

CISSP®

Practice Exams

Fifth Edition

Fully revised for
the 2018 CISSP
Body of Knowledge

- Hundreds of practice questions covering all 8 Certified Information Systems Security Professional exam domains

- Written by leading IT security certification and training experts



Digital content includes:

- 1000+ multiple-choice practice exam questions

- Hotspot and drag-and-drop practice exam questions

Mc
Graw
Hill
Education

SHON HARRIS, CISSP
JONATHAN HAM, CISSP, GSEC, GCIA, GCIH

ABOUT THE AUTHORS

Shon Harris, CISSP, was the founder and CEO of Shon Harris Security LLC and Logical Security LLC, a security consultant, a former engineer in the Air Force's Information Warfare unit, an instructor, and an author. Shon owned and ran her own training and consulting companies for 13 years prior to her death in 2014. She consulted with Fortune 100 corporations and government agencies on extensive security issues. She authored three best-selling CISSP books, was a contributing author to *Gray Hat Hacking: The Ethical Hacker's Handbook* and *Security Information and Event Management (SIEM) Implementation*, and a technical editor for *Information Security Magazine*.

Jonathan Ham, CISSP, GSEC, GCIA, GCIH, GMON, is an independent consultant who specializes in large-scale enterprise security issues, from policy and procedure, through team selection and training, to implementing scalable prevention, detection, and response technologies and techniques. With a keen understanding of ROI and TCO (and an emphasis on real-world practice over products), he has helped his clients achieve greater success for over 20 years, advising in both the public and private sectors, from small startups to the Fortune 50, and the U.S. Department of Defense across multiple engaged forces.

Mr. Ham has been commissioned to teach investigative techniques to the NSA, has trained NCIS investigators how to use intrusion detection technologies, has performed packet analysis from a facility more than 2,000 feet underground, and has chartered and trained the CIRT for one of the largest U.S. civilian federal agencies.

In addition to his professional certifications, Mr. Ham is a Principal Instructor and Author with the SANS Institute, and is a member of the GIAC Advisory Board. He has also consistently been the highest rated trainer at Black Hat events, teaching his course on Network Forensics. His groundbreaking textbook on the topic established him as a pioneer in the field.

A former combat medic with the U.S. Navy/Marine Corps, Mr. Ham has spent over a decade practicing a different kind of emergency response, volunteering and teaching for both the National Ski Patrol and the American Red Cross, as both a Senior Patroller and Instructor and a Professional Rescuer.

A Note from Jonathan

Shon and I never met in person, though my career has been inextricably linked to hers for more than a decade. The first time I was ever asked to teach a class for the SANS Institute was because Shon was scheduled and couldn't make it. I went on to teach SANS' extremely popular CISSP prep course (Mgt414) dozens of times, and my students routinely brought her books to my classroom.

As a result, I've gone on to teach thousands of students at both the graduate and post-graduate level, across six continents and in dozens of countries, and involving content ranging from hacking techniques to forensic investigations. Thanks to Shon, I am truly living the dream and giving it back in every way that I can.

I am also extremely honored to have been asked by McGraw-Hill Education to continue her work. We had so very many friends in common that nearly everyone I know professionally encouraged me to do it. She will be remembered with the respect of thousands of CISSPs.

And mine.

About the Technical Editor

Daniel Carter, CCSP, CISSP, CISM, CISA, is currently working as a senior systems engineer at Johns Hopkins University & Medicine. An IT security and systems professional for almost 20 years, Daniel has worked extensively with web-based applications and infrastructure, as well as LDAP and federated identity systems, PKI, SIEM, and Linux/Unix systems. He is currently working with enterprise authentication and single sign-on systems, including cloud-base deployments. Daniel holds a degree in criminology and criminal justice from the University of Maryland and a master's degree in technology management, with a focus on homeland security management, from the University of Maryland, University College.

CISSP®

Practice Exams

Fifth Edition

Shon Harris
Jonathan Ham



New York Chicago San Francisco
Athens London Madrid Mexico City
Milan New Delhi Singapore Sydney Toronto

McGraw-Hill Education is an independent entity from (ISC)² and is not affiliated with (ISC)² in any manner. This study/training guide and/or material is not sponsored by, endorsed by, or affiliated with (ISC)² in any manner. This publication and accompanying media may be used in assisting students to prepare for the CISSP exam. Neither (ISC)² nor McGraw-Hill Education warrants that use of this publication and accompanying media will ensure passing any exam. (ISC)², CISSP®, CAP®, ISSAP®, ISSEP®, ISSMP®, SSCP®, CCSP®, and CBK® are trademarks or registered trademarks of (ISC)² in the United States and certain other countries. All other trademarks are trademarks of their respective owners.

Copyright © 2019 by McGraw-Hill Education. All rights reserved. Except as permitted under the United States Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

ISBN: 978-1-26-014266-2

MHID: 1-26-014266-3

The material in this eBook also appears in the print version of this title: ISBN: 978-1-26-014267-9, MHID: 1-26-014267-1.

eBook conversion by codeMantra

Version 1.0

All trademarks are trademarks of their respective owners. Rather than put a trademark symbol after every occurrence of a trademarked name, we use names in an editorial fashion only, and to the benefit of the trademark owner, with no intention of infringement of the trademark. Where such designations appear in this book, they have been printed with initial caps.

McGraw-Hill Education eBooks are available at special quantity discounts to use as premiums and sales promotions or for use in corporate training programs. To contact a representative, please visit the Contact Us page at www.mhprofessional.com.

Information has been obtained by McGraw-Hill Education from sources believed to be reliable. However, because of the possibility of human or mechanical error by our sources, McGraw-Hill Education, or others, McGraw-Hill Education does not guarantee the accuracy, adequacy, or completeness of any information and is not responsible for any errors or omissions or the results obtained from the use of such information.

TERMS OF USE

This is a copyrighted work and McGraw-Hill Education and its licensors reserve all rights in and to the work. Use of this work is subject to these terms. Except as permitted under the Copyright Act of 1976 and the right to store and retrieve one copy of the work, you may not decompile, disassemble, reverse engineer, reproduce, modify, create derivative works based upon, transmit, distribute, disseminate, sell, publish or sublicense the work or any part of it without McGraw-Hill Education's prior consent. You may use the work for your own noncommercial and personal use; any other use of the work is strictly prohibited. Your right to use the work may be terminated if

you fail to comply with these terms.

THE WORK IS PROVIDED “AS IS.” McGRAW-HILL EDUCATION AND ITS LICENSORS MAKE NO GUARANTEES OR WARRANTIES AS TO THE ACCURACY, ADEQUACY OR COMPLETENESS OF OR RESULTS TO BE OBTAINED FROM USING THE WORK, INCLUDING ANY INFORMATION THAT CAN BE ACCESSED THROUGH THE WORK VIA HYPERLINK OR OTHERWISE, AND EXPRESSLY DISCLAIM ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. McGraw-Hill Education and its licensors do not warrant or guarantee that the functions contained in the work will meet your requirements or that its operation will be uninterrupted or error free. Neither McGraw-Hill Education nor its licensors shall be liable to you or anyone else for any inaccuracy, error or omission, regardless of cause, in the work or for any damages resulting therefrom. McGraw-Hill Education has no responsibility for the content of any information accessed through the work. Under no circumstances shall McGraw-Hill Education and/or its licensors be liable for any indirect, incidental, special, punitive, consequential or similar damages that result from the use of or inability to use the work, even if any of them has been advised of the possibility of such damages. This limitation of liability shall apply to any claim or cause whatsoever whether such claim or cause arises in contract, tort or otherwise.

It has been at the expense of my tribe that I have managed to continue Shon's work.

I honor them by name here, as elsewhere:

436861726C6965204D617269652048616D0D0A
56696F6C65742044616E67657220576573740D0A
5468756E646572204772657920576573740D0A
50616F6C6120436563696C696120476172636961204A756172657A0D0A

They are beautiful and brilliant each, and are *continue to be* loved more than they may ever know, *through each of these revisions, and their own.*

—*Jonathan Ham, April 13, 2016* August 1, 2018

CONTENTS

- Preface
- Introduction
- Chapter 1** Security and Risk Management
 - Questions
 - Quick Answer Key
 - Answers
- Chapter 2** Asset Security
 - Questions
 - Quick Answer Key
 - Answers
- Chapter 3** Security Architecture and Engineering
 - Questions
 - Quick Answer Key
 - Answers
- Chapter 4** Communication and Network Security
 - Questions
 - Quick Answer Key
 - Answers
- Chapter 5** Identity and Access Management
 - Questions
 - Quick Answer Key
 - Answers
- Chapter 6** Security Assessment and Testing
 - Questions
 - Quick Answer Key

[Answers](#)

[Chapter 7](#) [Security Operations](#)

[Questions](#)

[Quick Answer Key](#)

[Answers](#)

[Chapter 8](#) [Software Development Security](#)

[Questions](#)

[Quick Answer Key](#)

[Answers](#)

[Appendix](#) [About the Online Content](#)

[System Requirements](#)

[Your Total Seminars Training Hub Account](#)

[Single User License Terms and Conditions](#)

[TotalTester Online](#)

[Hotspot and Drag-and-Drop Questions](#)

[Technical Support](#)

PREFACE

The preface for the previous edition of this book began as follows:

Computer, information, and physical security are becoming more important at an exponential rate. Over the last few years, the necessity for computer and information security has grown rapidly as cyber attacks have increased, financial information is being stolen at a rapid pace, cyber warfare is affecting countries around the world, and today's malware is growing exponentially in its sophistication and dominating our threat landscape. The world's continuous dependency upon technology and the rapid increase in the complexities of these technologies make securing them a challenging and important task.

That was published roughly two years ago but still holds true today. If anything, the problems confronting information security professionals are more daunting than ever before.

A lot has happened in the world of information security since the previous edition was published in 2016, including some of the most notorious incidents and events in our sordid history. In the summer of 2016 an organization of Russian state-affiliated malicious actors calling themselves The Shadow Brokers (TSB) emerged publicly, and by March 2017 began pedaling zero-day exploits and hacking tools ostensibly stolen from the U.S. National Security Agency (NSA). Most famous among these involved a very old but previously unannounced vulnerability in version 1 of Microsoft's Server Message Block implementation (SMBv1), dubbed "EternalBlue." Microsoft immediately issued a patch for the issue (MS17-010)—out of cycle in order to try to assist its customers in getting ahead of the threat—but adoption was slow, and EternalBlue remains a nightmare of rather epic proportions.

The first widespread exploitation of this flaw was with the DoublePulsar back-door implant, which began spreading rapidly by April 2017 and which compromised at least 100,000 systems worldwide, though to very little fanfare. In May 2017, however, the WannaCry ransomware attack emerged targeting the same largely unpatched flaw. In December 2017 the U.S. government formally placed the blame for this campaign on North Korean actors, and some estimates of the worldwide damage from it top US\$4B.

Somewhat predictably, the NotPetya attack followed in June 2017, again leveraging the same vulnerability, but used only one minor vector as its initial

means of intrusion. This malware more notably stole credentials for lateral movement throughout compromised organizations, leveraging tools commonly used by Active Directory domain administrators to “live off the land” as it spread internally. Initially assumed to be another ransomware effort, the NotPetya attack is now widely understood to have been a supply-chain-based denial-of-service (DoS) attack on Ukraine that was nation-state sponsored, with worldwide collateral damage. Shipping transport companies FedEx and Maersk have reputedly suffered over US\$300M in damages each.

But perhaps the most notorious event in our recent history was the Equifax breach, which in hindsight was instructive on just about every conceivable level. This time the vulnerability was in the Internet-facing use of the Apache Struts web app framework, for which patches had been available for months. The result was the loss of sensitive personal and financial records of over 145 million consumers—most likely just about any U.S. citizen with a credit score, and many millions of others. Through the details of this event we were able to see failures in executive leadership, security processes and procedures for defensive posture, intrusion detection, incident response, and ultimately gross failures in public relations as well. Everything that could have gone wrong, at any stage, went wrong.

Among the ultimate results of this event were the departure of the CEO and other top-level executives of Equifax, and federal criminal indictments of several Equifax executives by the U.S. government for insider-trading violations, for allegedly dumping company stock upon learning of the breach but prior to its public announcement. The departed CEO, Richard Smith, was called by the U.S. Congress to testify publicly on the matter. This was followed by Facebook’s founder and CEO Mark Zuckerberg’s public U.S. Senate testimony in April 2018 about yet another (unrelated) very high-profile data breach involving Facebook.

On and on it goes, and we’ve only just scratched the surface.

So what is to be done? What is required is a better educated, better informed, and hence better prepared workforce of information security professionals to lead the charge, and to implement the changes that we as an industry—apparent evidence to the contrary—actually *do* know how to effect. The task falls to every last one of us to rise to this challenge, and to make a difference in the equation, everywhere we possibly can. It starts and ends with us.

You have in your hand a whole lot of answers. There are an equal number of questions posed to you as well, but it is the answers you need to understand, and why the correct ones are correct, and the incorrect ones are not. If you can master the questions and answers in this volume, you should

have little difficulty passing the CISSP certification exam (also newly revised) to demonstrate your knowledge to others in a somewhat shorthand manner, as a CISSP.

That, however, is just another step in a longer journey of what is required of you. Accomplish that step, then take the next, which is to get back out into the field, share what you have learned, and put what you know to work.

INTRODUCTION

The objective of this book is to prepare you for the CISSP exam by familiarizing you with the more difficult types of questions that may come up on the exam. The questions in this book delve into the more complex topics of the CISSP Common Body of Knowledge (CBK) that you may be faced with when you take the exam.

This book has been developed to be used in tandem with the *CISSP All-in-One Exam Guide, Eighth Edition*, both of which have been thoroughly revised since their last editions to reflect the most recent revision of the CISSP exam in 2018. The best approach to prepare for the exam using all of the material available to you is outlined here:

1. Review the questions and answer explanations in each chapter.
2. If further review is required, read the corresponding chapter(s) in the *CISSP All-in-One Exam Guide, Eighth Edition*.
3. Review all of the additional questions that are available. See the “Additional Questions Available” section at the end of this introduction.

Because the primary focus of this book is to help you pass the exam, the questions included cover all eight CISSP exam domains. Each question features a detailed explanation as to why one answer choice is the correct answer and why each of the other choices is incorrect. Because of this, we believe this book will serve as a valuable professional resource after your exam.

In This Book

This book has been organized so that each chapter consists of a battery of practice exam questions representing a single CISSP exam domain, appropriate for experienced information security professionals. Each practice exam question features answer explanations that provide the emphasis on the “why” as well as the “how-to” of working with and supporting the technology and concepts.

In Every Chapter

Included in each chapter are features that call your attention to the key steps of the testing and review process and that provide helpful exam-taking hints. Take a look at what you'll find in every chapter:

- Every chapter includes practice exam questions from one **CISSP CBK Security Domain**. Drill down on the questions from each domain that you will need to know how to answer in order to pass the exam.
- The **Practice Exam Questions** are similar to those found on the actual CISSP exam and are meant to present you with some of the most common and confusing problems that you may encounter when taking the actual exam. These questions are designed to help you anticipate what the exam will emphasize. Getting inside the exam with good practice questions will help ensure you know what you need to know to pass the exam.
- Each chapter includes a **Quick Answer Key**, which provides the question number and the corresponding letter for the correct answer choice. This allows you to score your answers quickly before you begin your review.
- Each question includes an **In-Depth Answer Explanation**—explanations are provided for both the correct and incorrect answer choices and can be found at the end of each chapter. By reading the answer explanations, you'll reinforce what you've learned from answering the questions in that chapter, while also becoming familiar with the structure of the exam questions.

Additional Questions Available

In addition to the questions in each chapter, there are more than 1,500 multiple-choice practice exam questions available to you. Also available are simulated hotspot and drag-and-drop questions. For more information on these question types and how to access them, please refer to the appendix.

Security and Risk Management

This domain includes questions from the following topics:

- Security terminology and principles
- Protection control types
- Security frameworks, models, standards, and best practices
- Computer laws and crimes
- Intellectual property
- Data breaches
- Risk management
- Threat modeling
- Business continuity and disaster recovery
- Personnel security
- Security governance

A security professional's responsibilities extend well beyond reacting to the latest news headlines of a new exploit or security breach. The day-to-day responsibilities of security professionals are far less exciting on the surface but are vital to keeping organizations protected against intrusions so that they don't become the next headline. The role of security within an organization is a complex one, as it touches every employee and must be managed companywide. It is important that you have an understanding of security beyond the technical details to include management and business issues, both for the CISSP exam and for success in the field.

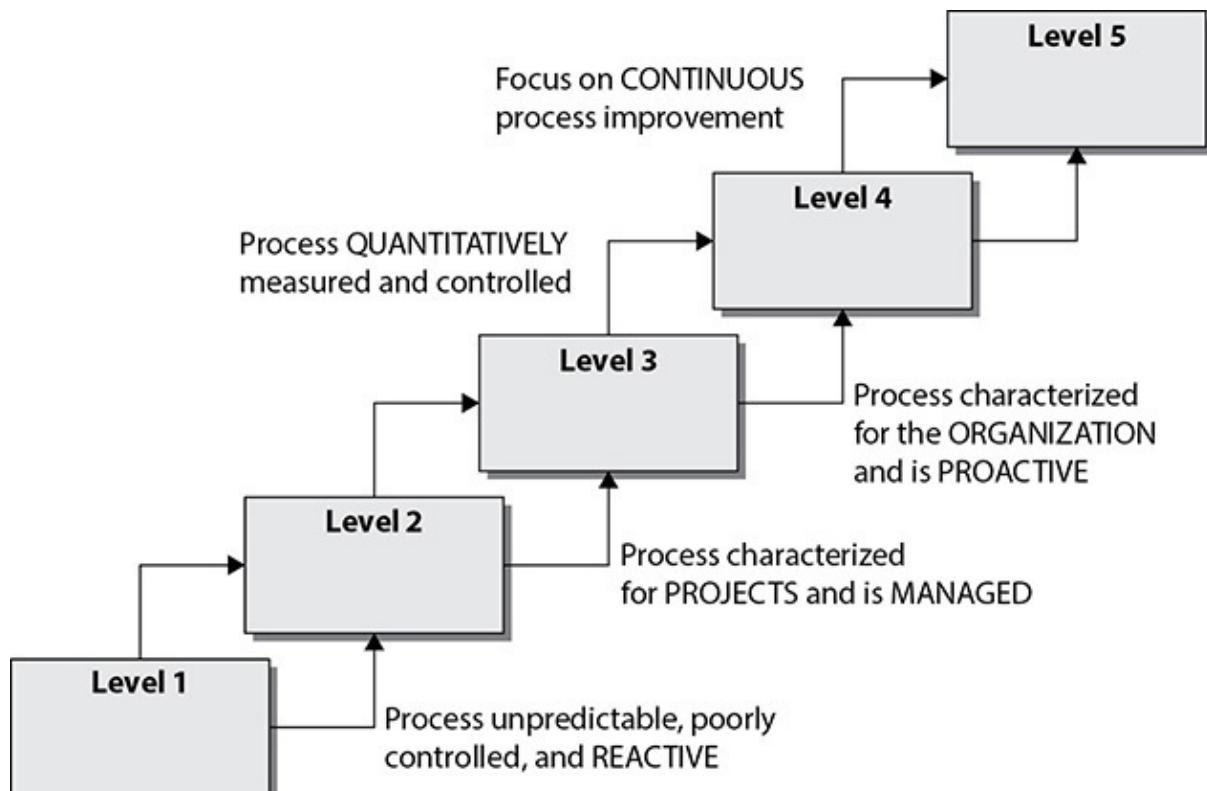
Q QUESTIONS

1. Which of the following best describes the relationship between COBIT and ITIL?
 - COBIT is a model for IT governance, whereas ITIL is a model for corporate governance.
 - COBIT provides a corporate governance roadmap, whereas ITIL is a customizable framework for IT service management.
 - COBIT defines IT goals, whereas ITIL provides the process-level

steps on how to achieve them.

