurations in the RDBMS, RAC, Data Guard, Golden Gate and other products. During his career, he has served on multiple board-of-directors including Silicon Valley Chapter - Cloud Security Alliance, Silicon Valley Chapter $(ISC)^2$, Oracle Development Tools User Group, and the International Oracle Users Group. He has spoken at local, national and international conferences. He is a published author and technical editor for both books and journals. Today he is a cloud cyber security consultant and can be reached at `billburke@cloudcybersec.com`.

Trevor L. Chandler has been a faculty member in higher education for more than 30 years, providing instruction in various programming languages, virtualization, networking, Linux System Administration, and cyber security. His experience also includes many years working in the capacity of UNIX System Administrator, and Network Administrator. Trevor holds a number of key IT certifications: CompTIA's CASP, EC-Council's CEH, and $(ISC)^2$'s coveted CISSP (Certified Information Systems Security Professional). Among his cloud-related certifications are Cloud+, CCSK, and the industry's premier cloud security certification, CCSP (Certified Cloud Security Professional). Trevor has a passion for advancing his knowledge in Information Technology by attending conferences and webinars.

Aaron Kraus began his career as a security auditor for US Federal Government clients. From there he moved into security risk management for healthcare and financial services, which offered more opportunities to travel, explore, and eat amazing food around the world. He currently works for a Cyber Risk Insurance startup in San Francisco and spends his free time dabbling in cooking, cocktail mixology, and photography.

Valerie Michelle Nelson, CISSP, CISM, CCSP, CEH, CSM, CPCU, has worked in information technology for over 25 years, currently with a large financial institution on its journey to the cloud. She has assisted in question workshops with $(ISC)^2$, taught as adjunct faculty, and generally loves educating friends and family (including her supportive parents, husband, and two children) on the cloud and the benefits and risks yet to be weathered.

Brian T. O'Hara CISA, CISM, CRISC, CCSP, CISSP, Chief Information Security Officer for the National Conference of Guaranty Funds, has been practicing Information Security for over 20 years specializing in Security, Audit and Risk Management in Healthcare, Financial Services and Manufacturing. He is a frequent speaker at local and national conferences such as "RSA", "SecureWorld", "Indy Big Data", and a regular IT Security and Audit SME contributor to ITProTV. He has published articles in the Indiana Bankers Journal, and served as Technical Editor of several recent Security and Audit books such as $(ISC)^2$ *CISSP Official Study Guide* (Wiley), $(ISC)_2$ *SSCP Official Study Guide* (Wiley), as well as co-author of *CISA: Certified Information Systems Auditor Study Guide, 4th Edition* (Wiley), and most recently $(ISC)^2$ *CCSP Official Study Guide* (Wiley). Mr. O'Hara holds a BA from Indiana University in Public Affairs and an MA in Counseling from the University of North Dakota. He serves in numerous leadership positions with local and national InfoSec organizations such as ISACA, ISC_2 and the InfraGard Indiana Members Alliance and was awarded Fellow status by the Information Systems Security Association (ISSA) in 2013 for his leadership activities. He also currently serves on the Indiana Executive Cybersecurity Council established by Governor Eric Holcomb. His responsibilities include those of the Financial Services Committee Co-Chair and member of the Public Awareness and Training Working Group. He can be reached at `brian@btohara.com`, or LinkedIn at `https://www.linkedin.com/in/brianohara`, and can be followed on Twitter `@brian_t_ohara`.

Jordan Pike, CISSP, CRISC, CCSP, GCIH, is the director of security operations for nCino, Inc., which is a leading cloud-based bank operating system built on the Salesforce platform. When he isn't in front of a keyboard, he spends his time hiking, volunteering for a nonprofit medical clinic, and reading all of Neal Stephenson's novels. He was a technical reviewer for *CCSP (ISC)² Certified Cloud Security Professional Official Study Guide* from Sybex/Wiley. You can reach him at `www.jordanpike.com`.

Contents at a Glance

Contents

Introduction

There is no magic formula for passing the CCSP certification exam. You can, however, prepare yourself for the challenge. This book is all about preparation.

We've included 1,000 questions related to the CCSP material in this book, which also includes access to the online databank (the same questions, but in a point-and-click format). They were created in accordance with the (ISC)^2 CCSP Common Body of Knowledge (CBK), the CCSP Training Guide, the *CCSP Study Guide*, and the CCSP Detailed Content Outline (DCO), which lists all the elements of practice that the candidate is expected to know for the certification.

How This Book Is Organized

The questions have been arranged in the order of the CBK, with varying amounts in proportion to (ISC)^2 published matrix describing how the exam is constructed, as shown in Table I.1.

TABLE I.1 How the Exam Is Constructed

Domains	Weight
1. Architectural Concepts and Design Requirements	19%
2. Cloud Data Security	20%
3. Cloud Platform and Infrastructure Security	19%
4. Cloud Application Security	15%
5. Operations	15%
6. Legal and Compliance	12%

There are six chapters, one for each of the CBK domains; each chapter contains a fraction of 750 practice questions, reflecting the percentage of questions from the respective domain on the exam (for example, Chapter 1 reflects Domain 1 of the CBK and has 143 questions). There are also two full-length practice exams, 125 questions each, at the end of the book (Chapters 7 and 8).

Who Should Read This Book

This book is intended for CCSP candidates. In order to earn the CCSP, you are expected to have professional experience in the field of information security/IT security, particularly experience related to cloud computing. The candidate will also need to provide evidence of their professional experience to (ISC)^2 in the event of passing the exam.

The author has drawn on his own experience studying for and passing the exam as well as years of teaching the CISSP and CCSP preparation courses for (ISC)^2. He also solicited feedback from colleagues and former students who have taken the prep course and the exam. The book should reflect the breadth and depth of question content you are likely to see on the exam. Some of the questions in this book are easier than what you will see on the exam; some of them may be harder. Hopefully, the book will prepare you for what you might encounter when you take the test.

The one thing we chose not to simulate in the book is the "interactive" questions; (ISC)^2 has stated that the current tests may go beyond the regular multiple-choice format and could include "matching" questions (a list of multiple answers and multiple terms, where the candidate has to arrange them all in order), drag-and-drop questions (where the candidate uses the mouse to arrange items on the screen), and "hot spot" questions (where the candidate puts the mouse on areas of the screen to indicate an answer). There will probably not be many of these on the exam you take, but they are weighted more in your score than the multiple-choice questions, so pay attention and be extra careful answering those.

Tools You Will Need

In addition to this book, we recommend the *CCSP (ISC)^2 Certified Cloud Security Professional Official Study Guide* (O'Hara, Malisow), also from Wiley (2017). There is, as stated in the introduction, no magic formula for passing the exam. No single particular book/source with all the answers to the exam exists. If someone claims to be able to provide you with such a product, please realize that they are mistaken or, worse, misleading you.

However, you can augment your studying by reviewing a significant portion of the likely sources used by the professionals who created the test. The following is a just a *sampling* of the possible professional resources the cloud practitioner should be familiar with:

- The Cloud Security Alliance's *Notorious Nine*:

  `https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf`

- The OWASP's *Top 10*:

  `https://www.owasp.org/index.php/Top_10_2013-Top_10`

- The OWASP's *XSS (Cross-Site Scripting) Prevention Cheat Sheet*:

  `https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet`

- The OWASP's *Testing Guide (v4)*:
  `https://www.owasp.org/images/1/19/OTGv4.pdf`
- NIST SP 500-292, *NIST Cloud Computing Reference Architecture*:
  `http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=909505`
- The CSA's *Security Guidance for Critical Areas of Focus in Cloud Computing v3.0*:
  `https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/csaguide.v3.0.pdf`
- ENISA's *Cloud Computing Benefits, Risks, and Recommendations for Information Security*:
  `https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment`
- The Uptime Institute's *Tier Standard: Topology* and *Tier Standard: Operational Sustainability* (the linked page includes download options for the documents):
  `https://uptimeinstitute.com/publications`

CCSP Certified Cloud Security Professional Objective Map

Domain 1: Architectural Concepts and Design Requirements

A. Understand Cloud Computing Concepts
- **A.1.** Cloud Computing Definitions
- **A.2.** Cloud Computing Roles
- **A.3.** Key Cloud Computing Characteristics
- **A.4.** Building Block Technologies

B. Describe Cloud Reference Architecture
- **B.1.** Cloud Computing Activities
- **B.2.** Cloud Service Capabilities
- **B.3.** Cloud Service Categories
- **B.4.** Cloud Deployment Models
- **B.5.** Cloud Cross-Cutting Aspects

C. Understand Security Concepts Relevant to Cloud Computing
- **C.1.** Cryptography
- **C.2.** Access Control
- **C.3.** Data and Media Sanitization
- **C.4.** Network Security

- **C.5.** Virtualization Security
- **C.6.** Common Threats
- **C.7.** Security Considerations for Different Cloud Categories

D. Understand Design Principles of Secure Cloud Computing

- **D.1.** Cloud Secure Data Lifecycle
- **D.2.** Cloud-Based Business Continuity/Disaster Recovery Planning
- **D.3.** Cost/Benefit Analysis
- **D.4.** Functional Security Requirements

E. Identify Trusted Cloud Sources

- **E.1.** Certification Against Criteria
- **E.2.** System/Subsystem Product Certifications

Domain 2: Cloud Data Security

A. Understand Cloud Data Lifecycle

- **A.1.** Phases
- **A.2.** Relevant Data Security Technologies

B. Design and Implement Cloud Data Storage Architectures

- **B.1.** Storage Types
- **B.2.** Threats to Storage Types
- **B.3.** Technologies Available to Address Threats

C. Design and Apply Data Security Strategies

- **C.1.** Encryption
- **C.2.** Key Management
- **C.3.** Masking
- **C.4.** Tokenization
- **C.5.** Application of Technologies
- **C.6.** Emerging Technologies

D. Understand and Implement Data Discovery and Classification Technologies

- **D.1.** Data Discovery
- **D.2.** Classification

E. Design and Implement Relevant Jurisdictional Data Protections for Personally Identifiable Information (PII)

- **E.1.** Data Privacy Acts
- **E.2.** Implementation of Data Discovery
- **E.3.** Classification of Discovered Sensitive Data

- **E.4.** Mapping and Definition of Controls
- **E.5.** Application of Defined Controls for PII

F. Design and Implement Data Rights Management

- **F.1.** Data Rights Objectives
- **F.2.** Appropriate Tools

G. Plan and Implement Data Retention, Deletion, and Archiving Policies

- **G.1.** Data Retention Policies
- **G.2.** Data Deletion Procedures and Mechanisms
- **G.3.** Data Archiving Procedures and Mechanisms

H. Design and Implement Auditability, Traceability and Accountability of Data Events

- **H.1.** Definition of Event Sources and Identity Attribution Requirement
- **H.2.** Data Event Logging
- **H.3.** Storage and Analysis of Data Events
- **H.4.** Continuous Optimizations
- **H.5.** Chain of Custody and Non-repudiation

Domain 3: Cloud Platform and Infrastructure Security

A. Comprehend Cloud Infrastructure Components

- **A.1.** Physical Environment
- **A.2.** Network and Communications
- **A.3.** Compute
- **A.4.** Virtualization
- **A.5.** Storage
- **A.6.** Management Plan

B. Analyze Risks Associated to Cloud Infrastructure

- **B.1.** Risk Assessment/Analysis
- **B.2.** Cloud Attack Vectors
- **B.3.** Virtualization Risks
- **B.4.** Counter-Measure Strategies

C. Design and Plan Security Controls

- **C.1.** Physical and Environmental Protection
- **C.2.** System and Communication Protection
- **C.3.** Virtualization Systems Protection
- **C.4.** Management of Identification, Authentication and Authorization in Cloud Infrastructure
- **C.5.** Audit Mechanisms

- **D.** Plan Disaster Recovery and Business Continuity Management
  - **D.1.** Understanding of the Cloud Environment
  - **D.2.** Understanding of the Business Requirements
  - **D.3.** Understanding the Risks
  - **D.4.** Disaster Recovery/Business Continuity Strategy
  - **D.5.** Creation of the Plan
  - **D.6.** Implementation of the Plan

Domain 4: Cloud Application Security

- **A.** Recognize the Need for Training and Awareness in Application Security
  - **A.1.** Cloud Development Basics
  - **A.2.** Common Pitfalls
  - **A.3.** Common Vulnerabilities
- **B.** Understand Cloud Software Assurance and Validation
  - **B.1.** Cloud-based Functional Testing
  - **B.2.** Cloud Secure Development Lifecycle
  - **B.3.** Security Testing
- **C.** Use Verified Secure Software
  - **C.1.** Approved API
  - **C.2.** Supply-Chain Management
  - **C.3.** Community Knowledge
- **D.** Comprehend the System Development Lifecycle (SDLC) Process
  - **D.1.** Phases & Methodologies
  - **D.2.** Business Requirements
  - **D.3.** Software Configuration Management & Versioning
- **E.** Apply the Secure Software Development Lifecycle
  - **E.1.** Common Vulnerabilities
  - **E.2.** Cloud-Specific Risks
  - **E.3.** Quality of Service
  - **E.4.** Threat Modeling
- **F.** Comprehend the Specifics of Cloud Application Architecture
  - **F.1.** Supplemental Security Devices
  - **F.2.** Cryptography
  - **F.3.** Sandboxing
  - **F.4.** Application Virtualization

- **G.** Design Appropriate Identity and Access Management (IAM) Solutions
  - **G.1.** Federated Identity
  - **G.2.** Identity Providers
  - **G.3.** Single Sign-On
  - **G.4.** Multi-factor Authentication

Domain 5: Operations

- **A.** Support the Planning Process for the Data Center Design
  - **A.1.** Logical Design
  - **A.2.** Physical Design
  - **A.3.** Environmental Design
- **B.** Implement and Build Physical Infrastructure for Cloud Environment
  - **B.1.** Secure Configuration of Hardware-Specific Requirements
  - **B.2.** Installation and Configuration of Virtualization Management Tools for the Host
- **C.** Run Physical Infrastructure for Cloud Environment
  - **C.1.** Configuration of Access Control for Local Access
  - **C.2.** Securing Network Configuration
  - **C.3.** OS Hardening via Application of Baseline
  - **C.4.** Availability of Stand-Alone Hosts
  - **C.5.** Availability of Clustered Hosts
- **D.** Manage Physical Infrastructure for Cloud Environment
  - **D.1.** Configuring Access Controls for Remote Access
  - **D.2.** OS Baseline Compliance Monitoring and Remediation
  - **D.3.** Patch Management
  - **D.4.** Performance Monitoring
  - **D.5.** Hardware Monitoring
  - **D.6.** Backup and Restore of Host Configuration
  - **D.7.** Implementation of Network Security Controls
  - **D.8.** Log Capture and Analysis
  - **D.9.** Management Plane
- **E.** Build Logical Infrastructure for Cloud Environment
  - **E.1.** Secure Configuration of Virtual Hardware-Specific Requirements
  - **E.2.** Installation of Guest O/S Virtualization Toolsets

- **F.** Run Logical Infrastructure for Cloud Environment
  - **F.1.** Secure Network Configuration
  - **F.2.** OS Hardening via Application of a Baseline
  - **F.3.** Availability of Guest OS
- **G.** Manage Logical Infrastructure for Cloud Environment
  - **G.1.** Access Control for Remote Access
  - **G.2.** OS Baseline Compliance Monitoring and Remediation
  - **G.3.** Patch Management
  - **G.4.** Performance Monitoring
  - **G.5.** Backup and Restore of Guest OS Configuration
  - **G.6.** Implementation of Network Security Controls
  - **G.7.** Log Capture and Analysis
  - **G.8.** Management Plane
- **H.** Ensure Compliance with Regulations and Controls
  - **H.1.** Change Management
  - **H.2.** Continuity Management
  - **H.3.** Information Security Management
  - **H.4.** Continual Service Improvement Management
  - **H.5.** Incident Management
  - **H.6.** Problem Management
  - **H.7.** Release Management
  - **H.8.** Deployment Management
  - **H.9.** Configuration Management
  - **H.10.** Service Level Management
  - **H.11.** Availability Management
  - **H.12.** Capacity Management
- **I.** Conduct Risk Assessment to Logical and Physical Infrastructure
- **J.** Understand the Collection, Acquisition and Preservation of Digital Evidence
  - **J.1.** Proper Methodologies for Forensic Collection of Data
  - **J.2.** Evidence Management
- **K.** Manage Communication with Relevant Parties
  - **K.1.** Vendors
  - **K.2.** Customers
  - **K.3.** Partners

- **K.4.** Regulators
- **K.5.** Other Stakeholders

Domain 6: Legal and Compliance

- **A.** Understand Legal Requirements and Unique Risks within the Cloud Environment
  - **A.1.** International Legislation Conflicts
  - **A.2.** Appraisal of Legal Risks Specific to Cloud Computing
  - **A.3.** Legal Controls
  - **A.4.** eDiscovery
  - **A.5.** Forensics Requirements
- **B.** Understand Privacy Issues, Including Jurisdictional Variation
  - **B.1.** Difference between Contractual and Regulated PII
  - **B.2.** Country-Specific Legislation Related to PII/Data Privacy
  - **B.3.** Difference Among Confidentiality, Integrity, Availability, and Privacy
- **C.** Understand Audit Process, Methodologies, and Required Adaptions for a Cloud Environment
  - **C.1.** Internal and External Audit Controls
  - **C.2.** Impact of Requirements Programs by the Use of Cloud
  - **C.3.** Assurance Challenges of Virtualization and Cloud
  - **C.4.** Types of Audit Reports
  - **C.5.** Restrictions of Audit Scope Statements
  - **C.6.** Gap Analysis
  - **C.7.** Audit Plan
  - **C.8.** Standards Requirements
  - **C.9.** Internal Information Security Management System
  - **C.10.** Internal Information Security Controls System
  - **C.11.** Policies
  - **C.12.** Identification and Involvement of Relevant Stakeholders
  - **C.13.** Specialized Compliance Requirements for Highly Regulated Industries
  - **C.14.** Impact of Distributed IT Model
- **D.** Understand Implications of Cloud to Enterprise Risk Management
  - **D.1.** Assess Providers Risk Management
  - **D.2.** Difference between Data Owner/Controller vs. Data Custodian/Processor
  - **D.3.** Provision of Regulatory Transparency Requirements
  - **D.4.** Risk Mitigation

- **D.5.** Different Risk Frameworks
- **D.6.** Metrics for Risk Management
- **D.7.** Assessment of Risk Environment

E. Understand Outsourcing and Cloud Contract Design

- **E.1.** Business Requirements
- **E.2.** Vendor Management
- **E.3.** Contract Management

F. Execute Vendor Management

- **F.1.** Supply-chain Management

Online Test Bank

To practice in an online testing version of the same questions, go to `www.wiley.com/go/sybextestprep` and register your book to get access to the Sybex Test Platform. Online you can mix questions from the domain chapters and practice exams, take timed tests, and have your answers graded.

Summary

As you go through the questions in this book, please remember the abbreviation RTFQ, which is short for "read the *full* question." There is no better advice you can possibly receive than this. Read every word of every question. Read every possible answer before selecting the one you like. The exam is 125 questions over four hours. You have more than enough time to consider each question thoroughly. There is no cause for hurry. Make sure you understand what the question is asking before responding.

Good luck on the exam. We're hoping this book helps you pass.

CCSP®

Official (ISC)²® Practice Tests

CCSP® Official (ISC)2® Practice Tests
By Ben Malisow

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

Chapter 2

CCSP® Official (ISC)2® Practice Tests
By Ben Malisow

Domain 2: Cloud Data Security

In Domain 2, the CBK focuses on the data owned by the cloud customer, hosted in the cloud. The domain discusses methods for securing the data, including specific tools and techniques.

1. In which of these options does the encryption engine reside within the application accessing the database?
   - **A.** Transparent encryption
   - **B.** Symmetric-key encryption
   - **C.** Application-level encryption
   - **D.** Homomorphic encryption

2. You are the security team leader for an organization that has an infrastructure as a service (IaaS) production environment hosted by a cloud provider. You want to implement an event monitoring (security information and event management (SIEM)/security information management (SIM)/security event management (SEM)) solution in your production environment in order to acquire better data for security defenses and decisions. Which of the following is probably your *most* significant concern about implementing this solution in the cloud?
   - **A.** The solution should give you better analysis capability by automating a great deal of the associated tasks.
   - **B.** Dashboards produced by the tool are a flawless management benefit.
   - **C.** You will have to coordinate with the cloud provider to ensure that the tool is acceptable and functioning properly.
   - **D.** Senior management will be required to approve the acquisition and implementation of the tool.

3. Which of the following is *not* a step in the crypto-shredding process?
   - **A.** Encrypt data with a particular encryption engine
   - **B.** Encrypt first resulting keys with another encryption engine
   - **C.** Save backup of second resulting keys
   - **D.** Destroy original second resulting keys

4. Which of the following sanitization methods is feasible for use in the cloud?
   - **A.** Crypto-shredding
   - **B.** Degaussing
   - **C.** Physical destruction
   - **D.** Overwriting

5. Which of the following is *not* a method for enhancing data portability?
   - **A.** Crypto-shredding
   - **B.** Using standard data formats
   - **C.** Avoiding proprietary services
   - **D.** Favorable contract terms

6. When implementing a digital rights management (DRM) solution in a cloud environment, which of the following does *not* pose an additional challenge for the cloud customer?
   - **A.** Users might be required to install a DRM agent on their local devices
   - **B.** DRM solutions might have difficulty interfacing with multiple different OSs and services
   - **C.** DRM solutions might have difficulty interacting with virtualized instances
   - **D.** Ownership of intellectual property might be difficult to ascertain

7. When implementing cryptography in a cloud environment, where is the worst place to store the keys?
   - **A.** With the cloud provider
   - **B.** Off the cloud, with the data owner
   - **C.** With a third-party provider, in key escrow
   - **D.** Anywhere but with the cloud provider

8. Which of the following is *not* a security concern related to archiving data for long-term storage?
   - **A.** Long-term storage of the related cryptographic keys
   - **B.** Format of the data
   - **C.** Media the data resides on
   - **D.** Underground depth of the storage facility

9. Data dispersion is a cloud data security technique that is most similar to which legacy implementation?
   - **A.** Business continuity and disaster recovery (BCDR)
   - **B.** Redundant Array of Inexpensive Disks (RAID)
   - **C.** Software-defined networking (SDN)
   - **D.** Content delivery network (CDN)

10. Data dispersion uses _____, where the legacy implementation was called "striping."
    - **A.** Chunking
    - **B.** Vaulting
    - **C.** Lumping
    - **D.** Grouping

11. Data dispersion uses _____, where the legacy implementation was called "parity bits."

A. Smurfing

B. Snarfing

C. Erasure coding

D. Real-time bitlinking

12. Data dispersion provides protection for all the following security aspects *except* _____.

A. Protecting confidentiality against external attack on the storage area

B. Loss of availability due to single storage device failure

C. Loss due to seizure by law enforcement in a multitenant environment

D. Protecting against loss due to user error

13. Your organization is migrating the production environment to an IaaS cloud implementation.

Your users will need to be able to get access to their data, install programs, and partition memory space for their own purposes. You should configure the cloud memory as _____.

A. Object

B. Volume

C. Synthetic

D. Database

14. Your organization is migrating the production environment to an IaaS cloud implementation.

Your users will need to be able to get access to their data and share data with other users in a defined, structured motif. You should configure the cloud memory as _____.

A. Object storage

B. Volume storage

C. Synthetic storage

D. Databases

15. What is one of the benefits of implementing an egress monitoring solution?

A. Preventing DDoS attacks

B. Inventorying data assets

C. Interviewing data owners

D. Protecting against natural disasters

16. Egress monitoring solutions usually include a function that _____.

A. Arbitrates contract breaches

B. Performs personnel evaluation reviews

C. Discovers data assets according to classification/categorization

D. Applies another level of access control

17. Egress monitoring solutions usually include a function that _____.

A. Uses biometrics to scan users

B. Inspects incoming packets

C. Resides on client machines

D. Uses stateful inspection

18. Digital rights management (DRM) solutions (sometimes referred to as information rights management, or IRM) can be used to protect all sorts of sensitive data but are usually particularly designed to secure _____.

A. Personally identifiable information (PII)

B. Intellectual property

C. Plans and policies

D. Marketing material

19. Digital rights management (DRM) solutions (sometimes referred to as information rights management, or IRM) often protect unauthorized distribution of what type of intellectual property?

A. Patents

B. Trademarks

C. Personally identifiable information (PII)

D. Copyright

20. Which of the following characteristics is associated with digital rights management (DRM) solutions (sometimes referred to as information rights management, or IRM)?

A. Persistence

B. Influence

C. Resistance

D. Trepidation

21. Which of the following characteristics is associated with digital rights management (DRM) solutions (sometimes referred to as information rights management, or IRM)?

A. Automatic expiration

B. Multilevel aggregation

C. Enhanced detail

D. Broad spectrum

22. Which of the following characteristics is associated with digital rights management (DRM) solutions (sometimes referred to as information rights management, or IRM)?

A. Transparent encryption modification

B. Bilateral enhancement

C. Continuous audit trail

D. Encompassing flow

23. Which of the following characteristics is associated with digital rights management (DRM) solutions (sometimes referred to as information rights management, or IRM)?

A. Mapping to existing access control lists (ACLs)

B. Delineating biometric catalogs

C. Preventing multifactor authentication

D. Prohibiting unauthorized transposition

24. According to the $(ISC)^2$ Cloud Secure Data Life Cycle, which phase comes soon after (or at the same time as) the Create phase?

A. Store

B. Use

C. Deploy

D. Archive

25. According to the $(ISC)^2$ Cloud Secure Data Life Cycle, which phase comes immediately before the Share phase?

A. Create

B. Destroy

C. Use

D. Encrypt

26. Why is the term *(ISC)*^{2} Cloud Secure Data Life Cycle actually somewhat inaccurate?

A. The term is not used only by $(ISC)^2$

B. Not all phases are secure

C. Not all phases take place in the cloud

D. It's not actually a cycle

27. According to the $(ISC)^2$ Cloud Secure Data Life Cycle, in which phase should the process of categorization/classification of data occur?

A. Create

B. Store

C. Define

D. Use

28. Which of the following should occur during the final phase of the Cloud Secure Data Life Cycle?

A. Data dispersion

B. Crypto-shredding

C. Cryptoparsing

D. Cryptosporidium

29. At what phase of the Cloud Secure Data Life Cycle does data enter long-term storage?

A. The first

B. The second

C. The fourth

D. The fifth

30. What is a form of cloud storage where data is stored as objects, arranged in a hierarchal structure, like a file tree?

A. Volume storage

B. Databases

C. Content delivery network (CDN)

D. Object storage

31. What is a form of cloud storage where data is stored in a logical storage area assigned to the user but not necessarily physically attached or even geographically proximate to the compute node the user is utilizing?

A. Volume storage

B. Databases

C. Content delivery network (CDN)

D. Object storage

32. What is a form of cloud storage often used for streaming multimedia data to users?

A. Volume storage

B. Databases

C. Content delivery network (CDN)

D. Neutral storage

33. What type of data storage is often used in PaaS arrangements?

A. Ephemeral

B. Database

C. Long-term

D. Nefarious

34. What is a form of cloud data protection where data is spread across multiple storage devices/locations, similar to RAID in the legacy environment?

A. Infringing

B. Data dispersion

C. Voiding

D. Crypto-shredding

35. Erasure coding, in the cloud, is similar to what element of RAID implementations in the legacy environment?

A. Deltas

B. Inversion

C. Parity bits

D. Transposition

36. DLP (data loss prevention or data leak protection) solutions are implemented in the hopes of securing _____.

A. Sensitive data that may leave the organization's control

B. All data within the organization's control

C. Data being processed by the organization's users

D. Data that could be intercepted while out of the organization's control

37. Which of the following will DLP solutions most likely *not* inspect?

A. Email content

B. FTP traffic

C. Material saved to portable media

D. VoIP conversations

38. DLP solutions may use all the following techniques to identify sensitive data *except* _____.

A. Pattern matching

B. Inference

C. Keyword identification

D. Metadata tags

39. You are the security manager of a small firm that has just purchased a data loss prevention or data leak protection (DLP) solution to implement in your cloud-based production environment.