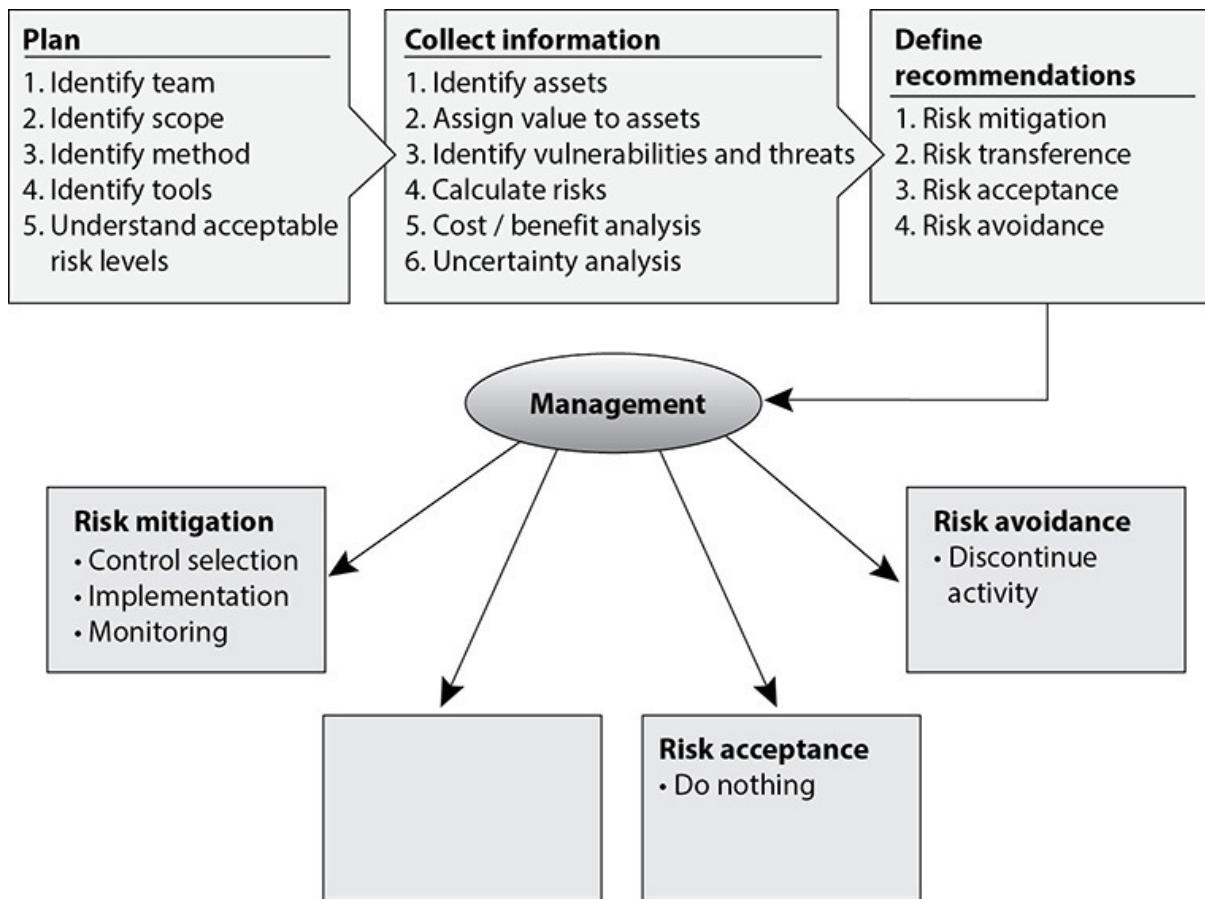
- D.** COBIT provides a framework for achieving business goals, whereas ITIL defines a framework for achieving IT service-level goals.
- 2.** Global organizations that transfer data across international boundaries must abide by guidelines and transborder information flow rules developed by an international organization that helps different governments come together and tackle the economic, social, and governance challenges of a globalized economy. What organization is this?
- A. Committee of Sponsoring Organizations of the Treadway Commission
- B.** The Organisation for Economic Co-operation and Development
- C. COBIT
- D. International Organization for Standardization
- 3.** Steve, a department manager, has been asked to join a committee that is responsible for defining an acceptable level of risk for the organization, reviewing risk assessment and audit reports, and approving significant changes to security policies and programs. What committee is he joining?
- A. Security policy committee
- B. Audit committee
- C. Risk management committee
- D.** Security steering committee
- 4.** Which of the following is not included in a risk assessment?
- A.** Discontinuing activities that introduce risk
- B. Identifying assets
- C. Identifying threats
- D. Analyzing risk in order of cost or criticality
- 5.** The integrity of data is not related to which of the following?
- A. Unauthorized manipulation or changes to data
- B. The modification of data without authorization
- C. The intentional or accidental substitution of data

- D.** The extraction of data to share with unauthorized entities
- 6.** As his company's CISO, George needs to demonstrate to the board of directors the necessity of a strong risk management program. Which of the following should George use to calculate the company's residual risk?
- threats × vulnerability × asset value = residual risk
 - SLE × frequency = ALE, which is equal to residual risk
 - (threats × vulnerability × asset value) × controls gap = residual risk
 - (total risk – asset value) × countermeasures = residual risk
- 7.** Capability Maturity Model Integration (CMMI) came from the software engineering world and is used within organizations to help lay out a pathway of how incremental improvement can take place. This model is used by organizations in self-assessment and to develop structured steps that can be followed so an organization can evolve from one level to the next and constantly improve its processes. In the CMMI model graphic shown, what is the proper sequence of the levels?

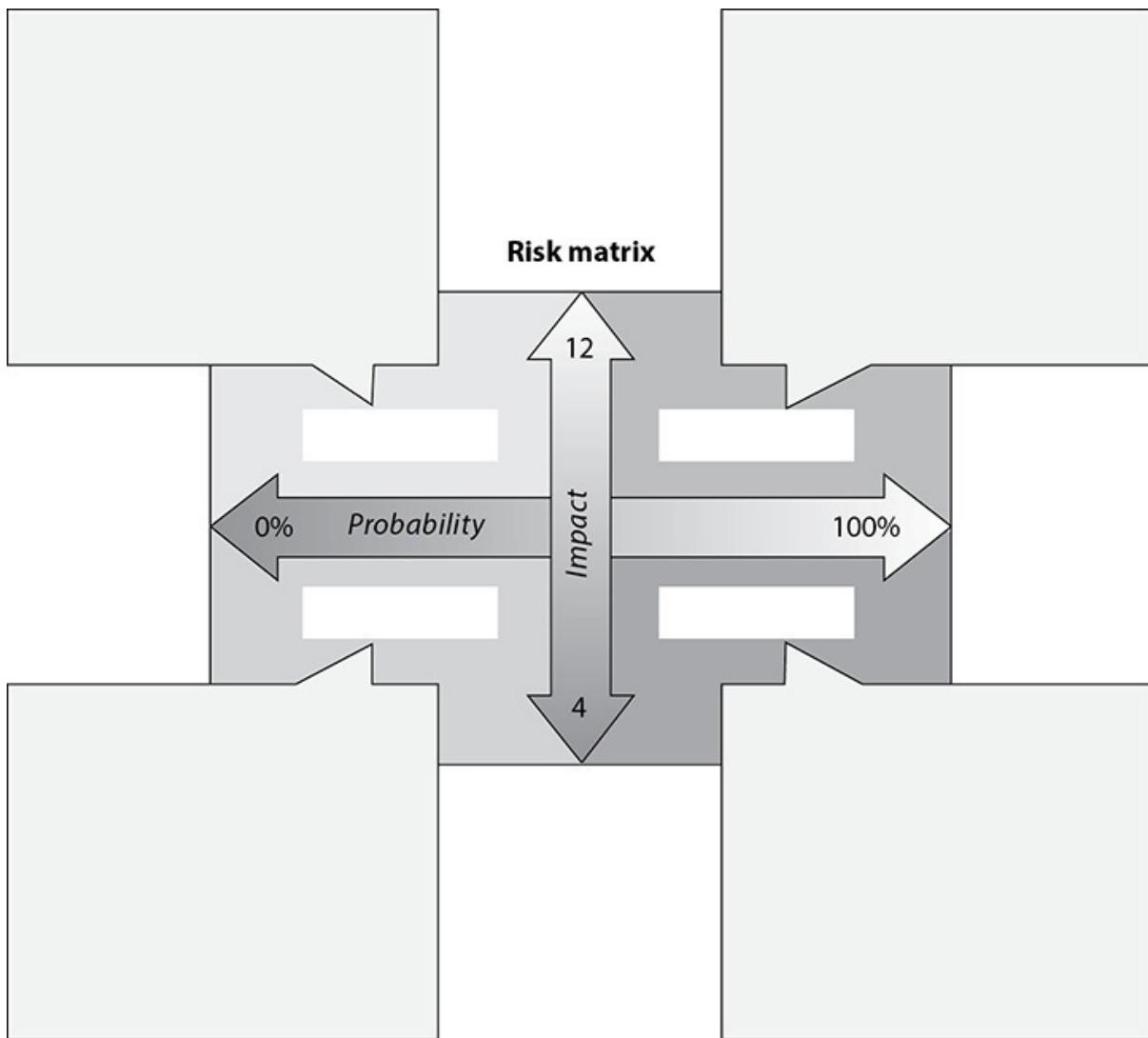


- Initial, Defined, Managed, Quantitatively Managed, Optimizing
- Initial, Defined, Quantitatively Managed, Optimizing, Managed
- Defined, Managed, Quantitatively Managed, Optimizing

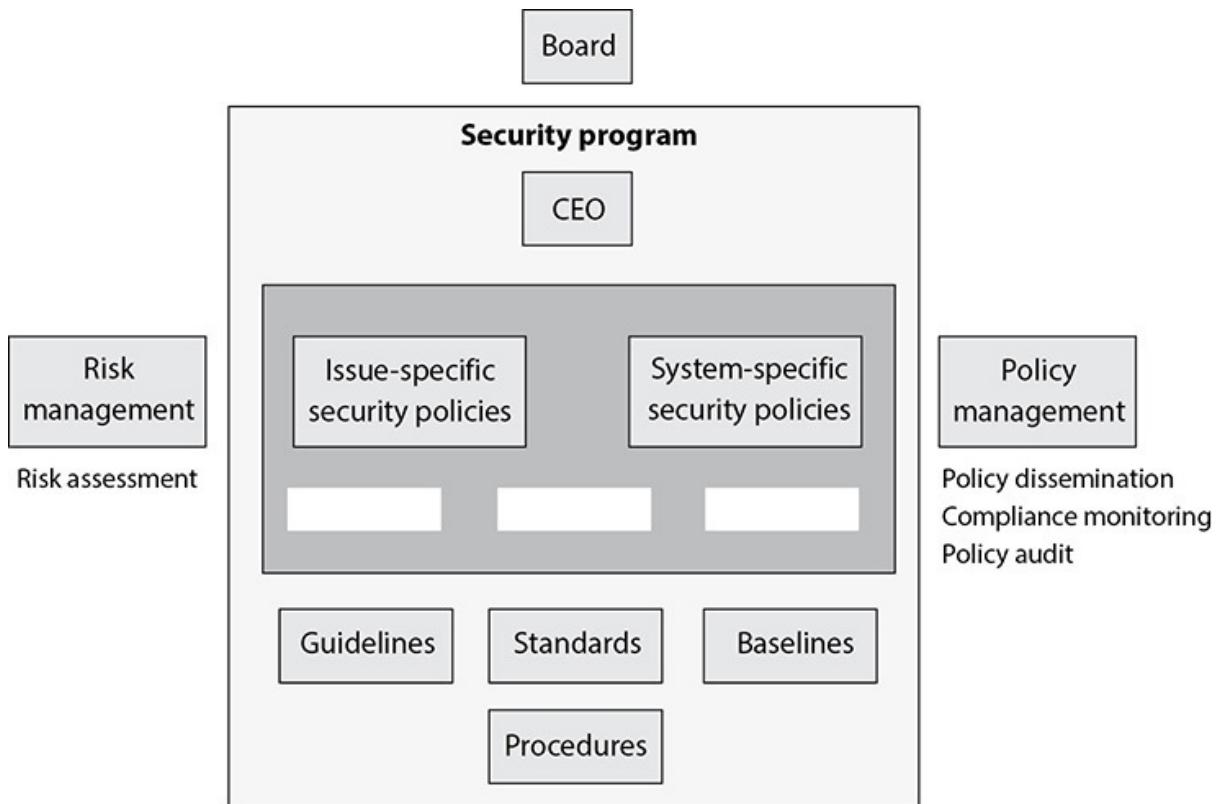
- D. Initial, Repeatable, Defined, Quantitatively Managed, Optimizing**
8. Risk assessment has several different methodologies. Which of the following official risk methodologies was not created for the purpose of analyzing security risks?
- A. FAP
 - B. OCTAVE
 - C. AS/NZS 4360**
 - D. NIST SP 800-30
9. Which of the following is not a characteristic of a company with a security governance program in place?
- A. Board members are updated quarterly on the company's state of security.
 - B. All security activity takes place within the security department.**
 - C. Security products, services, and consultants are deployed in an informed manner.
 - D. The organization has established metrics and goals for improving security.
10. There are four ways of dealing with risk. In the graphic that follows, which method is missing and what is the purpose of this method?



- A. Risk transference. Share the risk with other entities.
- B. Risk reduction. Reduce the risk to an acceptable level.
- C. Risk rejection. Accept the current risk.
- D. Risk assignment. Assign risk to a specific owner.
11. The following graphic contains a commonly used risk management scorecard. Identify the proper quadrant and its description.



- A. Top-right quadrant is high impact, low probability.
- B. Top-left quadrant is high impact, medium probability.
- C. Bottom-left quadrant is low impact, high probability.
- D. **Bottom-right quadrant is low impact, high probability.**
12. What are the three types of policies that are missing from the following graphic?



- A. Regulatory, Informative, Advisory**
- B. Regulatory, Mandatory, Advisory**
- C. Regulatory, Informative, Public**
- D. Regulatory, Informative, Internal Use**
- 13.** List in the proper order from the table shown the learning objectives that are missing and their proper definitions.

	Awareness	Training	Education
Attribute:	"What"	"How"	"Why"
Level:	Information	Knowledge	Insight
Learning objective:			
Example teaching method:	Media <ul style="list-style-type: none"> • Videos • Newsletters • Posters 	Practical instruction <ul style="list-style-type: none"> • Lecture and/or demo • Case study • Hands-on practice 	Theoretical instruction <ul style="list-style-type: none"> • Seminar and discussion • Reading and study • Research
Test measure:	True/False Multiple choice (Identify learning)	Problem solving, i.e., recognition and resolution (Apply learning)	Essay (Interpret learning)
Impact timeframe:	Short-term	Intermediate	Long-term

- A. Understanding, recognition and retention, skill
- B. Skill, recognition and retention, skill
- C. Recognition and retention, skill, understanding
- D. Skill, recognition and retention, understanding
14. What type of risk analysis approach does the following graphic provide?

High	7–10	7–10
Medium	4–6	4–6
Low	0–3	0–3

0	10	20	30	40	50	60	70	80	90	100
0	9	18	27	36	45	54	63	72	81	90
0	8	16	24	32	40	48	56	64	72	80
0	7	14	21	28	35	42	49	56	63	70
0	6	12	18	24	30	36	42	48	54	60
0	5	10	15	20	25	30	35	40	45	50
0	4	8	12	16	20	24	28	32	36	40
0	3	6	9	12	15	18	21	24	27	30
0	2	4	6	8	10	12	14	16	18	20
0	1	2	3	4	5	6	7	8	9	10

41–100	High
20–40	Medium
0–19	Low

A. Quantitative

B. Qualitative

C. Operationally Correct

D. Operationally Critical

15. ISO/IEC 27000 is part of a growing family of ISO/IEC information security management systems (ISMS) standards. It comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Which of the following provides an incorrect mapping of the individual standards that make up this family of standards?

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

B. ISO/IEC 27003: Guideline for ISMS implementation

C. ISO/IEC 27004: Guideline for information security management measurement and metrics framework

D. ISO/IEC 27005: Guideline for bodies providing audit and certification of information security management systems

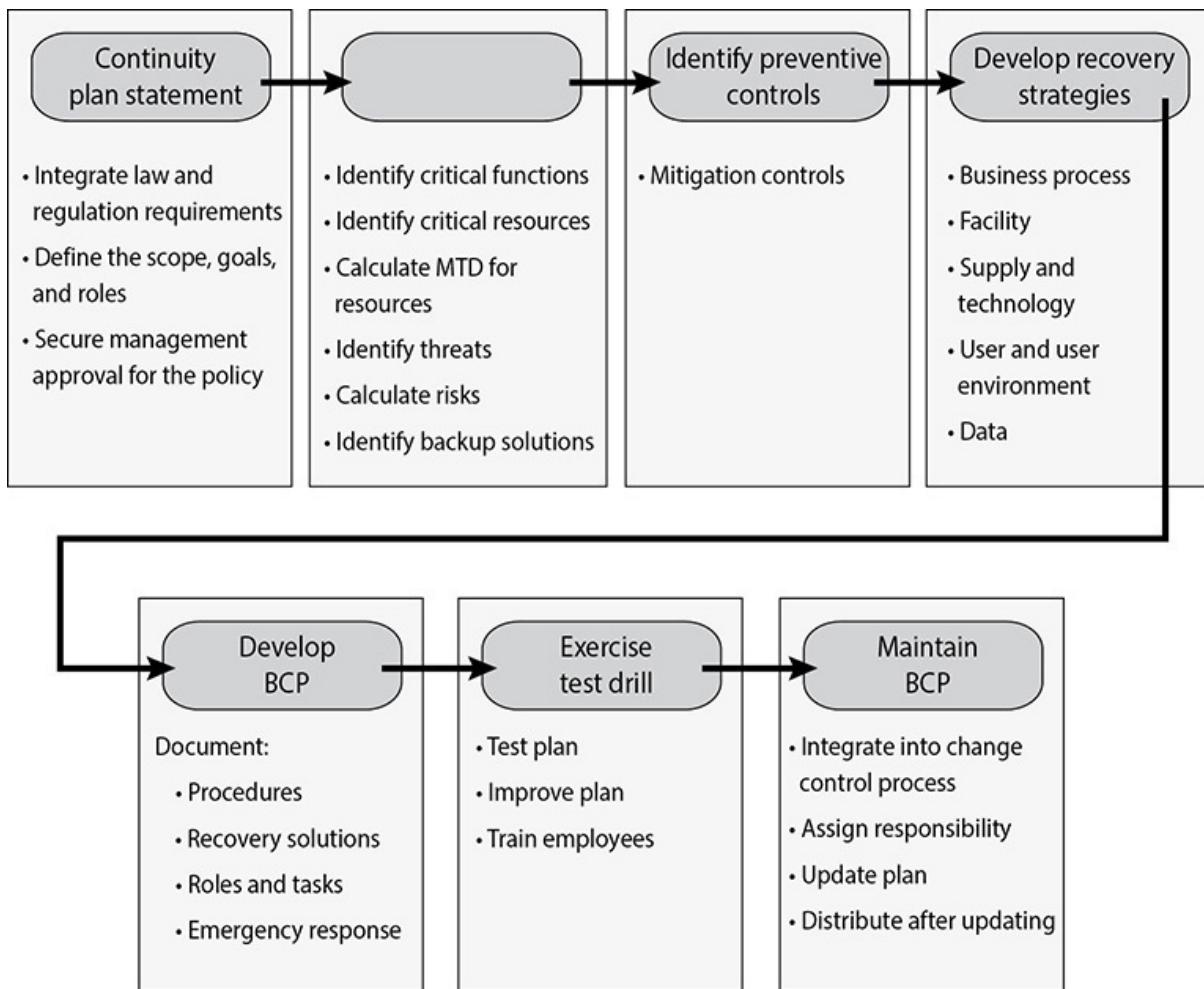
The following scenario applies to questions 16 and 17.

Sam is the security manager of a company that makes most of its revenue from its intellectual property. Sam has implemented a process improvement program that has been certified by an outside entity. His company received a Level 2 during an appraisal process, and he is putting in steps to increase this to a Level 3. A year ago when Sam carried out a risk analysis, he determined that the company was at too much of a risk when it came to potentially losing trade secrets. The countermeasure his team implemented reduced this risk, and Sam determined that the annualized loss expectancy of the risk of a trade secret being stolen once in a hundred-year period is now \$400.

- 16.** Which of the following is the criteria Sam's company was most likely certified under?
 - A. SABSA
 - B. Capability Maturity Model Integration**
 - C. Information Technology Infrastructure Library
 - D. Prince2
- 17.** What is the associated single loss expectancy value in this scenario?
 - A. \$65,000
 - B. \$400,000
 - C. \$40,000**
 - D. \$4,000
- 18.** The NIST organization has defined best practices for creating continuity plans. Which of the following phases deals with identifying and prioritizing critical functions and systems?
 - A. Identify preventive controls.
 - B. Develop the continuity planning policy statement.
 - C. Create contingency strategies.
 - D. Conduct the business impact analysis.**
- 19.** As his company's business continuity coordinator, Matthew is responsible for helping recruit members to the business continuity planning (BCP) committee. Which of the following does not correctly describe this effort?

- A. Committee members should be involved with the planning stages, as well as the testing and implementation stages.
 - B. The smaller the team, the better to keep meetings under control.**
 - C. The business continuity coordinator should work with management to appoint committee members.
 - D. The team should consist of people from different departments across the company.
- 20.** A business impact analysis is considered a functional analysis. Which of the following is not carried out during a business impact analysis?
- A. A parallel or full-interruption test**
 - B. The application of a classification scheme based on criticality levels
 - C. The gathering of information via interviews
 - D. Documentation of business functions
- 21.** Which of the following steps comes first in a business impact analysis?
- A. Calculate the risk for each different business function.
 - B. Identify critical business functions.
 - C. Create data-gathering techniques.**
 - D. Identify vulnerabilities and threats to business functions.
- 22.** It is not unusual for business continuity plans to become out of date. Which of the following is not a reason why plans become outdated?
- A. Changes in hardware, software, and applications
 - B. Infrastructure and environment changes
 - C. Personnel turnover
 - D. That the business continuity process is integrated into the change management process**
- 23.** Preplanned business continuity procedures provide organizations a number of benefits. Which of the following is not a capability enabled by business continuity planning?
- A. Resuming critical business functions
 - B. Letting business partners know your company is unprepared**
 - C. Protecting lives and ensuring safety
 - D. Ensuring survivability of the business

- 24.** Management support is critical to the success of a business continuity plan. Which of the following is the most important to be provided to management to obtain their support?
- A. Business case
B. Business impact analysis
C. Risk analysis
D. Threat report
- 25.** Which of the following is a critical first step in disaster recovery and contingency planning?
- A. Plan testing and drills.
B. Complete a business impact analysis.
C. Determine offsite backup facility alternatives.
D. Organize and create relevant documentation.
- 26.** Which of the following is not a reason to develop and implement a disaster recovery plan?
- A. Provide steps for a post-disaster recovery.
B. Extend backup operations to include more than just backing up data.
C. Outline business functions and systems.
D. Provide procedures for emergency responses.
- 27.** With what phase of a business continuity plan does a company proceed when it is ready to move back into its original site or a new site?
- A. Reconstitution phase
B. Recovery phase
C. Project initiation phase
D. Damage assessment phase
- 28.** What is the missing second step in the graphic that follows?