In which of the following cases would you *not* have to get permission from the cloud provider to install and implement the tool?

A. If it's hardware based and your production environment is in an IaaS model

B. If you purchased it from a vendor other than the cloud provider

C. If it's software based and your production environment is in a PaaS model

D. If it affects all guest instances on any given host device

40. You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.

Before implementing the solution, what should you explain to senior management?

A. The additional risks of external attack associated with using the tool

B. The production impact it will have on the environment

C. What the price of the tool was

D. How the solution works

41. You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.

Which of these activities should you perform before deploying the tool?

A. Survey your company's departments about the data under their control

B. Reconstruct your firewalls

C. Harden all your routers

D. Adjust the hypervisors

42. You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.

What should you expect immediately following the implementation of the DLP solution?

A. Immediate decrease in lost data

B. A series of false-positive indications

C. Increase in morale across the organization

D. Increase in gross revenue

43. You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.

What should you *not* expect the tool to address?

A. Sensitive data sent inadvertently in user emails

B. Sensitive data captured by screen shots

C. Sensitive data moved to external devices

D. Sensitive data in the contents of files sent via FTP

44. You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.

In order to get truly holistic coverage of your environment, you should be sure to include _____ as a step in the deployment process.

A. Getting signed user agreements from all users

B. Installation of the solution on all assets in the cloud data center

C. Adoption of the tool in all routers between your users and the cloud provider

D. All of your customers to install the tool

45. You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.

In order to increase the security value of the DLP, you should consider combining it with _____.

A. Digital rights management (DRM) and security event and incident management (SIEM) tools

B. An investment in upgraded project management software

C. Digital insurance policies

D. The Uptime Institute's Tier certification

46. You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.

You are interested in fielding the solution as an awareness tool, to optimize security for your organization through conditioning user behavior. You decide to set the solution to _____.

A. Suspend user accounts and notify the security office when it detects possible sensitive data egress attempted by a user

B. Halt the transaction and notify the user's supervisor when the user attempts to transfer sensitive data

C. Query the user as to whether they intend to send sensitive data upon detection of an attempted transfer

D. Sever remote connections upon detection of a possible sensitive data transfer

47. You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.

You understand that all of the following aspects of cloud computing may make proper deployment of the DLP difficult or costly *except* _____.

A. Data will not remain in one place or form in the cloud

B. The cloud environment will include redundant and resilient architecture

C. There will be a deleterious impact on production when installing the DLP tool

D. You might not have sufficient proper administrative rights in the cloud infrastructure

48. DLP solutions can aid all of the following security-related efforts *except* _____.

A. Access control

B. Egress monitoring

C. e-discovery/forensics

D. Data categorization/classification

49. The cloud security professional should be aware that encryption will most likely be necessary in all the following aspects of a cloud deployment *except* _____.

A. Data at rest

B. Data in motion

C. Data in use

D. Data of relief

50. As with the legacy environment, cloud data encryption includes all the following elements *except* _____.

A. The user

B. The data itself

C. The encryption engine

D. The encryption keys

51. Volume-storage encryption in an IaaS motif will protect against data loss due to all of the following activities *except* _____.

A. Physical loss or theft of a device

B. Disgruntled users

C. Malicious cloud administrators accessing the data

D. Virtual machine snapshots stolen from storage

52. In an IaaS motif, all of the following are examples of object-storage encryption *except* _____.

A. File-level encryption

B. Digital rights management (DRM)

C. Application-level encryption

D. Transport Layer Security (TLS)

53. All of the following are database encryption options that could be used in a PaaS implementation *except* _____.

A. File-level encryption

B. Secure Sockets Layer (SSL)

C. Transparent encryption

D. Application-level encryption

54. In application-level encryption, where does the encryption engine reside?

A. In the application accessing the database

B. In the OS on which the application is run

C. Within the database accessed by the application

D. In the volume where the database resides

55. Which of the following database encryption techniques can be used to encrypt specific tables within the database?

A. File-level encryption

B. Transparent encryption

C. Application-level encryption

D. Object-level encryption

56. Which of the following database encryption motifs makes it difficult to perform database functions (searches, indexing, etc.)?

A. File-level encryption

B. Transparent encryption

C. Application-level encryption

D. Volume encryption

57. According to $(ISC)^2$, where should the cloud customer's encryption keys be stored?

A. With the cloud customer

B. With a third-party provider

C. At the cloud provider data center

D. Anywhere but with the cloud provider

58. Which of the following is *not* used to determine data retention requirements?

A. Legislation

B. Business needs

C. Average media longevity

D. Contracts

59. Event monitoring tools (solutions variously referred to as SIEM/SEM/SIM) can aid in which of the following efforts?

A. External hacking detection

B. Prediction of physical device theft

C. Data classification/categorization issues

D. Social engineering attacks

60. Event monitoring tools (solutions variously referred to as SIEM/SEM/SIM) can aid in which of the following efforts?

A. Detecting untrained personnel

B. Predicting system outages

C. Sending alerts for conflicts of interest

D. Enforcing mandatory vacation

61. Event monitoring tools (solutions variously referred to as SIEM/SEM/SIM) can aid in which of the following efforts?

A. Reducing workload for production personnel

B. Decreasing size of log files

C. Optimizing performance

D. Ensuring adequate lighting of workspaces

62. Event monitoring tools (solutions variously referred to as SIEM/SEM/SIM) can aid in which of the following efforts?

A. Detecting ambient heating/ventilation/air conditioning (HVAC) problems

B. Ensuring proper cloud migration

C. Deciding risk parameters

D. Protecting all physical entry points against the threat of fire

63. In addition to predictive capabilities, event monitoring tools (solutions variously referred to as SIEM/SEM/SIM) are instrumental in what other security function?

A. Personnel safety

B. Vehicle tracking

C. Incident evidence

D. Acoustic dampening

64. Which of the following is one of the benefits of event monitoring tools (solutions variously referred to as SIEM/SEM/SIM)?

A. Greater physical security

B. Psychological deterrence

C. Cost savings

D. More logs can be reviewed, at faster speeds

65. As in the legacy environment, proper key management is crucial in the cloud. Which of the following principles is *not* true regarding key management?

A. It is good practice to introduce pseudorandom numbers when generating keys

B. Public keys should never be shared with anyone

C. Losing the keys is equivalent to losing the data

D. Symmetric keys should be passed out of band

66. Which of the following is a good business case for the use of data masking?

A. The shipping department should get only a masked version of the customer's address

B. The customer service department should get only a masked version of the customer's Social Security number

C. The billing department should get only a masked version of the customer's credit card number

D. The Human Resources department should get only a masked version of the employee's driver's license number

67. All of the following are methods of data masking suggested by the (ISC)^2 CBK *except* _____.

A. Random substitution

B. Algorithmic substitution

C. Deletion

D. Conflation

68. If data masking is being performed for software testing purposes, which of the following is *not* a good masking technique to use?

A. Random substitution

B. Shuffling

C. Deletion

D. Algorithmic substitution

69. For which use case would it probably be best to use static masking?

A. Creating a test environment for a new application

B. Allowing a customer service representative limited access to account data

C. Providing detailed reports to regulators

D. Notifying shareholders

70. For which use case would it probably be best to use dynamic masking?

A. Creating a test environment for a new application

B. Allowing a customer service representative limited access to account data

C. Sending incident response notifications

D. Implementing business continuity and disaster recovery (BCDR)

71. What is one possible risk associated with the use of algorithmic masking for obscuring a data set?

A. You could corrupt the production data.

B. The data could be subject to easy inadvertant disclosure.

C. Algorithms are two-way operations.

D. A null set has no test value.

72. _____ is a direct identifier, and _____ is an indirect identifier.

A. Username; password

B. User's name; user's age

C. User's IP address; user's MAC address

D. Location; income level

73. Anonymization is the process of removing _____ from data sets.

A. Access

B. Cryptographic keys

C. Numeric values

D. Identifying information

74. Tokenization is a method of obscuring data that, other than encryption, can be used to comply with _____ standards.

A. Gramm-Leach-Bliley Act (GLBA)

B. Payment Card Industry (PCI)

C. Child Online Protection Act (COPA)

D. Sarbanes-Oxley Act (SOX)

75. Tokenization requires at least __ database(s).

A. One

B. Two

C. Three

D. Four

76. Data owners might consider using tokenization for all of the following reasons *except* _____.

A. Regulatory or contractual compliance

B. Inference

C. Reduced cost of compliance

D. Mitigating risk from data lost to intrusion

77. Bit-splitting, also known as data dispersion, might be thought of as _____ in the cloud.

A. RAID

B. BIOS

C. DDoS

D. SYN-ACK

78. Bit-splitting also provides security against data breaches by _____.

A. Removing all access to unauthorized parties

B. Ensuring that an unauthorized user only gets a useless fragment of data

C. Moving data across jurisdictional boundaries

D. Tracking all incoming access requests

79. If bit-splitting is used to store data sets across multiple jurisdictions, how may this enhance security?

A. By making seizure of data by law enforcement more difficult

B. By hiding it from attackers in a specific jurisdiction

C. By ensuring that users can only accidentally disclose data to one geographic area

D. By restricting privilege user access

80. Which of the following is a possible negative aspect of bit-splitting?

A. Less security

B. Greatest risk of unauthorized access

C. Significantly greater processing overhead

D. Violating regulatory compliance

81. Which of the following is a possible negative aspect of bit-splitting?

A. It may require trust in additional third parties beyond the primary cloud service provider.

B. There may be cause for management concern that the technology will violate internal policy.

C. Users will have far greater difficulty understanding the implementation.

D. Limited vendors make acquisition and support challenging.

82. Which of the following is a possible negative aspect of bit-splitting?

A. Greater chance of physical theft of assets

B. Loss of public image

C. Some risk to availability, depending on the implementation

D. A small fire hazard

83. Which of the following is a theoretical technology that is intended to allow encrypted material to be processed and manipulated without decrypting it first?

A. Inverse postulation

B. Homomorphic encryption

C. Didactic alignment

D. Obverse reinstantiation

84. Which of the following is a data discovery approach used by e-commerce retailers to discern and predict shoppers' needs?

A. Big data

B. Real-time analytics

C. Agile analytics

D. Agile business intelligence

85. Which of the following is a data discovery approach that offers insight to trends of trends, using both historical and predictive approaches?

A. Obverse polyglotism

B. Big data

C. Real-time analytics

D. Agile analytics/business intelligence

86. Which of the following is *not* a data discovery technique?

A. Metadata

B. Labels

C. Content analysis

D. Data hover

87. Which of the following data discovery techniques involves using extra information automatically appended/included with the intended data when the data is created?

A. Metadata

B. Labels

C. Content analysis

D. Data hover

88. When labeling is used as a data discovery technique, who should be applying the labels?

A. The security office

B. Users

C. Data owners

D. Regulators

89. When data labels are being used in an environment (for discovery and other purposes), when should the labels be applied?

A. During the risk assessment

B. As part of the business impact analysis (BIA)

C. At collection/creation

D. When the discovery tools are implemented

90. Which of the following tools might be useful in data discovery efforts that are based on content analysis?

A. DLP

B. Digital Rights Management (DRM)

C. iSCSI

D. Fibre Channel over Ethernet (FCoE)

91. All of the following might be used as data discovery characteristics in a content-analysis-based data discovery effort *except* _____.

A. Keywords

B. Pattern-matching

C. Frequency

D. Inheritance

92. What is the risk to the organization posed by dashboards that display data discovery results?

A. Increased chance of external penetration

B. Flawed management decisions based on massaged displays

C. Higher likelihood of inadvertent disclosure

D. Raised incidence of physical theft

93. Which of these is *most* likely to have the greatest negative impact on data discovery effort?

A. Bandwidth latency issues

B. Poor physical security of the data center

C. Severe statutory regulation

D. Inaccurate or incomplete data

94. Cloud customers performing data discovery efforts will have to ensure that the cloud provider attends to all of the following requirements *except* _____.

A. Allowing sufficient access to large volumes of data

B. Preserving metadata tags

C. Assigning labels

D. Preserving and maintaining the data

95. Where should the cloud provider's data discovery requirements be listed?

A. NIST SP 800-53

B. Applicable laws and regulations

C. PCI DSS

D. The managed services contract and SLA

96. Who will determine data classifications for the cloud customer?

A. The cloud provider

B. NIST

C. Regulators

D. The cloud customer

97. An organization's data classification scheme *must* include which of the following categories?

A. File size

B. Origin of the data

C. Sensitivity of the data

D. Whatever the data owner decides

98. Classification is usually considered a facet of data _____.

A. Security

B. Labeling

C. Control

D. Markup

99. Data classification can be _____ or _____.

A. Inverse or obverse

B. Automatic or manual

C. Correct or incorrect

D. Diurnal or nocturnal

100. Data may need to be reclassified for all the following reasons *except* _____.

A. Color change

B. Time

C. Repurposing

D. Transfer of ownership

101. Proper _____ need to be assigned to each data classification/category.

A. Dollar values

B. Metadata

C. Security controls

D. Policies

102. Data transformation in a cloud environment should be of great concern to organizations considering cloud migration because _____ could affect data classification processes/implementations.

A. Multitenancy

B. Virtualization

C. Remote access

D. Physical distance

103. Who is ultimately responsible for a data breach that includes personally identifiable information (PII), in the event of negligence on the part of the cloud provider?

A. The user

B. The subject

C. The cloud provider

D. The cloud customer

104. In a personally identifiable information (PII) context, who is the subject?

A. The cloud customer

B. The cloud provider

C. The regulator

D. The individual

105. In a personally identifiable information (PII) context, who is the processor?

A. The cloud customer

B. The cloud provider

C. The regulator

D. The individual

106. In a personally identifiable information (PII) context, who is the controller?

A. The cloud customer

B. The cloud provider

C. The regulator

D. The individual

107. In a personally identifiable information (PII) context, which of the following is *not* normally considered "processing"?

A. Storing

B. Viewing

C. Destroying

D. Printing

108. Which of the following countries does *not* have a national privacy law that concerns personally identifiable information (PII) and applies to all entities?

A. Argentina

B. The United States

C. Italy

D. Australia

109. In protections afforded to personally identifiable information (PII) under the Health Information Portability and Accountability Act (HIPAA), the subject must ____ in order to allow the vendor to share their personal data.

A. Opt in

B. Opt out

C. Undergo screening

D. Provide a biometric template

110. In protections afforded to personally identifiable information (PII) under the Gramm-Leach-Bliley Act (GLBA), the subject must ____ in order to prevent the vendor from sharing their personal data.

A. Opt in

B. Opt out

C. Undergo screening

D. Provide a biometric template

111. The European Union, with its implementation of privacy directives and regulations, treats individual privacy as _____.

A. A passing fad

B. A human right

C. A legal obligation

D. A business expense

112. If your organization collects/creates privacy data associated with European Union (EU) citizens, and you operate in the cloud, you must *prevent* your provider from storing/moving/processing that data where?

A. Argentina

B. The United States

C. Japan

D. Israel

113. European Union (EU) personal privacy protections include the right to be _____.

A. Secure

B. Delivered

C. Forgotten

D. Protected

114. The Cloud Security Alliance (CSA) has developed a model for cloud privacy frameworks called the Privacy Level Agreement (PLA). Why might a cloud service provider be reluctant to issue or adhere to a PLA?

A. A PLA might limit the provider's liability

B. A PLA would force the provider to accept more liability

C. A PLA is nonbinding

D. A PLA is not enforceable

115. The Cloud Security Alliance's (CSA's) Cloud Controls Matrix (CCM) lists security controls from all the following frameworks *except* _____.

A. ISACA's COBIT

B. PCI DSS

C. The Capability Maturity Model (CMM)

D. ISO 27001

116. The Cloud Security Alliance's (CSA's) Cloud Controls Matrix (CCM) lists security controls from all the following laws *except* _____.

A. Health Information Portability and Accountability Act (HIPAA)

B. Family Education Rights and Privacy Act (FERPA)

C. Personal Information Protection and Electronic Documents Act (PIPEDA)

D. Digital Millennium Copyright Act (DMCA)

117. Digital rights management (DRM) tools might be used to protect all the following assets *except* _____.

A. A trusted device

B. Proprietary software

C. Medical records

D. Financial data

118. Deploying digital rights management (DRM) tools in a bring your own device (BYOD) environment will require _____.

A. User consent and action

B. Enhanced security protocols

C. Use of the cloud

D. Newer, upgraded devices

119. Deploying digital rights management (DRM) tools in a bring your own device (BYOD) environment will require _____.

A. A uniform browser installation

B. Platform-agnostic solutions

C. Turnstiles

D. A secondary BC/DR vendor

120. The Cloud Security Alliance's (CSA's) Cloud Controls Matrix (CCM) addresses all the following security architecture elements *except* _____.

A. Physical security

B. IaaS

C. Application security

D. Business drivers

121. DRM requires that every data resource is provisioned with _____.

A. A tracking device

B. An access policy

C. A hardware security module (HSM)

D. A biometric system

122. Digital rights management (DRM) tools can be combined with _____, to enhance security capabilities.

A. Roaming identity services (RIS)

B. Egress monitoring solutions (DLP)

C. Internal hardware settings (BIOS)

D. Remote Authentication Dial-In User Service (RADIUS)

123. Digital rights management (DRM) tools should enforce _____, which is the characteristic of access rights following the object, in whatever form or location it might be or move to.

A. Continuous audit trail

B. Limiting printing output

C. Persistence

D. Automatic expiration

124. Digital rights management (DRM) tools should enforce _____, which is the practice of capturing all relevant system events.

A. Continuous audit trail

B. Limiting printing output

C. Persistence

D. Automatic expiration

125. Digital rights management (DRM) tools should enforce _____, which is the capability to revoke access based on the decision of the object owner or an administrator action.

A. Integration with email filtering engines

B. Disabling screencap capabilities

C. Continuous audit trail

D. Dynamic policy control

126. Digital rights management (DRM) tools should enforce _____, which is the revocation of access based on time.

A. Persistence

B. Disabling screencap capabilities

C. Automatic expiration

D. Dynamic policy control

127. Digital rights management (DRM) tools should enforce _____, which is interoperability with the organization's other access control activities.

A. Persistence

B. Support for existing authentication security infrastructure

C. Continuous audit trail

D. Dynamic policy control

128. In a data retention policy, what is perhaps the *most* crucial element?

A. Location of the data archive

B. Frequency of backups

C. Security controls in long-term storage

D. Data recovery procedures

129. _____ is the practice of taking data out of the production environment and putting it into long-term storage.

A. Deletion

B. Archiving

C. Crypto-shredding

D. Storing

130. In general, all policies within an organization should include each of the following elements *except* _____.

A. The date on which the policy will expire

B. Assigning an entity to review the applicability of the possibility occasionally

C. The assignment of an entity to monitor and maintain the process described in the policy

D. A list of the laws, regulations, practices, and/or standards that drove the creation of the policy

131. The goals of secure sanitization (or "data destruction") include all of the following *except* _____.

A. Removing data objects/files

B. Minimizing or eliminating data remanence

C. Removing pointers and metadata about specific files/objects

D. Creating a secure, archived copy for business continuity and disaster recovery (BCDR) purposes

132. Why is deleting a file/object insufficient for secure sanitization purposes?

A. Drives/disks must be demagnetized for true secure destruction

B. Physical destruction is the only acceptable method of secure sanitization

C. Deletion usually only removes pointers/indicators of file location

D. Only administrators should be allowed to delete files/objects

133. Data destruction in the cloud is difficult because _____.

A. Cloud data doesn't have substance

B. Regulations prevent it

C. The hardware belongs to the provider

D. Most of the data is subterranean

134. Data destruction in the cloud is difficult because _____.

A. Data in the cloud is constantly being replicated and backed up

B. Delete commands are prohibited in the cloud

C. ISPs will not allow destruction of data stored in the cloud

D. The end clients may prevent it

135. Data destruction in the cloud is difficult because _____.

A. Only law enforcement is permitted to destroy cloud data

B. The largest cloud vendors have prevented customers from destroying data

C. Cloud data renews itself automatically

D. The cloud is often a multitenant environment

136. Which of the following is the best and only completely secure method of data destruction?

A. Degaussing

B. Crypto-shredding

C. Physical destruction of resources that store the data

D. Legal order issued by the prevailing jurisdiction where the data is geographically situated

137. Aside from the fact that the cloud customer probably cannot locate/reach the physical storage assets of the cloud provider, and that wiping an entire storage space would impact other customers, why would degaussing probably not be an effective means of secure sanitization in the cloud?

A. All the data storage space in the cloud is already gaussed.

B. Cloud data storage may not be affected by degaussing.

C. Federal law prohibits it in the United States.

D. The blast radius is too wide.

138. Is overwriting a feasible secure sanitization method in the cloud?

A. Yes, but only if you use multiple passes

B. No, because you can't get physical access to cloud storage resources

C. Yes, but it requires a final pass with all zeros or ones

D. No, because the logical location of the stored data is almost impossible to determine

139. All of the following are reasons overwriting is not a viable secure sanitization method for data stored in the cloud *except* _____.

A. Overwriting an entire storage resource would affect other tenants' data

B. Regulators usually frown on the practice

C. Locating the specific storage locations of cloud data is almost impossible

D. Data is being backed constantly in the cloud; before you finished overwriting an entire data set, it would have been replicated elsewhere

140. Which of the following might make crypto-shredding difficult or useless?

A. Cloud provider also managing the organization's keys

B. Lack of physical access to the environment

C. External attackers

D. Lack of user training and awareness

141. Crypto-shredding requires at least ___ cryptosystem(s).

A. One

B. Two

C. Three

D. Four

142. In addition to having it for business continuity and disaster recovery (BCDR) purposes, data archiving might also be useful for _____.

A. Ensuring profitability

B. Increasing performance

C. Motivating users

D. Correcting accidental errors

143. In addition to having it for business continuity and disaster recovery (BCDR) purposes, data archiving might also be useful for _____.

A. Team building and morale

B. Forensic investigation

C. Choosing security controls

D. Enhancing quality

144. In addition to having it for business continuity and disaster recovery (BCDR) purposes, data archiving might also be useful for _____.

A. Compliance/audit

B. Monitoring performance

C. Gathering investment

D. Enforcing policy

145. Who is responsible for performing archiving activities in a managed cloud environment?

A. The cloud customer

B. The cloud provider

C. The customer's regulator

D. Depends on the contract

146. Data archiving/retention policies should include _____.

A. How long the data must be kept before destruction

B. The depth of underground storage bunkers used for archiving

C. The names of specific personnel tasked with restoring data in the event of data loss in the operational environment

D. The name(s) of senior management involved in publishing the policy

147. What should data archiving/retention policies include?

A. Names of personnel allowed to receive backup media, if third-party offsite archiving services are used

B. Explicit statement of data formats and types of storage media

C. A list of personnel whose data will be archived on a regular basis

D. Which ISP should be used for backup procedures

148. If the organization operates in a cloud environment, security operations procedures should include specific contact information for all of the following *except* _____.

A. Applicable regulatory entities

B. Federal and local law enforcement

C. The originator or publisher of the governing policy

D. The cloud provider's security response office

149. If the organization operates in a cloud environment, security operations procedures should include guidance for all of the following audit/logging processes *except* _____.

A. Definition of security events/incidents

B. The brand/vendor of the cloud provider's audit/logging tool

C. Process for adding new audit/logging rules

D. Process for filtering out false positives by amending the rule set

150. What does *nonrepudiation* mean?

A. Prohibiting certain parties from a private conversation

B. Ensuring that a transaction is completed before saving the results

C. Ensuring that someone cannot turn off auditing capabilities while performing a function

D. Preventing any party that participates in a transaction from claiming that it did not

CCSP® Official (ISC)2® Practice Tests
By Ben Malisow

Chapter

3

Domain 3: Cloud Platform and Infrastructure Security

The third domain of the CBK concerns the underlying infrastructure of the cloud, including both hardware and software, the concept of pooled resources, and a detailed discussion of identity and access management (IAM).

1. You are in charge of creating the business continuity and disaster recovery (BCDR) plan and procedures for your organization.

   Your organization has its production environment hosted in a cloud environment. You are considering using cloud backup services for your BCDR purposes as well. What would probably be the best strategy for this approach, in terms of redundancy and resiliency?

   A. Have your cloud provider also provide BCDR backup

   B. Keep a BCDR backup on the premises of your corporate headquarters

   C. Use another cloud provider for the BCDR backup

   D. Move your production environment back into your corporate premises, and use your cloud provider to host your BCDR backup

2. You are in charge of creating the BCDR plan and procedures for your organization.

   You decide to have a tabletop test of the BCDR activity. Which of the following will offer the value during the test?

   A. Have all participants conduct their individual activities via remote meeting technology

   B. Task a moderator well-versed in BCDR actions to supervise and present scenarios to the participants, including randomized special events

   C. Provide copies of the BCDR policy to all participants

   D. Allow all users in your organization to participate

3. You are in charge of creating the BCDR plan and procedures for your organization.

   Your organization has its production environment hosted by a cloud provider, and you have appropriate protections in place. Which of the following is a significant consideration for your BCDR backup?

   A. Enough personnel at the BCDR recovery site to ensure proper operations

   B. Good cryptographic key management

   C. Access to the servers where the BCDR backup is stored

   D. Forensic analysis capabilities

4. You are in charge of creating the BCDR plan and procedures for your organization.

   You are going to conduct a full test of the BCDR plan. Which of the following strategies is an optimum technique to avoid major issues?

   A. Have another full backup of the production environment stored prior to the test

   B. Assign all personnel roles to perform during the test

   C. Have the cloud provider implement a simulated disaster at a random moment in order to maximize realistic testing

   D. Have your regulators present at the test so they can monitor performance

5. A SAML identity assertion token uses the _____ protocol.

   A. XML

   B. HTTP

   C. HTML

   D. ASCII

6. The minimum essential characteristics of a cloud data center are often referred to as "ping, power, pipe." What does this term mean?

   A. Remote access for customer to racked devices in the data center; electrical utilities; connectivity to an Internet service provider (ISP)/the Internet

   B. Application suitability; availability; connectivity

   C. IaaS; SaaS; PaaS

   D. Anti-malware tools; controls against DDoS attacks; physical/environmental security controls, including fire suppression

7. In order to support all aspects of the CIA triad (confidentiality/integrity/availability), all of the following aspects of a cloud data center need to be engineered with redundancies *except* _____.

   A. Power supply

   B. HVAC

   C. Administrative offices

   D. Internet service provider (ISP)/connectivity lines

8. Who is the cloud carrier?

   A. The cloud customer

   B. The cloud provider

   C. The regulator overseeing the cloud customer's industry

   D. The ISP between the cloud customer and provider

9. Which of the following terms describes a means to centralize logical control of all networked nodes in the environment, abstracted from the physical connections to each?
   - **A.** Virtual private network (VPN)
   - **B.** Software-defined network (SDN)
   - **C.** Access control lists (ACLs)
   - **D.** Role-based access control (RBAC)

10. In software-defined networking (SDN), the northbound interface (NBI) usually handles traffic between the _____ and _____.
   - **A.** Cloud customer; ISP
   - **B.** SDN controllers; SDN applications
   - **C.** Cloud provider; ISP
   - **D.** Router; host

11. Software-defined networking (SDN) allows network administrators/architects to perform all the following functions *except* _____.
   - **A.** Reroute traffic based on current customer demand
   - **B.** Create logical subnets without having to change any actual physical connections
   - **C.** Filter access to resources based on specific rules or settings
   - **D.** Deliver streaming media content in an efficient manner by placing it closer to the end user

12. Which of the following is a device specially purposed to handle the issuance, distribution, and storage of cryptographic keys?
   - **A.** Key management box (KMB)
   - **B.** Hardware security module (HSM)
   - **C.** Ticket-granting ticket (TGT)
   - **D.** Trusted computing base (TCB)

13. When discussing the cloud, we often segregate the data center into the terms *compute*, *storage*, and *networking*.

    Compute is made up of _____ and _____.
   - **A.** Routers; hosts
   - **B.** Application programming interface (APIs); Northbound interface (NBIs)
   - **C.** Central processing unit (CPU); Random-access memory (RAM)
   - **D.** Virtualized; actual hardware devices

14. All of the following can be used to properly apportion cloud resources *except* _____.
   - **A.** Reservations
   - **B.** Shares
   - **C.** Cancellations
   - **D.** Limits

15. Which of the following is a method for apportioning resources that involves setting guaranteed minimums for all tenants/customers within the environment?