- A. Identify continuity coordinator
- B. Business impact analysis**
- C. Identify BCP committee
- D. Dependency identification
29. Different threats need to be evaluated and ranked based upon their severity of business risk when developing a BCP. Which ranking approach is illustrated in the graphic that follows?

Choose the following statement that best describes the effect on this business unit/cost center should there be an unplanned interruption of normal business operations.

- 8 hours** of an interruption. This business unit/cost center is **Vital**.
- 24 hours** of an interruption. This business unit/cost center is **Critical**.
- 3 days** of an interruption. This business unit/cost center is **Essential**.
- 5 days** of an interruption. This business unit/cost center is **Important**.
- 10 days** of an interruption. This business unit/cost center is **Noncritical**.
- 30 days** of an interruption. This business unit/cost center is **Deferrable**.

- A. Mean time to repair
B. Mean time between failures
C. Maximum critical downtime
D. Maximum tolerable downtime
- 30.** Sean has been hired as business continuity coordinator. He has been told by management that he needs to ensure that the company is in compliance with the ISO/IEC standard that pertains to technology readiness for business continuity. He has also been instructed to find a way to transfer the risk of being unable to carry out critical business functions for a period of time because of a disaster. Which of the following is most likely the standard that Sean has been asked to comply with?
- A. ISO/IEC 27031
B. ISO/IEC 27005
C. ISO/IEC BS7799
D. ISO/IEC 2899
- 31.** Which organization has been developed to deal with economic, social, and governance issues and with how sensitive data is transported over borders?
- A. European Union
B. Council of Europe
C. Safe Harbor
D. Organisation for Economic Co-operation and Development
- 32.** Widgets, Inc., wishes to protect its logo from unauthorized use. Which

of the following will protect the logo and ensure that others cannot copy and use it?

- A. Patent
 - B. Copyright
 - C. Trademark**
 - D. Trade secret
- 33.** Which of the following means that a company did all it could have reasonably done to prevent a security breach?
- A. Downstream liability
 - B. Responsibility
 - C. Due diligence
 - D. Due care**
- 34.** Which of the following is a U.S. copyright law that criminalizes the production and dissemination of technology, devices, or services that circumvent access control measures put into place to protect copyright material?
- A. Copyright law
 - B. Digital Millennium Copyright Act**
 - C. Federal Privacy Act
 - D. SOPA
- 35.** What role does the Internet Architecture Board play regarding technology and ethics?
- A. It creates criminal sentencing guidelines.
 - B. It issues ethics-related statements concerning the use of the Internet.**
 - C. It edits Request for Comments.
 - D. It maintains the Ten Commandments of Computer Ethics.
- 36.** As a CISSP candidate, you must sign a Code of Ethics. Which of the following is from the (ISC)² Code of Ethics for the CISSP?
- A. Information should be shared freely and openly; thus, sharing confidential information should be ethical.
 - B. Think about the social consequences of the program you are writing or the system you are designing.

- C. Act honorably, honestly, justly, responsibly, and legally.
 - D. Do not participate in Internet-wide experiments in a negligent manner.
37. Which of the following was the first international treaty seeking to address computer crimes by coordinating national laws and improving investigative techniques and international cooperation?
- A. Council of Global Convention on Cybercrime
 - B. Council of Europe Convention on Cybercrime**
 - C. Organisation for Economic Co-operation and Development
 - D. Organisation for Cybercrime Co-operation and Development
38. Lee is a new security manager who is in charge of ensuring that his company complies with the European Union Principles on Privacy when his company is interacting with their European partners. The set of principles that deals with transmitting data considered private is encompassed within which of the following laws or regulations?
- A. Data Protection Directive**
 - B. Organisation for Economic Co-operation and Development
 - C. Federal Private Bill
 - D. Privacy Protection Law
39. Brandy could not figure out how Sam gained unauthorized access to her system, since he has little computer experience. Which of the following is most likely the attack Sam used?
- A. Dictionary attack
 - B. Shoulder surfing attack**
 - C. Covert channel attack
 - D. Timing attack
40. Jane has been charged with ensuring that the privacy of clients' personal health information is adequately protected before it is exchanged with a new European partner. What data security requirements must she adhere to?
- A. HIPAA
 - B. NIST SP 800-66
 - C. Safe Harbor**

D. European Union Principles on Privacy

- 41.** Sue has been tasked with implementing a number of security controls, including antivirus and antispam software, to protect the company's e-mail system. What type of approach is her company taking to handle the risk posed by the system?
- A. Risk mitigation
B. Risk acceptance
C. Risk avoidance
D. Risk transference
- 42.** A number of factors should be considered when assigning values to assets. Which of the following is not used to determine the value of an asset?
- A. The asset's value in the external marketplace
B. The level of insurance required to cover the asset
C. The initial and outgoing costs of purchasing, licensing, and supporting the asset
D. The asset's value to the organization's production operations
- 43.** The Zachman Architecture Framework is often used to set up an enterprise security architecture. Which of the following does not correctly describe the Zachman Framework?
- A. A two-dimensional model that uses communication interrogatives intersecting with different levels
B. A security-oriented model that gives instructions in a modular fashion
C. Used to build a robust enterprise architecture versus a technical security architecture
D. Uses six perspectives to describe a holistic information infrastructure
- 44.** John has been told to report to the board of directors with a vendor-neutral enterprise architecture framework that will help the company reduce fragmentation that results from the misalignment of IT and business processes. Which of the following frameworks should he suggest?
- A. DoDAF

- B. CMMI**
- C. ISO/IEC 42010**
- D. TOGAF**

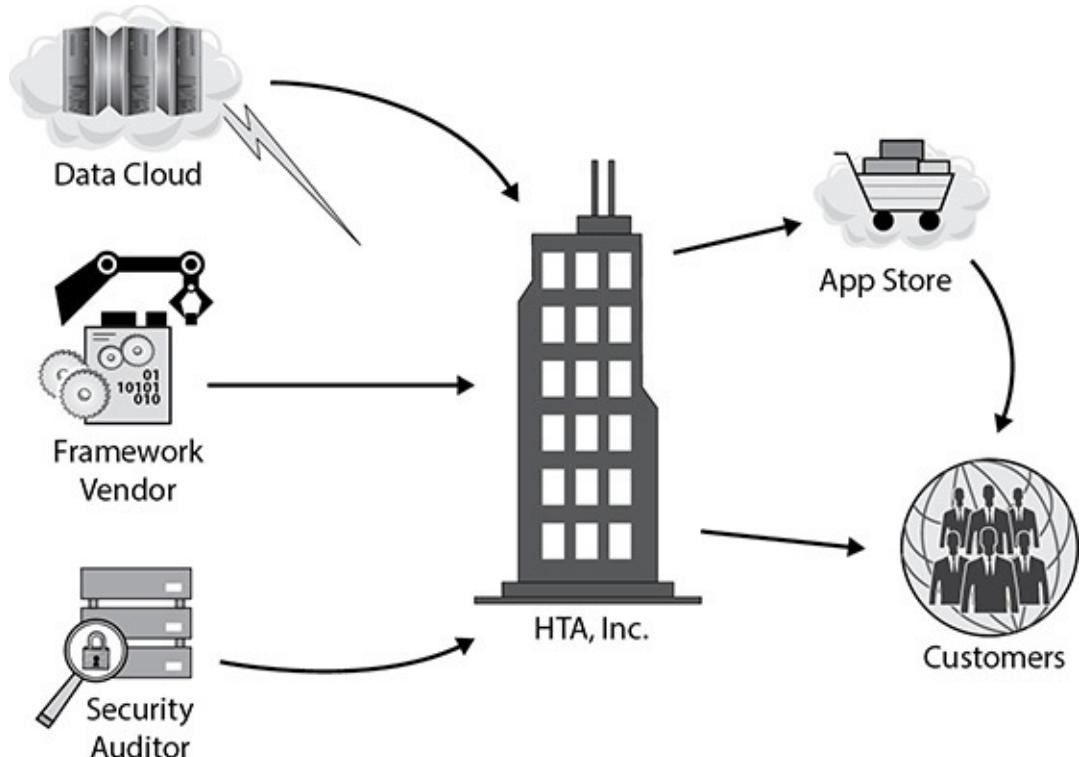
- 45.** The Information Technology Infrastructure Library (ITIL) consists of five sets of instructional books. Which of the following is considered the core set and focuses on the overall planning of the intended IT services?
- A. Service Operation**
 - B. Service Design**
 - C. Service Transition**
 - D. Service Strategy**
- 46.** Sarah and her security team have carried out many vulnerability tests over the years to locate the weaknesses and vulnerabilities within the systems on the network. The CISO has asked her to oversee the development of a threat model for the network. Which of the following best describes what this model is and what it would be used for?
- A. A threat model can help to assess the probability, the potential harm, and the priority of attacks, and thus help to minimize or eradicate the threats.**
 - B. A threat model combines the output of the various vulnerability tests and the penetration tests carried out to understand the security posture of the network as a whole.**
 - C. A threat model is a risk-based model that is used to calculate the probabilities of the various risks identified during the vulnerability tests.**
 - D. A threat model is used in software development practices to uncover programming errors.**

The following scenario applies to questions 47 through 51.

Health Tracking Apps, Inc. (HTA) is a U.S.-based corporation that develops and sells apps that its customers can use to track various aspects of their own health, from their daily exercise regimes to various medical test results and comparative statistics over time. These apps utilize cloud-based storage so that customers can access their data from multiple platforms, including smart mobile devices and desktop systems. Customers can also easily share the data the apps generate with their personal trainers and healthcare providers if they choose, on a subscription basis.

HTA's products are available in several languages, including English, French, Spanish, German, and Italian. All of HTA's software is developed by a dedicated staff within the United States, though HTA occasionally hires interns from the local university to assist with language translations for its various user interfaces.

The following entity relationship diagram illustrates HTA's business model dependencies:



47. Would HTA be required to comply with the General Data Protection Regulation (GDPR)? If so, why? If not, why?
1. Maybe, because HTA's HR records could contain protected privacy data about European citizens if any of HTA's interns are students studying from abroad.
 2. No, because the GDPR applies only to European-based companies.
 3. Yes, to the extent that HTA's stored private data includes that of any European customers.
 4. No, because any private data regarding European citizens that HTA's HR and customer records contain is stored within the United States.
- A. Statement 2 only
B. Statement 4 only

- C. Both statements 1 and 3
 - D. Statement 3 only
48. HTA's customer data is breached via a vulnerability in its application programming interface (API). This vulnerability is discovered to be a result of a recently announced security flaw in the underlying Java framework that HTA uses for the development of its apps. Which of the following best describes the root of this problem?
- A. HTA failed to manage risks associated with its supply chain.
 - B. HTA failed to apply a critical patch in a timely manner.
 - C. HTA stored critical/sensitive data in a cloud.
 - D. HTA chose a risky language and framework for its development.
49. HTA stores its customers' private data in a third-party cloud. What is the primary means through which HTA can ensure that its cloud service provider maintains compliance with any regulations—including the GDPR, if necessary—that HTA is subject to?
- A. Enforce an enterprise level agreement (ELA) that specifies how the service provider should conduct assurance activities.
 - B. Enforce a service level agreement (SLA) that specifies contractual penalties for the service provider's noncompliance.
 - C. Conduct an onsite inspection of the service provider's facilities to ensure they are compliant.
 - D. Review the service provider's security program.
50. Many of HTA's employees have either direct or indirect access to its customers' private data. HTA has to ensure that newly hired employees are aware of all security policies and procedures that apply to them, have only the necessary access through the accounts created for them, and have signed an agreement not to disclose the data inappropriately. Which of the following terms describes this process?
- A. Due diligence
 - B. Personnel security
 - C. Nondisclosure agreement (NDA)
 - D. Onboarding
51. HTA has an awareness program designed to educate all employees about security-relevant issues that apply to them, based on their role. IT

staff members are specifically instructed that it is important to be aware of new vulnerabilities as they are discovered, not only in the OSs that are used by HTA, but also in the applications and frameworks the developers use to build their software. The awareness program also stresses the importance of rapid mitigation by IT staff. As stated in question 48, HTA's customer data has been breached via a vulnerability in its API, a vulnerability discovered to be a result of a recently announced security flaw in the underlying Java framework that HTA uses for the development of its apps. Which of the following most likely contributed to the breach with respect to the security awareness program?

- A. HTA hasn't conducted periodic content reviews of the security awareness program.
- B. Assessment of the program's effectiveness has been insufficient.**
- C. Employees are improperly trained.
- D. The security awareness program was not relevant to the breach.

QUICK ANSWER KEY

- 1. C
- 2. B
- 3. D
- 4. A
- 5. D
- 6. C
- 7. D
- 8. C
- 9. B
- 10. A
- 11. D
- 12. A
- 13. C
- 14. B
- 15. D

16. B

17. C

18. D

19. B

20. A

21. C

22. D

23. B

24. A

25. B

26. C

27. A

28. B

29. D

30. A

31. D

32. C

33. D

34. B

35. B

36. C

37. B

38. A

39. B

40. C

41. A

42. B

43. B

44. D

45. D

46. A

47. C

48. A

49. B

50. D

51. B

ANSWERS

A

- 1.** Which of the following best describes the relationship between COBIT and ITIL?

 - A.** COBIT is a model for IT governance, whereas ITIL is a model for corporate governance.
 - B.** COBIT provides a corporate governance roadmap, whereas ITIL is a customizable framework for IT service management.
 - C.** COBIT defines IT goals, whereas ITIL provides the process-level steps on how to achieve them.
 - D.** COBIT provides a framework for achieving business goals, whereas ITIL defines a framework for achieving IT service-level goals.
- C.** The Control Objectives for Information and related Technology (COBIT) is a framework developed by ISACA (formerly the Information Systems Audit and Control Association) and the IT Governance Institute (ITGI). It defines goals for the controls that should be used to properly manage IT and to ensure IT maps to business needs, not specifically just security needs. The Information Technology Infrastructure Library (ITIL) is the de facto standard of best practices for IT service management. A customizable framework, ITIL provides the goals, the general activities necessary to achieve these goals, and the input and output values for each process required to meet these determined goals. In essence, COBIT addresses “what is to be achieved,” and ITIL addresses “how to achieve it.”
- A** is incorrect because, although COBIT can be used as a model for IT governance, ITIL is not a model for corporate governance. Actually, Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a model for corporate governance. COBIT

is derived from the COSO framework. You can think of COBIT as a way to meet many of the COSO objectives, but only from the IT perspective. In order to achieve many of the objectives addressed in COBIT, an organization can use ITIL, which provides process-level steps for achieving IT service management objectives.

- B** is incorrect because, as previously stated, COBIT can be used as a model for IT governance, not corporate governance. COSO is a model for corporate governance. The second half of the answer is correct. ITIL is a customizable framework that is available either as a series of books or online for IT service management.
 - D** is incorrect because COBIT defines goals for the controls that should be used to properly manage IT and ensure IT maps to business needs, not just IT security needs. ITIL provides steps for achieving IT service management goals as they relate to business needs. ITIL was created because of the increased dependence on information technology to meet business needs.
2. Global organizations that transfer data across international boundaries must abide by guidelines and transborder information flow rules developed by an international organization that helps different governments come together and tackle the economic, social, and governance challenges of a globalized economy. What organization is this?
- A. Committee of Sponsoring Organizations of the Treadway Commission
 - B. The Organisation for Economic Co-operation and Development**
 - C. COBIT
 - D. International Organization for Standardization
- B. Almost every country has its own rules pertaining to what constitutes private data and how it should be protected. As the digital and information age came upon us, these different laws started to negatively affect business and international trade. Thus, the Organisation for Economic Co-operation and Development (OECD) developed guidelines for various countries so that data is properly protected and everyone follows the same rules.**
 - A is incorrect because the Committee of Sponsoring Organizations of the Treadway Commission (COSO) was formed in 1985 to provide sponsorship for the National Commission on Fraudulent Financial Reporting, an organization that studies deceptive financial

reports and what elements lead to them. The acronym COSO refers to a model for corporate governance that addresses IT at a strategic level, company culture, financial accounting principles, and more.

- C** is incorrect because the Control Objectives for Information and related Technology (COBIT) is a framework that defines goals for the controls that should be used to properly manage IT and ensure that IT maps to business needs. It is an international open standard that provides requirements for the control and security of sensitive data and a reference framework.
 - D** is incorrect because the International Organization for Standardization (ISO) is an international standard-setting body consisting of representatives from national standards organizations. Its objective is to establish global standardizations. However, its standardizations go beyond the privacy of data as it travels across international borders. For example, some standards address quality control, and others address assurance and security.
3. Steve, a department manager, has been asked to join a committee that is responsible for defining an acceptable level of risk for the organization, reviewing risk assessment and audit reports, and approving significant changes to security policies and programs. What committee is he joining?
- A.** Security policy committee
 - B.** Audit committee
 - C.** Risk management committee
 - D. Security steering committee**
- D. Steve is joining a security steering committee, which is responsible for making decisions on tactical and strategic security issues within the enterprise. The committee should consist of individuals from throughout the organization and meet at least quarterly. In addition to the responsibilities listed in the question, the security steering committee is responsible for establishing a clearly defined vision statement that works with and supports the organizational intent of the business. It should provide support for the goals of availability, integrity, and confidentiality as they pertain to the organization's business objectives. This vision statement should, in turn, be supported by a mission statement that provides support and definition to the processes that will apply to the organization and allow it to reach its business goals.**

- A** is incorrect because a security policy committee is a committee chosen by senior management to produce security policies. Usually senior management has this responsibility unless they delegate it to a board or committee. Security policies dictate the role that security plays within the organization. They can be organizational, issue specific, or system specific. The steering committee does not directly create policies, but reviews and approves them if acceptable.
- B** is incorrect because the audit committee's goal is to provide independent and open communication among the board of directors, management, internal auditors, and external auditors. Its responsibilities include the company's system of internal controls, the engagement and performance of independent auditors, and the performance of the internal audit function. The audit committee would report its findings to the steering committee, but not be responsible for overseeing and approving any part of a security program.
- C** is incorrect because the purpose of a risk management committee is to understand the risks that the organization faces as a whole and work with senior management to reduce these risks to acceptable levels. This committee does not oversee the security program. The security steering committee usually reports its findings to the risk management committee as it relates to information security. A risk management committee must look at overall business risks, not just IT security risks.

4. Which of the following is not included in a risk assessment?

- A.** Discontinuing activities that introduce risk
 - B.** Identifying assets
 - C.** Identifying threats
 - D.** Analyzing risk in order of cost or criticality
- A.** Discontinuing activities that introduce risk is a way of responding to risk through avoidance. For example, there are many risks surrounding the use of instant messaging (IM) in the enterprise. If a company decides not to allow IM activity because there is not enough business need for its use, then prohibiting this service is an example of risk avoidance. Risk assessment does not include the implementation of countermeasures such as this.
- B** is incorrect because identifying assets is part of a risk assessment,

and the question asks to identify what is not included in a risk assessment. In order to determine the value of assets, those assets must first be identified. Asset identification and valuation are also important tasks of risk management.

- C** is incorrect because identifying threats is part of a risk assessment, and the question asks to identify what is not included in a risk assessment. Risk is present because of the possibility of a threat exploiting a vulnerability. If there were no threats, there would be no risk. Risk ties the vulnerability, threat, and likelihood of exploitation to the resulting business impact.
- D** is incorrect because analyzing risk in order of cost or criticality is part of the risk assessment process, and the question asks to identify what is not included in a risk assessment. A risk assessment researches and quantifies the risk a company faces. Dealing with risk must be done in a cost-effective manner. Knowing the severity of the risk allows the organization to determine how to address it effectively.

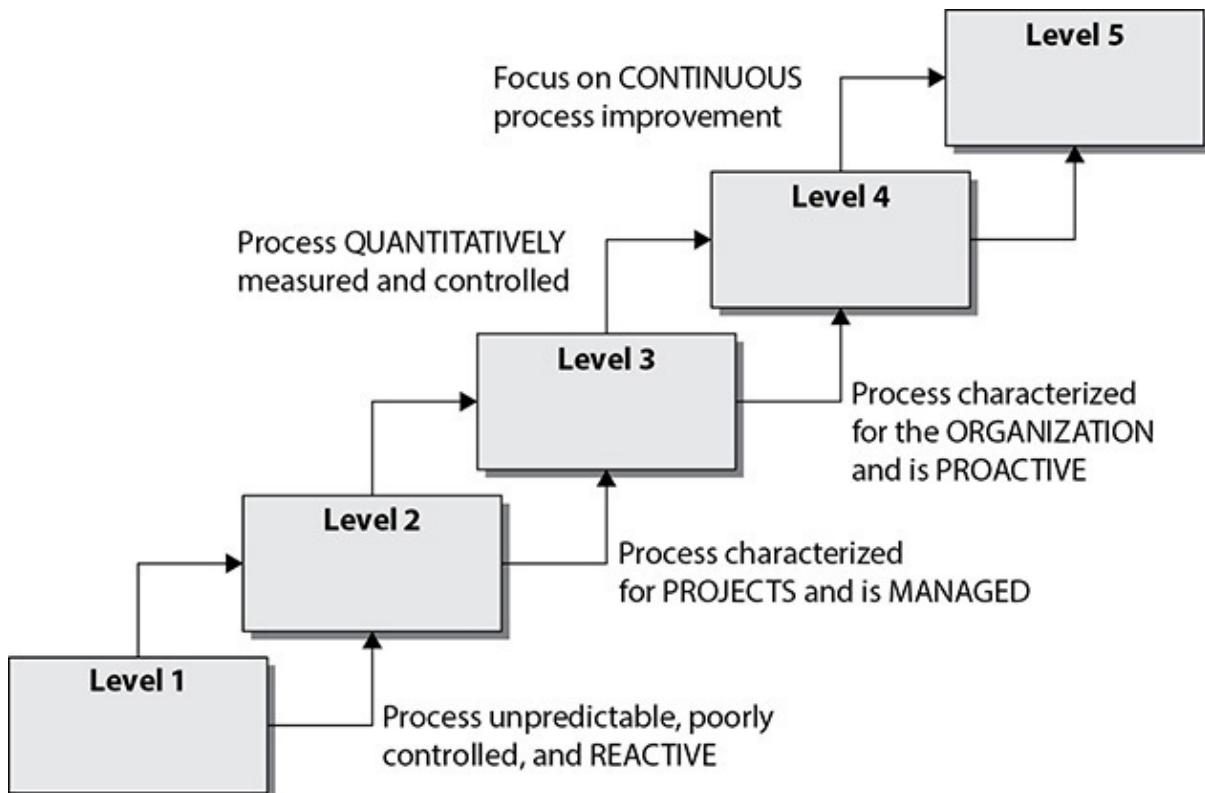
5. The integrity of data is not related to which of the following?