A. Reservations

B. Shares

C. Cancellations

D. Limits

16. Which of the following is a method for apportioning resources that involves setting maximum usage amounts for all tenants/customers within the environment?

A. Reservations

B. Shares

C. Cancellations

D. Limits

17. Which of the following is a method for apportioning resources that involves prioritizing resource requests to resolve contention situations?

A. Reservations

B. Shares

C. Cancellations

D. Limits

18. A bare-metal hypervisor is Type _____.

A. 1

B. 2

C. 3

D. 4

19. A hypervisor that runs inside another operating system (OS) is a Type _____ hypervisor.

A. 1

B. 2

C. 3

D. 4

20. A Type _____ hypervisor is probably more difficult to defend than other hypervisors.

A. 1

B. 2

C. 3

D. 4

21. One of the security challenges of operating in the cloud is that additional controls must be placed on file storage systems because _____.

- **A.** File stores are always kept in plain text in the cloud
- **B.** There is no way to sanitize file storage space in the cloud
- **C.** Virtualization necessarily prevents the use of application-based security controls
- **D.** Virtual machines are stored as snapshotted files when not in use

22. What is the main reason virtualization is used in the cloud?

- **A.** VMs are easier to administer
- **B.** If a VM is infected with malware, it can be easily replaced
- **C.** With VMs, the cloud provider does not have to deploy an entire hardware device for every new user
- **D.** VMs are easier to operate than actual devices

23. Orchestrating resource calls is the job of the _____.

- **A.** Administrator
- **B.** Router
- **C.** VM
- **D.** Hypervisor

24. Which of the following terms describes a cloud storage area that uses a file system/hierarchy?

- **A.** Volume storage
- **B.** Object storage
- **C.** Logical unit number (LUN)
- **D.** Block storage

25. Typically, which form of cloud storage is used in the near term for snapshotted virtual machine (VM) images?

- **A.** Volume storage
- **B.** Object storage
- **C.** Logical unit number (LUN)
- **D.** Block storage

26. Who operates the management plane?

- **A.** Regulators
- **B.** End consumers
- **C.** Privileged users
- **D.** Privacy data subjects

27. What is probably the *optimum* way to avoid vendor lock-in?

A. Use non-proprietary data formats

B. Use industry-standard media

C. Use strong cryptography

D. Use favorable contract language

28. Who will determine whether your organization's cloud migration is satisfactory from a compliance perspective?

A. The cloud provider

B. The cloud customer

C. The regulator(s)

D. The Internet service provider (ISP)

29. What is probably the best way to avoid problems associated with vendor lockout?

A. Use strong contract language

B. Use nonproprietary data and media formats

C. Use strong cryptography

D. Use another provider for backup purposes

30. In a managed cloud services arrangement, who creates governance that will determine which controls are selected for the environment and how they are deployed?

A. The cloud provider

B. The cloud customer

C. The regulator(s)

D. The end user

31. What is the term that describes the situation when a malicious user/attacker can exit the restrictions of a virtual machine (VM) and access another VM residing on the same host?

A. Host escape

B. Guest escape

C. Provider exit

D. Escalation of privileges

32. What is the term that describes the situation when a malicious user/attacker can exit the restrictions of a single host and access other nodes on the network?

A. Host escape

B. Guest escape

C. Provider exit

D. Escalation of privileges

33. _____ is/are probably the main cause of virtualization sprawl.

A. Malicious attackers

B. Lack of provider controls

C. Lack of customer controls

D. Ease of use

34. Sprawl is mainly a(n) _____ problem.

A. Technical

B. External

C. Management

D. Logical

35. Which of the following risks exists in the legacy environment but is dramatically increased by moving into the cloud?

A. Physical security breaches

B. Loss of utility power

C. Financial upheaval

D. Man-in-the-middle attacks

36. A fundamental aspect of security principles, _____ should be implemented in the cloud as well as in legacy environments.

A. Continual uptime

B. Defense in depth

C. Multifactor authentication

D. Separation of duties

37. From a security perspective, automation of configuration aids in _____.

A. Enhancing performance

B. Reducing potential attack vectors

C. Increasing ease of use of the systems

D. Reducing need for administrative personnel

38. _____ is the *most* prevalent protocol used in identity federation.

A. HTTP

B. SAML

C. FTP

D. WS-Federation

39. A user signs on to a cloud-based social media platform. In another browser tab, the user finds an article worth posting to the social media platform. The user clicks on the platform's icon listed on the article's website, and the article is automatically posted to the user's account on the social media platform.

This is an example of what?

A. Single sign-on

B. Insecure direct identifiers

C. Identity federation

D. Cross-site scripting

40. A group of clinics decides to create an identification federation for their users (medical providers and clinicians).

If they opt to review each other, for compliance with security governance and standards they all find acceptable, what is this federation model called?

A. Cross-certification

B. Proxy

C. Single sign-on

D. Regulated

41. A group of clinics decide to create an identification federation for their users (medical providers and clinicians).

If they opt to hire a third party to review each organization, for compliance with security governance and standards they all find acceptable, what is this federation model called?

A. Cross-certification

B. Proxy

C. Single sign-on

D. Regulated

42. A group of clinics decides to create an identification federation for their users (medical providers and clinicians).

If they opt to use the web of trust model for federation, who is/are the identity provider(s)?

A. Each organization

B. A trusted third party

C. The regulator overseeing their industry

D. All of their patients

43. A group of clinics decides to create an identification federation for their users (medical providers and clinicians).

If they opt to use the web of trust model for federation, who is/are the service providers?

A. Each organization

B. A trusted third party

C. The regulator overseeing their industry

D. All of their patients

44. A group of clinics decides to create an identification federation for their users (medical providers and clinicians).

In this federation, all of the participating organizations would need to be in compliance with what US federal regulation?

A. Gramm-Leach-Bliley Act (GLBA)

B. Family and Medical Leave Act (FMLA)

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

D. Health Information Portability and Accountability Act (HIPAA)

45. What is the process of granting access to resources?

A. Identification

B. Authentication

C. Authorization

D. Federation

46. The process of identity management includes all the following elements *except* _____.

A. Provisioning

B. Maintenance

C. Deprovisioning

D. Redaction

47. Which organizational entity usually performs the verification part of the provisioning element of the identification process?

A. IT

B. Security

C. HR

D. Sales

48. Of the following options, which is a reason cloud data center audits are often less trustworthy than legacy audits?

A. Data in the cloud can't be audited

B. Controls in the cloud can't be audited

C. Getting physical access can be difficult

D. There are no regulators for cloud operations

49. Of the following options, which is a reason cloud data center audits are often less trustworthy than legacy audits?

A. Cryptography is present

B. Auditors don't like the cloud

C. Cloud equipment is resistant to audit

D. They often rely on data the provider chooses to disclose

50. Of the following options, which is a reason cloud data center audits are often less trustworthy than audits in standard data centers?

A. They frequently rely on third parties

B. The standards are too difficult to follow

C. The paperwork is cumbersome

D. There aren't enough auditors

51. The cloud customer will usually not have physical access to the cloud data center. This enhances security by _____.

A. Reducing the need for qualified personnel

B. Limiting access to sensitive information

C. Reducing jurisdictional exposure

D. Ensuring statutory compliance

52. Which of the following controls would be useful to build into a virtual machine baseline image for a cloud environment?

A. GPS tracking/locator

B. Automated vulnerability scan on system startup

C. Access control list of authorized personnel

D. Write protection

53. Which of the following controls would be useful to build into a virtual machine baseline image for a cloud environment?

A. Automatic registration with the configuration management system

B. Enhanced user training and awareness media

C. Mechanisms that prevent the file from being copied

D. Keystroke loggers

54. Virtual machine (VM) configuration management (CM) tools should probably include _____.

A. Biometric recognition

B. Anti-tampering mechanisms

C. Log file generation

D. Hackback capabilities

55. Using a virtual machine baseline image could be very useful for which of the following options?

A. Physical security

B. Auditing

C. Training

D. Customization

56. What can be revealed by an audit of a baseline virtual image, used in a cloud environment?

A. Possible intrusions after they have happened

B. Potential criminal activity before it occurs

C. Whether necessary security controls are in place and functioning properly

D. Lack of user training and awareness

57. Using one cloud provider for your operational environment and another for your BCDR backup will also give you the additional benefit of _____.

A. Allowing any custom VM builds you use to be instantly ported to another environment

B. Avoiding vendor lock-in/lockout

C. Increased performance

D. Lower cost

58. Having your BCDR backup stored with the same cloud provider as your production environment can help you _____.

A. Maintain regulatory compliance

B. Spend less of your budget on traveling

C. Train your users about security awareness

D. Recover quickly from minor incidents

59. If you use the cloud for BCDR purposes, even if you don't operate your production environment in the cloud, you can cut costs by eliminating your _____.

A. Security personnel

B. BCDR policy

C. Old access credentials

D. Need for a physical hot site/warm site

60. If the cloud is used for BCDR purposes, the loss of _____ could gravely affect your organization's RTO.

A. The cloud server

B. A specific VM

C. Your policy and contract documentation

D. ISP connectivity

61. What is the *most* important asset to protect in cloud BCDR activities?

A. Intellectual property

B. Hardware at the cloud data center

C. Personnel

D. Data on portable media

62. When considering cloud data replication strategies (i.e., whether you are making backups at the block, file, or database level), which element of your organization's BCDR plan will be *most* affected by your choice?

A. Recovery time objective

B. Recovery point objective

C. Maximum allowable downtime

D. Mean time to failure

63. In addition to BCDR, what other benefit can your data archive/backup provide?

A. Physical security enforcement

B. Access control methodology

C. Security control against data breach

D. Identity management testing

64. Which of the following risks is probably *most* significant when choosing to use one cloud provider for your operational environment and another for BCDR backup/archive?

A. Physical intrusion

B. Proprietary formats/lack of interoperability

C. Vendor lock-in/lockout

D. Natural disasters

65. Return to normal operations is a phase in BCDR activity when the contingency event is over and regular production can resume. Which of the following can sometimes be the result when the organization uses two different cloud providers for the production and BCDR environments?

A. Both providers are affected by the contingency, extending the time before return to normal can occur

B. The BCDR provider becomes the new normal production environment

C. Regulators will find the organization in violation of compliance guidance

D. All data is lost irretrievably

66. Which of these determines the critical assets, recovery time objective (RTO), and recover point objective (RPO) for BCDR purposes?

A. Business drivers

B. User input

C. Regulator mandate

D. Industry standards

67. What artifact—which should already exist within the organization—can be used to determine the critical assets necessary to protect in the BCDR activity?

A. Quantitative risk analysis

B. Qualitative risk analysis

C. Business impact analysis

D. Risk appetite

68. Which of the following is probably the *most* important element to address if your organization is using two different cloud providers for the production and BCDR environments?

A. Do they cost the same?

B. Do they have similar facility protections in place?

C. What level of end-user support do they each offer?

D. Can the backup provider meet the same SLA requirements of the primary?

69. In a managed cloud services arrangement, who invokes a BCDR action?

A. The cloud provider

B. The cloud customer

C. Depends on the contract

D. Any user

70. What do you need to do in order to fully ensure that a BCDR action will function during a contingency?

A. Audit all performance functions

B. Audit all security functions

C. Perform a full-scale test

D. Mandate this capability in the contract

71. Which of the following is probably the *most* important activity, of those listed?

A. Regularly update the BCDR plan/process.

B. Have contact information for all personnel in the organization.

C. Have contact information for essential BCDR personnel.

D. Have contact information for local law enforcement.

72. The BCDR plan/policy should include all of the following *except* _____.

A. Tasking for the office responsible for maintaining/enforcing the plan

B. Contact information for essential entities, including BCDR personnel and emergency services agencies

C. Copies of the laws/regulations/standards governing specific elements of the plan

D. Checklists for BCDR personnel to follow

73. The BCDR plan/process should be written and documented in such a way that it can be used by _____.

A. Users

B. Essential BCDR team members

C. Regulators

D. Someone with the requisite skills

74. Which of the following probably poses the *most* significant risk to the organization?

A. Not having essential BCDR personnel available during a contingency

B. Not including all BCDR elements in the cloud contract

C. Returning to normal operations too soon

D. Telecommunications outages

75. Which of the following probably poses the *most* significant risk to the organization?

A. Lack of data confidentiality during a contingency

B. Lack of regulatory compliance during a contingency

C. Returning to normal operations too late

D. Lack of encrypted communications during a contingency

76. Why does the physical location of your data backup and/or BCDR failover environment matter?

A. It may affect regulatory compliance

B. Lack of physical security

C. Environmental factors such as humidity

D. It doesn't matter. Data can be saved anywhere without consequence

77. According to the European Union Agency for Network and Information Security (ENISA), a cloud risk assessment should provide a means for customers to accomplish all these assurance tasks *except* _____.

A. Assess risks associated with cloud migration

B. Compare offerings from different cloud providers

C. Reduce the risk of regulatory noncompliance

D. Reduce the assurance burden on cloud providers

78. The European Union Agency for Network and Information Security's (ENISA's) definition of cloud computing differs slightly from the definition offered by $(ISC)^2$ (and, for instance, NIST). What is one of the characteristics listed by ENISA but *not* included in the $(ISC)^2$ definition?

A. Metered service

B. Shared resources

C. Scalability

D. Programmatic management

79. Risk should always be considered from a business perspective. Risk is often balanced by corresponding _____.

A. Profit

B. Performance

C. Cost

D. Opportunity

80. When considering the option to migrate from an on-premises environment to a hosted cloud service, an organization should weigh the risks of allowing external entities to access the cloud data for collaborative purposes against _____.

A. Not securing the data in the legacy environment

B. Disclosing the data publicly

C. Inviting external personnel into the legacy workspace in order to enhance collaboration

D. Sending the data outside the legacy environment for collaborative purposes

81. There are many ways to handle risk. However, the usual methods for addressing risk are not all possible in the cloud because _____.

A. Cloud data risks cannot be mitigated

B. Migrating into a cloud environment necessarily means you are accepting all risks

C. Some risks cannot be transferred to a cloud provider

D. Cloud providers cannot avoid risk

82. In which cloud service model does the customer lose the *most* control over governance?

A. Infrastructure as a service (IaaS)

B. Platform as a service (PaaS)

C. Software as a service (SaaS)

D. Private cloud

83. Which of the following poses a *new* risk in the cloud, not affecting the legacy, on-premises environment?

A. Internal threats

B. Multitenancy

C. Natural disasters

D. Distributed denial of service (DDoS) attacks

84. In addition to the security offered by the cloud provider, a cloud customer must consider the security offered by _____.

A. The respective regulator

B. The end user(s)

C. Any vendor the cloud customer previously used in the on-premises environment

D. Any third parties the provider depends on

85. Which of the following poses a *new* risk in the cloud, not affecting the legacy, on-premises environment?

A. User carelessness

B. Inadvertent breach

C. Device failure

D. Resource exhaustion

86. Where is isolation failure probably *least* likely to pose a significant risk?

A. Public cloud

B. Private cloud

C. PaaS environment

D. SaaS environment

87. Which of the following poses a *new* risk in the cloud, not affecting the legacy, on-premises environment?

A. Fire

B. Legal seizure of another firm's assets

C. Mandatory privacy data breach notifications

D. Flooding

88. Which of these does the cloud customer need to ensure protection of intellectual property created in the cloud?

A. Digital rights management (DRM) solutions

B. Identity and access management (IAM) solutions

C. Strong contractual clauses

D. Crypto-shredding

89. What could be the result of failure of the cloud provider to secure the hypervisor in such a way that one user on a virtual machine can see the resource calls of another user's virtual machine?

A. Unauthorized data disclosure

B. Inference attacks

C. Social engineering

D. Physical intrusion

90. Key generation in a cloud environment might have less entropy than the legacy environment for all the following reasons *except* _____.

A. Lack of direct input devices

B. No social factors

C. Uniform build

D. Virtualization

91. Lack of industry-wide standards for cloud computing creates a potential for _____.

A. Privacy data breach

B. Privacy data disclosure

C. vendor lock-in

D. vendor lockout

92. What can hamper the ability of a cloud customer to protect their own assets in a managed services arrangement?

A. Prohibitions on port scanning and penetration testing

B. Geographical dispersion

C. Rules against training users

D. Laws that prevent them from doing so

93. Cloud administration almost necessarily violates the principles of the _____ security model.

A. Brewer-Nash (Chinese Wall)

B. Graham-Denning

C. Bell-LaPadula

D. Biba

94. The physical layout of a cloud data center campus should include redundancies of all the following *except* _____.

A. Physical perimeter security controls (fences, lights, walls, etc.)

B. The administration/support staff building

C. Electrical utility lines

D. Communications connectivity lines

95. Best practice for planning the physical resiliency for a cloud data center facility includes _____.

A. Having one point of egress for personnel

B. Ensuring that any cabling/connectivity enters the facility from different sides of the building/property

C. Ensuring that all parking areas are near generators so that personnel in high-traffic areas are always illuminated by emergency lighting, even when utility power is not available

D. Ensuring that the foundation of the facility is rated to withstand earthquake tremors

96. The physical layout of a cloud data center campus should include redundancies of all the following *except* _____.

A. Generators

B. HVAC units

C. Generator fuel storage

D. Points of personnel ingress

97. There are two reasons to conduct a test of the organization's recovery from backup in an environment other than the primary production environment. Which of the following is one of them?

A. It costs more to conduct a test at the same location as the primary workplace

B. You don't want to waste travel budget on what is only a test

C. The risk of negative impact to both production and backup is too high

D. There won't be enough room for everyone to sit in the primary facility

98. There are two reasons to conduct a test of the organization's recovery from backup in an environment other than the primary production environment. Which of the following is one of them?

A. It is good to invest in more than one community.

B. You want to approximate contingency conditions, which includes not operating in the primary location.

C. It is good for your personnel to see other places occasionally.

D. Your regulators won't follow you offsite, so you'll be unobserved during your test.

99. In an IaaS arrangement, who accepts responsibility for securing cloud-based applications?

A. The cloud provider

B. The cloud customer

C. The regulator

D. The end user/client

100. Industry best practices dictate that cloud customers do not _____.

A. Create their own identity and access management (IAM) solutions

B. Create contract language that favors them over the provider

C. Retrain personnel for cloud operations

D. Encrypt data before it reaches the cloud

101. It is possible for the cloud customer to transfer _____ risk to the provider, but the cloud customer always retains ultimate legal risk.

A. Market

B. Perception

C. Data

D. Financial

102. A process for _____ can aid in protecting against data disclosure due to lost devices.

A. User punishment

B. Credential revocation

C. Law enforcement notification

D. Device tracking

103. All of the following can be used in the process of anomaly detection *except* _____.

A. The ratio of failed to successful logins

B. Transactions completed successfully

C. Event time of day

D. Multiple concurrent logins

104. Critical components should be protected with _____.

A. Strong passwords

B. Chain-link fences

C. Homomorphic encryption

D. Multifactor authentication

105. It's important to maintain a current asset inventory list, including surveying your environment on a regular basis, in order to _____.

A. Prevent unknown, unpatched assets from being used as back doors to the environment

B. Ensure that any lost devices are automatically entered into the acquisition system for repurchasing and replacement

C. Maintain user morale by having their devices properly catalogued and annotated

D. Ensure that billing for all devices is handled by the appropriate departments

106. Which of the following can enhance data portability?

A. Interoperable export formats

B. Egress monitoring solutions

C. Strong physical protections

D. Agile business intelligence

107. Which of the following can enhance application portability?

A. Using the same cloud provider for the production environment and archiving

B. Conducting service trials in an alternate cloud provider environment

C. Providing cloud-usage training for all users

D. Tuning web application firewalls (WAFs) to detect anomalous activity in inbound communications

108. What should the cloud customer do to ensure that disaster recovery activities don't exceed the maximum allowable downtime (MAD)?

A. Make sure any alternate provider can support the application needs of the organization.

B. Ensure that contact information for all first responder agencies are correct and up-to-date at all times.

C. Select an appropriate recovery time objective (RTO).

D. Regularly review all regulatory directives for disaster response.

109. Which of the following would probably best aid an organization in deciding whether to migrate from a legacy environment to a particular cloud provider?

A. Rate sheets comparing a cloud provider to other cloud providers

B. Cloud provider offers to provide engineering assistance during the migration

C. The cost/benefit measure of closing the organization's relocation site (hot site/warm site) and using the cloud for disaster recovery instead

D. SLA satisfaction surveys from other (current and past) cloud customers

110. A cloud provider will probably require all of the following *except* _____ before a customer conducts a penetration test.

A. Notice

B. Description of scope of the test

C. Location of the launch point

D. Knowledge of time frame/duration

111. Cloud providers will probably not allow _____ as part of a customer's penetration test.

A. Network mapping

B. Vulnerability scanning

C. Reconnaissance

D. Social engineering

112. A cloud customer performing a penetration test without the provider's permission is risking _____.

A. Malware contamination

B. Excessive fees for SLA violations

C. Loss of market share

D. Prosecution

113. When a customer performs a penetration test in the cloud, why isn't the test an optimum simulation of attack conditions?

A. Attackers don't use remote access for cloud activity

B. Advanced notice removes the element of surprise

C. When cloud customers use malware, it's not the same as when attackers use malware

D. Regulator involvement changes the attack surface

114. Managed cloud services exist because the service is less expensive for each customer than creating the same services for themselves in a legacy environment.

What is the technology that creates most of the cost saving in the cloud environment?

A. Emulation

B. Secure remote access

C. Crypto-shredding

D. Virtualization

115. Managed cloud services exist because the service is less expensive for each customer than creating the same services for themselves in a legacy environment.

From the customer perspective, most of the cost differential created between the legacy environment and the cloud through virtualization is achieved by removing _____.

A. External risks

B. Internal risks

C. Regulatory compliance

D. Sunk capital investment

116. Managed cloud services exist because the service is less expensive for each customer than creating the same services for themselves in a legacy environment.

Using a managed service allows the customer to realize significant cost savings through the reduction of _____.

A. Risk

B. Security controls

C. Personnel

D. Data

117. Which of the following is a risk posed by the use of virtualization?

A. Internal threats interrupting service through physical accidents (spilling drinks, tripping over cables, etc.)

B. The ease of transporting stolen virtual machine images

C. Increased susceptibility of virtual systems to malware

D. Electromagnetic pulse

118. The tasks performed by the hypervisor in the virtual environment can most be likened to the tasks of the _____ in the legacy environment.

A. Central processing unit (CPU)

B. Security team

C. OS

D. PGP

119. Mass storage in the cloud will most likely currently involve _____.

A. Spinning platters

B. Tape drives

C. Magnetic disks

D. Solid-state drives (SSDs)

120. What is the type of cloud storage arrangement that involves the use of associating metadata with the saved data?

A. Volume

B. Block

C. Object

D. Redundant

121. According to the *NIST Cloud Computing Reference Architecture*, which of the following is most likely a cloud carrier?

A. Amazon Web Services

B. Netflix

C. Verizon

D. Nessus

122. Resolving resource contentions in the cloud will most likely be the job of the _____.

A. Router

B. Emulator

C. Regulator

D. Hypervisor

123. Security controls installed on a guest virtual machine operating system (VM OS) will *not* function when _____.

A. The user is accessing the VM remotely

B. The OS is not scanned for vulnerabilities

C. The OS is not subject to version control

D. The VM is not active while in storage

124. Typically, SSDs are _____.

A. More expensive than spinning platters

B. Larger than tape backup

C. Heavier than tape libraries

D. More subject to malware than legacy drives

125. Typically, SSDs are _____.

A. Harder to install than magnetic memory

B. Faster than magnetic drives

C. Harder to administer than tape libraries

D. More likely to fail than spinning platters

126. Typically, SSDs are _____.

A. Impossible to destroy physically

B. Not vulnerable to degaussing

C. Subject to a longer warranty

D. Protected by international trade laws

127. Of the following control techniques/solutions, which can be combined to enhance the protections offered by each?

A. Fences/firewalls

B. Asset inventories/personnel training

C. Data dispersion/encryption

D. Intrusion prevention solutions/intrusion detection solutions

128. Of the following control techniques/solutions, which can be combined to enhance the protections offered by each?

A. Razor tape/background checks

B. Least privilege/generators

C. DLP/DRM

D. Personnel badging/secure baselines

129. Risk assessment is the responsibility of _____.

A. Companies offering managed cloud services

B. Regulatory bodies

C. Every organization

D. Legislative entities

130. Which entity can *best* aid the organization in avoiding vendor lock-in?

A. Senior management

B. The IT security office

C. General counsel

D. The cloud security representative

131. Perhaps the best method for avoiding vendor lock-out is also a means for enhancing BCDR capabilities. This is _____.

A. Having a warm site within 250 miles of the primary production environment

B. Using one cloud provider for primary production and another for backup purposes

C. Building a data center above the flood plain

D. Cross-training all personnel

132. _____ can often be the result of inadvertent activity.

A. DDoS

B. Phishing

C. Sprawl

D. Disasters

133. Of the following, which is probably the *most* significant risk in a managed cloud environment?

A. DDoS

B. Management plane breach

C. Guest escape

D. Physical attack on the utility service lines

134. What is the optimal number of entrances to the cloud data center campus?

A. One

B. Two

C. Three

D. Four

135. The cloud data center campus physical access point should include all of the following *except* _____.

A. Reception area

B. Video surveillance

C. Badging procedure

D. Mantrap structures

136. Where should multiple egress points be included?

A. At the power distribution substation

B. Within the data center

C. In every building on the campus

D. In the security operations center

137. Which of the following is a risk in the cloud environment that is *not* existing or as prevalent in the legacy environment?

A. DDoS

B. Isolation failure

C. External attack

D. Internal attack

138. All security controls necessarily _____.

A. Are expensive

B. Degrade performance

C. Require senior management approval

D. Will work in the cloud environment as well as they worked in the legacy environment

139. Which of the following is a risk in the cloud environment that is *not* existing or is as prevalent in the legacy environment?

A. Legal liability in multiple jurisdictions

B. Loss of productivity due to DDoS

C. Ability of users to gain access to their physical workplace

D. Fire

140. Which of the following is a risk in the cloud environment that is *not* existing or as prevalent in the legacy environment?

A. Loss of availability due to DDoS

B. Loss of value due to DDoS

C. Loss of confidentiality due to DDoS

D. Loss of liability due to DDoS

141. DDoS attacks do not affect _____ for cloud customers.

A. Productivity

B. Availability

C. Connectivity

D. Integrity

142. Sprawl in the cloud can lead to significant additional costs to the organization because of _____.

A. Larger necessary physical footprint

B. Much larger utility consumption

C. Software licensing

D. Requisite additional training

143. It is best to use variables in _____.

A. Baseline configurations

B. Security control implementations

C. Contract language

D. BCDR tests

Chapter

4

CCSP® Official (ISC)2® Practice Tests
By Ben Malisow

Domain 4: Cloud Application Security

The fourth domain of the CCSP CBK covers applications in the cloud, from software development to challenges involved in migrating legacy apps. It also addresses software security and performance testing methods as well as proper identity and access management (IAM) principles. Because it is weighted less than the previous domains (according to this table published by (ISC)^2, `https://cccure.training/m/articles/view/CISSP-domains-weight-percentage-on-the-real-exam`), there are considerably fewer questions in this chapter.