- A.** Unauthorized manipulation or changes to data
 - B.** The modification of data without authorization
 - C.** The intentional or accidental substitution of data
 - D.** The extraction of data to share with unauthorized entities
- D.** The extraction of data to share with unauthorized entities is a confidentiality issue, not an integrity issue. Confidentiality ensures that the necessary level of secrecy is enforced at each junction of data processing and prevents unauthorized disclosure. This level of secrecy should prevail while data resides on systems and devices within the network, as it is transmitted, and once it reaches its destination. Integrity, on the other hand, is the principle that signifies the data has not been changed or manipulated in an unauthorized manner.
 - A** is incorrect because integrity is related to the unauthorized manipulation or changes to data. Integrity is upheld when any unauthorized modification is prevented. Hardware, software, and communication mechanisms must work in concert to maintain and process data correctly and move data to intended destinations without unexpected alteration. The systems and network should be protected from outside interference and contamination.

- B** is incorrect because the modification of data without authorization is related to integrity. Integrity is about protecting data so that it cannot be changed either by users or other systems that do not have the rights to do so.
 - C** is incorrect because the intentional or accidental substitution of data is related to integrity. Along with the assurance that data is not modified by unauthorized entities, integrity is upheld when the assurance of the accuracy and reliability of the information and systems is provided. An environment that enforces integrity prevents attackers, for example, from inserting a virus, logic bomb, or back door into a system that could corrupt or replace data. Users usually affect a system or its data's integrity by mistake (although internal users may also commit malicious deeds). For example, a user may insert incorrect values into a data processing application that ends up charging a customer \$3,000 instead of \$300.
6. As his company's CISO, George needs to demonstrate to the board of directors the necessity of a strong risk management program. Which of the following should George use to calculate the company's residual risk?
- A. threats × vulnerability × asset value = residual risk
 - B. SLE × frequency = ALE, which is equal to residual risk
 - C. (threats × vulnerability × asset value) × controls gap = residual risk**
 - D. (total risk – asset value) × countermeasures = residual risk
- C. Countermeasures are implemented to reduce overall risk to an acceptable level. However, no system or environment is 100 percent secure, and with every countermeasure some risk remains. The leftover risk after countermeasures are implemented is called residual risk. Residual risk differs from total risk, which is the risk companies face when they choose not to implement any countermeasures. While the total risk can be determined by calculating threats × vulnerability × asset value = total risk, residual risk can be determined by calculating (threats × vulnerability × asset value) × controls gap = residual risk. The controls gap is the amount of protection the control cannot provide.**
 - A is incorrect because threats × vulnerability × asset value does not equal residual risk. It is the equation to calculate total risk. Total risk is the risk a company faces in the absence of any security safeguards or actions to reduce the overall risk exposure. The total

risk is reduced by implementing safeguards and countermeasures, leaving the company with residual risk—or the risk left over after safeguards are implemented.

- B** is incorrect because SLE × frequency is the equation to calculate the annualized loss expectancy (ALE) as a result of a threat exploiting a vulnerability and the business impact. The frequency is the threat's annual rate of occurrence (ARO). The ALE is not equal to residual risk. ALE indicates how much money a specific type of threat is likely to cost the company over the course of a year. Knowing the real possibility of a threat and how much damage in monetary terms the threat can cause is important in determining how much should be spent to try and protect against that threat in the first place.
 - D** is incorrect and is a distracter answer. There is no such formula like this used in risk assessments. The actual equations are threats × vulnerability × asset value = total risk and (threats × vulnerability × asset value) × controls gap = residual risk.
7. Capability Maturity Model Integration (CMMI) came from the software engineering world and is used within organizations to help lay out a pathway of how incremental improvement can take place. This model is used by organizations in self-assessment and to develop structured steps that can be followed so an organization can evolve from one level to the next and constantly improve its processes. In the CMMI model graphic shown, what is the proper sequence of the levels?



- A. Initial, Defined, Quantitatively Managed, Optimizing
 - B. Initial, Defined, Quantitatively Managed, Optimizing, Managed
 - C. Defined, Managed, Quantitatively Managed, Optimizing
 - D. Initial, Repeatable, Defined, Quantitatively Managed, Optimizing**
- D. Capability Maturity Model Integration (CMMI) is an organizational development model for process improvement developed by Carnegie Mellon. While organizations know that they need to constantly make their security programs better, it is not always easy to accomplish because “better” is a vague and nonquantifiable concept. The only way we can really improve is to know where we are starting from, where we need to go, and the steps we need to take in between. This is how the security industry uses the CMMI model. A security program starts at Level 1 and is chaotic in nature. Processes are not predictable, and the security team is reactive to issues that arise—not proactive. The model uses the following maturity levels: Initial, Repeatable, Defined, Managed, Optimizing.**
- A** is incorrect because it has the Defined level as the second level in the model. The actual second level is referred to as Managed. The developer of CMMI is Carnegie Mellon University, and they have modified this model to be used in three main categories: product

and service development (CMMI-DEV), service establishment management (CMMI-SVC), and product and service acquisition (CMMI-ACQ). You do not need to know this level of detail for the exam, but you should understand that this is a flexible model that can be used for different situations. The Managed level will be defined slightly differently based upon how the model is being used. Different entities have modified the basic CMMI model to map to organizational security programs. For example, ISACA has laid out a CMMI model showing how ISO 27000 standards can be accomplished and IT security governance can be practiced. The latest version of CMMI has included these security topics:

- **OPSD** Organizational Preparedness for Secure Development
- **SMP** Security Management in Projects
- **SRTS** Security Requirements and Technical Solution
- **SVV** Security Verification and Validation

- B** is incorrect because the Defined and Managed levels are out of order. It might be confusing at first as to why Managed (Level 2) comes before Defined (Level 3). Level 2 basically means that the organization is not just practicing security by the seat of its pants. It is managing the processes—the processes are not managing the organization. An organization can only be considered to be at Level 3 if it has defined many things that will be tracked. This is the first part of creating a meaningful metric system for process improvement and optimization. Defining things means putting useful data about the security program into formats that can be used in quantitative analysis.
- C** is incorrect because the order of levels is wrong. The correct order is Initial, Managed, Defined, Quantitatively Managed, Optimizing. Organizations can only be assessed and assigned a level starting at Level 2. Level 1 basically means that there is no coherent structure. Level 2 means the program is being managed, Level 3 means things that can be counted are created, Level 4 means the organization is counting things and using quantitative measures to grade their improvement, and Level 5 means that the organization has control over the security program as a whole and is now focused on just making things more optimized. This is a process improvement model, and these levels are considered maturity levels—as the security program improves, it can be evaluated and achieve a higher maturity level.

8. Risk assessment has several different methodologies. Which of the following official risk methodologies was not created for the purpose of analyzing security risks?

- A.** FAP
- B.** OCTAVE
- C.** AS/NZS 4360
- D.** NIST SP 800-30

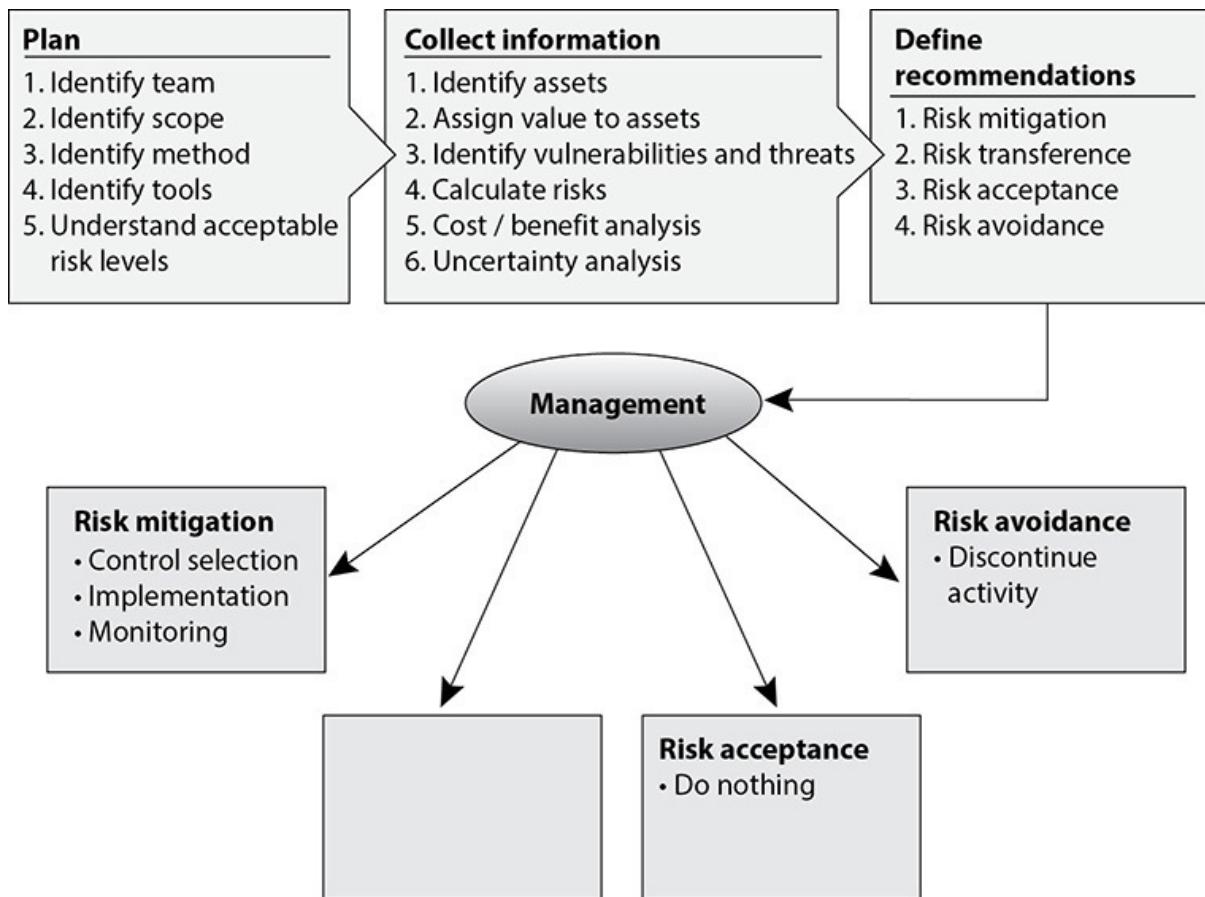
- C.** Although AS/NZS 4360 can be used to analyze security risks, it was not created for that purpose. It takes a much broader approach to risk management than other risk assessment methodologies, such as NIST and OCTAVE, which focus on IT threats and information security risks. AS/NZS 4360 can be used to understand a company's financial, capital, human safety, and business decisions risks.
- A** is incorrect because there is no formal FAP risk analysis approach. It is a distracter answer.
- B** is incorrect because OCTAVE focuses on IT threats and information security risks. OCTAVE is meant to be used in situations where people manage and direct the risk evaluation for information security within their organization. The organization's employees are given the power to determine the best approach for evaluating security.
- D** is incorrect because NIST SP 800-30 is specific to IT threats and how they relate to information security risks. It focuses mainly on systems. Data is collected from network and security practice assessments and from people within the organization. The data is then used as input values for the risk analysis steps outlined in the 800-30 document.

9. Which of the following is not a characteristic of a company with a security governance program in place?

- A.** Board members are updated quarterly on the company's state of security.
- B.** All security activity takes place within the security department.
- C.** Security products, services, and consultants are deployed in an informed manner.
- D.** The organization has established metrics and goals for improving security.

- B.** If all security activity takes place within the security department, then security is working within a silo and is not integrated throughout the organization. In a company with a security governance program, security responsibilities permeate the entire organization, from executive management down the chain of command. A common scenario would be executive management holding business unit managers responsible for carrying out risk management activities for their specific business units. In addition, employees are held accountable for any security breaches they participate in, either maliciously or accidentally.
- A** is incorrect because security governance is a set of responsibilities and practices exercised by the board and executive management of an organization with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately, and verifying that the organization's resources are used responsibly. An organization with a security governance program in place has a board of directors that understands the importance of security and is aware of the organization's security performance and breaches.
- C** is incorrect because security governance is a coherent system of integrated security components that includes products, personnel, training, processes, etc. Thus, an organization with a security governance program in place is likely to purchase and deploy security products, managed services, and consultants in an informed manner. They are also constantly reviewed to ensure they are cost effective.
- D** is incorrect because security governance requires performance measurement and oversight mechanisms. An organization with a security governance program in place continually reviews its processes, including security, with the goal of continued improvement. On the other hand, an organization that lacks a security governance program is likely to march forward without analyzing its performance and therefore repeatedly makes similar mistakes.

- 10.** There are four ways of dealing with risk. In the graphic that follows, which method is missing and what is the purpose of this method?

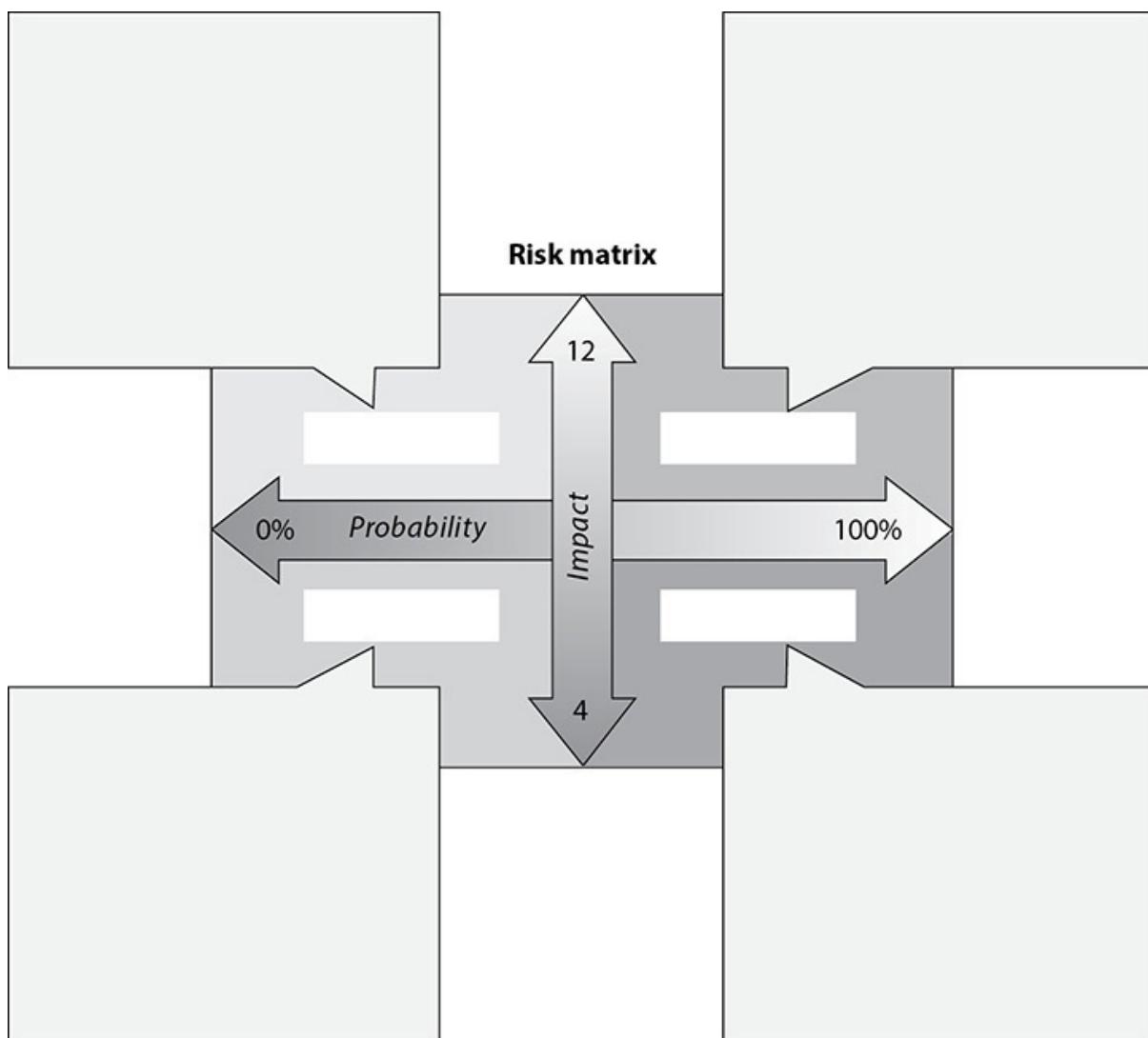


- A.** Risk transference. Share the risk with other entities.
- B.** Risk reduction. Reduce the risk to an acceptable level.
- C.** Risk rejection. Accept the current risk.
- D.** Risk assignment. Assign risk to a specific owner.
- A.** Once a company knows the amount of total and residual risk it is faced with, it must decide how to handle it. Risk can be dealt with in four basic ways: transfer it, avoid it, reduce it, or accept it. Many types of insurance are available to companies to protect their assets. If a company decides the total or residual risk is too high to gamble with, it can purchase insurance, which would transfer the risk to the insurance company.
- B** is incorrect because another approach is risk mitigation, where the risk is reduced to a level considered acceptable enough to continue conducting business. The implementation of firewalls, training, and intrusion/detection protection systems represent types of risk mitigation. Risk reduction is the same as risk mitigation, which is already listed in the graphic.
- C** is incorrect because companies should never reject risk, which basically means that they refuse to deal with it. Risk commonly has

a negative business impact, and if risk is not dealt with properly, the company could have to deal with things such as the loss of production resources, legal liability issues, or a negative effect on its reputation. It is important that identified risk be dealt with properly through transferring it, avoiding it, reducing it, or accepting it.

- D is incorrect because although someone could be delegated to deal with a specific risk, this is not one of the methods that is used to deal with risk. Even if risk was assigned to a specific entity to deal with it, she would still need to transfer, avoid, reduce, or accept the risk.

11. The following graphic contains a commonly used risk management scorecard. Identify the proper quadrant and its description.



- A. Top-right quadrant is high impact, low probability.
- B. Top-left quadrant is high impact, medium probability.

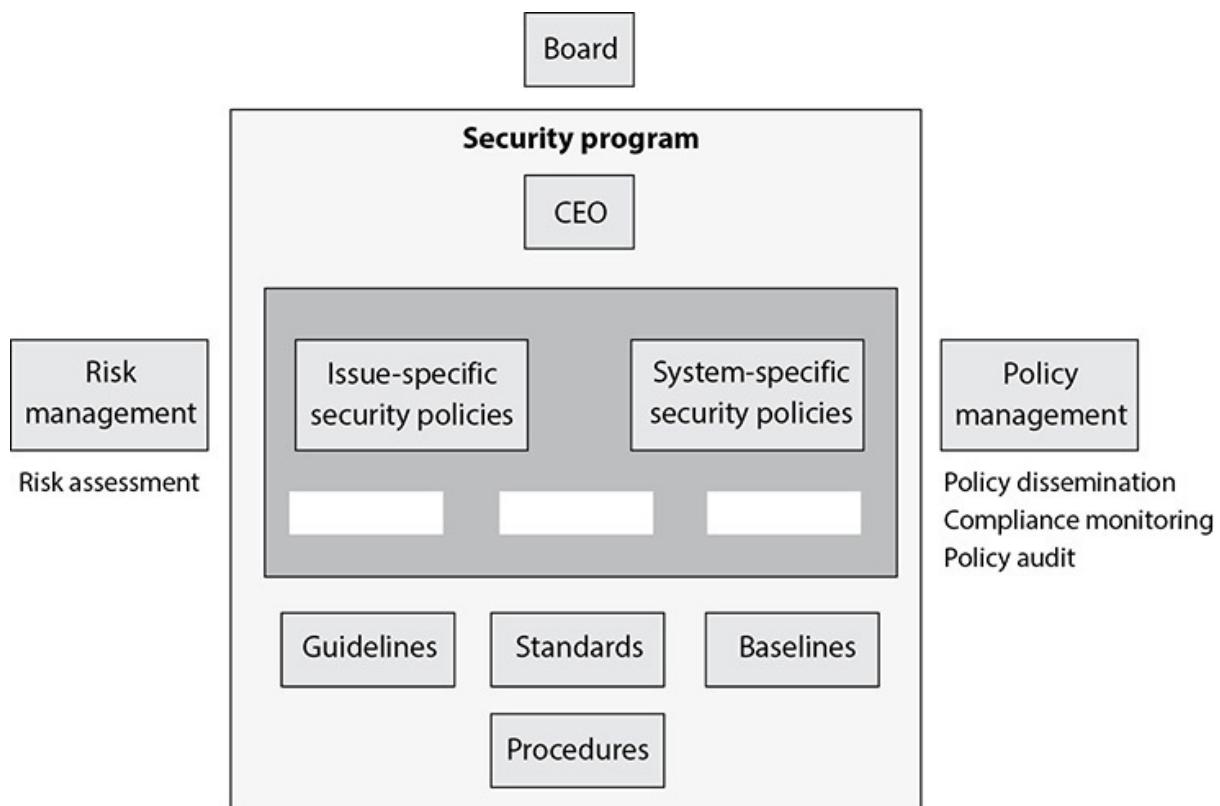
C. Bottom-left quadrant is low impact, high probability.

D. Bottom-right quadrant is low impact, high probability.

- D. The bottom-right quadrant contains low-impact, high-probability risks. This means that there is a high chance that specific threats will exploit specific vulnerabilities. Although these risks are commonly frequent, their business impact is low. Out of the four quadrants, the risks that reside in this quadrant should be dealt with after the risks that reside in the two higher quadrants. An example of a risk that could reside in this quadrant is a virus that infects a user workstation. Since viruses are so common, this would mean that this risk has a high probability of taking place. But since this is only a user workstation and not a production system, the impact would be low.**
- A** is incorrect because the top-right quadrant contains high-impact, high-probability risks. This means that there is a high chance that specific threats will exploit specific vulnerabilities. These risks are commonly frequent and their business impact is high. Out of the four quadrants, the risks that reside in this quadrant should be dealt with first. An example of a risk that would reside in this quadrant is an attacker compromising an internal mail server. If the proper countermeasures are not in place, there is a high probability that this would occur. Since this is a resource that the whole company depends upon, it would have a high business impact.
- B** is incorrect because the top-left quadrant contains high-impact, low-probability risks. This means that there is a low chance that specific threats will exploit specific vulnerabilities. These risks are commonly infrequent and their overall business impact is low. Out of the four quadrants, the risks that reside in this quadrant should be dealt with after the risks that reside in the top-right quadrant. An example of this type of risk is an attacker compromising an internal DNS server. If there is an external-facing DNS server and a DMZ is in place, the chances that an attacker being able to access an internal DNS server is low. But if this does happen, this would have a high business impact since all systems depend upon this resource.
- C** is incorrect because the bottom-left quadrant contains low-impact, low-probability risks. This means that there is a low chance that specific threats will exploit specific vulnerabilities. These risks are commonly infrequent and their business impact is low. Out of the four quadrants, the risks that reside in this quadrant should be dealt with after the risks in all of the other three quadrants. An example

of this type of risk would be a legacy file server that is hardly used failing and going offline. Since it is not commonly used by users, it would have a low business impact, and if the correct countermeasures are in place, there would be a low probability of this occurring.

12. What are the three types of policies that are missing from the following graphic?



- A. Regulatory, Informative, Advisory
- B. Regulatory, Mandatory, Advisory
- C. Regulatory, Informative, Public
- D. Regulatory, Informative, Internal Use

- A. A *Regulatory* type of policy ensures that the organization is following standards set by specific industry regulations. It is very detailed and specific to a type of industry. It is used in financial institutions, healthcare facilities, public utilities, and other government-regulated industries. An *Informative* type of policy informs employees of certain topics. It is not an enforceable policy, but rather one that teaches individuals about specific issues relevant to the company. It could explain how the company interacts with partners, indicate the company's goals and mission, and provide a general reporting structure in different situations. An *Advisory* type

of policy strongly advises employees as to which types of behaviors and activities should and should not take place within the organization. It also outlines possible ramifications if employees do not comply with the established behaviors and activities. This policy type can be used, for example, to describe how to handle medical information, how to handle financial transactions, or how to process confidential information.

- B** is incorrect because Mandatory is not one of the categories of a type of policy; thus, this answer is a distracter.
- C** is incorrect because Public is not one of the categories of a type of policy; thus, this answer is a distracter.
- D** is incorrect because Internal Use is not one of the categories of a type of policy; thus, this answer is a distracter.

- 13.** List in the proper order from the table shown the learning objectives that are missing and their proper definitions.

	Awareness	Training	Education
Attribute:	"What"	"How"	"Why"
Level:	Information	Knowledge	Insight
Learning objective:			
Example teaching method:	Media <ul style="list-style-type: none"> • Videos • Newsletters • Posters 	Practical instruction <ul style="list-style-type: none"> • Lecture and/or demo • Case study • Hands-on practice 	Theoretical instruction <ul style="list-style-type: none"> • Seminar and discussion • Reading and study • Research
Test measure:	True/False Multiple choice (Identify learning)	Problem solving, i.e., recognition and resolution (Apply learning)	Essay (Interpret learning)
Impact timeframe:	Short-term	Intermediate	Long-term

- A.** Understanding, recognition and retention, skill
- B.** Skill, recognition and retention, skill

C. Recognition and retention, skill, understanding

D. Skill, recognition and retention, understanding

- C. Awareness training and materials remind employees of their responsibilities pertaining to protecting company assets. Training provides skills needed to carry out specific tasks and functions. Education provides management skills and decision-making capabilities.**
- A** is incorrect because the different types of training and education do not map to the listed results. Companies today spend a lot of money on security devices and technologies, but they commonly overlook the fact that individuals must be trained to use these devices and technologies. Without such training, the money invested toward reducing threats can be wasted, and the company is still insecure.
- B** is incorrect because the different types of training and education do not map to the listed results. Different roles require different types of training or education. A skilled staff is one of the most critical components to the security of a company.
- D** is incorrect because the different types of training and education do not map to the listed results. A security awareness program is typically created for at least three types of audiences: management, staff, and technical employees. Each type of awareness training must be geared toward the individual audience to ensure each group understands its particular responsibilities, liabilities, and expectations.

14. What type of risk analysis approach does the following graphic provide?

High	7–10	7–10
Medium	4–6	4–6
Low	0–3	0–3

0	10	20	30	40	50	60	70	80	90	100
0	9	18	27	36	45	54	63	72	81	90
0	8	16	24	32	40	48	56	64	72	80
0	7	14	21	28	35	42	49	56	63	70
0	6	12	18	24	30	36	42	48	54	60
0	5	10	15	20	25	30	35	40	45	50
0	4	8	12	16	20	24	28	32	36	40
0	3	6	9	12	15	18	21	24	27	30
0	2	4	6	8	10	12	14	16	18	20
0	1	2	3	4	5	6	7	8	9	10

41–100	High
20–40	Medium
0–19	Low

A. Quantitative

B. Qualitative

C. Operationally Correct

D. Operationally Critical

B. A qualitative risk analysis approach does not assign monetary values to components and losses. Instead, qualitative methods walk through different scenarios of risk possibilities and rank the seriousness of the threats and the validity of the different possible countermeasures based on opinions. Qualitative analysis techniques include judgment, best practices, intuition, and experience. This graphic shows a rating system, which qualitative risk analysis uses instead of percentages and monetary numbers.

A is incorrect because a quantitative risk analysis attempts to assign percentages and monetary values to all elements of the risk analysis process. These elements may include safeguard costs, asset value, business impact, threat frequency, safeguard effectiveness, exploit probabilities, and so on. When all of these are quantified, the process is said to be quantitative. Each element within the analysis

(asset value, threat frequency, severity of vulnerability, impact damage, safeguard costs, safeguard effectiveness, uncertainty, and probability items) is quantified and entered into equations to determine total and residual risks.

- C** is incorrect because there is no Operationally Correct formal risk analysis approach. This is a distracter answer.
 - D** is incorrect because there is no formal Operationally Critical risk analysis approach. This is a distracter answer.
- 15.** ISO/IEC 27000 is part of a growing family of ISO/IEC information security management systems (ISMS) standards. It comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Which of the following provides an incorrect mapping of the individual standards that make up this family of standards?
- A.** ISO/IEC 27002: Code of practice for information security management
 - B.** ISO/IEC 27003: Guideline for ISMS implementation
 - C.** ISO/IEC 27004: Guideline for information security management measurement and metrics framework
 - D. ISO/IEC 27005: Guideline for bodies providing audit and certification of information security management systems**
- D. The ISO/IEC 27005 standard is the guideline for information security risk management. ISO/IEC 27005 is an international standard for how risk management should be carried out in the framework of an ISMS.**
 - A** is incorrect because ISO/IEC 27002 is the code of practice for information security management; thus, it has a correct mapping. ISO/IEC 27002 provides best practice recommendations and guidelines as they pertain to initiating, implementing, or maintaining an ISMS.
 - B** is incorrect because ISO/IEC 27003 is the guideline for ISMS implementation; thus, it has a correct mapping. It focuses on the critical aspects needed for successful design and implementation of an ISMS in accordance with ISO/IEC 27001:2013. It describes the process of ISMS specification and design from inception to the production of implementation plans.

- C is incorrect because ISO/IEC 27004 is the guideline for information security management measurement and metrics framework; thus, it has a correct mapping. It provides guidance on the development and use of measures and measurement in order to assess the effectiveness of an ISMS and controls or groups of controls, as specified in ISO/IEC 27001.

The following scenario applies to questions 16 and 17.

Sam is the security manager of a company that makes most of its revenue from its intellectual property. Sam has implemented a process improvement program that has been certified by an outside entity. His company received a Level 2 during an appraisal process, and he is putting in steps to increase this to a Level 3. A year ago when Sam carried out a risk analysis, he determined that the company was at too much of a risk when it came to potentially losing trade secrets. The countermeasure his team implemented reduced this risk, and Sam determined that the annualized loss expectancy of the risk of a trade secret being stolen once in a hundred-year period is now \$400.

- 16.** Which of the following is the criteria Sam's company was most likely certified under?
- A. SABSA
 - B. Capability Maturity Model Integration**
 - C. Information Technology Infrastructure Library
 - D. Prince2
- B. Capability Maturity Model Integration (CMMI)** is a process improvement approach that is used to help organizations improve their performance. The CMMI model may also be used as a framework for appraising the process maturity of the organization. The levels used in CMMI are Level 1–Initial, Level 2–Managed, Level 3–Defined, Level 4–Quantitatively Managed, and Level 5–Optimizing.
 - A is incorrect because Sherwood Applied Business Security Architecture (SABSA) is a model and methodology for the development of information security enterprise architectures. Since it is a framework, this means it provides a structure for individual architectures to be built from. Since it is a methodology also, this means it provides the processes to follow to build and maintain this architecture.
 - C is incorrect because the Information Technology Infrastructure

Library (ITIL) is the de facto standard of best practices for IT service management. ITIL was created because of the increased dependence on information technology to meet business needs. Although ITIL has a component that deals with security, its focus is more on internal service level agreements between the IT department and the “customers” it serves. The customers are usually internal departments. ITIL does not use the levels described in the scenario.

- D** is incorrect because PRINCE2 (PRojects IN Controlled Environments) is a process-based method for effective project management. It is commonly used by the UK government and is not a topic covered by the CISSP exam.
- 17.** What is the associated single loss expectancy value in this scenario?
 - A.** \$65,000
 - B.** \$400,000
 - C.** \$40,000
 - D.** \$4,000
- C.** The formula to calculate the annualized loss expectancy (ALE) value is single loss expectancy (SLE) \times annualized rate of occurrence (ARO). The formula to calculate the SLE is asset value \times exposure factor. In this scenario, if the ALE of the risk of a trade secret being stolen once in a hundred-year period is \$400, then you have to work backward to obtain the SLE value. If the ALE is \$400 and the ARO is 0.01, then the SLE is \$40,000.
- A** is incorrect because the formula to obtain the SLE is asset value \times exposure factor = SLE, and ALE is SLE \times ARO = ALE. If the ALE of the risk of a trade secret being stolen once in a hundred-year period is \$400, then you have to work backward to obtain the SLE value. If the ALE is \$400 and the ARO is 0.01, then the resulting SLE value is \$40,000.
- B** is incorrect because the formula to obtain the SLE is asset value \times exposure factor = SLE, and ALE is SLE \times ARO = ALE. In this scenario, the risk of an asset being stolen once in a hundred-year period is calculated at the ALE being \$400. If the ALE is \$400 and the ARO is 0.01, then the resulting SLE value is \$40,000.
- D** is incorrect because the formula to obtain the SLE is asset value \times exposure factor = SLE, and ALE is SLE \times ARO = ALE. The goal

of carrying out these calculations is to fully understand the criticality of specific risks and to know how much can be spent on implementing a countermeasure in a cost-effective manner.

- 18.** The NIST organization has defined best practices for creating continuity plans. Which of the following phases deals with identifying and prioritizing critical functions and systems?
- A. Identify preventive controls.
 - B. Develop the continuity planning policy statement.
 - C. Create contingency strategies.
 - D. Conduct the business impact analysis.
- D.** Although no specific scientific equation must be followed to create continuity plans, certain best practices have proven themselves over time. The National Institute of Standards and Technology (NIST) organization is responsible for developing many of these best practices and documenting them so that they are easily available to all. NIST outlines seven steps in its Special Publication 800-34 Rev 1, “Continuity Planning Guide for Federal Information Systems”: develop the continuity planning policy statement; conduct the business impact analysis; identify preventive controls; create contingency strategies; develop an information system contingency plan; ensure plan testing, training, and exercises; and ensure plan maintain. Conducting a business impact analysis involves identifying critical functions and systems and allowing the organization to prioritize them based on necessity. It also includes identifying vulnerabilities and threats and calculating risks.
- A** is incorrect because identifying preventive controls must be done after critical functions and systems have been prioritized and their vulnerabilities, threats, and risks identified—which is all part of the business impact analysis. Conducting a business impact analysis is step two of creating a continuity plan, and identifying preventive controls is step three.
- B** is incorrect because developing the continuity planning policy statement involves writing a policy that provides the guidance necessary to develop a business continuity plan and that assigns authority to the necessary roles to carry out these tasks. It is the first step in creating a business continuity plan and thus comes before identifying and prioritizing critical systems and functions, which is

part of the business impact analysis.

- C** is incorrect because creating contingency strategies involves formulating methods to ensure systems and critical functions can be brought online quickly. Before this can be done, a business impact analysis must be carried out to determine which systems and functions are critical and should be given priority during recovery.
- 19.** As his company's business continuity coordinator, Matthew is responsible for helping recruit members to the business continuity planning (BCP) committee. Which of the following does not correctly describe this effort?
 - A.** Committee members should be involved with the planning stages, as well as the testing and implementation stages.
 - B.** The smaller the team, the better to keep meetings under control.
 - C.** The business continuity coordinator should work with management to appoint committee members.
 - D.** The team should consist of people from different departments across the company.
- B.** The BCP committee should be as large as it needs to be in order to represent each department within the organization. The team must be composed of people who are familiar with the different departments within the company, because each department is unique in its functionality and has distinctive risks and threats. The best plan is developed when all issues and threats are brought to the table and discussed. This cannot be done effectively with a few people who are familiar with only a couple of departments. The committee should be made up of representatives from at least the following departments: business units, senior management, IT department, security department, communications department, and legal department.
- A** is incorrect because it is true that committee members should be involved with the planning stages, as well as the testing and implementation stages. If Matthew, the BCP coordinator, is a good management leader, he will understand that it is best to make team members feel a sense of ownership pertaining to their tasks and roles. The people who develop the BCP should also be the ones who execute it. If you knew that in a time of crisis you would be expected to carry out some critical tasks, you might pay more attention during the planning and testing phases.

- C** is incorrect because the BCP coordinator should work with management to appoint committee members. But management's involvement does not stop there. The BCP team should work with management to develop the ultimate goals of the plan, identify the critical parts of the business that must be dealt with first during a disaster, and ascertain the priorities of departments and tasks. Management also needs to help direct the team on the scope of the project and the specific objectives.
 - D** is incorrect because it is true that the team should be composed of people from different departments across the company. This is the only way the team will be able to consider the distinctive risks and threats that each department faces.
- 20.** A business impact analysis is considered a functional analysis. Which of the following is not carried out during a business impact analysis?
- A.** A parallel or full-interruption test
 - B.** The application of a classification scheme based on criticality levels
 - C.** The gathering of information via interviews
 - D.** Documentation of business functions
- A.** A business impact analysis (BIA) is considered a functional analysis, in which a team collects data through interviews and documentary sources; documents business functions, activities, and transactions; develops a hierarchy of business functions; and finally applies a classification scheme to indicate each individual function's criticality level. Parallel and full-interruption tests are not part of a BIA. These tests are carried out to ensure the continued validity of a business continuity plan, since environments continually change. A parallel test is done to ensure that specific systems can actually perform adequately at the alternate offsite facility, while a full-interruption test involves shutting down the original site and resuming operations and processing at the alternate site.
 - B** is incorrect because the application of a classification scheme based on criticality levels is carried out during a BIA. This is done by identifying the critical assets of the company and mapping them to the following characteristics: maximum tolerable downtime, operational disruption and productivity, financial considerations, regulatory responsibilities, and reputation.
 - C** is incorrect because the gathering of information during

interviews is conducted during a BIA. The BCP committee will not truly understand all business processes, the steps that must take place, or the resources and supplies those processes require. So the committee must gather this information from the people who do know, which are department managers and specific employees throughout the organization. The committee must identify the individuals who will provide information and how that information will be collected (surveys, interviews, or workshops).

- D** is incorrect because the BCP committee does document business functions as part of a BIA. Business activities and transactions must also be documented. This information is obtained from the department managers and specific employees who are interviewed or surveyed. Once the information is documented, the BCP committee can conduct an analysis to determine which processes, devices, or operational activities are the most critical.
- 21.** Which of the following steps comes first in a business impact analysis?
 - A.** Calculate the risk for each different business function.
 - B.** Identify critical business functions.
 - C.** Create data-gathering techniques.
 - D.** Identify vulnerabilities and threats to business functions.
- C.** Of the steps listed, the first step in a business impact analysis (BIA) is creating data-gathering techniques. The BCP committee can use surveys, questionnaires, and interviews to gather information from key personnel about how different tasks get accomplished within the organization, whether it's a process, transaction, or service, along with any relevant dependencies. Process flow diagrams should be built from this data, which will be used throughout the BIA and plan development stages.
- A** is incorrect because calculating the risk of each business function occurs after business functions have been identified. And before that can happen, the BCP team must gather data from key personnel. To calculate the risk of each business function, qualitative and quantitative impact information should be gathered and properly analyzed and interpreted. Upon completion of the data analysis, it should be reviewed with the most knowledgeable people within the company to ensure that the findings are appropriate and describe the real risks and impacts the organization faces. This will help flush out any additional data points not originally obtained and

will give a fuller understanding of all the possible business impacts.

- B** is incorrect because identifying critical business functions takes place after the BCP committee has learned about the business functions that exist by interviewing and surveying key personnel. Upon completion of the data collection phase, the BCP committee conducts an analysis to establish which processes, devices, or operational activities are critical. If a system stands on its own, doesn't affect other systems, and is of low criticality, then it can be classified as a tier-two or tier-three recovery step. This means these resources will not be dealt with during the recovery stages until the most critical (tier one) resources are up and running.
- D** is incorrect because identifying vulnerabilities and threats to business functions takes place toward the end of a business impact analysis. Of the steps listed in the answers, it is the last one. Threats can be manmade, natural, or technical. It is important to identify all possible threats and estimate the probability of them happening. Some issues may not immediately come to mind when developing these plans. These issues are often best addressed in a group with scenario-based exercises. This ensures that if a threat becomes a reality, the plan includes the ramifications on all business tasks, departments, and critical operations. The more issues that are thought of and planned for, the better prepared a company will be if and when these events occur.

- 22.** It is not unusual for business continuity plans to become out of date. Which of the following is not a reason why plans become outdated?
- A. Changes in hardware, software, and applications
 - B. Infrastructure and environment changes
 - C. Personnel turnover
 - D. That the business continuity process is integrated into the change management process
- D. Unfortunately, business continuity plans can become quickly out of date. An out-of-date BCP may provide a company with a false sense of security, which could be devastating if and when a disaster actually takes place. One of the simplest and most cost-effective and process-efficient ways to keep a plan up to date is to incorporate it within the change management process of the organization. When you think about it, it makes a lot of sense.
Where do you document new applications, equipment, or services?

Where do you document updates and patches? Your change management process should be updated to incorporate fields and triggers that alert the BCP team when a significant change will occur and should provide a means to update the recovery documentation. Other measures that can help ensure that the BCP remains current include the performance of regular drills that use the plan, including the plan's maintenance in personnel evaluations, and making business continuity a part of every business decision.

- A** is incorrect because changes in hardware, software, and applications occur frequently, and unless the BCP is part of the change management process, then these changes are unlikely to be included in the BCP. When changes to the environment take place, the BCP needs to be updated. If it is not updated after changes, it is out of date.
 - B** is incorrect because infrastructure and environment changes occur frequently. Just as with software, hardware, and application changes, unless the BCP is part of the change management process, infrastructure and environment changes are unlikely to make it into the BCP.
 - C** is incorrect because plans often become outdated as a result of personnel turnover. It is not unusual for a BCP to become abandoned when the person or people responsible for its maintenance leave the organization. These responsibilities must be reassigned. To ensure this happens, maintenance responsibilities should be incorporated into job descriptions and properly monitored.
- 23.** Preplanned business continuity procedures provide organizations a number of benefits. Which of the following is not a capability enabled by business continuity planning?
- A.** Resuming critical business functions
 - B.** Letting business partners know your company is unprepared
 - C.** Protecting lives and ensuring safety
 - D.** Ensuring survivability of the business
- B.** Preplanned business continuity procedures afford organizations a number of benefits. They allow an organization to provide an immediate and appropriate response to emergency situations, reduce business impact, and work with outside vendors during a recovery period—in addition to the other answer options listed

earlier. The efforts in these areas should be communicated to business partners to let them know that the company is prepared in case a disaster takes place.