1. ISO 27034 mandates a framework for application security within an organization. According to the standard, each organization should have a(n) _____, and each application within the organization should have its own _____.
   - **A.** Organizational Normative Framework (ONF), Application Normative Framework (ANF)
   - **B.** Application Normative Framework (ANF), Organizational Normative Framework (ONF)
   - **C.** Standard Application Security (SAS), Application Normative Framework (ANF)
   - **D.** Organizational Normative Framework (ONF), Standard Application Security (SAS)

2. According to ISO 27034, there is one Organizational Normative Framework (ONF) in the organization, and _____ Application Normative Framework (ANF(s)) for each application within that organization.
   - **A.** Many
   - **B.** Three
   - **C.** No
   - **D.** One

3. What language is used in the simple object access protocol (SOAP) application design protocol?
   - **A.** HTML
   - **B.** X.509
   - **C.** XML
   - **D.** HTTP

4. Typically, REST interactions do *not* require _____.
   - **A.** Credentials
   - **B.** Sessions
   - **C.** Servers
   - **D.** Clients

5. REST APIs use _____ protocol verbs.
   - **A.** HTML
   - **B.** HTTP
   - **C.** XML
   - **D.** ASCII

6. The architecture of the World Wide Web, as it works today, is _____.
   - **A.** JSON
   - **B.** DoS
   - **C.** REST
   - **D.** XML

7. RESTful responses can come from the server in _____ or _____ formats.
   - **A.** XML, JSON
   - **B.** HTTP, X.509
   - **C.** ASCII, text
   - **D.** HTML, XML

8. Which of the following is an informal industry term for moving applications from a legacy environment into the cloud?
   - **A.** Instantiation
   - **B.** Porting
   - **C.** Grandslamming
   - **D.** Forklifting

9. Developers creating software for the cloud environment should bear in mind cloud-specific risks such as _____ and _____.
   - **A.** DoS and DDoS
   - **B.** Multitenancy and third-party administrators
   - **C.** Unprotected servers and unprotected clients
   - **D.** Default configurations and user error

10. When an organization considers cloud migrations, the organization's software developers will need to know which _____ and which _____ the organization will be using, in order to properly and securely create suitable applications.
    - **A.** Geographic location, native language
    - **B.** Legal restrictions, specific ISP
    - **C.** Service model, deployment model
    - **D.** Available bandwidth, telecommunications country code

11. Which of the following is perhaps the best method for reducing the risk of a specific application *not* delivering the proper level of functionality and performance when it is moved from the legacy environment into the cloud?

A. Remove the application from the organization's production environment, and replace it with something else.

B. Negotiate and conduct a trial run in the cloud environment for that application before permanently migrating.

C. Make sure the application is fully updated and patched according to all vendor specifications.

D. Run the application in an emulator.

12. Software developers designing applications for the cloud should expect to include options to ensure all of the following capabilities *except* _____.

A. Encryption of data at rest

B. Encryption of data in transit

C. Data masking

D. Hashing database fields

13. In a PaaS model, who should *most* likely be responsible for the security of the applications in the production environment?

A. Cloud customer

B. Cloud provider

C. Regulator

D. Programmers

14. In the testing phase of the software development life cycle (SDLC), software performance and _____ should both be reviewed.

A. Quality

B. Brevity

C. Requirements

D. Security

15. Regardless of which model the organization uses for system development, in which phase of the SDLC will user input be requested and considered?

A. Define

B. Design

C. Develop

D. Detect

16. Which phase of the SDLC is most likely to involve crypto-shredding?
    - **A.** Define
    - **B.** Design
    - **C.** Test
    - **D.** Disposal

17. Where are business requirements most likely to be mapped to software construction?
    - **A.** Define
    - **B.** Design
    - **C.** Test
    - **D.** Secure Operations

18. All of the following are usually nonfunctional requirements *except* _____.
    - **A.** Color
    - **B.** Sound
    - **C.** Security
    - **D.** Function

19. Designers making applications for the cloud have to take into consideration risks and operational constraints that did not exist or were not as pronounced in the legacy environment.

    Which of the following is an element cloud app designers may have to consider incorporating in software for the cloud that might not have been as important in the legacy environment?
    - **A.** IAM capability
    - **B.** DDoS resistance
    - **C.** Encryption for data at rest and in motion
    - **D.** Field validation

20. Designers making applications for the cloud have to take into consideration risks and operational constraints that did not exist or were not as pronounced in the legacy environment.

    Which of the following is an element cloud app designers may have to consider incorporating in software for the cloud that might not have been as important in the legacy environment?
    - **A.** Application isolation
    - **B.** Inference framing
    - **C.** Known secure library components
    - **D.** Testing that uses known bad data

21. Designers making applications for the cloud have to take into consideration risks and operational constraints that did not exist or were not as pronounced in the legacy environment.

Which of the following is an element cloud app designers may not be able to use as readily in the cloud environment as it was deployed in the legacy environment?

A. Cryptography

B. STRIDE testing

C. Field validation

D. Logging

22. All of these can affect the quality of service expected from an application *except* _____.

A. Encryption

B. Egress monitoring

C. Anti-malware tools

D. Use of known secure libraries/components

23. The possibility that a user could gain access or control of an application so as to take on administrator or management capabilities is called _____.

A. Inversion

B. Spoofing

C. Repudiation

D. Escalation of privilege

24. Which of the following is *not* checked when using the STRIDE threat model?

A. The ability of users to gain administrative access rights without proper permission

B. The ability of internal personnel to trigger business continuity/disaster recovery activities

C. The ability of a participant in a transaction to refute that they've taken part in the transaction

D. The ability of an unauthorized user to pretend to be an authorized user

25. It is very likely that your organization's users will utilize unapproved APIs, especially in a BYOD environment, because _____.

A. Users are constantly trying to break the security of your environment

B. APIs can't ever be secure

C. Hackers are constantly infiltrating all APIs

D. Users enhance their productivity however they can

26. Many current software developers are not aware of security problems within the programs they're creating because _____.

- **A.** Young programmers are not nearly as disciplined in their coding practices as older programmers
- **B.** Many current programmers don't write code line by line and instead use code component libraries
- **C.** Coding languages have not been secure for 20 years
- **D.** Users are not clear in defining their requirements at the outset of the SDLC

27. What is the *most* secure form of code testing and review?

- **A.** Open source
- **B.** Proprietary/internal
- **C.** Neither open source nor proprietary
- **D.** Combination of open source and proprietary

28. What is the major difference between authentication/authorization?

- **A.** Code verification/code implementation
- **B.** Identity validation/access permission
- **C.** Inverse incantation/obverse instantiation
- **D.** User access/privileged access

29. Access should be based on _____.

- **A.** Regulatory mandates
- **B.** Business needs and acceptable risk
- **C.** User requirements and management requests
- **D.** Optimum performance and security provision

30. Who should determine which users have access to which specific objects?

- **A.** The cloud provider
- **B.** Senior management
- **C.** Data owners
- **D.** System administrators

31. All of the following are identity federation standards commonly found in use today *except* _____.

- **A.** WS-Federation
- **B.** OpenID
- **C.** OAuth
- **D.** PGP

32. Which of the following is a federation standard/protocol that does *not* rely on SOAP/SAML/XML?

A. WS-Federation

B. OpenID Connect

C. SOC 2

D. OWASP

33. Authentication mechanisms typically include any or all of the following *except* _____.

A. Something you know

B. Someone you know

C. Something you have

D. Something you are

34. Which of the following constitutes a multifactor authentication process/procedure?

A. Using an ATM to get cash with your credit/debit card

B. Using a password and PIN to log in to a website

C. Presenting a voice sample and fingerprint to access a secure facility

D. Displaying a Social Security card and a credit card

35. Typically, multifactor authentication should be used _____.

A. In every IT transaction

B. For high-risk operations and data that is particularly sensitive

C. When remote users are logging into the cloud environment

D. Only in the legacy environment

36. A web application firewall (WAF) usually operates at layer _____ of the OSI model.

A. 2

B. 3

C. 7

D. Q

37. A web application firewall (WAF) can understand and act on _____ traffic.

A. Malicious

B. SMTP

C. ICMP

D. HTTP

38. WAFs can be used to reduce the likelihood that _____ attacks will be successful.

A. Social engineering

B. Physical theft

C. Obverse inflection

D. Cross-site scripting

39. A database activity monitor (DAM) tool usually operates at layer _____ of the OSI model.

A. 2

B. 3

C. 7

D. Q

40. Database activity monitors (DAMs) can be used to reduce the potential success of _____ attacks.

A. SQL injection

B. Cross-site scripting

C. Insecure direct-object reference

D. Social engineering

41. This security tool can do content inspection of SFTP communications.

A. WAF

B. DAM

C. XML gateway

D. SSO

42. In order to deploy a set of microservices to clients instead of building one monolithic application, it is best to use a(n) _____ to coordinate client requests.

A. XML gateway

B. API gateway

C. WAF

D. DAM

43. Firewalls can detect attack traffic by using all these methods *except* _____.

A. Known past behavior in the environment

B. Identity of the malicious user

C. Point of origination

D. Signature matching

44. TLS provides _____ and _____ for communications.

A. Privacy, security

B. Security, optimization

C. Privacy, integrity

D. Enhancement, privacy

45. TLS uses a new _____ for each secure connection.

A. Symmetric key

B. Asymmetric key

C. Public-private key pair

D. Inverse comparison

46. A virtual private network is used to protect data in transit by _____.

A. Securing each end of a client-server connection

B. Creating an encrypted tunnel between two endpoints

C. Encrypting databases

D. Restricting key access to only eight parties

47. The process of tokenization can be most likened to _____.

A. Taking a ticket at the sandwich shop and waiting to be called

B. Giving your car to a valet and getting a ticket in return

C. Buying a ticket to see a movie

D. Being issued a ticket by a traffic cop

48. Typically, masking data is a way to _____.

A. Obscure data content while retaining format

B. Obscure data format while retaining content

C. Secure data content by obscuring access credentials

D. Secure data content by obscuring access permissions

49. Sandboxing can often be used for _____.

A. Optimizing the production environment by moving processes that are not frequently used into the sandbox

B. Allowing secure remote access for users who need resources in the cloud environment

C. Running malware for analysis purposes

D. Creating secure subnets of the production environment

50. Sandboxing can often be used for _____.

A. Testing user awareness and training

B. Testing security response capabilities

C. Testing software before putting it into production

D. Testing regulatory response to new configurations and modifications

51. Application virtualization can typically be used for _____.

A. Running an application in a non-native environment

B. Installing updates to a system's OS

C. Preventing escalation of privilege by untrusted users

D. Enhancing performance of systems

52. Application virtualization can typically be used for _____.

A. Denying access to untrusted users

B. Detecting and mitigating DDoS attacks

C. Replacing encryption as a necessary control

D. Running an application on an endpoint without installing it

53. Any organization that complies with ISO 27034 will have a maximum of _____ ONF(s).

A. 0

B. 1

C. 5

D. 25

54. Under ISO 27034, every application within a given organization will have an attendant set of controls assigned to it; the controls for a given application are listed in the _____.

A. ONF

B. ANF

C. TTF

D. FTP

55. Static application security testing (SAST) is usually considered a _____ form of testing.

A. White-box

B. Black-box

C. Gray-box

D. Parched field

56. SAST examines _____.

A. Software outcomes

B. User performance

C. System durability

D. Source code

57. Dynamic application security testing (DAST) is usually considered a _____ form of testing.

A. White-box

B. Black-box

C. Gray-box

D. Parched field

58. DAST checks software functionality in _____.

A. The production environment

B. A runtime state

C. The cloud

D. An IaaS configuration

59. Vulnerability scans are dependent on _____ in order to function.

A. Privileged access

B. Vulnerability signatures

C. Malware libraries

D. Forensic analysis

60. Due to their reliance on vulnerability signatures, vulnerability scanners will not detect _____.

A. User error

B. Improper control selection

C. Cloud vulnerabilities

D. Unknown vulnerabilities

61. Penetration testing is a(n) _____ form of security assessment.

A. Active

B. Comprehensive

C. Total

D. Inexpensive

62. Dynamic software security testing should include _____.

A. Source code review

B. User training

C. Penetration testing

D. Known bad data

63. According to OWASP recommendations, active software security testing should include all of the following *except* _____.

A. Information gathering

B. User surveys

C. Configuration and deployment management testing

D. Identity management testing

64. According to OWASP recommendations, active software security testing should include all of the following *except* _____.

A. Authentication testing

B. Authorization testing

C. Session management testing

D. Privacy review testing

65. According to OWASP recommendations, active software security testing should include all of the following *except* _____.

A. Session initiation testing

B. Input validation testing

C. Testing for error handling

D. Testing for weak cryptography

66. According to OWASP recommendations, active software security testing should include all of the following *except* _____.

A. Business logic testing

B. Client-side testing

C. Intuition testing

D. Information gathering

67. Static software security testing typically uses _____ as a measure of how thorough the testing was.

A. Number of testers

B. Flaws detected

C. Code coverage

D. Malware hits

68. Dynamic software security testing typically uses _____ as a measure of how thorough the testing was.

A. User coverage

B. Code coverage

C. Path coverage

D. Total coverage

69. Software security testing should involve both known good and known bad data in order to simulate both _____ and _____.

A. Managers, users

B. Regulators, users

C. Vendors, users

D. Users, attackers

70. Training programs should be tracked and monitored in order to fulfill both _____ and _____ requirements. Choose the best response.

A. Business, security

B. Regulatory, legal

C. User, managerial

D. Vendor, supplier

71. Training is typically for _____.

A. All personnel

B. Specific personnel

C. Management personnel

D. HR personnel

72. Awareness training is typically for _____.

A. All personnel

B. Specific personnel

C. Management personnel

D. HR personnel

73. Why is cloud security training particularly important for software developers?

A. Software developers are the mainstay of every cloud environment.

B. You can't have a cloud environment without software developers.

C. Security controls cannot be added to software after the fact and must be included from the very first steps of software development.

D. Most modern software developers don't understand how the code underlying the libraries they use actually works.

74. Software developers should receive cloud-specific training that highlights the specific challenges involved with having a production environment that operates in the cloud. One of these challenges is _____.

A. The massive additional hacking threat, especially from foreign sources

B. The prevalent use of encryption in all data life cycle phases

C. Drastic increase of risk due to DDoS attacks

D. Additional regulatory mandates

75. Software developers should receive cloud-specific training that highlights the specific challenges involved with having a production environment that operates in the cloud. One of these challenges is _____.

A. Lack of management oversight

B. Additional workload in creating governance for two environments (the cloud data center and client devices)

C. Increased threat of malware

D. The need for process isolation

76. Which security technique is *most* preferable when creating a limited functionality for customer service personnel to review account data related to sales made to your clientele?

A. Anonymization

B. Masking

C. Encryption

D. Training

77. At which phase of the software development life cycle (SDLC) is user involvement *most* crucial?

A. Define

B. Design

C. Develop

D. Test

78. At which phase of the SDLC should security personnel first be involved?

A. Define

B. Design

C. Develop

D. Test

79. At which phase of the SDLC is it probably *most* useful to involve third-party personnel?

A. Define

B. Design

C. Develop

D. Test

80. In SDLC implementations that include a Secure Operations phase, which of the following security techniques/tools are implemented during that phase?

A. Vulnerability assessments and penetration testing

B. Performance testing and security control validation

C. Requirements fulfillment testing

D. Threat modeling and secure design review

81. A cloud environment that lacks security controls is vulnerable to exploitation, data loss, and interruptions. Conversely, excessive use of security controls _____.

- **A.** Can lead to data breaches
- **B.** Causes electromagnetic interference
- **C.** Will affect quality of service
- **D.** Can cause regulatory noncompliance

82. A cloud environment that lacks security controls is vulnerable to exploitation, data loss, and interruptions. Conversely, excessive use of security controls _____.

- **A.** Can lead to DDoS
- **B.** Allows malware infections
- **C.** Increases the risk of adverse environmental effects
- **D.** Is an unnecessary expense

83. A cloud environment that lacks security controls is vulnerable to exploitation, data loss, and interruptions. Conversely, excessive use of security controls _____.

- **A.** Can lead to customer dissatisfaction
- **B.** Is a risk to health and human safety
- **C.** Brings down the organization's stock price
- **D.** Negates the need for insurance

84. You are the security manager for an online retail sales company with 100 employees and a production environment hosted in a PaaS model with a major cloud provider. Your company policies have allowed for a bring your own device (BYOD) workforce that work equally from the company offices and their own homes or other locations. The policies also dictate which APIs can be utilized to access and manipulate company data and the process for getting an API added to the list of approved programs. You conduct an approved scan of the company data set in the cloud, with the provider's permission. This allows you to catalog all APIs that have accessed and manipulated company data through authorized user accounts in the last month. The scan reveals that 300 different APIs were used by authorized personnel. Of these, 30 had been approved by the company and were on the list. Of the following, what is the *most* reasonable immediate action?

- **A.** Delete accounts of all users who had utilized unapproved APIs to access company data.
- **B.** Suspend access for all users who had utilized unapproved APIs to access company data.
- **C.** Block all unapproved APIs from accessing company data.
- **D.** Notify whomever you report to in the company hierarchy, and suggest bringing the matter to the attention of senior management immediately.

85. You are the security manager for an online retail sales company with 100 employees and a production environment hosted in a PaaS model with a major cloud provider. Your company policies have allowed for a BYOD workforce that work equally from the company offices and their own homes or other locations. The policies also dictate which APIs can be utilized to access and manipulate company data and the process for getting an API added to the list of approved programs. You conduct an approved scan of the company data set in the cloud, with the provider's permission. This allows you to catalog all APIs that have accessed and manipulated company data through authorized user accounts in the last month. The scan reveals that 300 different APIs were used by authorized personnel. Of these, 30 had been approved by the company and were on the list. You've brought the matter to the attention of the CEO, who understands the issue and asks for your recommendation. What is probably the best suggestion?

A. Gather more data about how users are utilizing the APIs and for what purposes.

B. Delete accounts of all users who had utilized unapproved APIs to access company data.

C. Suspend access for all users who had utilized unapproved APIs to access company data.

D. Block all unapproved APIs from accessing company data.

86. You are the security manager for an online retail sales company with 100 employees and a production environment hosted in a PaaS model with a major cloud provider. Your company policies have allowed for a BYOD workforce that work equally from the company offices and their own homes or other locations. The policies also dictate which APIs can be utilized to access and manipulate company data and the process for getting an API added to the list of approved programs. You conduct an approved scan of the company data set in the cloud, with the provider's permission. This allows you to catalog all APIs that have accessed and manipulated company data through authorized user accounts in the last month. The scan reveals that 300 different APIs were used by authorized personnel. Of these, 30 had been approved by the company and were on the list. Upon performing an information-gathering investigation at the behest of the CEO, you determine that these APIs increased productivity 387 percent over the period since they were adopted, at a cost that is negligible compared to shepherding even one API through the company's current approval process. What is your suggestion on how to handle the situation?

A. Retroactively put all the APIs currently in use through the formal approval process, and require that all future APIs users want to install also get approved.

B. Have the CEO waive formal approval processing for all APIs currently in use, granting them approval, but require all future APIs be approved through that process.

C. Punish all employees who have installed or used any of the rogue APIs for violating company policy.

D. Change the policy.

87. You are the security manager for an online retail sales company with 100 employees and a production environment hosted in a PaaS model with a major cloud provider. Your company policies have allowed for a BYOD workforce that work equally from the company offices and their own homes or other locations. The policies also dictate which APIs can be utilized to access and manipulate company data, and the process for getting an API added to the list of approved programs. After finding that users were routinely violating the API approval process but that the result of their violation was a massive increase in productivity and no appreciable increase in company expense, the CEO changed the company policies to allow users to select APIs with which to access and manipulate company data. As a subject matter expert, what should you also recommend to the CEO?

A. Reward the users who committed the infractions, for aiding the company even when they were violating the policy.

B. Replace all the personnel that violated the policy, and have the new personnel use the new policy from their start of hire.

C. Restrict user access to possible APIs.

D. Augment the current set of security controls used by the company in order to offset risks posed by the anticipated use of even more APIs from unknown sources.

88. You are the security manager for an online retail sales company with 100 employees and a production environment hosted in a PaaS model with a major cloud provider. Your company policies have allowed for a BYOD workforce that work equally from the company offices and their own homes or other locations. The policies also allow users to select which APIs they install and use on their own devices in order to access and manipulate company data. Of the following, what is a security control you'd like to implement to offset the risk(s) incurred by this practice?

A. Encrypt all routers between mobile users and the cloud.

B. Use additional anti-malware detection capabilities on both user devices and the environment to which they connect.

C. Implement strong multifactor authentication on all user-owned devices.

D. Employ regular performance monitoring in the cloud environment to ensure that the cloud provider is meeting the SLA targets.

89. You are the security manager for an online retail sales company with 100 employees and a production environment hosted in a PaaS model with a major cloud provider. Your company policies have allowed for a BYOD workforce that work equally from the company offices and their own homes or other locations. The policies also allow users to select which APIs they install and use on their own devices in order to access and manipulate company data. Of the following, what is a security control you'd like to implement to offset the risk(s) incurred by this practice?

A. Regular and widespread integrity checks on sampled data throughout the managed environment

B. More extensive and granular background checks on all employees, particularly new hires

C. Inclusion of references to all applicable regulations in the policy documents

D. Increased enforcement of separation of duties for all workflows

90. You are the security manager for an online retail sales company with 100 employees and a production environment hosted in a PaaS model with a major cloud provider. Your company policies have allowed for a BYOD workforce that work equally from the company offices and their own homes or other locations. The policies also allow users to select which APIs they install and use on their own devices in order to access and manipulate company data. Of the following, what is a security control you'd like to implement to offset the risk(s) incurred by this practice?

A. Enact secure connections between the user devices and the cloud environment using end-to-end encryption.

B. Enact secure connections between the user devices and the cloud environment using link encryption.

C. Employ additional user training.

D. Tunnel all connections with a VPN.

91. Users in your organization have been leveraging APIs for enhancing their productivity in the cloud environment. In order to ensure that you are securing API access to the production environment, you should deploy _____ and _____.

A. SSL and message-level cryptography

B. TLS and message-level cryptography

C. SSL and whole drive encryption

D. TLS and whole drive encryption

92. We implement IAM in order to control access between subjects and objects. What is the ultimate purpose of this effort?

A. Identification. Determine who the specific, individual subjects are.

B. Authentication. Verify and validate any identification assertions.

C. Authorization. Grant subjects permissions to objects once they've been authenticated.

D. Accountability. Be able to reconstruct a narrative of who accessed what.

93. _____ is perhaps the main external factor driving IAM efforts.

A. Regulation

B. Business need

C. The evolving threat landscape

D. Monetary value

94. Whether in a cloud or legacy environment, it is important to implement both _____ and _____ access controls.

A. Internal and managed

B. Provider and customer

C. Physical and logical

D. Administrative and technical

95. Access to specific data sets should be granted by _____.

A. The data subjects

B. The data owners

C. The data processors

D. The data regulators

96. Access should be granted based on all of the following *except* _____.

A. Policy

B. Business needs

C. Performance

D. Acceptable risk

97. Federation allows _____ across organizations.

A. Role replication

B. Encryption

C. Policy

D. Access

98. Federation should be _____ to the users.

A. Hostile

B. Proportional

C. Transparent

D. Expensive

99. A web application firewall (WAF) understands which protocol(s)?

A. All protocols that use the Internet as a medium

B. TLS

C. HTTP

D. FTP

100. Web application firewalls and database activity monitors function at levels _____ and _____ of the OSI model, respectively.

A. 1 and 7

B. 7 and 1

C. 7 and 7

D. 3 and 4

101. What can tokenization be used for?

A. Encryption

B. Compliance with PCI DSS

C. Enhancing the user experience

D. Giving management oversight to e-commerce functions

102. Merchants who accept credit card payments can avoid some of the compliance burden for PCI DSS by outsourcing the tokenization function to _____.

A. A third party

B. The data owner

C. The data subject

D. The PCI Security Standards Council

103. Which of the following is an example of useful and sufficient data masking of the string "CCSP"?

A. XCSP

B. PSCC

C. TtLp

D. 3X91

104. A cloud-based sandbox should *not* be used for _____.

A. Application interoperability testing

B. Processing sensitive data

C. Application security testing

D. Malware analysis

105. Which of the following should occur at each stage of the SDLC?

A. Added functionality

B. Management review

C. Verification and validation

D. Repurposing of any newly developed components

106. Software that includes security elements from the outset of the SDLC process will be _____.

A. More secure in deployment

B. Less secure in deployment

C. More likely to malfunction

D. Less likely to malfunction

107. Software that includes security elements from the outset of the SDLC process will _____.

A. Be less expensive to operate securely in the production environment

B. Be more expensive to operate securely in the production environment

C. Not be interoperable with other software and systems in the production environment

D. Have a greater likelihood of interoperability with other software and systems in the production environment

108. The inclusion of security controls in the software design process is dictated by _____.

A. NIST 800-37

B. AICPA

C. ISO 27034

D. HIPAA

109. Software development should be perceived as _____.

A. Including all members of the organization

B. The paramount goal of the organization

C. The greatest risk to the organization

D. A life cycle

110. Dynamic testing of software is perhaps most useful for _____.

A. Simulating negative test cases

B. Finding errors in the source code

C. Determining the effect of social engineering

D. Penetration tests

111. The employment of users in dynamic software testing should best be augmented by _____.

A. Having the developers review the code

B. Having the developers perform dynamic testing

C. Using automated agents to perform dynamic testing

D. Social engineering

112. Why do developers have an inherent conflict of interest in testing software they've created?

A. They are notoriously bad, as a group, at testing.

B. They work for the same department as the testing personnel.

C. They have a vested interest in having the software perform well.

D. They are never trained on testing procedures.

Chapter

5

CCSP® Official (ISC)2® Practice Tests
By Ben Malisow

Domain 5: Operations

Domain 5 in the CBK both introduces some significant new concepts, such as the physical design of a data center and the attendant standards and guidelines, and restates some material covered in earlier domains, such as multitenancy, resource pooling, and the like.

1. What is the PRIMARY incident response goal?
   - **A.** Remediating the incident
   - **B.** Reverting to the last known good state
   - **C.** Determining the scope of the possible loss
   - **D.** Outcomes dictated by business requirements

2. You are in charge of building a cloud data center. Which raised floor level is sufficient to meet standard requirements?
   - **A.** 10 inches
   - **B.** 8 inches
   - **C.** 18 inches
   - **D.** 2 feet

3. You are in charge of building a cloud data center. What purposes does this raised floor serve?
   - **A.** Allows airflow and increases structural soundness for holding large components
   - **B.** Cold air feed and a place to run wires for the machines
   - **C.** Additional storage for critical components and a dedicated access to a landline
   - **D.** Fire suppression systems and personnel safety

4. You are in charge of building a cloud data center. Which of the following is a useful rack configuration for regulating airflow?
   - **A.** Exhaust fans on racks facing the inlet vents of other racks
   - **B.** Inlet fans on racks facing exhaust fans of other racks
   - **C.** All racks perpendicular to each other
   - **D.** Exhaust fans on racks facing exhaust fans on other racks

5. An event is something that can be measured within the environment. An incident is a(n) _____ event.
   - **A.** Deleterious
   - **B.** Negative

C. Unscheduled

D. Major

6. Which of the following factors would probably *most* affect the design of a cloud data center?

A. Geographic location

B. Functional purpose

C. Cost

D. Intended customers

7. All of the following elements must be considered in the design of a cloud data center *except* _____.

A. External standards, such as ITIL or ISO 27001

B. Physical environment

C. Types of services offered

D. Native language of the majority of customers

8. In designing a data center to meet their own needs and provide optimum revenue/profit, the cloud provider will most likely aim to enhance _____.

A. Functionality

B. Automation of services

C. Aesthetic value

D. Inherent value

9. You are the security officer for a small cloud provider offering public cloud IaaS; your clients are predominantly from the education sector, located in North America. Of the following technology architecture traits, which is probably the one your organization would most likely want to focus on?

A. Reducing mean time to repair (MTTR)

B. Reducing mean time between failure (MTBF)

C. Reducing the recovery time objective (RTO)

D. Automating service enablement

10. What is perhaps the *main* way in which software-defined networking (SDN) solutions facilitate security in the cloud environment?

A. Monitoring outbound traffic

B. Monitoring inbound traffic

C. Segmenting networks

D. Preventing DDoS attacks

11. The logical design of a cloud environment can enhance the security offered in that environment. For instance, in an SaaS cloud, the provider can incorporate _____ capabilities into the application itself.

A. High-speed processing

B. Logging

C. Performance-enhancing

D. Cross-platform functionality

12. You are tasked with managing a cloud data center in Los Angeles; your customers are mostly from the entertainment industry, and you are offering both PaaS and SaaS capabilities. From a physical design standpoint, you are probably going to be most concerned with _____.

A. Offering digital rights management (DRM) capabilities

B. Insuring against seasonal floods

C. Preventing all malware infection potential

D. Ensuring that the racks and utilities can endure an earthquake

13. You are the security manager for a small retail business involved mainly in direct e-commerce transactions with individual customers (members of the public). The bulk of your market is in Asia, but you do fulfill orders globally. Your company has its own data center located within its headquarters building in Hong Kong, but it also uses a public cloud environment for contingency backup and archiving purposes.