- A** is incorrect because a business continuity plan allows an organization to resume critical business functions. As part of the BCP creation, the BCP team conducts a business impact analysis, which includes identifying the maximum tolerable downtime for critical resources. This effort helps the team prioritize recovery efforts so that the most critical resources can be recovered first.
 - C** is incorrect because a business continuity plan allows an organization to protect lives and ensure safety. People are a company's most valuable asset; thus, human resources are a critical component to any recovery and continuity process and need to be fully thought out and integrated into the plan. When this is done, a business continuity plan helps a company protect its employees.
 - D** is incorrect because a preplanned business continuity plan allows a company to ensure the survivability of the business. A business continuity plan provides methods and procedures for dealing with longer-term outages and disasters. It includes getting critical systems to another environment while the original facility is being repaired and conducting business operations in a different mode until regular operations are back in place. In short, the business continuity plan deals with how business is conducted during the aftermath of an emergency.
- 24.** Management support is critical to the success of a business continuity plan. Which of the following is the most important to be provided to management to obtain their support?
- A.** Business case
 - B.** Business impact analysis
 - C.** Risk analysis
 - D.** Threat report
- A.** The most critical part of establishing and maintaining a current continuity plan is management support. Management may need to be convinced of the necessity of such a plan. Therefore, a business case must be made to obtain this support. The business case may include current vulnerabilities, regulatory and legal obligations, the current status of recovery plans, and recommendations. Management is commonly most concerned with cost/benefit issues,

so preliminary numbers can be gathered and potential losses estimated. The decision of how a company should recover is a business decision and should always be treated as such.

- B** is incorrect because a business impact analysis (BIA) is conducted after the BCP team has obtained management's support for their efforts. A BIA is performed to identify the areas that would suffer the greatest financial or operational loss in the event of a disaster or disruption. It identifies the company's critical systems needed for survival and estimates the outage time that can be tolerated by the company as a result of a disaster or disruption.
 - C** is incorrect because a risk analysis is a method of identifying risks and assessing the possible damage that could be caused in order to justify security safeguards. In the context of BCP, risk analysis methodologies are used during a BIA to establish which processes, devices, or operational activities are critical and should therefore be recovered first.
 - D** is incorrect because threat report is a distracter answer. However, it is critical that management understand what the real threats are to the company, the consequences of those threats, and the potential loss values for each threat. Without this understanding, management may only give lip service to continuity planning, and in some cases that is worse than not having any plans at all because of the false sense of security that it creates.
- 25.** Which of the following is a critical first step in disaster recovery and contingency planning?
- A.** Plan testing and drills.
 - B.** Complete a business impact analysis.
 - C.** Determine offsite backup facility alternatives.
 - D.** Organize and create relevant documentation.
- B.** Of the steps listed in this question, completing a business impact analysis would take the highest priority. The BIA is essential in determining the most critical business functions and identifying the threats that correlate to them. Qualitative and quantitative data needs to be gathered, analyzed, interpreted, and presented to management.
 - A** is incorrect because plan testing and drills are some of the last steps in disaster recovery and contingency planning. It is important

to test the business continuity plan regularly because environments continually change. Tests and disaster recovery drills and exercises should be performed at least once a year. Most companies cannot afford for these exercises to interrupt production or productivity, so the exercises may need to take place in sections or at specific times, which requires logistical planning.

- C** is incorrect because determining offsite backup facility alternatives is part of the contingency strategy, which takes place in the middle of the disaster recovery and contingency planning process. Organizations must have alternative offsite backup facilities in the case of a larger disaster. Generally, contracts are established with third-party vendors to provide such services. The client pays a monthly fee to retain the right to use the facility in a time of need and then incurs an activation fee when the facility has to be used.
 - D** is incorrect because organizing and creating relevant documentation takes place toward the end of the disaster recovery and contingency planning process. Procedures need to be documented because when they are actually needed, it will most likely be a chaotic and frantic atmosphere with a demanding time schedule. The documentation may need to include information on how to install images, configure operating systems and servers, and properly install utilities and proprietary software. Other documentation could include a calling tree and contact information for specific vendors, emergency agencies, offsite facilities, etc.
- 26.** Which of the following is not a reason to develop and implement a disaster recovery plan?
- A.** Provide steps for a post-disaster recovery.
 - B.** Extend backup operations to include more than just backing up data.
 - C.** Outline business functions and systems.
 - D.** Provide procedures for emergency responses.
- C.** Outlining business functions and systems is not a viable reason to create and implement a disaster recovery plan. Although these tasks will most likely be accomplished as a result of a disaster recovery plan, it is not a good reason to carry out the plan compared to the other answers in the question. You don't develop and implement a disaster recovery plan just to outline business functions and

systems, although that usually takes place during the planning process.

- A** is incorrect because providing steps for a post-disaster recovery is a good reason to develop and implement a disaster recovery plan. In fact, that is exactly what a disaster recovery plan provides. The goal of disaster recovery is to minimize the effects of a disaster and take the necessary steps to ensure that the resources, personnel, and business processes are able to resume operation in a timely manner. The goal of a disaster recovery plan is to handle the disaster and its ramifications right after the disaster hits.
- B** is incorrect because extending backup operations to include more than just backing up data is a good reason to develop and implement a disaster recovery plan. When looking at disaster recovery plans, some companies focus mainly on backing up data and providing redundant hardware. Although these items are extremely important, they are just small pieces of the company's overall operations. Hardware and computers need people to configure and operate them, and data is usually not useful unless it is accessible by other systems and possibly outside entities. All of these things can require backups, not just data.
- D** is incorrect because providing procedures for emergency responses is a good reason to develop and implement a disaster recovery plan. A disaster recovery plan is carried out when everything is still in emergency mode and everyone is scrambling to get all critical systems back online. Having well-thought-out written procedures makes this whole process much more effective.

27. With what phase of a business continuity plan does a company proceed when it is ready to move back into its original site or a new site?

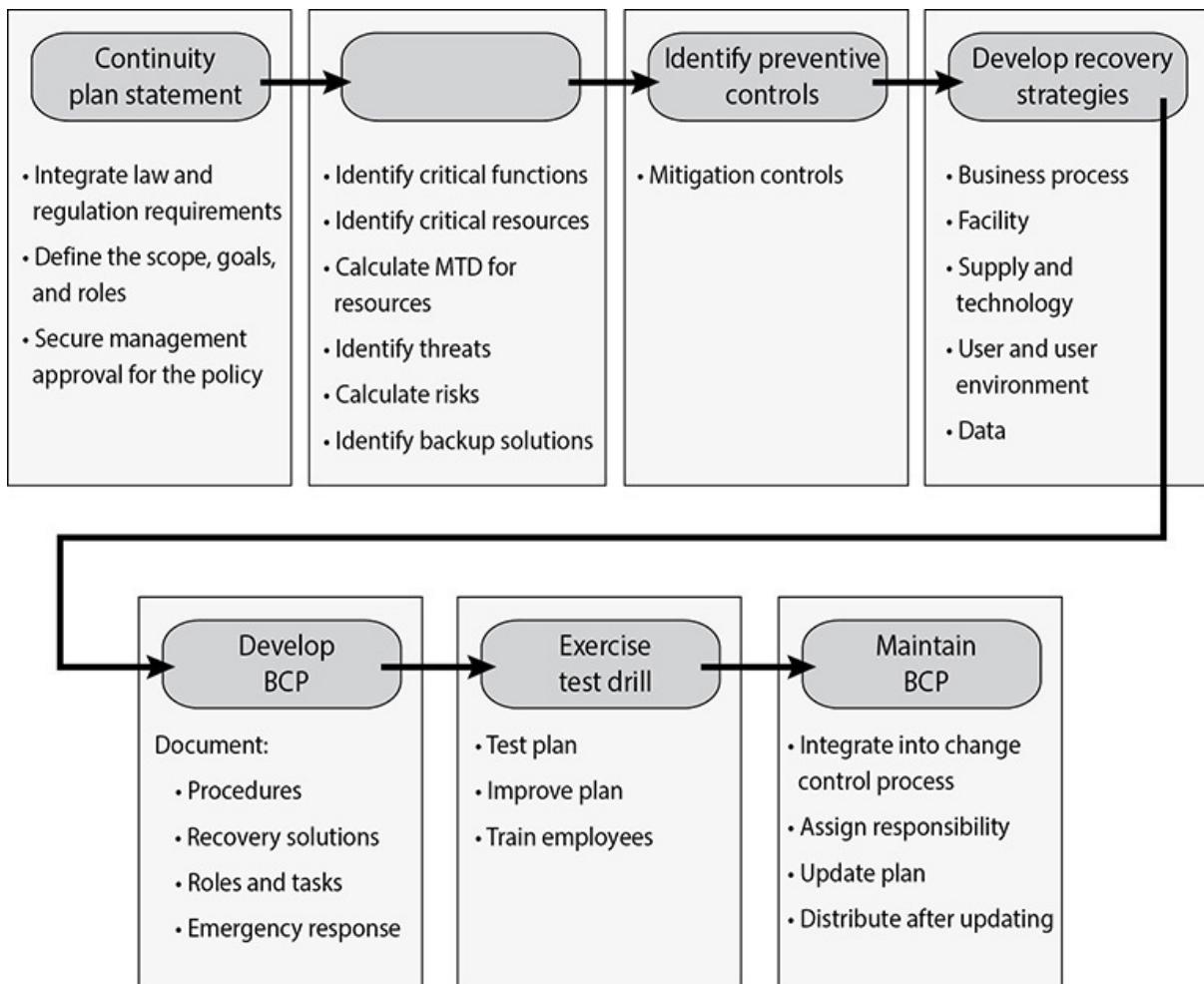
- A.** Reconstitution phase
- B.** Recovery phase
- C.** Project initiation phase
- D.** Damage assessment phase

- A.** When it is time for the company to move back into its original site or a new site, the company is ready to enter into the reconstitution phase. A company is not out of an emergency state until it is back in operation at the original primary site or a new site that was constructed to replace the primary site, because the company is always vulnerable while operating in a backup facility.

Many logistical issues need to be considered as to when a company must return from the alternate site to the original site. Some of these issues include ensuring the safety of the employees, ensuring proper communications and connectivity methods are working, and properly testing the new environment. Once the coordinator, management, and salvage team sign off on the readiness of the facility, the salvage team should back up data from the alternate site and restore it within the new facility, carefully terminate contingency operations, and securely transport equipment and personnel to the new facility.

- B** is incorrect because the recovery phase includes the preparation of the offsite facility (if needed), the rebuilding of the network and systems, and the organization of staff to move into a new facility. The recovery process needs to be as organized as possible to get the company up and running as soon as possible. Templates should be developed during the plan development stage that can be used by the different teams during the recovery phase to step them through the necessary phases and to document their findings. The templates keep the teams on task and quickly tell the team leaders about the progress, obstacles, and potential recovery time.
- C** is incorrect because the project initiation phase is how the actual planning of the business continuity plan begins. It does not occur during the execution of the plan. The project initiation phase involves getting management support, developing the scope of the plan, and securing funding and resources.
- D** is incorrect because the damage assessment takes place at the start of actually carrying out the business continuity procedures. A damage assessment helps determine whether the business continuity plan should be put into action based on activation criteria predefined by the BCP coordinator and team. After the damage assessment, if one or more of the situations outlined in the criteria have taken place, then the team is moved into recovery mode.

28. What is the missing second step in the graphic that follows?



- A. Identify continuity coordinator
- B. Business impact analysis
- C. Identify BCP committee
- D. Dependency identification
- B. A business impact analysis (BIA) is considered a functional analysis, in which a team collects data through interviews and documentary sources; documents business functions, activities, and transactions; develops a hierarchy of business functions; and finally applies a classification scheme to indicate each individual function's criticality level. It is one of the most important first steps in the planning development of a business continuity plan (BCP). Qualitative and quantitative data need to be gathered, analyzed, interpreted, and presented to management. Identifying critical functions and systems allow the organization to prioritize them based on necessity.
- A is incorrect because the business continuity coordinator needs to be put into position before this whole process starts. He will be the

leader for the BCP team and will oversee the development, implementation, and testing of the continuity and disaster recovery plans. The coordinator should be identified in the project initiation and oversee all the steps shown in the graphic. It is best if this person has good social skills and is somewhat of a politician because he will need to coordinate a lot of different departments and busy individuals who have their own agendas. This person needs to have direct access to management and have the credibility and authority to carry out leadership tasks.

- C** is incorrect because a BCP committee needs to be put together after the coordinator is identified to help carry out all the steps in the graphic. Management and the coordinator should work together to appoint specific qualified people to be on this committee. The team must be composed of people who are familiar with the different departments within the company, because each department is unique in its functionality and has distinctive risks and threats. The best plan is when all issues and threats are brought to the table and discussed. This cannot be done effectively with a few people who are familiar with only a couple of departments. Representatives from each department must be involved with not only the planning stages but also the testing and implementation stages.
- D** is incorrect because dependencies between company-critical functions and resources are carried out during the BIA. This is only one of the components in the overall BIA process. Identifying these types of dependencies is critical because it is important to look at a company as a complex animal instead of a static two-dimensional entity. It comprises many types of equipment, people, tasks, departments, communications mechanisms, and interfaces to the outer world. The biggest challenge of true continuity planning is understanding all of these intricacies and their interrelationships. A team may develop plans to back up and restore data, implement redundant data processing equipment, educate employees on how to carry out automated tasks manually, and obtain redundant power supplies. But if all of these components don't know how to work together in a different environment to get the products out the door, it might all be a waste of time.

- 29.** Different threats need to be evaluated and ranked based upon their severity of business risk when developing a BCP. Which ranking approach is illustrated in the graphic that follows?

Choose the following statement that best describes the effect on this business unit/cost center should there be an unplanned interruption of normal business operations.

- 8 hours** of an interruption. This business unit/cost center is **Vital**.
- 24 hours** of an interruption. This business unit/cost center is **Critical**.
- 3 days** of an interruption. This business unit/cost center is **Essential**.
- 5 days** of an interruption. This business unit/cost center is **Important**.
- 10 days** of an interruption. This business unit/cost center is **Noncritical**.
- 30 days** of an interruption. This business unit/cost center is **Deferrable**.

- A. Mean time to repair
 - B. Mean time between failures
 - C. Maximum critical downtime
 - D. Maximum tolerable downtime
- D. The BIA identifies which of the company's critical systems are needed for survival and estimates the outage time that can be tolerated by the company as a result of various unfortunate events. The outage time that can be endured by a company is referred to as the maximum tolerable downtime (MTD). This is the timeframe between an unplanned interruption of business operations and the resumption of business at a reduced level of service. During the BIA, the BCP team identifies the maximum tolerable downtime for the critical resources. This is done to understand the business impact that would be caused if the assets were unavailable for one reason or another.
- A is incorrect because the mean time to repair (MTTR) is the amount of time it will be expected to take to get a device fixed and back into production. For a hard drive in a redundant array, the MTTR is the amount of time between the actual failure and the time when, after noticing the failure, someone has replaced the failed drive and the redundant array has completed rewriting the information on the new drive. This is likely to be measured in hours. For an unplanned reboot, the MTTR is the amount of time between the failure of the system and the point in time when it has rebooted its operating system, checked the state of its disks (hopefully finding nothing that its file systems cannot handle), restarted its applications, allowed its applications to check the

consistency of their data (hopefully finding nothing that their journals cannot handle), and once again begun processing transactions. For well-built hardware running high-quality, well-managed operating systems and software, this may be only minutes. For commodity equipment without high-performance journaling file systems and databases, this may be hours, or, worse, days if automated recovery/rollback does not work and a restore of data from tape is required.

- B** is incorrect because the mean time between failures (MTBF) is the estimated lifespan of a piece of equipment. MTBF is calculated by the vendor of the equipment or a third party. The reason for using this value is to know approximately when a particular device will need to be replaced. Either based on historical data or scientifically estimated by vendors, it is used as a benchmark for reliability by predicting the average time that will pass in the operation of a component or a system until its final death. Organizations trending MTBF over time for the device they use may be able to identify types of devices that are failing above the averages promised by manufacturers and take action, such as proactively contacting manufacturers under warranty or deciding that old devices are reaching the end of their useful life and choosing to replace them en masse before larger-scale failures and operational disruptions occur.
 - C** is incorrect because maximum critical downtime is not an official term used in BCP and is a distracter answer.
- 30.** Sean has been hired as business continuity coordinator. He has been told by management that he needs to ensure that the company is in compliance with the ISO/IEC standard that pertains to technology readiness for business continuity. He has also been instructed to find a way to transfer the risk of being unable to carry out critical business functions for a period of time because of a disaster. Which of the following is most likely the standard that Sean has been asked to comply with?
- A.** ISO/IEC 27031
 - B.** ISO/IEC 27005
 - C.** ISO/IEC BS7799
 - D.** ISO/IEC 2899
- A.** ISO/IEC 27031:2011 is a set of guidelines for information and communications technology readiness for business continuity. It is a

component of the overall ISO/IEC 27000 series.

- B** is incorrect because the purpose of ISO/IEC 27005 is to provide guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. This standard deals with developing a formal risk management approach and not necessarily continuity issues.
 - C** is incorrect because this is a distracter answer. There is no official standard called ISO/IEC BS7799.
 - D** is incorrect because this is a distracter answer. There is no official standard called ISO/IEC 2899.
- 31.** Which organization has been developed to deal with economic, social, and governance issues and with how sensitive data is transported over borders?
- A.** European Union
 - B.** Council of Europe
 - C.** Safe Harbor
 - D.** Organisation for Economic Co-operation and Development
- D.** Global organizations that move data across other country boundaries must be aware of and follow the Organisation for Economic Co-operation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Since most countries have a different set of laws pertaining to the definition of private data and how it should be protected, international trade and business gets more convoluted and can negatively affect the economy of nations. The OECD is an international organization that helps different governments come together and tackle the economic, social, and governance challenges of a globalized economy. Because of this, the OECD came up with guidelines for the various countries to follow so that data is properly protected and everyone follows the same type of rules. One of these rules is that subjects should be able to find out whether an organization has their personal information and, if so, what that information is, to correct erroneous data, and to challenge denied requests to do so.
 - A** is incorrect because the European Union is not an organization

that deals with economic, social, and governance issues, but does address the protection of sensitive data. The European Union Principles on Privacy are as follows: The reason for the gathering of data must be specified at the time of collection; data cannot be used for other purposes; unnecessary data should not be collected; data should only be kept for as long as it is needed to accomplish the stated task; only the necessary individuals who are required to accomplish the stated task should be allowed access to the data; and whoever is responsible for securely storing the data should not allow unintentional “leaking” of data.

- B** is incorrect because the Council of Europe is responsible for the creation of the Convention on Cybercrime. The Council of Europe Convention on Cybercrime is one example of an attempt to create a standard international response to cybercrime. In fact, it is the first international treaty seeking to address computer crimes by coordinating national laws and improving investigative techniques and international cooperation. The convention’s objectives include the creation of a framework for establishing jurisdiction and extradition of the accused. For example, extradition is only available by treaty and when the event is a crime in both jurisdictions.
- C** is incorrect because Safe Harbor is not an organization but a set of requirements for organizations that wish to exchange data with European entities. Europe has always had tighter control over protecting privacy information than the United States and other parts of the world. So in the past when U.S. and European companies needed to exchange data, confusion erupted and business was interrupted because the lawyers had to get involved to figure out how to work within the structures of the differing laws. To clear up this mess, a “safe harbor” framework was created, which outlines how any entity that is going to move privacy data to and from Europe must go about protecting it. U.S. companies that deal with European entities can become certified against this rule base so data transfer can happen more quickly and easily.

32. Widgets, Inc., wishes to protect its logo from unauthorized use. Which of the following will protect the logo and ensure that others cannot copy and use it?

- A.** Patent
- B.** Copyright

C. Trademark

D. Trade secret

- C.** Intellectual property can be protected by several different laws, depending upon the type of resource it is. A trademark is used to protect a word, name, symbol, sound, shape, color, or combination of these—such as a logo. The reason a company would trademark one of these, or a combination, is that it represents their company (brand identity) to a group of people or to the world. Companies have marketing departments that work very hard to create something new that will cause the company to be noticed and stand out in a crowd of competitors, and trademarking the result of this work with a government registrar is a way of properly protecting it and ensuring others cannot copy and use it.
- A** is incorrect because a patent covers an invention, whereas a trademark protects a word, name, symbol, sound, shape, color, or combination thereof. Patents are given to individuals or companies to grant them legal ownership of, and enable them to exclude others from using or copying, the invention covered by the patent. The invention must be novel, useful, and not obvious. A patent is the strongest form of intellectual property protection.
- B** is incorrect because in the United States, copyright law protects the right the creator of an original work to control the public distribution, reproduction, display, and adaptation of that original work. The law covers many categories of work: pictorial, graphic, musical, dramatic, literary, pantomimes, motion picture, sculptural, sound recording, and architectural. Copyright law does not cover the specific resource. It protects the expression of the idea of the resource instead of the resource itself. A copyright law is usually used to protect an author's writings, an artist's drawings, a programmer's source code, or specific rhythms and structures of a musician's creation.
- D** is incorrect because trade secret law protects certain types of information or resources from unauthorized use or disclosure. A trade secret is something that is proprietary to a company and important for its survival and profitability. For a company to have its resource qualify as a trade secret, the resource must provide the company with some type of competitive value or advantage. A trade secret can be protected by law if developing it requires special skill, ingenuity, and/or expenditure of money and effort.

- 33.** Which of the following means that a company did all it could have reasonably done to prevent a security breach?
- A. Downstream liability
 - B. Responsibility
 - C. Due diligence
 - D. Due care
- D.** Due care means that a company did all it could have reasonably done, under the circumstances, to prevent security breaches and took reasonable steps to ensure that if a security breach did take place, proper controls or countermeasures were in place to mitigate the damages. In short, due care means that a company practiced common sense and prudent management and acted responsibly. If a company has a facility that burns to the ground, the arsonist is only one small piece of this tragedy. The company is responsible for providing fire detection and suppression systems, fire-resistant construction material in certain areas, alarms, exits, fire extinguishers, and backups of all the important information that could be affected by a fire. If a fire burns a company's building to the ground and consumes all the records (customer data, inventory records, and similar information that is necessary to rebuild the business), then the company did not exercise due care to ensure it was protected from such loss (by backing up to an offsite location, for example). In this case, the employees, shareholders, customers, and everyone affected could potentially successfully sue the company. However, if the company did everything expected of it in the previously listed respects, it is harder to successfully sue for failure to practice due care.
- A** is incorrect because downstream liability means that one company's activities—or lack of them—can negatively affect another company. If one of the companies does not provide the necessary level of protection and its negligence affects a partner it is working with, the affected company can sue the upstream company. For example, let's say company A and company B have constructed an extranet. Company A does not put in controls to detect and deal with viruses. Company A gets infected with a destructive virus, which is spread to company B through the extranet. The virus corrupts critical data and causes a massive disruption to company B's production. Therefore, company B can sue company A for being negligent. This is an example of downstream liability.

- B** is incorrect because responsibility generally refers to the obligations and expected actions and behaviors of a particular party. An obligation may have a defined set of specific actions that are required or a more general and open approach, which enables the party to decide how it will fulfill the particular obligation. Due diligence is a better answer to this question. Responsibility is not considered a legal term, as the other answers are.
 - C** is incorrect because due diligence means that the company properly investigated all of its possible weaknesses and vulnerabilities. Before you can figure out how to properly protect yourself, you need to find out what it is you are protecting yourself against. This is what due diligence is all about—researching and assessing the current level of vulnerabilities so that the true risk level is understood. Only after these steps and assessments take place can effective controls and safeguards be identified and implemented. Due diligence means identifying all of the potential risks, whereas due care means actually doing something to mitigate those risks.
- 34.** Which of the following is a U.S. copyright law that criminalizes the production and dissemination of technology, devices, or services that circumvent access control measures put into place to protect copyright material?
- A.** Copyright law
 - B.** Digital Millennium Copyright Act
 - C.** Federal Privacy Act
 - D.** SOPA
- B.** The Digital Millennium Copyright Act (DMCA) is a U.S. copyright law that criminalizes the production and dissemination of technology, devices, or services that circumvent access control measures that are put into place to protect copyright material. So if you figure out a way to “unlock” the proprietary way that Barnes & Noble protects its e-books, you can be charged under this act. Even if you don’t share the actual copyright-protected books with someone, you still broke this specific law and can be found guilty. The United States already had a copyright protection law on the books that grants the creator of an original work exclusive rights to its use and distribution, with the goal of allowing the creator to receive compensation for their work. As copyright-protected works were distributed more and more in the digital world, the industry

needed a way to implement access control of these works to ensure only the authorized individuals had access to it. Various digital rights management (DRM) technologies were developed and deployed to protect these works, which were quickly hacked and compromised, allowing unauthorized access to copyright-protected content. The DMCA was created to make the breaking of these DRM technologies illegal.

- ☒ **A** is incorrect because the copyright law has nothing to do with circumventing access controls. Copyright is a form of intellectual property protection that grants the creator of an original work exclusive rights to its use and distribution, usually for a limited time, to allow the creator to receive compensation for their work. Copyright is applicable to any expressible form of an idea or information that is substantive and discrete. There are national copyright laws and international copyright agreements that have unique requirements, but all have the same overall goal of protecting creative works. Copyright is usually enforced through the civil legal system, but in some situations, breaking this law is considered a criminal act. So the copyright law protects the content (i.e., book, song, art), and DMCA protects the access control technology put in place to prevent unauthorized individuals from gaining access to this content.
- ☒ **C** is incorrect because there is no law specifically called the Federal Privacy Act. The Privacy Act of 1974 is a U.S. federal law that establishes a Code of Fair Information Practice that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies. So this privacy law has nothing to do with copyright content or access control technologies. The focus of this law is to keep the government in check and not allow it to gather too much data on its citizens that could be used for Big Brother-type activities. This law outlines what type of data government agencies can gather, how long they can keep it, how they have to protect the gathered data, and the agencies' responsibilities pertaining to sharing and destroying this type of data.
- ☒ **D** is incorrect because the Stop Online Piracy Act (SOPA) is a U.S. bill that was introduced, but never passed, to expand the ability of law enforcement to enforce online copyright infringement rules and restrict online trafficking in counterfeit goods. The goal of this

proposed law was to restrict access to websites that host or facilitate the trading of pirated content. SOPA does not deal with access control technologies like DMCA, but provides a legal structure to go after owners of websites who share content that they do not own. Content developers in the United States could rely upon the copyright law, but this only applies within the United States. SOPA has an international reach and would require search engines and hosting companies to cut off access to websites that were serving up content that they did not own. There was a lot of push back to SOPA, and as of this writing it has not been passed.

35. What role does the Internet Architecture Board play regarding technology and ethics?
- A. It creates criminal sentencing guidelines.
 - B. It issues ethics-related statements concerning the use of the Internet.
 - C. It edits Request for Comments.
 - D. It maintains the Ten Commandments of Computer Ethics.
- B.** The Internet Architecture Board (IAB) is the coordinating committee for Internet design, engineering, and management. It is responsible for the architectural oversight of the Internet Engineering Task Force (IETF) activities, Internet Standards Process oversight and appeal, and editor of Request for Comments (RFC). The IAB issues ethics-related statements concerning the use of the Internet. It considers the Internet to be a resource that depends upon availability and accessibility to be useful to a wide range of people. It is mainly concerned with irresponsible acts on the Internet that could threaten its existence or negatively affect others. It sees the Internet as a great gift and works hard to protect it for all who depend upon it. The IAB sees the use of the Internet as a privilege, which should be treated as such and used with respect.
- A** is incorrect because the IAB has nothing to do with the Federal Sentencing Guidelines, which are rules used by judges when determining the proper punitive sentences for specific felonies or misdemeanors that individuals or corporations commit. The guidelines work as a uniform sentencing policy for entities that carry out felonies and/or serious misdemeanors in the U.S. federal court system.
- C** is incorrect because, although the Internet Architecture Board is responsible for editing Request for Comments (RFC), this task is

not related to ethics. This answer is a distracter.

- D** is incorrect because the Computer Ethics Institute, not the IAB, developed and maintains the Ten Commandments of Computer Ethics, listed next. The Computer Ethics Institute is a nonprofit organization that works to help advance technology by ethical means.

1. Thou shalt not use a computer to harm other people.
 2. Thou shalt not interfere with other people's computer work.
 3. Thou shalt not snoop around in other people's computer files.
 4. Thou shalt not use a computer to steal.
 5. Thou shalt not use a computer to bear false witness.
 6. Thou shalt not copy or use proprietary software for which you have not paid.
 7. Thou shalt not use other people's computer resources without authorization or proper compensation.
 8. Thou shalt not appropriate other people's intellectual output.
 9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
 10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.
- 36.** As a CISSP candidate, you must sign a Code of Ethics. Which of the following is from the (ISC)² Code of Ethics for the CISSP?
- A. Information should be shared freely and openly; thus, sharing confidential information should be ethical.
 - B. Think about the social consequences of the program you are writing or the system you are designing.
 - C. Act honorably, honestly, justly, responsibly, and legally.
 - D. Do not participate in Internet-wide experiments in a negligent manner.
- C.** (ISC)² requires all certified system security professionals to commit to fully supporting its Code of Ethics. If a CISSP intentionally or knowingly violates this Code of Ethics, he or she may be subject to a peer-review panel, which will decide whether the certification should be relinquished. The following list is an

overview, but each CISSP candidate should read the full version and understand the Code of Ethics before attempting this exam:

- Act honorably, honestly, justly, responsibly, and legally and protect society.
- Work diligently, provide competent services, and advance the security profession.
- Encourage the growth of research—teach, mentor, and value the certification.
- Discourage unnecessary fear or doubt, and do not consent to bad practices.
- Discourage unsafe practices, and preserve and strengthen the integrity of public infrastructures.
- Observe and abide by all contracts, expressed or implied, and give prudent advice.
- Avoid any conflict of interest, respect the trust that others put in you, and take on only those jobs you are fully qualified to perform.
- Stay current on skills, and do not become involved with activities that could injure the reputation of other security professionals.

- A** is incorrect because it is not an ethics statement within the (ISC)² canons. It is an ethical fallacy used by many in the computing world to justify unethical acts. Some people in the industry feel as though all information should be available to all people; thus, they might release sensitive information to the world that was not theirs to release because they feel as though they are doing something right.
- B** is incorrect because the statement is from the Computer Ethics Institute's Ten Commandments of Computer Ethics, not the (ISC)² canons. The Computer Ethics Institute is a nonprofit organization that works to help advance technology by ethical means.
- D** is incorrect because it is an ethics statement issued by the Internet Architecture Board (IAB). The IAB issues ethics-related statements concerning the use of the Internet. It considers the Internet to be a resource that depends upon availability and accessibility to be useful to a wide range of people. It is mainly concerned with irresponsible acts on the Internet that could threaten its existence or negatively affect others. It sees the Internet as a great gift and works hard to protect it for all who depend upon it.

- 37.** Which of the following was the first international treaty seeking to address computer crimes by coordinating national laws and improving investigative techniques and international cooperation?
- A. Council of Global Convention on Cybercrime
 - B. Council of Europe Convention on Cybercrime
 - C. Organisation for Economic Co-operation and Development
 - D. Organisation for Cybercrime Co-operation and Development
- B.** The Council of Europe (CoE) Convention on Cybercrime is one example of an attempt to create a standard international response to cybercrime. It is the first international treaty seeking to address computer crimes by coordinating national laws and improving investigative techniques and international cooperation. The convention's objectives include the creation of a framework for establishing jurisdiction and extradition of the accused. For example, extradition can only take place when the event is a crime in both jurisdictions.
- A** is incorrect because it is a distracter answer. The official name for the treaty is Council of Europe Convention on Cybercrime. It serves as a guideline for any country developing comprehensive national legislation against cybercrime and as a framework for international cooperation between state parties to this treaty.
- C** is incorrect because the Organisation for Economic Co-operation and Development (OECD) is an international organization that helps different governments come together and tackle the economic, social, and governance challenges of a globalized economy. Because of this, the OECD came up with guidelines for the various countries to follow so that data is properly protected and everyone follows the same type of rules.
- D** is incorrect because this is a distracter answer. There is no official entity with this name.
- 38.** Lee is a new security manager who is in charge of ensuring that his company complies with the European Union Principles on Privacy when his company is interacting with their European partners. The set of principles that deals with transmitting data considered private is encompassed within which of the following laws or regulations?
- A. Data Protection Directive
 - B. Organisation for Economic Co-operation and Development

C. Federal Private Bill

D. Privacy Protection Law

- A.** The European Union (EU) in many cases takes individual privacy much more seriously than most other countries in the world, so they have strict laws pertaining to data that is considered private, which are based on the European Union Principles on Privacy. This set of principles addresses using and transmitting information considered private in nature. The principles and how they are to be followed are encompassed within the EU's Data Protection Directive. All states in Europe must abide by these principles to be in compliance, and any company that wants to do business with an EU company must comply with this directive if the business will include exchanging privacy type of data.
- B** is incorrect because the Organisation for Economic Co-operation and Development (OECD) is an international organization that helps different governments come together and tackle the economic, social, and governance challenges of a globalized economy. Because of this, the OECD came up with guidelines for the various countries to follow so that data is properly protected and everyone follows the same type of rules.
- C** is incorrect because this is a distracter answer. There is no official bill with this name.
- D** is incorrect because this is a distracter answer. There is no official law with this name.

39. Brandy could not figure out how Sam gained unauthorized access to her system, since he has little computer experience. Which of the following is most likely the attack Sam used?

A. Dictionary attack

B. Shoulder surfing attack

C. Covert channel attack

D. Timing attack

- B.** Shoulder surfing is a type of browsing attack in which an attacker looks over another's shoulder to see items on that person's monitor or what is being typed in at the keyboard. Sam probably viewed Brandy's password as she typed it. Of the attacks listed, this is the easiest to execute in that it does not require any real knowledge of computer systems.

- A** is incorrect because a dictionary attack is an automated attack involving the use of tools like Crack or L0phtcrack. Sam would need to be aware of these tools and know how to find and use them. A dictionary attack requires more knowledge of how computer systems work compared to shoulder surfing.
 - C** is incorrect because a covert channel attack requires computer expertise. A covert channel is a communications path that enables a process to transmit information in a way that violates the system's security policy. Identifying and using a covert channel requires a lot more computer expertise compared to a shoulder surfing attack.
 - D** is incorrect because a timing attack requires intimate knowledge of how software executes its instruction sets so that they can be manipulated. A person who could successfully carry out this attack typically requires programming experience.
- 40.** Jane has been charged with ensuring that the privacy of clients' personal health information is adequately protected before it is exchanged with a new European partner. What data security requirements must she adhere to?
- A.** HIPAA
 - B.** NIST SP 800-66
 - C.** Safe Harbor
 - D.** European Union Principles on Privacy
- C.** The Safe Harbor requirements were created to harmonize the data privacy practices of the United States with the European Union's stricter privacy controls and to prevent accidental information disclosure and loss. The framework outlines how any entity that is going to move private data to and from Europe must go about protecting it. By certifying against this rule base, U.S. companies that work with European entities can more quickly and easily transfer data.
 - A** is incorrect because the Health Insurance Portability and Accountability Act (HIPAA) does not specifically address data protection for the purposes of sharing it with European entities. HIPAA provides a framework and guidelines to ensure security, integrity, and privacy when handling confidential medical information within the United States. The U.S. federal regulation also outlines how security should be managed for any facility that creates, accesses, shares, or destroys medical information.

- B** is incorrect because NIST SP 800-66 is a risk assessment methodology. It does not point out specific data privacy requirements. NIST SP 800-66 does apply to health care. It was originally designed to be implemented in the healthcare field and can be used by HIPAA clients to help achieve compliance.
 - D** is incorrect because the European Union Principles on Privacy are the foundation for the European Union's strict laws pertaining to data that is considered private. The purpose of the principles is not to prepare data specifically for its exchange with U.S. companies, nor are the requirements mandated for U.S. companies. This set of principles has six areas that address using and transmitting sensitive information, and all European states must abide by these principles to be in compliance.
- 41.** Sue has been tasked with implementing a number of security controls, including antivirus and antispam software, to protect the company's e-mail system. What type of approach is her company taking to handle the risk posed by the system?
- A.** Risk mitigation
 - B.** Risk acceptance
 - C.** Risk avoidance
 - D.** Risk transference
- A.** Risk can be dealt with in four basic ways: transfer it, avoid it, reduce it, or accept it. By implementing security controls such as antivirus and antispam software, Sue is reducing the risk posed by her company's e-mail system. This is also referred to as risk mitigation, where the risk is decreased to a level considered acceptable. In addition to the use of IT security controls and countermeasures, risk can be mitigated by improving procedures, altering the environment, erecting barriers to the threat, and implementing early detection methods to stop threats as they occur, thereby reducing their possible damage.
 - B** is incorrect because risk acceptance does not involve spending money on protection or countermeasures, such as antivirus software. When accepting risk, the company understands the level of risk it is faced with, as well as the potential cost of damage, and decides to live with it without implementing countermeasures. Many companies accept risk when the cost/benefit ratio indicates that the cost of the countermeasure outweighs the potential loss

value.

- C** is incorrect because risk avoidance involves discontinuing the activity that is causing the risk, and in this case Sue's company has chosen to continue to use e-mail. A company may choose to terminate an activity that introduces risk if that risk outweighs the activity's business need. For example, a company may choose to block social media websites for some departments because of the risk they pose to employee productivity.
 - D** is incorrect because risk transference involves sharing the risks with another entity, as in purchasing of insurance to transfer some of the risk to the insurance company. Many types of insurance are available to companies to protect their assets. If a company decides the total or residual risk is too high to gamble with, it can purchase insurance.
- 42.** A number of factors should be considered when assigning values to assets. Which of the following is not used to determine the value of an asset?
- A.** The asset's value in the external marketplace
 - B.** The level of insurance required to cover the asset
 - C.** The initial and outgoing costs of purchasing, licensing, and supporting the asset
 - D.** The asset's value to the organization's production operations
- B.** The level of insurance required to cover the asset is not a consideration when assigning values to assets. It is actually the other way around: By knowing the value of an asset, an organization can more easily determine the level of insurance coverage to purchase for that asset. In fact, understanding the value of an asset is the first step to understanding what security mechanisms should be put in place and what funds should go toward protecting it. This knowledge can also help companies perform effective cost/benefit analyses, understand exactly what is at risk, and comply with legal and regulatory requirements.
 - A** is incorrect because the asset's value in the external marketplace is a factor that should be considered when determining the value of an asset. It should also include the value the asset might have to competitors or what others are willing to pay for a given asset.
 - C** is incorrect because the initial and outgoing costs of purchasing,

licensing, and supporting the asset are considerations when determining the cost and value of an asset. The asset must be cost effective to the business directly. If the supporting requirements of maintaining the asset outweighs the business need for the asset, its value will decrease.

- D** is incorrect because it is a factor to be considered when determining an asset's value. The asset's value to the organization's production operations is the determination of cost to an organization if the asset is not available for a certain period of time. Along these same lines, the asset's usefulness and role in the organization should be considered, as well as the operational and production activities affected, if the asset is unavailable. If the asset helps operations, it is valuable; the trick is to figure out how valuable.
- 43.** The Zachman Architecture Framework is often used to set up an enterprise security architecture. Which of the following does not correctly describe the Zachman Framework?
 - A.** A two-dimensional model that uses communication interrogatives intersecting with different levels
 - B.** A security-oriented model that gives instructions in a modular fashion
 - C.** Used to build a robust enterprise architecture versus a technical security architecture
 - D.** Uses six perspectives to describe a holistic information infrastructure
- B.** The Zachman Framework is not security oriented, but it is a good template to work with to build an enterprise security architecture because it gives direction on how to understand the enterprise in a modular fashion. This framework is structured and formal and is used as a tool to understand any type of enterprise from many different angles. The Zachman Framework was developed in the 1980s by John Zachman and is based on the principles of classical architecture that contains rules that govern an ordered set of relationships.
- A** is incorrect because the Zachman Framework is a two-dimensional model that addresses the what, how, where, who, when, and why from six different perspectives: the planner or visionary, the owner, the architect, the designer, the builder, and the working system. Together, this information gives a holistic view of

the enterprise.

- C** is incorrect because the Zachman Framework is used to create a robust enterprise architecture, not a security architecture, technical or not. The framework is not security specific. Almost all robust enterprise security architectures work with the structure provided by the Zachman Framework in one way or another. When we talk about a robust security architecture, we are talking about one that deals with many components throughout the organization—not just a network and the systems within that network.
- D** is incorrect because the Zachman Framework uses six perspectives to build a holistic view of the enterprise. Those perspectives are the planner or visionary, owner, architect, designer, builder, and the working system. Those using the framework address what, how, where, who, when, and why as they relate to each of these perspectives. This is to ensure that regardless of the order in which they are put in place, components of the enterprise are organized and relationships are clearly defined so that they create a complete system. The framework does not just specify an information infrastructure.

44. John has been told to report to the board of directors with a vendor-neutral enterprise architecture framework that will help the company reduce fragmentation that results from the misalignment of IT and business processes. Which of the following frameworks should he suggest?

- A.** DoDAF
 - B.** CMMI
 - C.** ISO/IEC 42010
 - D.** TOGAF
- D.** The Open Group Architecture Framework (TOGAF) is a vendor-neutral platform for developing and implementing enterprise architectures. It focuses on effectively managing corporate data through the use of metamodels and service-oriented architecture (SOA). A proficient implementation of TOGAF is meant to reduce fragmentation that occurs due to misalignment of traditional IT systems and actual business processes. It also adjusts to new innovations and capabilities to ensure new changes can easily be integrated into the enterprise platform.
 - A** is incorrect because the Department of Defense Architecture

Framework (DoDAF) provides guidelines for the organization of enterprise architecture for the U.S. Department of Defense systems. All DoD weapons and IT systems are required to design and document enterprise architecture according to these guidelines. They are also suitable for large and complex integrated systems in military, private, or public sectors.

- B** is incorrect because Capability Maturity Model Integration (CMMI) is used during software development to design and further enhance software. The CMMI provides a standard for software development process where the level of maturity of the development process can be measured. It was developed by the Carnegie Mellon Software Engineering Institute and is an upgraded version of Capability Maturity Model (CMM).
 - C** is incorrect because the ISO/IEC 42010 consists of a set of recommended practices intended to simplify the design and conception of software-intensive system architectures. This standard provides a type of language (terminology) to describe the different components of a software architecture and how to integrate it into the life cycle of development. Many times the overall vision of the architecture of a piece of software is lost as the developers get caught up in the actual development procedures. This standard provides a conceptual framework to follow for architecture development and implementation.
- 45.** The Information Technology Infrastructure Library (ITIL) consists of five sets of instructional books. Which of the following is considered the core set and focuses on the overall planning of the intended IT services?
- A.** Service Operation
 - B.** Service Design
 - C.** Service Transition
 - D.** Service Strategy
- D.** The fundamental approach of ITIL lies in the creation of Service Strategy, which focuses on the overall planning of the intended IT services. Once the initial planning has been concluded, the Service Design provides guidelines on designing valid IT services and overall implementation policies. The Service Transition stage is then initiated, where guidelines regarding evaluation, testing, and validation of the IT services are provided. This allows the transition

from business environments into technology services. The Service Operation makes sure that all the decided services have met their objectives. Finally, the Continual Service Improvement points out the areas of improvements in the entire service life cycle. The Service Strategy is considered to be the core of ITIL. It consists of a set of guidelines that include best practices regarding strategy and value planning, design, and alignment between the IT and business approaches, market analysis, service assets, setting targets toward providing quality service to the clients, and implementation of service strategies.