Your cloud provider is changing its business model at the end of your contract term, and you have to find a new provider. In choosing providers, which Tier of the Uptime Institute rating system should you be looking for?

A. 1

B. 3

C. 4

D. 8

14. You are the security manager for a small retail business involved mainly in direct e-commerce transactions with individual customers (members of the public). The bulk of your market is in Asia, but you do fulfill orders globally. Your company has its own data center located within its headquarters building in Hong Kong, but it also uses a public cloud environment for contingency backup and archiving purposes.

Your cloud provider is changing its business model at the end of your contract term, and you have to find a new provider. In choosing providers, which of the following functionalities will you consider absolutely essential?

A. DDoS protections

B. Constant data mirroring

C. Encryption

D. Hashing

15. You are the security manager for a small retail business involved mainly in direct e-commerce transactions with individual customers (members of the public). The bulk of your market is in Asia, but you do fulfill orders globally. Your company has its own data center located within its headquarters building in Hong Kong, but it also uses a public cloud environment for contingency backup and archiving purposes.

Which of the following standards are you most likely to adopt?

A. NIST 800-37

B. GDPR

C. ISO 27001

D. SOX

16. You are the security manager for a small retail business involved mainly in direct e-commerce transactions with individual customers (members of the public). The bulk of your market is in Asia, but you do fulfill orders globally. Your company has its own data center located within its headquarters building in Hong Kong, but it also uses a public cloud environment for contingency backup and archiving purposes.

Your company has decided to expand its business to include selling and monitoring life-support equipment for medical providers. What characteristic do you need to ensure is offered by your cloud provider?

A. Full automation of security controls within the cloud data center

B. Tier 4 of the Uptime Institute certifications

C. Global remote access

D. Prevention of ransomware infections

17. When designing a cloud data center, which of the following aspects is *not* necessary to ensure continuity of operations during contingency operations?

A. Access to clean water

B. Broadband data connection

C. Extended battery backup

D. Physical access to the data center

18. You are the security manager for a small surgical center. Your organization is reviewing upgrade options for its current, on-premises data center. In order to best meet your needs, which one of the following options would you recommend to senior management?

A. Building a completely new data center

B. Leasing a data center that is currently owned by another firm

C. Renting private cloud space in a Tier 2 data center

D. Staying with the current data center

19. When building a new data center within an urban environment, which of the following is probably the *most* restrictive aspect?

A. The size of the plot

B. Utility availability

C. Staffing

D. Municipal codes

20. When building a new data center in a rural setting, which of the following is probably the *most* restrictive aspect?

A. Natural disasters

B. Staffing

C. Availability of emergency services

D. Municipal codes

21. All Tiers of the Uptime Institute standards for data centers require _____ hours of on-site generator fuel.

A. 6

B. 10

C. 12

D. 15

22. The American Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE) guidelines for internal environmental conditions within a data center suggest that a temperature setting of _____ degrees (F) would be too high.

A. 93

B. 80

C. 72

D. 32

23. Internal data center conditions that exceed ASHRAE guidelines for humidity could lead to an increase of the potential for all of the following *except* _____.

A. Biological intrusion

B. Electrical shorting

C. Corrosion/oxidation

D. Social engineering

24. Setting thermostat controls by measuring the _____ temperature will result in the highest energy costs.

A. Server inlet

B. Return air

C. Under-floor

D. External ambient

25. Heating, ventilation, and air conditioning (HVAC) systems cool the data center by pushing warm air into _____.

A. The server inlets

B. Underfloor plenums

C. HVAC intakes

D. The outside world

26. It is important to include _____ in the design of underfloor plenums if they are also used for wiring.

A. Mantraps

B. Sequestered channels

C. Heat sinks

D. Tight gaskets

27. Cable management includes all of the following *except* _____.

A. Tagging cables

B. Removing unused/obsolete cables

C. Banding and bundling cables

D. Removing unused machines

28. How often should cable management efforts take place? _____.

A. Annually

B. Continually

C. Quarterly

D. Weekly

29. You are designing a private cloud data center for an insurance underwriter, to be located in a major metropolitan area. Which of the following airflow management schemes is preferable?

A. Hot aisle

B. Cold aisle

C. Either hot aisle or cold aisle

D. Free flow

30. Which of the following factors will probably have the *most* impact on the cost of running your HVAC systems?

A. Whether you choose hot or cold aisle containment

B. The external ambient environment

C. The initial cost of the HVAC systems

D. Proper cable maintenance

31. You are designing a Tier 4 data center for a large hospital. In order to plan for the possibility of losing utility power, in addition to having sufficient generators, you should also plan to locate the data center _____.

A. In an urban setting

B. In a rural environment

C. Near a coast

D. At the border of different counties/regions/states

32. Because most cloud environments rely heavily on virtualization, it is important to lock down or harden the virtualization software, or any software involved in virtualization. Which of the following is *not* an element of hardening software?

A. Removing unused services/libraries

B. Maintaining a strict license catalog

C. Patching and updating as necessary

D. Removing default accounts

33. Which of the following is *not* an aspect of host hardening?

A. Removing all unnecessary software and services

B. Patching and updating as needed

C. Performing more frequent and thorough audits on the host

D. Installing host-based firewall and intrusion detection system (IDS)

34. Which of the following is *not* an element of ongoing configuration maintenance?

A. Penetration tests of guest OSs and hosts

B. Social engineering tests of all users

C. Patch management of guest OSs, hosts, and applications

D. Vulnerability scans of guest OSs and hosts

35. Storage controllers will be used in conjunction with all the following protocols *except* _____.

A. HTTPS

B. iSCSI

C. Fibre Channel

D. Fibre Channel over Ethernet

36. Which of these characteristics of a virtualized network adds risks to the cloud environment?

A. Redundancy

B. Scalability

C. Pay-per-use

D. Self-service

37. Security best practices in a virtualized network environment would include which of the following?

- **A.** Using distinct ports and port groups for various VLANs on a virtual switch rather than running them through the same port
- **B.** Running iSCSI traffic unencrypted in order to have it observed and monitored by NIDS
- **C.** Adding HIDS to all virtual guests
- **D.** Hardening all outward-facing firewalls in order to make them resistant to attack

38. In order to enhance virtual environment isolation and security, a best practice is to _____.

- **A.** Ensure that all virtual switches are not connected to the physical network
- **B.** Ensure that management systems are connected to a different physical network than the production systems
- **C.** Never connect a virtual switch to a physical host
- **D.** Connect physical devices only with virtual switches

39. Which of the following is a risk that stems from a virtualized environment?

- **A.** Live virtual machines in the production environment are moved from one host to another in the clear.
- **B.** Cloud data centers can become a single point of failure.
- **C.** It is difficult to find and contract with multiple utility providers of the same type (electric, water, etc.).
- **D.** Modern SLA demands are stringent and very hard to meet.

40. Which of the following is a risk that stems from a pooled-resources environment?

- **A.** Loss of data to widespread phishing attacks
- **B.** Loss of availability due to widespread DDoS attacks
- **C.** Loss of data to widespread insider threat
- **D.** Loss of data to law enforcement seizure of neighboring assets

41. Modern managed cloud service providers will often use secure keyboard/video/mouse (KVM) devices within their data centers. These devices are extremely expensive compared to their non-secured counterparts. Which of the following is one of the reasons cloud service providers do this?

- **A.** They have plenty of revenue and can afford it.
- **B.** They are gravely concerned with insider threats.
- **C.** Cloud data centers need very few of these devices.
- **D.** Managed cloud providers often manufacture their own devices as well.

42. The ASHRAE guidelines for internal environmental conditions within a data center suggest that a temperature setting of _____ degrees (F) would be too low.

A. 93

B. 80

C. 72

D. 32

43. Modern managed cloud service providers will often use secure KVM devices within their data centers. These devices are extremely expensive compared to their non-secured counterparts. Which of the following is one of the reasons cloud service providers do this?

A. The risk of transferring data from one customer to another is significant.

B. The risk of devices leaving the cloud data center is significant.

C. It makes physical inventories much easier to maintain.

D. Audit purposes.

44. A truly airgapped machine selector will _____.

A. Terminate a connection before creating a new connection

B. Be made of composites and not metal

C. Have total Faraday properties

D. Not be portable

45. Which of the following cloud data center functions do *not* have to be performed on isolated networks?

A. Customer access provision

B. Management system control interface

C. Storage controller access

D. Customer production activities

46. Which of the following is *not* a characteristic of a VLAN?

A. Broadcast packets sent by a machine inside the VLAN will reach all other machines in that VLAN.

B. Broadcast packets sent from outside the VLAN will not reach other machines outside the VLAN.

C. Broadcast packets sent from a machine outside the VLAN will not reach machines inside the VLAN.

D. Broadcast packets sent by a machine inside the VLAN will not reach machines outside the VLAN.

47. In order for communications from inside a VLAN to reach endpoints outside the VLAN, _____.

A. The communications must go through a gateway

B. The traffic must be encrypted

C. A repeater must be used

D. The external endpoint must be in receive mode

48. TLS uses _____ to authenticate a connection and create a shared secret for the duration of the session.

A. SAML 2.0

B. X.509 certificates

C. 802.11X

D. The Diffie-Hellman process

49. Halon is now illegal to use for data center fire suppression. What is the reason it was outlawed?

A. It poses a threat to health and human safety when deployed.

B. It can harm the environment.

C. It does not adequately suppress fires.

D. It causes undue damage to electronic systems.

50. When cloud computing professionals use the term *ping, power, pipe*, which of the following characteristics is *not* being described?

A. Logical connectivity

B. Human interaction

C. Electricity

D. HVAC

51. Which of the following is *not* a goal of a site survey?

A. Threat definition

B. Target identification

C. Penetration testing

D. Facility characteristics

52. Designing system redundancy into a cloud data center allows all the following capabilities *except* _____.

A. Incorporating additional hardware into the production environment

B. Preventing any chance of service interruption

C. Load-sharing/balancing

D. Planned, controlled failover during contingency operations

53. Gaseous fire suppression systems that function by displacing oxygen need to be installed in conjunction with _____.

A. Water cooling

B. Filters

C. Occupant training

D. Failsafe or “last man out” switches

54. What aspect of data center planning occurs first?

A. Logical design

B. Physical design

C. Audit

D. Policy revision

55. Which of the following are *not* examples of personnel controls?

A. Background checks

B. Reference checks

C. Strict access control mechanisms

D. Continuous security training

56. Updating virtual machine management tools will require _____.

A. An infusion of capital

B. An alternate data center

C. Sufficient redundancy

D. Peer review

57. Access control to virtualization management tools should be _____.

A. Rule-based

B. Role-based

C. User-based

D. Discretionary

58. Before deploying a specific brand of virtualization toolset, it is important to configure it according to _____.

A. Industry standards

B. Prevailing law of that jurisdiction

C. Vendor guidance

D. Expert opinion

59. Which of the following is essential for getting full security value from your system baseline?

A. Personnel training

B. Documentation

C. HIDS

D. Encryption

60. Which of the following is essential for getting full security value from your system baseline?

A. Capturing and storing an image of the baseline

B. Keeping a copy of upcoming suggested modifications to the baseline

C. Having the baseline vetted by an objective third party

D. Using a baseline from another industry member so as not to engage in repetitious efforts

61. Patching can be viewed as a configuration modification and therefore subject to the organization's configuration management program and methods. What might also be an aspect of patching in terms of configuration management?

A. Patching doesn't need to be performed as a distinct effort; patching can go through the normal change request process like all other modifications.

B. Any patches suggested/required by vendors to maintain compliance with service contracts must be made immediately, regardless of internal process restrictions.

C. Any patches suggested by third parties should not be considered as they may invalidate service contracts/warranties and negatively affect the organization's security posture.

D. The configuration/change management committee/board might grant blanket approval for patches (at a certain impact level) without need to go through the formal change process.

62. Clustering hosts allows you to do all the following *except* _____.

A. Meet high-availability demands

B. Optimize performance with load balancing

C. Enhance scalability

D. Apply updates/patches/configuration modifications instantly

63. Which of the following is *not* a way to apportion resources in a pooled environment?

A. Reservations

B. Limits

C. Tokens

D. Shares

64. A loosely coupled storage cluster will have performance and capacity limitations based on the _____.

A. Physical backplane connecting it

B. Total number of nodes in the cluster

C. Amount of usage demanded

D. The performance and capacity in each node

65. When putting a system into maintenance mode, it's important to do all of the following *except* _____.

A. Transfer any live virtual guests off the host

B. Turn off logging

C. Lock out the system from accepting any new guests

D. Notify customers if there are any interruptions

66. Typically, a cloud customer seeking stand-alone hosting will expect all of the following *except* _____.

A. More control over governance of the environment

B. Greater granular control of the environment

C. Higher overall security of the environment

D. Lower costs for the environment

67. Methods for achieving "high availability" cloud environments include all of the following *except* _____.

A. Extreme redundancy

B. Multiple system vendors for the same services

C. Explicitly documented BCDR functions in the SLA/contract

D. Failover capability back to the customer's on-premises environment

68. You are in charge of a cloud migration for your organization. You anticipate attack traffic from various sources, each using a variety of both automated and manual intrusion techniques. In order to deter novel attacks used only against your organization, it would be best to employ firewalls that use _____ to detect threats.

A. Attack signatures

B. Behavioral outliers

C. Content filters

D. Biometric templates

69. Firewalls can be included in all the following aspects of a cloud environment *except* _____.

A. The guest OS

B. The cloud data center physical architecture

C. Bandwidth providers used to connect to the cloud

D. Applications used to manipulate data in the cloud

70. A honeypot can be used for all the following purposes *except* _____.

A. Gathering threat intelligence

B. Luring attackers

C. Distracting attackers

D. Delaying attackers

71. Which of the following should honeypots contain?

A. Inward-facing connections

B. Network schematics

C. Production data

D. Detection systems

72. Because all cloud access is remote access, contact between users and the environment should include all of the following *except* _____.

A. Encryption

B. Secure login with complex passwords

C. Once in-all in

D. Logging and audits

73. Most attacks that overcome encryption protections exploit _____.

A. Mathematical principles

B. Misconfigurations

C. Supercomputers

D. Statistical probabilities

74. Administrators and engineers who work for cloud service providers will have a significant amount of control over multiple customer environments and therefore pose a severe risk. Which of the following is *not* a technique used to mitigate this level of increased risk from privileged users in the cloud data center?

A. Two-person control

B. Enhanced logging of administrative activity

C. Granting privileged access only on a temporary basis

D. Assigning permanent administrators to select customer accounts

75. Which of these is a vital action to determine whether the BCDR effort has a chance of being successful?

A. Perform an integrity check on archived data to ensure that the backup process is not corrupting the data.

B. Encrypt all archived data in order to ensure that it can't be exposed while at rest in the long term.

C. Periodically restore from backups.

D. Train all personnel on BCDR actions they should take to preserve health and human safety.

76. Patches do all the following *except* _____.

A. Address newly discovered vulnerabilities

B. Solve cloud interoperability problems

C. Add new features and capabilities to existing systems

D. Address performance issues

77. When applying patches, it is necessary to do all of the following *except* _____.

A. Test the patch in a sandbox that simulates the production environment

B. Put the patch through the formal change management process

C. Be prepared to roll back to the last known good build

D. Inform users of any impact/interruptions

78. Which of the following is a risk associated with automated patching?

- **A.** Users can be leveraged by intruders.
- **B.** A patch might not be applicable to a given environment.
- **C.** Patches can come loaded with malware, in a Trojan horse attack.
- **D.** Automated patching is slow and inefficient.

79. Which of the following is a risk associated with automated patching, especially in the cloud?

- **A.** Snapshot/saved VM images won't take a patch.
- **B.** Remote access disallows patching.
- **C.** Cloud service providers aren't responsible for patching.
- **D.** Patches aren't applied among all cloud data centers.

80. Which of the following is a risk associated with automated patching, especially in the cloud?

- **A.** Patches might interfere with some tenants' production environments.
- **B.** Patches don't work with SaaS service models.
- **C.** Patches don't work with private cloud builds.
- **D.** Vendors don't issue patches to cloud providers.

81. Which of the following is a risk associated with manual patching, especially in the cloud?

- **A.** It can happen too quickly.
- **B.** Vendors only release patches that work with their proprietary automated tools.
- **C.** It's not scalable.
- **D.** Users can be tricked into installing malware that looks like a patch.

82. Which of the following is a risk associated with manual patching especially in the cloud?

- **A.** No notice before the impact is realized
- **B.** Lack of applicability to the environment
- **C.** Patches may or may not address the vulnerability they were designed to fix.
- **D.** The possibility for human error

83. You are the security manager for an organization that uses the cloud for its production environment. According to your contract with the cloud provider, your organization is responsible for patching. A new patch is issued by one of your vendors. You decide not to apply it immediately, for fear of interoperability problems. What additional risk are you accepting?

- **A.** The cloud provider will suspend your access for violating its terms of service.
- **B.** The cloud provider may sue your organization for breach of contract.

C. Your organization is subject to the vulnerability the patch addresses.

D. Your end clients will no longer trust your organization, and this will hurt your revenue flow.

84. You are the security manager for an organization that uses the cloud for its production environment. According to your contract with the cloud provider, your organization is responsible for patching. A new patch is issued by one of your vendors. You decide not to apply it immediately, for fear of interoperability problems. Who might impose penalties on your organization for this decision if the vulnerability is exploited?

A. The cloud provider

B. Regulators

C. Your end clients

D. Your ISP

85. Which of the following aspects of a cloud environment is *most* likely to add risk to the patch management process?

A. Variations in user training/familiarity with the cloud

B. A cloud services contract that specifies which parties are responsible for which aspects of patching

C. VMs located physically in one location but operating in different time zones

D. The prevalence of attacker activity at the time the patch is applied

86. Which type of web application monitoring most closely measures actual activity?

A. Synthetic performance monitoring

B. Real-user monitoring (RUM)

C. Security information and event management (SIEM)

D. Database application monitor (DAM)

87. When utilizing real-user monitoring (RUM) for web application activity analysis, which of the following do you need to take into account?

A. False positives

B. Attacker baseline actions

C. Privacy concerns

D. Sandboxed environments

88. Synthetic performance monitoring may be preferable to real user monitoring (RUM) because _____.

A. It costs less.

B. It is a more accurate depiction of user behavior.

C. It is more comprehensive.

D. It can take place in the cloud.

89. You are the security manager for an organization with a cloud-based production environment. You are tasked with setting up the event monitoring and logging systems. In your jurisdiction, private entities are allowed to monitor all activity involving their systems, without exception. Which of the following best describes a logging motif you would recommend?

A. Logging every event, at all levels of granularity, including continual screen shots, keystroke logging, and browser history

B. Sufficient logging to reconstruct a narrative of events at some later date

C. Only logging data related to incidents after they have occurred

D. Logging specific data sets recommended by industry standards and guidelines

90. Who should be performing log review?

A. Only certified, trained log review professionals with a great deal of experience with the logging tool

B. The internal audit body

C. External audit providers

D. Someone with knowledge of the operation and a security background

91. Which of these subsystems is probably *most* important for acquiring useful log information?

A. Fan

B. RAM

C. Clock

D. UPS

92. A SIEM (security information and event management) system does *not* eliminate the need for human participation in _____.

A. Log collection

B. Responding to alerts

C. Mathematical normalization of different logs

D. Detecting and alerts

93. Log data should be protected _____.

A. One level below the sensitivity level of the systems from which it was collected

B. At least at the same sensitivity level as the systems from which it was collected

C. With encryption in transit, at rest, and in use

D. According to NIST guidelines

94. Risk is usually viewed with consideration for all the following elements *except* _____.

A. Impact that could occur if a given circumstance is realized

B. The likelihood/probability a circumstance will occur

C. In the context of specific threats to an organization

D. According to risks recently realized by other organizations in the same industry

95. Risk management entails evaluating all of the following *except* _____.

A. Threats

B. Vulnerabilities

C. Countermeasures

D. Customers

96. Impact resulting from risk being realized is often measured in terms of _____.

A. Amount of data lost

B. Money

C. Amount of property lost

D. Number of people affected

97. You are the security officer for a small nonprofit organization. You are tasked with performing a risk assessment for your organization; you have one month to complete it. The IT personnel you work with have been with the organization for many years and have built the systems and infrastructure from the ground up. They have little training and experience in the field of risk. Which type of risk assessment would you choose to conduct?

A. Quantitative

B. Qualitative

C. Pro forma

D. Informal

98. Which of the following is *most* useful in determining the single loss expectancy (SLE) of an asset?

A. The frequency with which you expect that type of loss to occur

B. The dollar value of the asset

C. The sensitivity of the asset

D. The size and scope of the asset

99. Which of the following will likely *best* help you predict the annualized rate of occurrence (ARO) of a specific loss?

A. Threat intelligence data

B. Historical data

C. Vulnerability scans

D. Aggregation analysis

100. Which of the following has the *most* effect on exposure factor (EF)?

A. The type of threat vector

B. The source location of the attack

C. The target of the attack

D. The jurisdiction where the attack takes place

101. You are a consultant, performing an external security review on a large manufacturing firm. You determine that its newest assembly plant, which cost $24 million, could be completely destroyed by a fire but that a fire suppression system could effectively protect the plant. The fire suppression system costs $15 million. An insurance policy that would cover the full replacement cost of the plant costs $1 million per month. What is the annual rate of occurrence (ARO) in this scenario?

A. 12

B. $24 million

C. 1

D. $10 million

102. You are a consultant performing an external security review on a large manufacturing firm. You determine that its newest assembly plant, which cost $24 million, could be completely destroyed by a fire but that a fire suppression system could effectively protect the plant. The fire suppression system costs $15 million. An insurance policy that would cover the full replacement cost of the plant costs $1 million per month. What would you recommend?

A. Accept the risk of fire, and save money by not spending anything on controls/countermeasures.

B. Get the fire suppression system.

C. Get the insurance policy.

D. It is impossible to decide from this information.

103. You are a consultant performing an external security review on a large manufacturing firm. You determine that its newest assembly plant, which cost $24 million, could be completely destroyed by a fire but that a fire suppression system could effectively protect the plant. The fire suppression system costs $15 million. An insurance policy that would cover the full replacement cost of the plant costs $1 million per month. In order to establish the true annualized loss expectancy (ALE), you would need all of the following information *except* _____.

A. The amount of revenue generated by the plant

B. The rate at which the plant generates revenue

C. The length of time it would take to rebuild the plant

D. The amount of product the plant creates

104. You are a consultant performing an external security review on a large manufacturing firm. You determine that its newest assembly plant, which cost $24 million, could be completely destroyed by a fire but that a fire suppression system could effectively protect the plant. The fire suppression system costs $15 million. An insurance policy that would cover the full replacement cost of the plant costs $1 million per month. The plant generates $2 million of revenue each month. The time to rebuild the plant at the current location is six months. What should you recommend?

A. Accept the risk of fire, and save money by not spending anything on controls/countermeasures.

B. Get the fire suppression system.

C. Get the insurance policy.

D. It is impossible to decide from this information.

105. Risk mitigation must *always* also entail which other method of addressing risk?

A. Risk acceptance

B. Risk avoidance

C. Risk transfer

D. Risk attenuation

106. Which of the following poses a secondary risk?

A. Fire exit signs

B. Oxygen-displacing fire suppression

C. Automated fire detection systems

D. Fail-safe fire egress paths

107. Which of the following is *not* true about risk mitigation?

A. A given control/countermeasure should never cost more than the impact of the risk it mitigates.

B. Risk cannot be reduced to zero.

C. The end state of risk mitigation is risk at a tolerable level.

D. Risk mitigation is always the best means to address risk.

108. Which of the following is *not* true about risk mitigation?

A. The cost of the control/countermeasure per year is simple: the overall cost (of acquisition, implementation, and maintenance) divided by life span, in years.

B. Ignoring risk is not risk mitigation; ignoring risk is risk acceptance.

C. The cost of mitigation can be compared against the cost of a control/countermeasure to determine the optimum course of action.

D. Risk is fluid, so all risk assessments are pointless.

109. Which comes first?

A. Accreditation

B. Operation

C. Maintenance

D. Certification

110. The NIST Risk Management Framework (RMF) is required for federal agencies in the United States. Which of the following is *not* a characteristic of the RMF?

A. Automation of controls wherever possible

B. Focuses on continual improvement and near real-time risk management

C. Is based on cost metrics and perceived threats

D. Links risk management at the process level to risk management at the managerial level

111. Symmetric encryption involves _____.

A. Two key pairs, mathematically related

B. Unknown parties, sharing information

C. Signed certificates

D. A shared secret

112. Symmetric encryption involves _____.

A. The Diffie-Hellman key exchange

B. Passing keys out of band

C. Mathematically related key pairs

D. A one-way mathematical algorithm for validating messages

Chapter

6

CCSP® Official (ISC)2® Practice Tests
By Ben Malisow

Domain 6: Legal and Compliance

Domain 6 contains material that some candidates find the most awkward and confusing: the legal and policy elements. It also delves into compliance and how cloud customers ensure that their organization is fulfilling its regulatory requirements. It is weighted much less than the previous domains on the exam, though, so this chapter is much shorter than the ones you've seen so far.

1. The current American Institute of Certified Public Accountants (AICPA) standard was created in reaction to what US federal law?
   - **A.** Gramm-Leach-Bliley Act (GLBA)
   - **B.** Sarbanes-Oxley Act (SOX)
   - **C.** Family Education Rights and Privacy Act (FERPA)
   - **D.** Payment Card Industry Data Security Standards (PCI DSS)

2. The Cloud Security Alliance (CSA) Security, Trust, and Assurance Registry (STAR) program has _____ tiers.
   - **A.** Two
   - **B.** Three
   - **C.** Four
   - **D.** Eight

3. The Cloud Security Alliance (CSA) Security, Trust, and Assurance Registry (STAR) program's tier of self-assessment is which of the following?
   - **A.** Tier 1
   - **B.** Tier 2
   - **C.** Tier 5
   - **D.** Tier 8

4. Alice and Bob want to use the Internet to communicate privately. They each have their own asymmetric key pairs and want to use them to create temporary symmetric keys for each connection/session. Which of the following will enable them to do this?
   - **A.** Remote Authentication Dial-In User Service (RADIUS)
   - **B.** Rivest-Shamir-Adelman (RSA) encryption
   - **C.** Diffie-Hellman exchange
   - **D.** Terminal Access Controller Access-Control System (TACACS)

5. Which one of the following technologies allows you to utilize your existing TCP/IP network to manage data storage elements using IP traffic?
   - **A.** Internet Small Computer System Interface (iSCSI)
   - **B.** Fibre Channel
   - **C.** Fibre Channel over Ethernet (FCoE)
   - **D.** Storage area networks (SAN)

6. When implementing iSCSI in your network environment, what is one of the possible problems you can accidentally create?
   - **A.** Neutrality
   - **B.** Oversubscription
   - **C.** Dampening
   - **D.** Surges

7. Which of the following is *not* a way of managing risk?
   - **A.** Mitigation
   - **B.** Acceptance
   - **C.** Avoidance
   - **D.** Streamlining

8. The Organization for Economic Cooperation and Development (OECD) is a multinational entity that creates nonbinding policy suggestions for its member countries. The OECD has published recommendations for privacy laws. One of the characteristics the OECD suggests that privacy laws include is the _____.
   - **A.** Amorphous curtailment principle
   - **B.** Collection limitation principle
   - **C.** State-based incorporation principle
   - **D.** Hard-copy instantiation principle

9. The Organization for Economic Cooperation and Development (OECD) is a multinational entity that creates nonbinding policy suggestions for its member countries. The OECD has published recommendations for privacy laws. One of the characteristics the OECD suggests that privacy laws include is the _____.
   - **A.** Data quality principle
   - **B.** Transformative neologism principle
   - **C.** Encryption matrices principle
   - **D.** Restful state principle

10. The Organization for Economic Cooperation and Development (OECD) is a multinational entity that creates nonbinding policy suggestions for its member countries. The OECD has published recommendations for privacy laws. One of the characteristics the OECD suggests that privacy laws include is the _____.

A. Archipelago enhancement principle

B. Solidity restoration principle

C. Netherworking substrate principle

D. Purpose specification principle

11. The Organization for Economic Cooperation and Development (OECD) is a multinational entity that creates nonbinding policy suggestions for its member countries. The OECD has published recommendations for privacy laws. One of the characteristics the OECD suggests that privacy laws include is the _____.

A. Use limitation principle

B. Erstwhile substitution principle

C. Flatline cohesion principle

D. Airstream fluidity principle

12. The Organization for Economic Cooperation and Development (OECD) is a multinational entity that creates nonbinding policy suggestions for its member countries. The OECD has published recommendations for privacy laws. One of the characteristics the OECD suggests that privacy laws include is the _____.

A. Transient data principle

B. Security safeguards principle

C. Longtrack resiliency principle

D. Arbitrary insulation principle

13. The Organization for Economic Cooperation and Development (OECD) is a multinational entity that creates nonbinding policy suggestions for its member countries. The OECD has published recommendations for privacy laws. One of the characteristics the OECD suggests that privacy laws include is the _____.

A. Volcanic principle

B. Inherency principle

C. Repository principle

D. Openness principle

14. The Organization for Economic Cooperation and Development (OECD) is a multinational entity that creates non-binding policy suggestions for its member countries. The OECD has published recommendations for privacy laws. The OECD privacy principles influenced which lawmaking body and are readily apparent in the law(s) it created?

A. US Congress

B. European Union

C. Politburo

D. International Standards Organization (ISO)

15. Which of the following is *not* a way in which an entity located outside the EU can be allowed to gather/process privacy data belonging to EU citizens?

A. Be located in a country with a nationwide law that complies with the EU laws

B. Appeal to the EU High Court for permission

C. Create binding contractual language that complies with the EU laws

D. Join the Safe Harbor/Privacy Shield program in its own country

16. The Privacy Shield program is _____.

A. Voluntary for non-EU entities

B. Mandatory for all EU entities

C. Mandatory for all non-EU entities

D. Voluntary for all EU entities

17. Which of the following countries does *not* have a federal privacy law that complies with the EU Data Directive/Privacy Regulation?

A. Canada

B. United States

C. Switzerland

D. Japan

18. Which of the following countries does *not* have a federal privacy law that complies with the EU Data Directive/Privacy Regulation?

A. Argentina

B. Israel

C. Australia

D. Brazil

19. In the United States, who manages the Safe Harbor/Privacy Shield program for voluntary compliance with EU data privacy laws?

A. Department of State

B. Department of Interior

C. Department of Trade

D. Department of Commerce

20. You're a sophomore at a small, private medical teaching college in the midwestern United States; you make your tuition payments directly from your bank account via a debit card. Which of the following laws and standards will *not* be applicable to you, your personal data, or the data you work with as a student?

A. Sarbanes-Oxley Act (SOX)

B. Health Information Portability and Accountability Act (HIPAA)

C. Payment Card Industry Data Security Standards (PCI DSS)

D. Family Educational Rights and Privacy Act (FERPA)

21. Which of the following is one of the advantages of using automation in configuration management?

A. Reduce potential for human error

B. Streamline novelty aspects

C. Avoid time zone conflicts

D. Hard-copy tracking

22. Which of the following is one of the advantages of using automation in configuration management?

A. Development

B. Uniformity

C. Texture

D. Distinguishing applicability

23. Which of the following is one of the advantages of using automation in configuration management?

A. Speed

B. Knowledge

C. Customization

D. Price

24. Under European Union law, what is the difference between a directive and a regulation?

A. A directive is enforced by the member states; a regulation is enforced by an international body

B. A directive is put in place by statute; a regulation is put in place by precedent

C. A directive is for local laws; a regulation is for laws dealing with matters outside the EU

D. A directive allows member states to create their own laws; a regulation is applied to all member states

25. You work for a European government agency providing tax counseling services to taxpayers. On your website home page, you include a banner with the following text: "As a visitor to this website, I agree that any information I disclose to the Tax Counseling Agency can be used for any and all purposes under the General Data Protection Regulation (GDPR)." This is followed by a button that says, "I Agree": users have to click the button, or they are taken to a page that says, "Goodbye. Thank you for visiting the Tax Counseling Agency, and have a nice day."

This method of collecting personal information is _____.

A. Illegal under the GDPR because it is electronic and needs to be in hard copy

B. Legal under the GDPR

C. Illegal under the GDPR because it doesn't allow service if the visitor refuses

D. Illegal under the GDPR because it doesn't ask the nationality of the visitor

26. Administrative penalties for violating the General Data Protection Regulation (GDPR) can range up to _____.

A. US$100,000

B. 500,000 euros

C. 20,000,000 euros

D. 1,000,000 euros

27. The EU General Data Protection Regulation (GDPR) addresses performance by _____.

A. Data subjects

B. Data controllers

C. Data processors

D. Data controllers and processors

28. You are the security manager for a mid-sized nonprofit organization. Your organization has decided to use an SaaS public cloud provider for its production environment. A service contract audit reveals that while your organization has budgeted for 76 user accounts, there are currently 89 active user accounts. Your organization is paying the contract price, plus a per-account fee for every account over the contracted number.

This is an example of costs incurred by _____.

A. Data breach

B. Shadow IT

C. Intrusions

D. Insider threat

29. An audit against the _____ will demonstrate that an organization has a holistic, comprehensive security program.

A. SAS 70 standard

B. SSAE 16 standard

C. SOC 2, Type 2 report matrix

D. ISO 27001 certification requirements

30. An audit against the _____ reporting mechanism will demonstrate that an organization has an adequate security control design.

A. SOC 1

B. SOC 2, Type 1

C. SOC 2, Type 2

D. SOC 3

31. A(n) _____ includes reviewing the organization's current position/performance as revealed by an audit against a given standard.

A. SOC report

B. Gap analysis

C. Audit scoping statement

D. Federal guideline

32. An audit against the _____ will demonstrate that an organization has adequate security controls to meet its ISO 27001 requirements.

A. SAS 70 standard

B. SSAE 16 standard

C. ISO 27002 certification criteria

D. NIST SP 800-53

33. An audit scoping statement might include constraints on all of the following aspects of an environment *except* _____.

A. Time spent in the production space

B. Business areas/topics to be reviewed

C. Automated audit tools allowed in the environment

D. Not reviewing illicit activities that may be discovered

34. An audit scoping statement might include constraints on all of the following aspects of an environment *except* _____.

A. Limitation on destructive techniques

B. Prohibition of all personnel interviews

C. Prohibition on access to the production environment

D. Mandate of particular time zone review

35. You are the IT director for a European cloud service provider. In reviewing possible certifications your company may want to acquire for its data centers, you consider the possibilities of the CSA STAR program, the Uptime Institute's Tier certification motif, and _____.

A. NIST Risk Management Framework (SP 800-37)

B. FedRAMP

C. ISO 27034

D. EuroCloud Star Audit program

36. Who should perform the gap analysis following an audit?

A. The security office

B. The auditor

C. A department other than the audit target

D. An external audit body, other than the original auditor

37. An IT security audit is designed to reveal all of the following *except* _____.

A. Financial fraud

B. Malfunctioning controls

C. Inadequate controls

D. Failure to meet target standards/guidelines

38. What was first international privacy standard specifically for cloud providers?

A. NIST SP 800-37

B. PIPEDA

C. PCI

D. ISO 27018

39. Choose the entity that has *not* published a privacy principle document that includes recognizing privacy as a general human right including: a subject's right to access any of their own privacy data; limitations on the use of privacy data collected from subjects; and security measures for privacy data.

A. OECD

B. AICPA

C. The EU parliament

D. United States Congress

40. The field of digital forensics does *not* include the practice of securely _____ data.

A. Collecting

B. Creating

C. Analyzing

D. Presenting

41. Which of the following is a legal practice of removing a suspect from one jurisdiction to another in order for the suspect to face prosecution for violating laws in the latter.

A. Applicable law

B. Judgements

C. Criminal law

D. Extradition

42. In which court must the defendant be determined to have acted in a certain fashion according to the preponderance of the evidence?

A. Civil court

B. Criminal court

C. Religious court

D. Tribal court

43. You are the security manager for a retail sales company that uses an SaaS public cloud service. One of your employees uploads sensitive information they were *not* authorized to put in the cloud. An administrator working for the cloud provider accesses that information and uses it for an illegal purpose, benefiting the administrator and causing harm to your organization.

After you perform all the incident-response activity related to the situation, your organization determines that the price of the damage was US$125,000. Your organization sues the cloud provider, and the jury determines that your organization shares in the blame (liability) for the loss because it was your employee performing an unauthorized action that created the situation.

If the jury determines that 25 percent of the evidence shows that the situation was your organization's fault and 75 percent of the evidence shows that the situation was the cloud provider's fault, what is the likely outcome?

A. Your organization owes the cloud provider $31,250

B. The cloud provider owes your organization $93,750

C. Neither side owes the other party anything

D. The cloud provider owes your organization $125,000

44. You are the security manager for a small American tech firm and investigate an incident. Upon analysis, you determine that one of your employees was stealing proprietary material and selling it to a competitor. You inform law enforcement and turn over the forensic data with which you determined the source and nature of the theft.

The prosecutor can use the material you delivered because of _____.

A. The doctrine of plain view

B. The silver platter doctrine

C. The General Data Protection Regulation

D. The Federal Information System Management Act

45. You are the security director for an online retailer in Belgium. In February 2019, an audit reveals that your company may have been responsible for exposing personal data belonging to some of your customers over the previous month.

Which law is applicable in this instance?

A. Belgian law

B. The General Data Protection Act

C. NIST SP 800-53

D. The Federal Information Systems Management Act

46. You are the security manager for a software company that uses PaaS in a public cloud service. Your company's general counsel informs you that they have received a letter from a former employee who is filing a lawsuit against your company.

You should immediately issue a(n) _____ to all personnel and offices within your company.

A. Litigation hold notice

B. Audit scoping letter

C. Stop loss memo

D. Memorandum of agreement

47. You are the security manager for a software company that uses PaaS in a public cloud service. Your company's general counsel informs you that they have received a letter from a former employee who is filing a lawsuit against your company.

If you do not take proper steps to retain, capture, and deliver pertinent data to the person making the request (or their attorney), the company could be facing legal problems with _____ as well as the lawsuit.

A. Spoliation

B. Fraud

C. Jurisdiction

D. Recompositing

48. You are the CIO for an IT hardware manufacturer. Your company uses cloud-based SaaS services, including email. You receive a legal request for data pertinent to a case. Your e-discovery efforts will largely be dependent on _____.

A. The cloud provider

B. Regulators

C. The cloud customer

D. Internal IT personnel

49. You work for a company that operates a production environment in the cloud. Another company using the same cloud provider is under investigation by law enforcement for racketeering. Your company should be concerned about this because of the cloud characteristic of _____.

A. Virtualization

B. Pooled resources

C. Elasticity

D. Automated self-service

50. You are the security manager for a software company that uses PaaS in a public cloud service. Your company's general counsel informs you that they have received a letter from a former employee who is filing a lawsuit against your company.

What is one of the common practices used in your industry that will have to be halted until the resolution of the case?

A. Versioning

B. Patching

C. Threat modeling

D. Secure destruction

51. Your company receives a litigation hold notice from a customer that is suing you for harm caused by one of your products. You are using a managed cloud service for your production environment. You determine that the data requested by the litigant is vast and is going be very difficult to review for pertinence to the case.

The senior executive at your firm who is making decisions about this case suggests handing over all data the company has archived for the time frame related to the case, whether or not it may be pertinent, in order to both allow the litigant to find the pertinent data and reduce the costs your company would incur if it performed the reform.

What should be your response to the executive?

A. This is an excellent idea: it fulfills the company's legal requirements and reduces the overall costs of the litigation

B. This is a good idea: it may alleviate some of the costs associated with the court case

C. This is a bad idea: the company might not realize the full cost savings that it expects

D. This is a horrible idea: it could lead to extensive unauthorized disclosure and additional lawsuits

52. Your company receives a litigation hold notice from a customer that is suing you for harm caused by one of your products. You are using a managed cloud service for your production environment. You determine that the data requested by the litigant is vast and is going be very difficult to review for pertinence to the case.

Which security control mechanism may also be useful in the e-discovery effort?

A. Trained and aware personnel

B. An egress monitoring solution (DLP)

C. A digital rights management (DRM) solution

D. A multifactor authentication implementation

53. When targeting a cloud customer, a court grants an order allowing a law enforcement entity to seize _____.

A. Electronic data

B. Hardware

C. Electronic data and the hardware on which it resides

D. Only data extracted from hardware

54. Your company is defending itself during a civil trial for a breach of contract case. Personnel from your IT department have performed forensic analysis on event logs that reflect the circumstances related to the case.

In order for your personnel to present the evidence they collected during forensic analysis as expert witnesses, you should ensure that _____

A. Their testimony is scripted, and they do not deviate from the script

B. They only present evidence that is favorable to your side of the case

C. They are trained and certified in the tools they used

D. They are paid for their time while they are appearing in the courtroom

55. In some jurisdictions, it is mandatory that personnel conducting forensic analysis collection or analysis have a proper _____.

A. Training credential

B. License

C. Background check

D. Approved toolset

56. You run an IT security incident response team. When seizing and analyzing data for forensic purposes, your investigative personnel modify the data from its original content. For courtroom evidentiary purpose, this makes the data _____.

A. Inadmissible

B. Less believable, if the changes aren't documented

C. Harder to control

D. Easily refutable

57. You are the security manager for a small investing firm. After a heated debate regarding security control implementation, one of your employees strikes another employee with a keyboard. The local media hear about the incident and broadcast/publish stories about it under the title "Computer-related attack."

What may be the result of this situation?

A. A criminal trial

B. A civil case

C. Both criminal and civil proceedings

D. Federal racketeering charges

58. You are the security manager for a small investing firm. After a heated debate regarding security control implementation, one of your employees strikes another employee with a keyboard. The local media hear about the incident and broadcast/publish stories about it under the title "Computer-related attack."

In this circumstance, who would likely be prosecuted?

A. Your organization

B. The attacker

C. The victim

D. You, as the manager of both parties

59. _____ is the legal concept that describes the actions and processes a cloud customer uses to ensure that a reasonable level of protection is applied to the data in their control.

A. Due care

B. Due diligence

C. Liability

D. Reciprocity

60. Which of the following aspects of virtualization make the technology useful for evidence collection?

A. Hypervisors

B. Pooled resources

C. Snapshotting

D. Live migration

61. Which of the following practices can enhance both operational capabilities and forensic readiness?

A. Highly trained forensic personnel

B. Regular full backups

C. A highly secure data archive

D. Homomorphic encryption

62. Which of the following practices can enhance both operational capabilities and configuration management efforts?

A. Regular backups

B. Constant uptime

C. Multifactor authentication

D. File hashes

63. Which of the following is probably the *most* volatile form of data that might serve a forensic purpose?

A. Virtual instance RAM

B. Hardware RAM

C. Hypervisor logs

D. Drive storage

64. You are the security representative of a small company doing business through a cloud provider. Your company comes under investigation by law enforcement for possible wrongdoing. In performing e-discovery activity so as to comply with a court order, the cloud provider offers to ship a piece of hardware, a storage drive, from their data center to you for inspection/analysis.

What should probably be your response?

A. Yes. You want it because it gives you the most granular and comprehensive view of the pertinent data

B. Yes. You want to be able to inspect it before law enforcement has the opportunity to review it

C. No. You don't want the liability of possibly disclosing someone else's privacy data

D. No. You don't want the liability of possibly damaging someone else's property

65. The Reporting phase of forensic investigation usually involves presenting findings to _____.

A. Senior management

B. Regulators

C. The court

D. Stakeholders

66. When presenting forensic evidence in court as testimony, you should include, if at all possible _____.

A. Your personal opinion

B. A clear, concise view of your side of the case

C. Alternative explanations

D. Historical examples that have bearing on the circumstances of the current case

67. When collecting digital evidence for forensic purposes, it is important to compare the integrity value for any copied material against _____.

A. The original

B. The backup

C. Another copy

D. The industry standard

68. Who should be responsible for ensuring the state, security, and control of all evidence, from the time it's collected until it is presented in court?

A. The data controller

B. The evidence custodian

C. The security manager

D. The IT director

69. When accessing an electronic storage file for forensic purposes, it is a best practice to use _____.

A. Gloves

B. A trusted computing base

C. Sysadmin access

D. A write-blocker

70. Which of the following should *not* be true about any tests performed during forensic analysis?

A. tests should be repeatable by opposing attorneys

B. tests should be standard to the forensics industry

C. tests should be performed by trained, certified professionals

D. tests should be tailored and customized for specific purposes

71. Which of the following pieces of data is considered PII in the EU but *not* in the US?

A. Name

B. Home address

C. Birth date

D. Mobile phone number

72. The Safe Harbor program, while no longer used, allowed US companies to collect and process privacy information about EU citizens. The program was included in which law?

A. FISMA

B. The EU Data Directive

C. HIPAA

D. Sarbanes-Oxley Act

73. You are the security manager for a US-based company that has branches abroad, including offices in Germany, Italy, and Brazil. If your company wants to process EU citizen PII data, one of the options is to use standard contractual clauses (also known as model contracts, or binding rules).

If you choose this option, your company will have to get approval from _____.

A. Privacy officials in Italy

B. Privacy officials in Brazil

C. Privacy officials in Italy and Germany

D. Privacy officials in Italy, Germany, and Brazil

74. Using cloud storage is considered _____ under most privacy frameworks and laws.

A. Illegal

B. Data collection

C. Opt-in

D. Processing

75. Which US federal government entity was the regulator for the American Safe Harbor program and is now in charge of administering the Privacy Shield program?

A. State Department

B. Privacy Protection Office

C. Federal Trade Commission

D. Department of Health and Human Services

76. In deciding which cloud provider to use, one of the characteristics you may want to determine about the provider is their level of professionalism. Which of the following tools could be used to determine the thoroughness, detail, and repeatability of the processes and procedures offered by a cloud provider?

A. The CSA-STAR certification program

B. The Risk Management Framework (RMF)

C. The Capability Maturity Model (CMM)

D. The Eurocloud Star Audit Certification

77. SOC 2 reports were intended to be _____.

A. Released to the public

B. Only technical assessments

C. Retained for internal use

D. Nonbinding

78. In order to receive a SOC 2 Type 2 report from a potential provider, the provider may require you to perform/provide a(n) _____.

A. Security deposit

B. Non-disclosure agreement (NDA)

C. CSA STAR certification application

D. Act of fealty

79. The Generally Accepted Privacy Principles described by the AICPA are very similar to the privacy principles described by _____.

A. The OECD and EU Data Directive/GDPR

B. NIST and ENISA

C. HIPAA and GLBA

D. The FTC and the US State Department

80. The Payment Card Industry Data Security Standard (PCI DSS) requires that all merchants who want to process credit card transactions be compliant with a wide variety of security control requirements.

Approximately how many controls are listed in the PCI DSS?

A. Around a dozen

B. About 20

C. About 100

D. Over 200

81. The Payment Card Industry Data Security Standard (PCI DSS) requires that all merchants who want to process credit card transactions be compliant with a wide variety of security control requirements.

Merchants are assigned different tier levels under PCI DSS, based on _____.

A. Availability

B. Redundancy

C. Location of their corporate headquarters

D. Number of transactions per year

82. The Payment Card Industry Data Security Standard (PCI DSS) requires that all merchants who want to process credit card transaction be compliant with a wide variety of security control requirements.

The different merchant tier requirements will dictate _____

A. Different types of audits each must conduct

B. Different amounts of audits each must conduct

C. Different control sets based on tier level

D. Different cost of controls based on tier level

83. Under the Common Criteria, the EAL rating should describe the thoroughness of the design and testing of the security controls in a(n) _____.

A. Product

B. Risk management framework

C. Environment

D. Given infrastructure

84. _____ are required to use *only* cryptographic modules that are compliant with FIPS 140-2.

A. Americans

B. Cloud providers

C. IaaS providers

D. US federal agencies

85. In performing vendor management and selection, one of the questions you, as the potential cloud customer, might ask is, "Does it seem as if this vendor is subject to any pending acquisitions or mergers?" In gathering data to answer this question, what are you are trying to avoid?

A. Vendor lockout

B. Due care

C. Third-party dependencies

D. Regulatory oversight

86. US federal entities are required to only use cloud data centers within the borders of the United States. Which law/standard/requirement mandates this?

A. FISMA

B. FedRAMP

C. OECD

D. GDPR

87. The CSA STAR program includes a level of certification for cloud providers that acquire third-party assessments of their environment and controls. Which STAR level is this?

A. 1

B. 2

C. 3

D. 4

88. _____ is the legal concept whereby a cloud customer is held to a reasonable expectation for providing security of its users' and clients' privacy data.

A. Due care

B. Due diligence

C. Liability

D. Reciprocity

89. Under EU law, a cloud customer who gives sensitive data to a cloud provider is still legally responsible for the damages resulting from a data breach caused by the provider; the EU would say that it is the cloud customer's fault for choosing the wrong provider. This is an example of insufficient _____.

A. Proof

B. Evidence

C. Due diligence

D. Application of reasonableness

90. Which of the following is *not* an enforceable governmental request?

A. Warrant

B. Subpoena

C. Court order

D. Affidavit

Chapter 7

CCSP® Official (ISC)2® Practice Tests
By Ben Malisow

Practice Exam 1

1. You work for a government research facility. Your organization often shares data with other government research organizations. You would like to create a single sign-on experience across the organizations, where users at each organization can sign in with the user ID/authentication issued by that organization, then access research data in all the other organizations. Instead of replicating the data stores of each organization at every other organization (which is one way of accomplishing this goal), you instead want every user to have access to each organization's specific storage resources.

   What is the term for this kind of arrangement?

   A. Public-key infrastructure (PKI)

   B. Portability

   C. Federation

   D. Repudiation

2. You work for a government research facility. Your organization often shares data with other government research organizations. You would like to create a single sign-on experience across the organizations, where users at each organization can sign in with the user ID/authentication issued by that organization, then access research data in all the other organizations. Instead of replicating the data stores of each organization at every other organization (which is one way of accomplishing this goal), you instead want every user to have access to each organization's specific storage resources.

   You want to connect your organization to 13 other organizations. You consider using the cross-certification model but then decide against it. What is the *most* likely reason for declining that option?

   A. It is impossible to trust more than two organizations.

   B. If you work for the government, the maximum parties allowed to share data is five.

   C. Trying to maintain currency in reviewing and approving the security governance and configurations of that many entities would create an overwhelming task.

   D. Data shared among that many entities loses its inherent value.

3. You work for a government research facility. Your organization often shares data with other government research organizations. You would like to create a single sign-on experience across the organizations, where users at each organization can sign in with the user ID/authentication issued by that organization, then access research data in all the other organizations. Instead of replicating the data stores of each organization at every other organization (which is one way of accomplishing this goal), you instead want every user to have access to each organization's specific storage resources.

   In order to pass the user IDs and authenticating credentials of each user among the organizations, what protocol/language/motif will you *most* likely utilize?

   A. Representational State Transfer (REST)

   B. Security Assertion Markup Language (SAML)

   C. Simple Object Access Protocol (SOAP)

   D. Hypertext Markup Language (HTML)

4. You work for a government research facility. Your organization often shares data with other government research organizations. You would like to create a single sign-on experience across the organizations, where users at each organization can sign in with the user ID/authentication issued by that organization, then access research data in all the other organizations. Instead of replicating the data stores of each organization at every other organization (which is one way of accomplishing this goal), you instead want every user to have access to each organization's specific storage resources.

   If you don't use cross-certification, what other model can you implement for this purpose?

   A. Third-party identity broker

   B. Cloud reseller

   C. Intractable nuanced variance

   D. Mandatory access control (MAC)

5. You work for a government research facility. Your organization often shares data with other government research organizations. You would like to create a single sign-on experience across the organizations, where users at each organization can sign in with the user ID/authentication issued by that organization, then access research data in all the other organizations. Instead of replicating the data stores of each organization at every other organization (which is one way of accomplishing this goal), you instead want every user to have access to each organization's specific storage resources.

   If you are in the United States, one of the standards you should adhere to is _____.

   A. NIST 800-53

   B. Payment Card Industry (PCI)

   C. ISO 27014

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

6. You work for a government research facility. Your organization often shares data with other government research organizations. You would like to create a single sign-on experience across the organizations, where users at each organization can sign in with the user ID/authentication issued by that organization, then access research data in all the other organizations. Instead of replicating the data stores of each organization at every other organization (which is one way of accomplishing this goal), you instead want every user to have access to each organization's specific storage resources.

   If you are in Canada, one of the standards you will have to adhere to is _____.

   A. FIPS 140-2

   B. PIPEDA

   C. HIPAA

   D. EFTA

7. You are the security policy lead for your organization, which is considering migrating from your on-premises, legacy environment into the cloud. You are reviewing the Cloud Security Alliance Cloud Controls Matrix (CSA CCM) as a tool for your organization.

   Which of the following benefits will the CSA CCM offer your organization?

   A. Simplifying regulatory compliance

   B. Collecting multiple data streams from your log files

   C. Ensuring that the baseline configuration is applied to all systems

   D. Enforcing contract terms between your organization and the cloud provider

8. You are the security policy lead for your organization, which is considering migrating from your on-premises, legacy environment into the cloud. You are reviewing the Cloud Security Alliance Cloud Controls Matrix (CSA CCM) as a tool for your organization.

   Which of the following regulatory frameworks is *not* covered by the CCM?

   A. ISACA's Control Objectives for Information and Related Technologies (COBIT)

   B. Canada's PIPEDA privacy law

   C. The ALL-TRUST framework from the environmental industry

   D. The US Federal Risk and Authorization Management Program (FedRAMP)

9. You are the security policy lead for your organization, which is considering migrating from your on-premises, legacy environment into the cloud. You are reviewing the Cloud Security Alliance Cloud Controls Matrix (CSA CCM) as a tool for your organization.

   Which tool, also available from the CSA, can be used in conjunction with the CCM to aid you in selecting/applying the proper controls to meet your organization's regulatory needs?

   A. The Consensus Assessments Initiative Questionnaire (CAIQ)

   B. The Open Web Application Security Project (OWASP) Top Ten

   C. The Critical Security Controls (CSC) list

   D. NIST FIPS 140-2

10. You are the security policy lead for your organization, which is considering migrating from your on-premises, legacy environment into the cloud. You are reviewing the Cloud Security Alliance Cloud Controls Matrix (CSA CCM) as a tool for your organization.

    What is probably the *best* benefit offered by the CCM?

    A. The low cost of the tool

    B. Allowing your organization to leverage existing controls across multiple frameworks so as not to duplicate effort

    C. Simplicity of control selection from the list of approved choices

    D. Ease of implementation by choosing controls from the list of qualified vendors

11. You are the IT security subject matter expert for a hobbyist collective that researches and archives old music.

Your collective is set up in such a way that the members own various pieces of the network themselves, pool resources and data, and communicate and share files via the Internet. This is an example of what cloud model?

A. Hydrogenous

B. Private

C. Public

D. Community

12. You are the IT security subject matter expert for a hobbyist collective that researches and archives old music.

Your collective wants to create a single sign-on experience for all members of the collective, where assurance and trust in the various members are created by having each member review all the others' policies, governance, procedures, and controls before allowing them to participate. This is an example of what kind of arrangement?

A. SAML

B. Cross-certification federation

C. Third-party certification federation

D. JSON

13. You are the IT security subject matter expert for a hobbyist collective that researches and archives old music.

Your collective exchanges music files in two forms: images of written sheet music, and electronic copies of recordings. Both of these are protected by what intellectual property legal construct?

A. Trademark

B. Copyright

C. Patent

D. Trade secret

14. You are the IT security subject matter expert for a hobbyist collective that researches and archives old music.

If you create a federated identity management structure for all the participants in the collective using a third-party certification model, who would be the federated service provider(s) in that structure?

A. The third party

B. A cloud access security broker (CASB)

C. The various members of the collective

D. The cloud provider

15. You are the IT security subject matter expert for a hobbyist collective that researches and archives old music.

You receive a Digital Millennium Copyright Act (DMCA) takedown notice from someone who claims that your collective is hosting music that does not belong to you. You are fairly certain the complaint is not applicable, and that the material in question does not belong to anyone else. What should you do in order to comply with the law?

A. Take the material down, do an investigation, and then repost the material if the claim turns out to be unfounded.

B. Leave the material up, do an investigation, and post the results of the investigation alongside the material itself once the investigation is complete.

C. Ignore the complaint.

D. Leave the material up until such time as the complainant delivers an enforceable governmental request, such as a warrant or subpoena.

16. You are the IT security subject matter expert for a hobbyist collective that researches and archives old music.

You receive a Digital Millennium Copyright Act (DMCA) takedown notice from someone who claims that your collective is hosting music that does not belong to you. Upon investigation, you determine that the material in question is the sheet music for a concerto written in 1872. What should you do in order to comply with the law?

A. Contact the current owners of the copyright in order to get proper permissions to host and exchange the data.

B. Nothing. The material is so old it is in the public domain, and you have as much right as anyone else to use it in any way you see fit.

C. Apply for a new copyright based on the new usage of the material.

D. Offer to pay the complainant for the usage of the material.

17. Bob is designing a data center to support his organization, a financial services firm.

What Uptime Institute Tier rating should Bob try to attain in order to meet his company's needs without adding extraneous costs?

A. 1

B. 2

C. 3

D. 4

18. Bob is designing a data center to support his organization, a financial services firm.

Bob's data center will definitely have to be approved by regulators using a framework under which law?

A. Health Industry Portability and Accountability Act

B. Payment Card Industry

C. Gramm-Leach-Bliley

D. Sarbanes-Oxley Act

19. Bob is designing a data center to support his organization, a financial services firm.

Which of the following actions would *best* enhance Bob's efforts to create redundancy and resiliency in the data center?

A. Ensure that all entrances are secured with biometric-based locks.

B. Purchase UPSs from different vendors.

C. Include financial background checks in all personnel reviews for administrators.

D. Make sure all raised floors have at least 24 inches of clearance.

20. Bob is designing a data center to support his organization, a financial services firm.

How long should the UPS provide power to the systems in the data center?

A. Twelve hours

B. An hour

C. Ten minutes

D. Long enough to perform graceful shutdown of the data center systems

21. You are the IT security manager for a video game software development company.

For your company, minimizing security flaws in the delivered product is *probably* a _____.

A. Functional requirement

B. Nonfunctional requirement

C. Regulatory issue

D. Third-party function

22. You are the IT security manager for a video game software development company.

In order to test your products for security defects and performance issues, your firm decides to utilize a small team of game testers recruited from a public pool of interested gamers who apply for a chance to take part. This is an example of _____.

A. Static testing

B. Dynamic testing

C. Code review

D. Open-source review

23. You are the IT security manager for a video game software development company.

In order to test your products for security defects and performance issues, your firm decides to utilize a small team of game testers recruited from a public pool of interested gamers who apply for a chance to take part. In order to optimize this situation, the test will need to involve _____.

A. Management oversight

B. A database administrator

C. A trained moderator

D. Members of the security team

24. You are the IT security manager for a video game software development company.

In order to test your products for security defects and performance issues, your firm decides to utilize a small team of game testers recruited from a public pool of interested gamers who apply for a chance to take part. Of the parties listed, who should *most* be excluded from the test?

A. Management

B. Security personnel

C. Billing department representatives

D. The game developers

25. You are the IT security manager for a video game software development company.

In order to test your products for security defects and performance issues, your firm decides to utilize a small team of game testers recruited from a public pool of interested gamers who apply for a chance to take part. It is absolutely crucial to include _____ as part of this process.

A. Managerial oversight

B. Signed nondisclosure agreements

C. Health benefits

D. The programming team

26. You are the IT security manager for a video game software development company.

Which of the following is *most* likely to be your primary concern on a daily basis?

A. Health and human safety

B. Security flaws in your products

C. Security flaws in your organization

D. Regulatory compliance

27. You are the IT security manager for a video game software development company.

Which type of intellectual property protection will your company likely rely upon for legally enforcing your rights?

A. Trademark

B. Patent

C. Copyright

D. Trade secret

28. You are the IT security manager for a video game software development company.

In order to test your products for security defects and performance issues, your firm decides to utilize a small team of game testers recruited from a public pool of interested gamers who apply for a chance to take part. Gamers are notorious for attempting to perform actions that were never anticipated or intended by the programmers. Results gathered from this activity are _____.

A. Useless

B. Harmful

C. Desirable

D. Illegal

29. You are the IT security manager for a video game software development company.

In order to test your products for security defects and performance issues, your firm decides to utilize a small team of game testers recruited from a public pool of interested gamers who apply for a chance to take part. Gamers are notorious for attempting to perform actions that were never anticipated or intended by the programmers. Trying to replicate this phenomenon in a testbed environment with internal testing mechanisms is called _____.

A. Source code review

B. Deep testing

C. Fuzz testing

D. White-box testing

30. You are the IT security manager for a video game software development company.

Your development team hired an external game development lab to work on part of the game engine. A few weeks before the initial release of your game, the company that owns the lab publishes a strikingly similar game, with many of the features and elements that appear in your work. Which of the following methods could be used to determine if your ownership rights were violated?

A. Physical surveillance of their property and personnel

B. Communications tapping of their offices

C. Code signing

D. Subverting insiders

31. You are the IT security manager for a video game software development company.

Your development team hired an external game development lab to work on part of the game engine. A few weeks before the initial release of your game, the company that owns the lab publishes a strikingly similar game, with many of the features and elements that appear in your work. Which of the following legal methods are you likely able to exercise to defend your rights?

A. Criminal prosecution

B. Public hearings

C. Civil court

D. Arrest and detention

32. You are the IT security manager for a video game software development company.

In order to test the functionality of online multiplayer game content, your testing team wants to use a cloud service independent from the internal production environment. You suggest that a(n) _____ service model will best meet this requirement.

A. IaaS

B. PaaS

C. SaaS

D. TaaS

33. You are the IT security manager for a video game software development company.

In order to test the functionality of online multiplayer game content, your testing team wants to use a cloud service independent from the internal production environment. You remind them that it is absolutely crucial that they perform _____ before including any sample player or billing data.

A. Vulnerability scans

B. Intrusion detection

C. Masking

D. Malware scans

34. Which of the following is not an essential element defining cloud computing?

A. Broad network access

B. Metered service

C. Offsite storage

D. On-demand self-service

35. Which of the following is not an essential element defining cloud computing?

A. Rapid elasticity

B. Pooled resources

C. On-demand self-service

D. Immediate customer support

36. In what cloud computing service model is the customer responsible for installing and maintaining the operating system?

A. IaaS

B. PaaS

C. SaaS

D. QaaS

37. Your company is considering migrating its production environment to the cloud. In reviewing the proposed contract, you notice that it includes a clause that requires an additional fee, equal to six monthly payments (equal to half the term of the contract) for ending the contract at any point prior to the scheduled date.

This is best described as an example of _____.

A. Favorable contract terms

B. Strong negotiation

C. IaaS

D. Vendor lock-in

38. There are two general types of smoke detectors. Which type uses a small portion of radioactive material?

A. Photoelectric

B. Ionization

C. Electron pulse

D. Integral field

39. You are the privacy data officer for a large hospital and trauma center. You are called on to give your opinion of the hospital's plans to migrate all IT functions to a cloud service.

Which of the following Uptime Institute Tier level ratings would you insist be included for any data center offered by potential providers?

A. 1

B. 2

C. 3

D. 4

40. What is the *most* important factor when considering the lowest temperature setting within a data center?

A. System performance

B. Health and human safety

C. Risk of fire

D. Regulatory issues

41. Storage controllers will typically be involved with each of the following storage protocols *except* _____.

A. iSCSI

B. RAID

C. Fibre Channel

D. Fibre Channel over Ethernet

42. When using a storage protocol that involves a storage controller, it is very important that the controller be configured in accordance with _____.

A. Internal guidance

B. Industry standards

C. Vendor guidance

D. Regulatory dictates

43. What is the importance of adhering to vendor guidance in configuration settings?

A. Conforming with federal law

B. Demonstrating due diligence

C. Staying one step ahead of aggressors

D. Maintaining customer satisfaction

44. Which of the following is a true statement about the virtualization management toolset?

A. It can be regarded as something public facing.

B. It must be on a distinct, isolated management network (VLAN).

C. It connects physically to the specific storage area allocated to a given customer.

D. The responsibility for securely installing and updating it falls on the customer.

45. In order to ensure proper _____ in a secure cloud network environment, it is important to consider the use of DNSSEC, IPSec, and TLS.

A. Isolation

B. Motif

C. Multitenancy

D. Signal modulation

46. DNSSEC provides all of the following *except* _____.

A. Payload encryption

B. Origin authority

C. Data integrity

D. Authenticated denial of existence

47. All of the following are activities that should be performed when capturing and maintaining an accurate, secure system baseline *except* _____.

A. Update the OS baseline image according to a schedule interval, to include any necessary security patches and configuration modifications

B. Start with a clean installation (hardware or virtual) of the desired OS

C. Include only the default account credentials, nothing customized

D. Halt or remove all unnecessary services

48. All of the following are activities that should be performed when capturing and maintaining an accurate, secure system baseline *except* _____.

A. Remove all nonessential programs from the baseline image

B. Exclude the target system you intend to baseline from any scheduled updates/patching used in production systems

C. Include the baseline image in the asset inventory/configuration management database

D. Configure the host OS according to the baseline requirements

49. All of the following are activities that should be performed when capturing and maintaining an accurate, secure system baseline, *except* _____.

A. Audit the baseline to ensure that all configuration items have been included and applied correctly

B. Impose the baseline throughout the environment

C. Capture an image of the baseline system for future reference/versioning/rollback purposes

D. Document all baseline configuration elements and versioning data

50. You are the IT director for a small contracting firm. Your company is considering migrating to a cloud production environment.

Which service model would *best* fit your needs if you wanted an option that reduced the chance of vendor lock-in but also did not require the highest degree of administration by your own personnel?

A. IaaS

B. PaaS

C. SaaS

D. TanstaafL

51. You are the data manager for a retail company; you anticipate a much higher volume of sales activity in the final quarter of each calendar year than the other quarters. In order to handle these increased transactions, and to accommodate the temporary sales personnel you will hire for only that time period, you consider augmenting your internal, on-premises production environment with a cloud capability for a specific duration, and will return to operating fully on-premises after the period of increased activity.

This is an example of _____.

A. Cloud framing

B. Cloud enhancement

C. Cloud fragility

D. Cloud bursting

52. You are the data manager for a retail company; you anticipate a much higher volume of sales activity in the final quarter of each calendar year than the other quarters. In order to handle these increased transactions, and to accommodate the temporary sales personnel you will hire for only that time period, you consider augmenting your internal, on-premises production environment with a cloud capability for a specific duration, and will return to operating fully on-premises after the period of increased activity.

Which facet of cloud computing is *most* important for making this possible?

A. Broad network access

B. Rapid elasticity

C. Metered service

D. Resource pooling

53. You are the data manager for a retail company; you anticipate a much higher volume of sales activity in the final quarter of each calendar year than the other quarters. In order to handle these increased transactions, and to accommodate the temporary sales personnel you will hire for only that time period, you consider augmenting your internal, on-premises production environment with a cloud capability for a specific duration, and will return to operating fully on-premises after the period of increased activity.

Which deployment model best describes this type of arrangement?

A. Private cloud

B. Community cloud

C. Public cloud

D. Hybrid cloud

54. You are the security manager for a research and development firm. Your company does contract work for a number of highly sensitive industries, including aerospace and pharmaceuticals.

Your company's senior management is considering cloud migration and wants an option that is highly secure but still offers some of the flexibility and reduced overhead of the cloud. Which of the following deployment models do you recommend?

A. Private cloud

B. Community cloud

C. Public cloud

D. Hybrid cloud

55. You are the IT director for a small engineering services company. During the last year, one of your managing partners left the firm, and you lost several large customers, creating a cash flow problem. The remaining partners are looking to use a cloud environment as a means of drastically and quickly cutting costs, migrating away from the expense of operating an internal network.

Which cloud deployment model would you suggest to best meet their needs?

A. Private cloud

B. Community cloud

C. Public cloud

D. Hybrid cloud

56. You run an online club for antique piano enthusiasts. In order to better share photo files and other data online, you want to establish a cloud-based environment where all your members can connect their own devices and files to each other, at their discretion. You do not want to centralize payment for such services as ISP connectivity, and you want to leave that up to the members.

Which cloud deployment model would best suit your needs?

A. Private cloud

B. Community cloud

C. Public cloud

D. Hybrid cloud

57. Full isolation of user activity, processes, and virtual network segments in a cloud environment is incredibly important because of risks due to _____.

A. DDoS

B. Unencrypted packets

C. Multitenancy

D. Insider threat

58. You are the security manager for a small European appliance rental company. The senior management of your company is considering cloud migration for the production environment, which handles marketing, billing, and logistics.

Which cloud deployment model should you be *most* likely to recommend?

A. Private cloud

B. Community cloud

C. Public cloud

D. Hybrid cloud

59. You are the security manager for a data analysis company. Your senior management is considering a cloud migration in order to use the greater capabilities of a cloud provider to perform calculations and computations. Your company wants to ensure that neither the contractual nor the technical setup of the cloud service will affect your data sets in any way so that you are not locked-in to a single provider.

Which of the following criteria will probably be *most* crucial for your choice of cloud providers?

A. Portability

B. Interoperability

C. Resiliency

D. Governance

60. Migrating to a cloud environment will reduce an organization's dependence on _____.

A. Capital expenditures for IT

B. Operational expenditures for IT

C. Data-driven workflows

D. Customer satisfaction

61. Firewalls, DLP and DRM solutions, and security information and event management (SIEM) products are all examples of _____ controls.

A. Technical

B. Administrative

C. Physical

D. Competing

62. Fiber-optic lines are considered part of layer _____ of the OSI model.

A. 1

B. 3

C. 5

D. 7

63. It is probably fair to assume that SaaS functions take place at layer _____ of the OSI model.

A. 1

B. 3

C. 5

D. 7

64. Because of the nature of the cloud, all access is remote access. One of the preferred technologies employed for secure remote access is _____.

A. VPN

B. HTML

C. DEED

D. DNS

65. You are the security manager for a small retailer engaged in e-commerce. A large part of your sales is transacted through the use of credit/debit cards.

You have determined that the costs of maintaining an encrypted storage capability in order to meet compliance requirements is cost-prohibitive. What other technology can you use instead, to meet the needs?

A. Obfuscation

B. Masking

C. Tokenization

D. Hashing

66. Which of the following mechanisms *cannot* be used by a data loss prevention (DLP) solution to sort data?

A. Labels

B. Metadata

C. Content strings

D. Inverse signifiers

67. You are the security manager for an online marketing company. Your company has recently migrated to a cloud production environment and has deployed a number of new cloud-based protection mechanisms offered by both third parties and the cloud provider, including DLP and SIEM solutions.

After one week of operation, your security team reports an inordinate amount of time responding to potential incidents that have turned out to only be false-positive reports. Management is concerned that the cloud migration was a bad idea and that it is too costly in terms of misspent security efforts. What do you recommend?

A. Change the control set so that you use only security products not offered by the cloud provider.

B. Change the control set so that you use only security products only offered by the cloud provider.

C. Wait three weeks before making a final decision.

D. Move back to an on-premises environment as soon as possible to avoid additional wasted funds/effort.

68. In a cloud context, who determines the risk appetite of your organization?

A. The cloud provider

B. Your ISP

C. Federal regulators

D. Senior management

69. You are the security manager for a small application development company. Your company is considering the use of the cloud for software testing purposes.

Which of the following traits of cloud functionality is probably the *most* crucial, in terms of deciding which cloud provider you will choose?

A. Portability

B. Interoperability

C. Resiliency

D. Governance

70. You are the security manager for a small application development company. Your company is considering the use of the cloud for software testing purposes.

Which cloud service model is *most* likely to suit your needs?

A. IaaS

B. PaaS

C. SaaS

D. LaaS

71. ISO 31000 is most similar to which of the following regulations/standards/guidelines/frameworks?

A. NIST 800-37

B. COBIT

C. ITIL

D. GDPR

72. Which of the following entities publishes a cloud-centric set of risk-benefit recommendations that includes a "Top 8" list of security risks an organization might face during a cloud migration, based on likelihood and impact?

A. NIST

B. ISO

C. ENISA

D. PCI

73. Which standards body depends heavily on contributions and input from its open membership base?

A. NIST

B. ISO

C. ICANN

D. CSA

74. In regard to most privacy guidance, the data subject is _____.

A. The individual described by the privacy data

B. The entity that collects or creates the privacy data

C. The entity that utilizes privacy data on behalf of the controller

D. The entity that regulates privacy data

75. In regard to most privacy guidance, the data controller is _____.

A. The individual described by the privacy data

B. The entity that collects or creates the privacy data

C. The entity that utilizes privacy data on behalf of the controller

D. The entity that regulates privacy data

76. In regard to most privacy guidance, the data processor is _____.

A. The individual described by the privacy data

B. The entity that collects or creates the privacy data

C. The entity that utilizes privacy data on behalf of the controller

D. The entity that regulates privacy data

77. In most privacy-regulation situations, which entity is *most* responsible for deciding how a particular privacy-related data set will be used or processed?

A. The data subject

B. The data controller

C. The data steward

D. The data custodian

78. In most privacy-regulation situations, which entity is *most* responsible for the day-to-day maintenance and security of a privacy-related data set?

A. The data subject

B. The data controller

C. The data steward

D. The data custodian

79. You are the compliance officer for a medical device manufacturing firm. Your company maintains a cloud-based list of patients currently fitted with your devices, for long-term care and quality assurance purposes. The list is maintained in a database that cross-references details about the hardware and some billing data.

In this situation, who is likely to be considered the data custodian, under many privacy regulations/laws?

A. You (the compliance officer)

B. The cloud provider's network security team

C. Your company

D. The database administrator

80. Which of the following is probably *least* suited for inclusion in the service-level agreement (SLA) between a cloud customer and cloud provider?

A. Bandwidth

B. Jurisdiction

C. Storage space

D. Availability

81. Which of the following items, included in the contract between a cloud customer and cloud provider, can best aid in reducing vendor lock-in?

A. Data format type and structure

B. Availability

C. Storage space

D. List of available OSs

82. Which of the following contract terms *most* incentivizes the cloud provider to meet the requirements listed in the SLA?

A. Regulatory oversight

B. Financial penalties

C. Performance details

D. Desire to maintain customer satisfaction

83. Which of the following contract terms *most* incentivizes the cloud customer to meet the requirements listed in the contract?

A. Financial penalties

B. Regulatory oversight

C. Suspension of service

D. Media attention

84. Which of the following is *not* a reason for conducting audits?

A. Regulatory compliance

B. User satisfaction

C. Determination of service quality

D. Security assurance

85. Which of the following is a tool that can be used to perform security control audits?

A. FIPS 140-2

B. The GDPR

C. ISO 27001

D. The CSA CCM

86. Which of the following dictates the requirements for US federal agencies operating in a cloud environment?

A. ISO 27002

B. NIST SP 800-37

C. ENISA

D. FedRAMP

87. Which of the following common aspects of cloud computing can aid in audit efforts?

A. Scalability

B. Virtualization

C. Multitenancy

D. Metered self-service

88. Which of the following does *not* typically represent a means for enhanced authentication?

A. Challenge questions

B. Variable keystrokes

C. Out-of-band identity confirmation

D. Dynamic end-user knowledge

89. Which of the following is *not* a common identity federation standard?

A. WS-Federation

B. OpenID

C. OISame

D. SAML

90. Multifactor authentication typically includes two or more of all the following elements *except* _____.

A. What you know

B. Who you know

C. What you are

D. What you have

91. Which of the following aspects of cloud computing can enhance the customer's BC/DR efforts?

A. Multitenancy

B. Pooled resources

C. Virtualization

D. Remote access

92. Which of the following aspects of cloud computing can enhance the customer's BC/DR efforts?

A. Rapid elasticity

B. Online collaboration

C. Support of common regulatory frameworks

D. Attention to customer service

93. Which of the following aspects of cloud computing can enhance the customer's BC/DR efforts?

A. On-demand self-service

B. Pooled resources

C. Virtualization

D. The control plane

94. What functional process can also aid BC/DR efforts?

A. The system development life cycle (SDLC)

B. Data classification

C. Honeypots

D. Identity management

95. Which common security tool can aid in the overall BC/DR process?

A. Honeypots

B. DLP

C. SIEM

D. Firewalls

96. Which of the following aspects of cloud computing can enhance the customer's BC/DR efforts?

A. Geographical separation of data centers

B. Hypervisor security

C. Pooled resources

D. Multitenancy

97. Which of the following is *not* typically utilized as an information source for BC/DR event anticipation?

A. Open-source news

B. Business threat intelligence

C. SIEM solutions

D. Weather monitoring agencies

98. Which of the following aspects of the BC/DR process poses a risk to the organization?

A. Premature return to normal operations

B. Event anticipation information

C. Assigning roles for BC/DR activities

D. Preparing the continuity-of-operations plan

99. Which of the following aspects of the BC/DR process poses a risk to the organization?

A. Threat intelligence gathering

B. Preplacement of response assets

C. Budgeting for disaster

D. Full testing of the plan

100. In container virtualization, unlike standard virtualization, what is *not* included?

A. Hardware emulation

B. OS replication

C. A single kernel

D. The possibility for multiple containers

101. Which of the following is *not* typically a phase in the SDLC?

A. Define

B. Test

C. Develop

D. Sanitization

102. An API gateway can typically offer all of the following capabilities *except* _____.

A. Rate limiting

B. Access control

C. Hardware confirmation

D. Logging

103. Cloud customers in a managed service environment can place all the following types of firewalls *except* _____.

A. Provider operated

B. Host based

C. Third party

D. Hardware

104. The Transport Layer Security (TLS) protocol creates a secure communications channel over public media (such as the Internet).

In a typical TLS session, who initiates the protocol?

A. The server

B. The client

C. The certifying authority

D. The ISP

105. The Transport Layer Security (TLS) protocol creates a secure communications channel over public media (such as the Internet).

In a typical TLS session, what is the *usual* means for establishing trust between the parties?

A. Out-of-band authentication

B. Multifactor authentication

C. PKI certificates

D. Preexisting knowledge of each other

106. The Transport Layer Security (TLS) protocol creates a secure communications channel over public media (such as the Internet).

In a typical TLS session, what form of cryptography is used for the session key?

A. Symmetric key

B. Asymmetric key pairs

C. Hashing

D. One asymmetric key pair

107. DevOps is a form of software development that typically joins the software development team with _____.

A. The production team

B. The testing team

C. The security office

D. Management

108. The Agile Manifesto for software development focuses largely on _____.

A. Secure build

B. Thorough documentation

C. Working prototypes

D. Proper planning

109. When a program's source code is open to review by the public, what is that software called?

A. Freeware

B. Malware

C. Open source

D. Shareware

110. Why is SOAP used for accessing web services instead of DCOM and CORBA?

A. SOAP provides a much more lightweight solution.

B. SOAP replaces binary messaging with XML.

C. SOAP is much more secure.

D. SOAP is newer.

111. How does REST make web service requests?

A. XML

B. SAML

C. URIs

D. TLS

112. REST outputs often take the form of _____.

A. JSON

B. Certificates

C. Database entries

D. WS-Policy

113. "Sensitive data exposure" is often included on the list of the OWASP Top Ten web application vulnerabilities. In addition to programming discipline and technological controls, what other approach is important for attenuating this risk?

A. Physical access control to the facility

B. User training

C. Crafting sophisticated policies

D. Redundant backup power

114. During maintenance mode for a given node in a virtualized environment, which of the following conditions is *not* accurate?

A. Generation of new instances is prevented.

B. Admin access is prevented.

C. Alerting mechanisms are suspended.

D. Events are logged.

115. How are virtual machines moved from active hosts when the host is being put into maintenance mode?

A. As a snapshotted image file

B. In encrypted form

C. As a live instance

D. Via portable media

116. Which of the following is *not* a typical mechanism used by IDS/IPS solutions to detect threats?

A. Signature-based detection

B. Content-based detection

C. Statistical-based detection

D. Heuristic detection

117. When deploying a honeypot/honeynet, it is best to fill it with _____ data.

A. Masked

B. Raw

C. Encrypted

D. Useless

118. The cloud provider should be required to make proof of vulnerability scans available to all of the following *except* _____.

A. Regulators

B. The public

C. Auditors

D. The cloud customer

119. You are the security director for a chain of automotive repair centers across several states. Your company uses a cloud SaaS provider, for business functions that cross several of the locations of your facilities, such as: 1) ordering parts 2) logistics and inventory 3) billing, and 4) marketing.

The manager at one of your newest locations reports that there is a competing car repair company that has a logo that looks almost exactly like the one your company uses. This intellectual property is likely protected as a _____.

A. Copyright

B. Trademark

C. Patent

D. Trade secret

120. You are the security director for a chain of automotive repair centers across several states. Your company uses a cloud SaaS provider, for business functions that cross several of the locations of your facilities, such as: 1) ordering parts 2) logistics and inventory 3) billing, and 4) marketing.

The manager at one of your newest locations reports that there is a competing car repair company that has a logo that looks almost exactly like the one your company uses. This conflict will *most* likely have to be resolved with what legal method?

A. Breach of contract lawsuit

B. Criminal prosecution

C. Civil suit

D. Military tribunal

121. You are the security director for a chain of automotive repair centers across several states. Your company uses a cloud SaaS provider, for business functions that cross several of the locations of your facilities, such as: 1) ordering parts 2) logistics and inventory 3) billing, and 4) marketing.

The manager at one of your newest locations reports that there is a competing car repair company that has a logo that looks almost exactly like the one your company uses. What will *most likely* affect the determination of who has ownership of the logo?

A. Whoever first used the logo

B. The jurisdiction where both businesses are using the logo simultaneously

C. Whoever first applied for legal protection of the logo

D. Whichever entity has the most customers that recognize the logo

122. Which SSAE 16 audit report is simply an attestation of audit results?

A. SOC 1

B. SOC 2, Type 1

C. SOC 2, Type 2

D. SOC 3

123. Which SSAE 16 report is purposefully designed for public release (for instance, to be posted on a company's website)?

A. SOC 1

B. SOC 2, Type 1

C. SOC 2, Type 2

D. SOC 3

124. Which of the following countries has a national privacy law that conforms to EU legislation?

A. The United States

B. Australia

C. Jamaica

D. Honduras

125. Which of the following countries has a national privacy law that conforms to EU legislation?

A. Japan

B. Alaska

C. Belize

D. Madagascar

CCSP® Official (ISC)2® Practice Tests
By Ben Malisow

Chapter

8

Practice Exam 2

1. You are the IT director for an automotive parts supply distribution service; your company wants to operate a production environment in the cloud. In reviewing provider options, management considers an offer from Cloud Services Corp., who has contracts with several cloud providers and data centers and has offered to tailor a package of services for your company's needs. In this case, Cloud Services Corp. is considered a _____.
   - **A.** Cloud provider
   - **B.** Cloud customer
   - **C.** Cloud reseller
   - **D.** Cloud database

2. You are the IT director for an automotive parts supply distribution service; your company wants to operate a production environment in the cloud. Management has expressed a concern that any cloud provider the company chooses will have your company at a disadvantage; that your company will be at great risk because the provider will have your data and operational capability, and that the provider could hold the data "hostage" in order to raise the price of the service dramatically at the end of the contract term. To address management's concerns, you should try to find a cloud offering that places a great deal of emphasis on the _____ trait of cloud computing.
   - **A.** Resource pooling
   - **B.** Scalability
   - **C.** Portability
   - **D.** Metered service

3. You are the IT director for an automotive parts supply distribution service; your company wants to operate a production environment in the cloud. As you consider possible providers, you are careful to check that they each offer the essential traits of cloud computing. These include all of the following *except* _____.
   - **A.** Broad network access
   - **B.** Metered service
   - **C.** On-demand self-service
   - **D.** Automatic anti-malware and intrusion prevention

4. You are the IT director for an automotive parts supply distribution service; your company wants to operate a production environment in the cloud. Your company wants to install its own software solutions in a managed environment to decrease the cost of purchasing and maintaining the hardware of a data center. You should *most* likely be considering a(n) _____ offering.
   - **A.** IaaS
   - **B.** PaaS
   - **C.** SaaS
   - **D.** Hybrid

5. If a company wanted to retain some of its own internal legacy hardware but use the cloud as a means of performing software testing functions, which service and deployment models should it probably use?
   - **A.** PaaS, hybrid
   - **B.** IaaS, private
   - **C.** PaaS, community
   - **D.** SaaS, hybrid

6. A company wants to absolutely minimize their involvement in administration of IT; which combination of cloud service model and deployment should it consider?
   - **A.** IaaS, private
   - **B.** PaaS, private
   - **C.** SaaS, private
   - **D.** SaaS, public

7. During a cost-benefit analysis, your company determines that it spends a disproportionate amount of money on software licensing and administration. Which cloud model may best help your company to reduce these costs?
   - **A.** IaaS
   - **B.** PaaS
   - **C.** SaaS
   - **D.** Hybrid

8. Your company does not have a well-trained, experienced IT staff and is reluctant to spend more money on training personnel (in recent company history, personnel have received training and then immediately quit the company to work for competitors). If senior management considers cloud migration, which deployment model would probably best suit their needs?
   - **A.** Public
   - **B.** Private
   - **C.** Community
   - **D.** Hybrid

9. Your company operates under a high degree of regulatory scrutiny. Senior management wants to migrate to a cloud environment but is concerned that providers will not meet the company's compliance needs. Which deployment model would probably best suit the company's needs?
   - **A.** Public
   - **B.** Private
   - **C.** Community
   - **D.** Hybrid

10. Your company operates in a highly competitive market, with extremely high-value data assets. Senior management wants to migrate to a cloud environment but is concerned that providers will not meet the company's security needs. Which deployment model would probably best suit the company's needs?
    - **A.** Public
    - **B.** Private
    - **C.** Community
    - **D.** Hybrid

11. Your company operates in a highly cooperative market, with a high degree of information sharing between participants. Senior management wants to migrate to a cloud environment but is concerned that providers will not meet the company's collaboration needs. Which deployment model would probably best suit the company's needs?
    - **A.** Public
    - **B.** Private
    - **C.** Community
    - **D.** Hybrid

12. Your company maintains an on-premises data center for daily production activities but wants to use a cloud service to augment this capability during times of increased demand (cloud bursting). Which deployment model would probably best suit the company's needs?
    - **A.** Public
    - **B.** Private
    - **C.** Community
    - **D.** Hybrid

13. A company is considering a cloud migration to a PaaS environment. Which of the following facts might make the company *less* likely to choose the cloud environment?
    - **A.** The company wants to reduce overhead costs.
    - **B.** The company operates proprietary software.
    - **C.** The company hopes to reduce energy costs related to operation of a data center.
    - **D.** The company is seeking to enhance its BCDR capabilities.

14. Which mechanism *best* aids to ensure that the cloud customer receives dependable, consistent performance in the cloud environment?
    - **A.** Audits
    - **B.** The SLA
    - **C.** Regulators
    - **D.** Training

15. What is the business advantage of shifting from capital expenditure in an on-premises environment to the operating expenditures of a cloud environment?

A. Reduces the overall cost

B. Reduces tax exposure

C. Reduces cash flow risks

D. Increases profit

16. A host-based firewall in a virtualized cloud environment might have aspects of all the following types of controls *except* _____.

A. Administrative

B. Deterrent

C. Corrective

D. Preventive

17. A virtual network interface card (NIC) exists at layer _____ of the OSI model.

A. 2

B. 4

C. 6

D. 8

18. Which technology is *most* associated with tunneling?

A. IPSec

B. GRE

C. IaaS

D. XML

19. Secure Shell (SSH) tunneling can include all of the following services *except* _____.

A. Remote log-on

B. Content filtering

C. Port forwarding

D. Command execution

20. Transport Layer Security (TLS) is a session encryption tool that uses _____ encryption to create a _____ session key.

A. Symmetric, symmetric

B. Asymmetric, symmetric

C. Asymmetric, asymmetric

D. Symmetric, asymmetric

21. Which of the following architecture frameworks was designed for service delivery entities, from the perspective of how they serve customers?
    - **A.** SABSA
    - **B.** ITIL
    - **C.** COBIT (Control Objectives for Information and Related Technologies)
    - **D.** TOGAF (The Open Group Architecture Framework)

22. The Cloud Security Alliance (CSA) created the Trusted Cloud Initiative (TCI) to define principles of cloud computing that providers should strive for in order to foster a clear understanding of the cloud marketplace and to enhance that market. Which of the following is not one of the CSA's TCI fundamental principles?
    - **A.** Delegate or federate access control when appropriate.
    - **B.** Ensure the [trusted cloud] architecture is resilient, elastic, and flexible.
    - **C.** Ensure the [trusted cloud] architecture addresses and supports multiple levels of protection.
    - **D.** Provides economical services to all customers, regardless of point of origin.

23. DLP solutions typically involve all of the following aspects *except* _____.
    - **A.** Data discovery
    - **B.** Tokenization
    - **C.** Monitoring
    - **D.** Enforcement

24. A typical DLP tool can enhance the organization's efforts at accomplishing what legal task?
    - **A.** Evidence collection
    - **B.** Delivering testimony
    - **C.** Criminal prosecution
    - **D.** Enforcement of intellectual property rights

25. Which of the following activities can enhance the usefulness and abilities of a DLP solution?
    - **A.** Perform emergency egress training for all personnel.
    - **B.** Require data owners/stewards/custodians to properly classify and label data at time of creation/collection.
    - **C.** Require senior management to participate in all security functions, including initial, recurring, and refresher training.
    - **D.** Display security guidance in a variety of formats, including a web page, banner, posters, and hard-copy material.

26. Data archiving can also provide what production capability?
    - **A.** Enhanced database mechanisms
    - **B.** Near-term data recovery

C. New data-driven business workflows

D. Greater management insight into productivity

27. Data archiving can be required for regulatory compliance, as a legal mandate. What other business function is also often tied to archiving?

A. Marketing

B. BCDR

C. Personnel development

D. Intellectual property protection

28. Which of the following is probably *most* important to include in a data archiving policy?

A. Data format and type

B. Data classification

C. Encryption procedures and standards

D. Data audit and review processes

29. The destruction of a cloud customer's data can be required by all of the following *except* _____.

A. Statute

B. Regulation

C. The cloud provider's policy

D. Contract

30. Which of the following data storage types is most associated with SaaS?

A. Content delivery network (CDN)

B. Databases

C. Volume storage

D. Data warehousing

31. You are the security manager for a bookkeeping firm that is considering moving to a cloud-based production environment. In selecting a cloud provider, your company is reviewing many criteria. One of these is enhancing the company's BCDR capabilities. You want to ensure that the cloud provider you select will allow for migration to an alternate provider in the event of contingencies. The provider you choose should be able to support a migration to an alternate provider within _____.

A. 24 hours

B. 1 hour

C. Your company's recovery time objective (RTO)

D. Your company's recovery point objective (RPO)

32. In which phase of the Cloud Secure Data Life Cycle does data leave the production environment and go into long-term storage?

A. Store

B. Use

C. Share

D. Archive

33. In which phase of the Cloud Secure Data Life Cycle should classifications and labels be assigned to data?

A. Create

B. Store

C. Use

D. Share

34. Which of the following is *not* included in the OWASP Top Ten web application security threats?

A. Injection

B. Cross-site scripting

C. Internal theft

D. Sensitive data exposure

35. Your organization is developing software for wide use by the public. You have decided to test it in a cloud environment, in a PaaS model. Which of the following should be of particular concern to your organization for this situation?

A. Vendor lock-in

B. Backdoors

C. Regulatory compliance

D. High-speed network connectivity

36. Which of the following management risks can make an organization's cloud environment unviable?

A. Insider trading

B. VM sprawl

C. Hostile takeover

D. Improper personnel selection

37. You are the security manager for a company that is considering cloud migration to an IaaS environment. You are assisting your company's IT architects in constructing the environment. Which of the following options do you recommend?

A. Unrestricted public access

B. Use of a Type I hypervisor

C. Use of a Type II hypervisor

D. Enhanced productivity without encryption

38. Your company uses a managed cloud service provider to host the production environment. The provider has notified you, along with several other of the provider's customers, that an engineer working for the provider has been using administrative access to steal sensitive data and has been selling it to your competitors. Some of this sensitive data included personally identifiable information (PII) related to your employees. Your company's general counsel informs you that there are at least three jurisdictions involved that have laws requiring data breach notification for PII. Who has *legal* liability for the costs involved with making the required notifications?

A. The cloud provider

B. Your company

C. The ISP

D. Your regulators

39. Which of the following techniques is *not* recommended for privileged user management?

A. Increased password/phrase complexity

B. More frequent password/phrase changes

C. More detailed background checks

D. Less detailed audit trail

40. You are the security officer for a company operating a production environment in the cloud. Your company's assets have a high degree of sensitivity/value, and your company has decided to retain control/ownership of the encryption key management system. In order to do so, your company will have to have which of the following cloud service/deployment models?

A. Public

B. IaaS

C. Hybrid

D. SaaS

41. Which security principle dictates that encryption key management/storage should be isolated from the data encrypted with those keys?

A. Least privilege

B. Two-person integrity

C. Compartmentalization

D. Separation of duties

42. Which cloud data storage technique involves encrypting a data set, then splitting the data into pieces, splitting the key into pieces, then signing the data pieces and key pieces and distributing them to various cloud storage locations?

A. RAID

B. Secret sharing made short (SSMS)

C. Homomorphic encryption

D. Asymmetric encryption

43. Which theoretical technique would allow encrypted data to be manipulated without decrypting it first?

A. RAID

B. Secret sharing made short (SSMS)

C. Homomorphic encryption

D. Asymmetric encryption

44. Which theoretical technology would allow superposition of physical states to increase both computing capacity and encryption keyspace?

A. All-or-nothing-transform with Reed-Solomon (AONT-RS)

B. Quantum computing

C. Filigree investment

D. Sharding

45. In a virtualized environment, suspended VM instances at rest are subject to increased risk because _____.

A. There is no way to encrypt instances at rest

B. Insider threats are greater for data storage locations than processing locations

C. The instances are saved as image snapshots and highly portable

D. They are unprotected unless multifactor authentication is required

46. In a virtualized cloud environment, the management plane is usually responsible for provisioning virtual machine instances with all of the following resources *except* _____.

A. CPU

B. Memory

C. User interface

D. Permanent storage

47. Which of the following BCDR testing methodologies is least intrusive?

A. Walk-through

B. Simulation

C. Tabletop

D. Full test

48. In order for an organization to determine if its backup solution is adequate for meeting the RPO, what *must* be done?

A. Conduct full backups at least daily.

B. Use a data mirroring solution.

C. Put all backups in the cloud.

D. Practice a restore from backup.

49. Which common characteristic of the cloud data center also serves customer BCDR needs?

A. Multitenancy

B. Virtualization

C. Redundancy

D. Software-defined networking

50. Which phase of the BCDR process can result in a second disaster?

A. Event anticipation

B. Creating BCDR plans and policy

C. Return to normal operations

D. Incident initiation

51. Which process artifact aids the organization in determining the critical assets/functions that need to continue operations during a BCDR contingency?

A. SOC 2, Type 2

B. Business impact analysis (BIA)

C. Qualitative risk analysis report

D. Annual loss expectancy (ALE) calculation

52. In general, a cloud BCDR solution will be _____ than a physical solution.

A. Slower

B. Less expensive

C. Larger

D. More difficult to engineer

53. Which of the following is not a common federation technology?

A. WS-Federation

B. OWASP

C. OpenID

D. OAuth

54. Which of the following is an audit report on the design of an organization's controls?

A. SOC 1

B. SOC 2, Type 1

C. SOC 3

D. SOC 4

55. Which of the following is not usually suitable for inclusion in an SLA for managed cloud services?

A. Service availability

B. Number of users/virtual machines

C. Background checks for provider personnel

D. Amount of cloud storage

56. Which of the following is *not* a typical physical access control mechanism in the cloud data center?

A. Cage locks

B. Video surveillance

C. Rack locks

D. Fire suppression

57. Which of the following cloud environment accounts should only be granted on a temporary basis?

A. Remote users

B. Senior management

C. Internal users

D. External vendors

58. Which of the following attack vectors is new to the cloud environment and was not typically found in an on-premises, legacy environments?

A. DDoS

B. Guest escape

C. Internal threats

D. Inadvertent disclosure

59. Which of the following is a file server that provides data access to multiple, heterogeneous machines/users on the network?

A. Storage area network (SAN)

B. Network-attached storage (NAS)

C. Hardware security module (HSM)

D. Content delivery network (CDN)

60. You are the security manager for a retail company that is considering cloud migration to a public, SaaS solution both for your current internal production environment (an on-premises data center) and host your e-commerce presence. Which of the following is a new concern you should bring up to senior management for them to consider before the migration?

A. Regulatory compliance for your credit card processing transactions

B. Inadvertent disclosure by internal (company) personnel

C. Data disclosure through insufficiently isolated resources

D. Malicious intrusion by external entities

61. When a data center is configured such that the backs of the devices face each other and the ambient temperature in the work area is cool, it is called _____.

A. Hot aisle containment

B. Cold aisle containment

C. Thermo-optimized

D. HVAC modulated

62. Disciplined cable management is crucial for cloud data centers because it provides greater assurance of only authorized lines operating in the environment and _____.

A. Reduces unproductive HVAC activity

B. Reduces the risk of slip, trip, and fall hazard

C. Greatly reduces the environmental footprint

D. Ensures regulatory compliance

63. In order to optimize air flow within a data center according to industry standards, a raised floor used as an air plenum must have at least _____ of clearance.

A. One foot

B. One meter

C. 24 inches

D. 30 inches

64. Raised flooring can serve as both an air plenum and _____.

A. A convenient location for RAID arrays

B. Cool storage for data center personnel meals

C. A conduit for running cable

D. Disaster shelter locations

65. Typically, when raised flooring is used as an air plenum, _____ air is directed through it.

A. Warm

B. Cold

C. Bleed

D. Exhaust

66. There are two general types of smoke detectors. One type uses a light source to detect the presence of particulate matter resulting from a fire, and the other uses _____.

A. Electric pulses

B. Small amounts of radioactive material

C. Fiber-optic mechanisms

D. A water-pressure plate

67. Fire suppression systems are often linked to a detection system. Common detection systems include all of the following *except* _____.

A. Heat

B. Pressure

C. Flame

D. Smoke

68. FM-200 has all the following properties *except* _____.

A. It's nontoxic at levels used for fire suppression

B. It's gaseous at room temperature

C. It may deplete the Earth's ozone layer

D. It does not leave a film or coagulant after use

69. FM-200 has all the following properties *except* _____.

A. It is colorless

B. It leaves a faint chemical residue after use

C. It is liquid when stored

D. It is non-conducive

70. DHCP servers in a network will provide the clients with all of the following *except* _____.

A. A temporary IP address

B. Encryption protocols

C. A default gateway

D. Time server synchronization

71. You are the security officer for a cloud deployment. In order to isolate data in transit, you can choose to implement all of the following techniques/technologies *except* _____.

A. DNSSEC

B. TLS

C. IDS/IPS

D. IPSec

72. All of the following techniques are used in OS hardening *except* _____.

A. Removing default accounts

B. Disallowing local save of credentials

C. Removing unnecessary services

D. Preventing all administrative access

73. You are performing an audit of the security controls used in a cloud environment. Which of the following would *best* serve your purpose?

A. The business impact analysis (BIA)

B. A copy of the VM baseline configuration

C. The latest version of the company's financial records

D. A SOC 3 report from another (external) auditor

74. In a cloud environment, prior to putting a node into maintenance mode, all of the following actions should be taken *except* _____.

A. Prevent any new users from logging on/creating any new instances

B. Migrate any existing guest VMs to another node

C. Disable alerts from host-based IDS/IPS/firewalls

D. Disable logging functions/tools

75. A cloud provider conducting scheduled maintenance of the environment should do all the following *except* _____.

A. Notify any customers who may be affected

B. Require reverification of all user accounts

C. Follow approved change-management procedures/processes

D. Confirm that remaining resources are sufficient to manage the minimum load as dictated by SLAs

76. Which of the following is characterized by a set maximum capacity?

A. A secret-sharing-made-short (SSMS) bit-splitting implementation

B. A tightly coupled cloud storage cluster

C. A loosely coupled cloud storage cluster

D. A public-key infrastructure

77. Which of the following is an open-source cloud-based software project characterized by a toolset that includes components called Nova, Neutron, Heat, Ironic, and Cinder?

A. OWASP

B. OAuth

C. OpenStack

D. Mozilla

78. You are the security directory for a call center that provides live support for customers of various vendors. Your staff handles calls regarding refunds, complaints, and the use of products customers have purchased. In order to process refunds, your staff will have access to purchase information, determine which credit card the customer used, and will need to identify specific elements of personal data. How should you best protect this sensitive data, and still accomplish the purpose?

A. Encrypt the data while it is at rest, but allow the call center personnel to decrypt it for refund transactions.

B. Encrypt the data while call center personnel are performing their operations.

C. Mask the data while call center personnel are performing their operations.

D. Have the call center personnel request the pertinent information from the customer for every refund transaction.

79. Which of the following is *not* typically included as a basic phase of the software development life cycle?

A. Define

B. Design

C. Describe

D. Develop

80. What is the most important input to the SDLC?

A. Senior management direction

B. Legislation/regulation

C. Investor oversight

D. Business requirements

81. Which of the following can be included in the cloud security architecture as a means to identify and deter hostile SQL commands?

A. Web application firewall (WAF)

B. API gateway

C. Data leak protection (DLP)

D. Database activity monitor (DAM)

82. You are the security manager for a software development firm. Your company is interested in using a managed cloud service provider for hosting its testing environment. Which cloud service/deployment model would probably best suit your needs?

A. IaaS

B. PaaS

C. SaaS

D. Community

83. You are the security manager for a software development firm. Your company is interested in using a managed cloud service provider for hosting its testing environment. Which of the following tools/technologies/techniques may be very useful for your purposes?

A. Data leak protection (DLP)

B. Digital rights management (DRM)

C. Sandboxing

D. Web application firewall (WAF)

84. You are the security manager for a software development firm. Your company is interested in using a managed cloud service provider for hosting its testing environment. Previous releases have shipped with major flaws that were not detected in the testing phase; leadership wants to avoid repeating that problem. What tool/technique/technology might you suggest to aid in identifying programming errors?

A. Vulnerability scans

B. Open source review

C. SOC audits

D. Regulatory review

85. You are the security manager for a software development firm. Your company is interested in using a managed cloud service provider for hosting its testing environment. Previous releases have shipped with major flaws that were not detected in the testing phase; leadership wants to avoid repeating that problem. It is important to prevent _____ from being present during the testing.

A. Senior management

B. Marketing department personnel

C. Finance analysts

D. Programmers who worked on the software

86. You are the security manager for a software development firm. Your company is interested in using a managed cloud service provider for hosting its testing environment. Management is interested in adopting an Agile development style. When you explain what impact this will have, you note that _____ may be decreased by this option.

A. Speed of development

B. Thoroughness of documentation

C. Availability of prototypes

D. Customer collaboration

87. You are the security manager for a software development firm. Your company is interested in using a managed cloud service provider for hosting its testing environment. Management is interested in adopting an Agile development style. In order for this to happen, the company will have to increase the involvement of _____.

A. Security personnel

B. Budget and finance representatives

C. Members of the user group

D. Senior management

88. You are the security manager for a software development firm. Your company is interested in using a managed cloud service provider for hosting its testing environment. Management is interested in adopting an Agile development style. This will be typified by which of the following traits?

A. Reliance on a concrete plan formulated during the Define phase

B. Rigorous, repeated security testing

C. Isolated programming experts for specific functional elements

D. Short, iterative work periods

89. You are the security manager for a software development firm. Your company is interested in using a managed cloud service provider for hosting its testing environment. Management is interested in adopting an Agile development style. This will be typified by which of the following traits?

A. Daily meetings

B. A specific shared toolset

C. Defined plans that dictate all efforts

D. Addressing customer needs with an exhaustive initial contract

90. You are the security manager for a software development firm. Your company is interested in using a managed cloud service provider for hosting its testing environment. The back end of the software will have the data structured in a way to optimize XML requests. Which API programming style should programmers most likely concentrate on for the front-end interface?

A. SOAP

B. REST

C. SAML

D. DLP

91. You are the security manager for a software development firm. Your company is interested in using a managed cloud service provider for hosting its testing environment. You recommend the use of STRIDE threat modeling to assess potential risks associated with the software. Which of the following is *not* addressed by STRIDE?

A. External parties presenting false credentials

B. External parties illicitly modifying information

C. Participants able to deny a transaction

D. Users unprepared for secure operation by lack of training

92. You are the security manager for a software development firm. Your company is interested in using a managed cloud service provider for hosting its testing environment. Management has decided that the company will deploy encryption, DLP, and DRM in the cloud environment for additional protection. When consulting with management, you explain that these tools will be most likely to reduce _____.

A. External threats

B. Internal threats

C. Software vulnerabilities

D. Quality of service

93. You are the security manager for a software development firm. Your company is interested in using a managed cloud service provider for hosting its testing environment. Your company has, and wishes to retain, ISO 27034 certification. For every new application it creates, it will also have to create a(n) _____.

A. Organizational normative framework (ONF)

B. Application normative framework (ANF)

C. Intrinsic normative framework (INF)

D. SOC 3 report

94. You are the security manager for a software development firm. Your company is interested in using a managed cloud service provider for hosting a customer-facing production environment. Many of your end users are located in the European Union and will provide personal data as they utilize your software. Your company will not be allowed to use a cloud data center in which of the following countries?

A. Japan

B. Australia

C. Belgium

D. Chile

95. You are the security manager for a software development firm. Your company is interested in using a managed cloud service provider for hosting a customer-facing production environment. Many of your end users are located in the European Union, and will provide personal data as they utilize your software. Your company will not be allowed to use a cloud data center in which of the following countries?

A. Argentina

B. Israel

C. Korea

D. Switzerland

96. You are the security manager for a software development firm. Your company is interested in using a managed cloud service provider for hosting a customer-facing production environment. Many of your end users are located in the European Union and will provide personal data as they utilize your software. Your company will not be allowed to use a cloud data center in which of the following countries?

A. Canada

B. Singapore

C. France

D. Kenya

97. Which of the following is not a core principle included in the OECD privacy guidelines?

A. The individual must have the ability to refrain from sharing their data.

B. The individual must have the ability to correct errors in their data.

C. The individual must be able to request a purge of their data.

D. The entity holding the data must secure it.

98. Who is the entity identified by personal data?

A. The data owner

B. The data processor

C. The data custodian

D. The data subject

99. What is the current EU privacy legislation that restricts dissemination of personal data outside the EU?

A. The EU Data Directive

B. Privacy Shield

C. The General Data Protection Regulation

D. Sarbanes-Oxley

100. In order for American companies to process personal data belonging to EU citizens, they must comply with the Privacy Shield program. The program is administered by the US Department of Transportation and the _____.

A. US State Department

B. Fish and Wildlife Service

C. Federal Trade Commission

D. Federal Communication Commission

101. In addition to the Privacy Shield program, what other means can non-EU companies use, to be allowed to process personal data of EU citizens?

A. Enhanced security controls

B. Standard contractual clauses

C. Increased oversight

D. Modified legal regulation

102. Which entity is legally responsible for the protection of personal data?

A. The data subject

B. The data controller

C. The data processor

D. The data steward

103. When a company is first starting and has no defined processes and little documentation, it can be said to be at level _____ of the Capability Maturity Model.

A. 1

B. 2

C. 3

D. 4

104. Which of the following standards addresses a company's entire security program, involving all aspects of various security disciplines?

A. ISO 27001

B. ISO 27002

C. NIST 800-37

D. SSAE 16

105. A cloud provider might only release SOC 2, Type 2 reports to _____.

A. Regulators

B. The public

C. Potential customers

D. Current customers

106. A cloud provider's SOC 1 report may not be useful to customers interested in determining the provider's security posture because the SOC 1 report only contains information about _____.

A. Sales projections

B. Financial reporting

C. Previous customer satisfaction

D. Process definition

107. The Payment Card Industry Data Security Standard requires different levels of activity based on participants' _____.

A. Number of personnel

B. Branch Locations

C. Number of transactions per year

D. Preferred banking institutions

108. Which IT product review framework is intended to determine the accuracy of vendor claims regarding security functions of the product?

A. Underwriters Laboratories

B. FIPS 140-2

C. PCI DSS

D. Common Criteria

109. What is the lowest level of cryptographic security for a cryptographic module, according to the FIPS 140-2 standard?

A. 1

B. 2

C. 3

D. 4

110. What is the highest level of the Cloud Security Alliance's Security, Trust, and Assurance Registry certification program for cloud service providers?

A. 1

B. 2

C. 3

D. 4

111. Every cloud service provider that opts to join the CSA STAR program registry must complete a _____.

A. SOC 2, Type 2 audit report

B. Consensus Assessment Initiative Questionnaire (CAIQ)

C. NIST 800-37 RMF audit

D. ISO 27001 ISMS review

112. The term *cloud carrier* most often refers to _____.

A. The cloud provider

B. The cloud customer

C. An ISP

D. A cloud manager

113. In a centralized broker identity federation, which entity typically creates and sends the SAML token?

A. The cloud provider

B. The ISP

C. The broker

D. The cloud customer

114. Which of the following tools incorporates and references the requirements listed in all the others?

A. ISO 27001

B. CSA Cloud Controls Matrix

C. FedRAMP

D. ENISA

115. Which of the following is an example of true multifactor authentication?

A. Having a login that requires both a password and a PIN

B. Using a thumbprint and voice recognition software for access control

C. Presenting a credit card along with a Social Security card

D. Signing a personal check

116. Which of the following is appropriate to include in an SLA?

A. That the provider deliver excellent uptime

B. That the provider only host the customer's data within specific jurisdictions

C. That any conflicts arising from the contract be settled within a particular jurisdiction

D. The specific amount of data that can be uploaded to the cloud environment in any given month

117. Which of the following is not typically included in the list of critical assets specified for continuity during BCDR contingency operations?

A. Systems

B. Data

C. Cash

D. Personnel

118. Which of the following is not typically a BCDR construct involving cloud computing?

A. On-premises production environment; cloud BCDR environment

B. Cloud production environment; same provider BCDR environment

C. Cloud production environment; different provider BCDR environment

D. Cloud production environment; on-premises BCDR environment

119. A database activity monitor (DAM) functions at layer _____ of the OSI model.

A. 1

B. 3

C. 5

D. 7

120. Which of the following API construction models is most popular among web developers currently?

A. Simple object access protocol (SOAP)

B. Graphical user interface (GUI)

C. Representational state transfer (REST)

D. HTML

121. Why is it important to force all instantiated virtual machines to check current configuration records?

A. Snapshotted images don't take patches.

B. Configurations are constantly changing.

C. Documentation is difficult in the cloud.

D. Users are always changing configurations.

122. Which of the following standards is typically used to convey public key information in a PKI arrangement?

A. SAML

B. X.400

C. X.509

D. 802.11

123. Which of the following is *not* commonly considered a form of privacy data processing?

A. Storing

B. Computing

C. Destroying

D. Buying

124. Who should be the only entity allowed to declare that an organization can return to normal following contingency or BCDR operations?

A. Regulators

B. Law enforcement

C. The incident manager

D. Senior management

125. All of the following entitles are required to use FedRAMP-accredited Cloud Service Providers *except* _____.

A. The US post office

B. The Department of Homeland Security

C. Federal Express

D. The CIA

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Comprehensive Online Learning Environment

Register on Sybex.com to gain access to the online interactive test bank to help you study for your CCSP certification - included with your purchase of this book! All of the practice tests in this book are included in the online test bank so you can practice in a timed and graded setting.

Go to www.wiley.com/go/sybextestprep to register and gain access to this study tool.

Do you need more? If you have not already read Sybex's CCSP (ISC)^2 Certified Cloud Security Professional Official Study Guide by Brian T. O'Hara, Ben Malisow (ISBN: 978-1-119-27741-5) and are not seeing passing grades on these practice tests, this book is an excellent resource to master any CCSP topics causing problems. This book maps every official exam objective to the corresponding chapter in the book to help track exam prep objective by objective, challenging review questions in each chapter to prepare for exam day, and online test prep materials with flashcards and additional practice tests.

SYBEX®
A Wiley Brand