- ☒ **A** is incorrect because Service Operation refers to an important component of the life cycle in which the services are actually delivered. This part of the life cycle defines a set of guidelines that makes sure that the agreed levels of services are delivered to the customers. The various genres incorporated by Service Operation include Event Management, Problem Management, Access Management, Incident Management, Application Management, Technical Management, and Operations Management. Service Operation also balances between the conflicting goals, such as technology vs. business requirements, stability vs. response, cost vs. quality of service, and reactive vs. proactive activities.
- ☒ **B** is incorrect because the Service Design comprises a set of optimal practices for the designing of IT services, including their processes, architectures, policies, and documentation, in order to fulfill the current and future business requirements. The target of the Service Design is to design services according to their agreed business objectives; design such processes that can support life cycle, identification and management of risks; and involvement in the improvement of IT service quality as a whole.
- ☒ **C** is incorrect because Service Transition focuses on delivering services proposed by business strategy into operational use. It also contains guidelines that enable the smooth transition of the business model into technology services. If the requirements of a service have changed after its design, the Service Transition ensures that those requirements are delivered according to its modified design. The areas focused on by these guidelines include Transition Planning and Support, Change Management, Knowledge Management, Release and Deployment Management, Service Validation and Testing, and Evaluation, along with the responsibilities of personnel involved with the Service Transition.

- 46.** Sarah and her security team have carried out many vulnerability tests over the years to locate the weaknesses and vulnerabilities within the systems on the network. The CISO has asked her to oversee the development of a threat model for the network. Which of the following best describes what this model is and what it would be used for?
- A.** A threat model can help to assess the probability, the potential harm, and the priority of attacks, and thus help to minimize or eradicate the threats.
 - B.** A threat model combines the output of the various vulnerability tests and the penetration tests carried out to understand the security posture of the network as a whole.
 - C.** A threat model is a risk-based model that is used to calculate the probabilities of the various risks identified during the vulnerability tests.
 - D.** A threat model is used in software development practices to uncover programming errors.
- A.** Threat modeling is a structured approach to identifying potential threats that could exploit vulnerabilities. A threat modeling approach looks at who would most likely want to attack an organization and how could they successfully do this. A threat model can help to assess the probability, the potential harm, and the priority of attacks, and thus help to minimize or eradicate the threats. Threat modeling is a process of identifying the threats that could negatively affect an asset and the attack vectors they would use to achieve their goals.
- B** is incorrect because a threat model is very different from vulnerability and penetration tests. These types of tests are carried out to look for and at specific items in a very focused manner. A threat model is a conceptual construct that is developed to understand a system or network at an abstraction level. A threat model is used as a tool to think through all possible attack vectors, while these tests are carried out to detect if specific vulnerabilities exist to allow certain attacks to take place.
- C** is incorrect because a threat model is not used for calculations. Quantitative risk analysis procedures are commonly carried out to calculate the probability of identified vulnerabilities turning into true risks. These procedures can be carried out after a threat model is developed, but they are not one and the same.

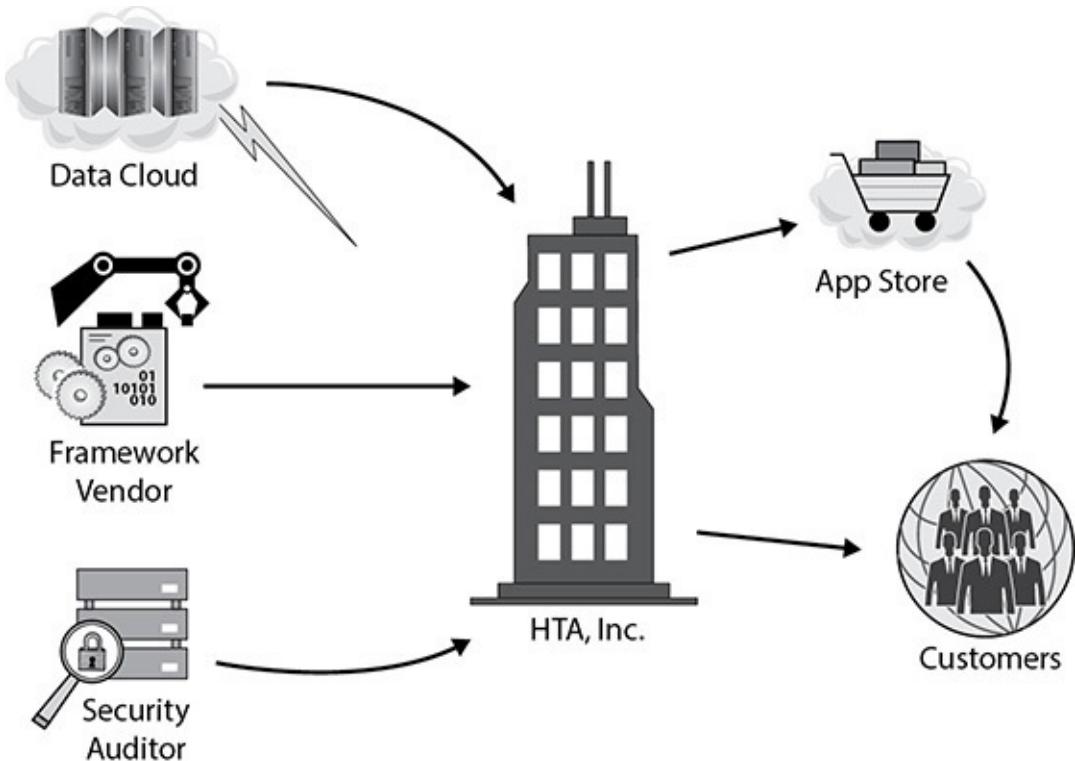
- D** is incorrect because although a threat model can be used in software development, it is not restricted to just this portion of the industry. It is important to be able to understand all types of threats—software, physical, personnel, etc. A threat model is a high-level construct that can be used to understand different types of threats for different assets. A threat model would not necessarily be used to identify programming errors. The model is used to understand potential threats against an asset.

The following scenario applies to questions 47 through 51.

Health Tracking Apps, Inc. (HTA) is a U.S.-based corporation that develops and sells apps that its customers can use to track various aspects of their own health, from their daily exercise regimes to various medical test results and comparative statistics over time. These apps utilize cloud-based storage so that customers can access their data from multiple platforms, including smart mobile devices and desktop systems. Customers can also easily share the data the apps generate with their personal trainers and healthcare providers if they choose, on a subscription basis.

HTA's products are available in several languages, including English, French, Spanish, German, and Italian. All of HTA's software is developed by a dedicated staff within the United States, though HTA occasionally hires interns from the local university to assist with language translations for its various user interfaces.

The following entity relationship diagram illustrates HTA's business model dependencies:



- 47.** Would HTA be required to comply with the General Data Protection Regulation (GDPR)? If so, why? If not, why?
1. Maybe, because HTA's HR records could contain protected privacy data about European citizens if any of HTA's interns are students studying from abroad.
 2. No, because the GDPR applies only to European-based companies.
 3. Yes, to the extent that HTA's stored private data includes that of any European customers.
 4. No, because any private data regarding European citizens that HTA's HR and customer records contain is stored within the United States.
- A. Statement 2 only
B. Statement 4 only
C. Both statements 1 and 3
D. Statement 3 only
- C. Statements 1 and 3 are both correct. European citizens do not lose their inherent privacy rights by working outside of their native country. By hiring EU citizens, HTA must adhere to the GDPR with respect to their private data, or risk stiff penalties in HTA's business

dealings with EU customers.

Likewise, any private data that HTA stores or processes regarding EU customers must be protected according to the terms of the GDPR. In HTA's case, the company's business model explicitly involves the collection, storage, and processing of health data, which is in turn explicitly protected by the GDPR. HTA likely has EU customers because it offers versions of its products in French, Spanish, German, and Italian.

- A** is incorrect because statement 2 is incorrect. While the GDPR, as a European Union regulation, has the full weight of law only in the 28 member nations of the EU, it does impact every organization that holds or uses European personal data, whether the organization is within Europe or not. A non-EU company that does business with European customers can have its ability to do so curtailed if it does not comply with the GDPR with respect to Protected Data.
 - B** is incorrect because statement #4 is also incorrect. At issue with the GDPR is how private data about European citizens is protected, regardless of where it is stored. Storing data subject to the GDPR outside of the EU does not give an organization "safe harbor" from regulatory requirements.
 - D** is incorrect because while statement #3 is correct, so is statement #1, as explained.
- 48.** HTA's customer data is breached via a vulnerability in its application programming interface (API). This vulnerability is discovered to be a result of a recently announced security flaw in the underlying Java framework that HTA uses for the development of its apps. Which of the following best describes the root of this problem?
- A.** HTA failed to manage risks associated with its supply chain.
 - B.** HTA failed to apply a critical patch in a timely manner.
 - C.** HTA stored critical/sensitive data in a cloud.
 - D.** HTA chose a risky language and framework for its development.
- A.** Per the entity relationship diagram shown, it is clear that the flawed Java framework in question is provided to HTA by an upstream supplier. Proper supply chain risk management would have involved overt recognition that such problems will eventually arise. HTA may have little means to influence its suppliers' software development security practices, but HTA can and must plan in

advance for such an eventuality.

- B** is incorrect because in the case of a flaw in a development framework, the solution is often not simply an easy-to-deploy patch, but rather a time-consuming redevelopment process. Again, HTA should have been prepared with other mitigating countermeasures, perhaps including temporarily disabling the availability of its API, prior to a devastating and more costly breach.
 - C** is incorrect because while the upstream supplier HTA uses for customer data storage introduces its own distinct supply chain risk management issues, in this case that supplier was not identified as problematic.
 - D** is incorrect because, although it may be true that some languages/frameworks for software development are commonly deemed “riskier” than others, a secure development environment and life-cycle process is of far greater concern than the language chosen.
- 49.** HTA stores its customers’ private data in a third-party cloud. What is the primary means through which HTA can ensure that its cloud service provider maintains compliance with any regulations—including the GDPR, if necessary—that HTA is subject to?
- A.** Enforce an enterprise level agreement (ELA) that specifies how the service provider should conduct assurance activities.
 - B.** Enforce a service level agreement (SLA) that specifies contractual penalties for the service provider’s noncompliance.
 - C.** Conduct an onsite inspection of the service provider’s facilities to ensure they are compliant.
 - D.** Review the service provider’s security program.
- B.** An SLA is a contractual agreement that specifies how a provider will guarantee that what it delivers is what has been agreed upon, along with timelines for access and assistance. In this case, the SLA must allow HTA to validate the cloud provider’s level of compliance in some way, such as via inspections, documentation and process review, external audits, and so forth. But the key element in ensuring compliance is contractual enforcement of the SLA once accepted.
 - A** is incorrect because specifying how the upstream provider conducts assurance activities with respect to the services delivered

is only one component of an SLA, albeit an important one.

- C** is incorrect because the ability of HTA to conduct an onsite inspection of a service provider's facilities requires an SLA to be in place, making the SLA the primary means through which to ensure that HTA's service provider maintains compliance with any regulations.
 - D** is incorrect because the ability of HTA to review the service provider's security program also requires an SLA to be in place, making the SLA the primary means to assert its right to review.
- 50.** Many of HTA's employees have either direct or indirect access to its customers' private data. HTA has to ensure that newly hired employees are aware of all security policies and procedures that apply to them, have only the necessary access through the accounts created for them, and have signed an agreement not to disclose the data inappropriately. Which of the following terms describes this process?
- A.** Due diligence
 - B.** Personnel security
 - C.** Nondisclosure agreement (NDA)
 - D.** Onboarding
- D.** Onboarding refers specifically to the process by which a previously untrusted outsider becomes a “trusted” (or better yet, trustworthy) insider. Onboarding typically begins with the new hire agreeing to, and signing, a nondisclosure agreement (NDA), prior to any further indoctrination. Next is ensuring that the employee has read all relevant corporate policies, understands them, and has agreed to adhere to them. Initial security awareness training is also a necessary step, prior to the appropriate provision of access to corporate resources.
 - A** is incorrect because, although a proper process for the initiation of new employees prior to granting them trusted status is certainly a requirement for the conduct of due diligence toward a standard of due care, it is but one aspect of it. “Onboarding” is the more specific answer in this context.
 - B** is incorrect because proper onboarding is only one of many key aspects and processes within the practice of personnel security. Also included would be its opposite but equally important process, termination. However, the breadth of practices within personnel

security are beyond the scope of this question. “Onboarding” is more specific.

- C is incorrect because the signing of an NDA is only the first step in ensuring a new hire is ready to become a trusted employee, in the process of onboarding.

51. HTA has an awareness program designed to educate all employees about security-relevant issues that apply to them, based on their role. IT staff members are specifically instructed that it is important to be aware of new vulnerabilities as they are discovered, not only in the OSs that are used by HTA, but also in the applications and frameworks the developers use to build their software. The awareness program also stresses the importance of rapid mitigation by IT staff. As stated in question 48, HTA’s customer data has been breached via a vulnerability in its API, a vulnerability discovered to be a result of a recently announced security flaw in the underlying Java framework that HTA uses for the development of its apps. Which of the following most likely contributed to the breach with respect to the security awareness program?

- A. HTA hasn’t conducted periodic content reviews of the security awareness program.
- B. Assessment of the program’s effectiveness has been insufficient.
- C. Employees are improperly trained.
- D. The security awareness program was not relevant to the breach.

- B. HTA’s security awareness program clearly addressed the importance of the IT staff being aware of new vulnerabilities and mitigating them rapidly, but the IT staff still failed to mitigate the critical vulnerability in its API that allowed a significant breach to occur. This indicates that the security awareness program was not sufficiently assessed and deemed effective.

Of course there may have been other, more structural factors, such as the unavailability of a patch or the lack of a process for the rapid redevelopment of the API around a patched framework. However, HTA should have been able to leverage the IT staff’s hands-on awareness of such issues in order to enable them to escalate such deficiencies to management, effectively augmenting *their* awareness.

- A is incorrect because, though the periodic review of a security awareness program’s content is important, it shouldn’t necessitate

the enumeration of individual vulnerabilities as they are discovered.

- C** is incorrect because there is nothing in the scenario's description that would suggest that the IT staff's training is either incomplete or poorly targeted. The only indication is that it is not working.
- D** is incorrect because, due to their scope (all employees) and role-specificity, security awareness programs are generally relevant to all aspects of an enterprise's security posture. After all, it is invariably the actions or inactions of people that lead to breaches.

Asset Security

This domain includes questions from the following topics:

- Information life cycle
- Information classification and protection
- Information ownership
- Protection of privacy
- Information retention
- Data security controls
- Data handling requirements

While Domain 1 sets the stage for the basis of how security programs should be constructed and managed, the point of security programs is entirely to protect the assets identified as critical to the enterprise. To do this effectively—and especially cost effectively—one has to understand the nature of what needs to be protected, why it needs to be protected, and how to protect it. Domain 2 focuses on understanding which information assets need to be protected and why, and how to categorize their value for the prioritization of protection efforts to be implemented throughout the life cycle of each asset.



QUESTIONS

1. As head of sales, Jim is the data owner for the sales department. Which of the following is not Jim's responsibility as data owner?
 - A. Assigning information classifications
 - B. Dictating how data should be protected
 - C. Verifying the availability of data
 - D. Determining how long to retain data
2. Assigning data classification levels can help with all of the following except:
 - A. The grouping of classified information with hierarchical and restrictive security
 - B. Ensuring that nonsensitive data is not being protected by unnecessary controls

- C. Extracting data from a database
 - D. Lowering the costs of protecting data
3. Susan, an attorney, has been hired to fill a new position at Widgets, Inc.: chief privacy officer (CPO). What is the primary function of her new role?
- A. Ensuring the protection of partner data
 - B. Ensuring the accuracy and protection of company financial information
 - C. Ensuring that security policies are defined and enforced
 - D. Ensuring the protection of customer, company, and employee data
4. Jared plays a role in his company's data classification system. In this role, he must practice due care when accessing data and ensure that the data is used only in accordance with allowed policy while abiding by the rules set for the classification of the data. He does not determine, maintain, or evaluate controls, so what is Jared's role?
- A. Data owner
 - B. Data custodian
 - C. Data user
 - D. Information systems auditor
5. Michael is charged with developing a data classification program for his company. Which of the following should he do first?
- A. Understand the different levels of protection that must be provided.
 - B. Specify data classification criteria.
 - C. Identify the data custodians.
 - D. Determine protection mechanisms for each classification level.
6. Which of the following is NOT a factor in determining the sensitivity of data?
- A. Who should be accessing the data
 - B. The value of the data
 - C. How the data will be used
 - D. The level of damage that could be caused should the data be exposed

- 7.** What is the chief security responsibility of a data owner?

 - A.** Determining how the data should be preserved
 - B.** Determining the data classification
 - C.** Determining the data value
 - D.** Determining how the data will be used
- 8.** Which is the most valuable technique when determining if a specific security control should be implemented?

 - A.** Risk analysis
 - B.** Cost/benefit analysis
 - C.** ALE results
 - D.** Identifying the vulnerabilities and threats causing the risk
- 9.** Which of the following is the LEAST important stage in the life-cycle management of information?

 - A.** Data specification and classification
 - B.** Continuous monitoring and auditing of data access
 - C.** Data archival
 - D.** Database migration
- 10.** Which of the following are effective methods of preventing data remanence on solid-state devices (SSDs)?

 - i.** Clearing
 - ii.** Purging
 - iii.** Degaussing
 - iv.** Destruction
 - A.** i, ii
 - B.** i, iii, iv
 - C.** iv
 - D.** All of the above
- 11.** The requirement of erasure is the end of the media life cycle if the media contains sensitive information. Which of the following best describes purging?

 - A.** Changing the polarization of the atoms on the media.

- B. It is unacceptable when media are to be reused in the same physical environment for the same purposes.
 - C. Data formerly on the media is made unrecoverable by overwriting it with a pattern.
 - D. Information is made unrecoverable, even with extraordinary effort.
- 12. Sam plans to establish mobile phone service using the personal information he has stolen from his former boss. What type of identity theft is this?
 - A. Phishing
 - B. True name
 - C. Pharming
 - D. Account takeover
- 13. Which of the following are common military categories of data classification?
 - A. Top Secret, Secret, Classified, Unclassified
 - B. Top Secret, Secret, Confidential, Private
 - C. Top Secret, Secret, Confidential, Unclassified
 - D. Classified, Unclassified, Public
- 14. Joan needs to document a data classification scheme for her organization. Which criteria should she use to guide her decisions?
 - A. The value of the data and the age of the data
 - B. Legal responsibilities based on ISO regulations
 - C. Who will be responsible for protecting the data and how
 - D. How an adverse data breach would be handled
- 15. Which of the following means of data removal makes the data unrecoverable even with extraordinary effort, such as with physical forensics in a laboratory?
 - A. Deletion of the data
 - B. Sanitization of the media
 - C. Purging via overwriting
 - D. None of the above
- 16. When classifying information, its sensitivity refers to:

- A. The magnitude of damage or loss an organization would sustain if the information was lost or made unavailable
 - B. The magnitude of damage or loss an organization would sustain if the information was revealed to unauthorized individuals
 - C. The ways in which an organization protects its information from third parties
 - D. The ways in which an organization protects its information from internal abuse
- 17.** When classifying information, its criticality refers to:
- A. The magnitude of damage or loss an organization would sustain if the information was lost or made unavailable
 - B. The magnitude of damage or loss an organization would sustain if the information was revealed to unauthorized individuals
 - C. The ways in which an organization protects its information from third parties
 - D. The ways in which an organization protects its information from internal abuse
- 18.** Which of the following classification levels are most commonly used in commercial industry?
- A. Confidential, Secret, Top Secret
 - B. Unclassified, Sensitive but unclassified
 - C. Private, Proprietary, Sensitive
 - D. Unrestricted, For government use only
- 19.** Which of the following classification levels are most commonly used in military environments?
- A. Confidential, Secret, Top Secret
 - B. Unclassified, Sensitive but unclassified
 - C. Private, Proprietary, Sensitive
 - D. Unrestricted, For government use only
- 20.** Which of the following is true regarding data retention requirements?
- A. Legal requirements for data retention are uniform across all regulated business sectors, and must be followed to reduce risk of criminal litigation.

- B. To comply with various data retention regulations, it is best to retain all data to the lengthiest legal requirement.
 - C. Retaining the largest amount of data possible makes responding to electronic discovery (e-discovery) orders easier and more straightforward.
 - D. A well-documented policy for the retention of data is a minimum but necessary component of regulatory compliance.
- 21.** Why is the issue of data remanence sometimes problematic?
- A. Data retention policies don't usually specify when data should be deleted.
 - B. With most file systems, deleting data doesn't ensure that it cannot be recovered.
 - C. With most modern file systems, accidentally overwriting a small part of a file makes the remaining remnants unrecoverable.
 - D. Physical destruction is the only way to ensure data cannot be recovered, and this is usually too prohibitively expensive.
- 22.** For which of the following physical media is degaussing a relatively cheap and effective means of eradicating data?
- A. Optical disks (CDs/DVDs)
 - B. Backup tapes
 - C. USB thumb drives
 - D. Hard disk drives (HDDs)
- 23.** Which of the following approaches is the most effective way for an organization to reduce its liability regarding the protection of private data?
- A. Collect any and all data that has business utility, but ensure that the legal team has reviewed and approved all policies with respect to its protection.
 - B. Never collect or store any privacy-protected data.
 - C. Limit the amount of private data collected to that which is legally allowed.
 - D. Limit the amount of private data collected to that which is required for business functions.
- 24.** When protecting information assets, which of the following security

controls is most effective for data in motion?

- A. Requiring whole-disk encryption for all devices with the Advanced Encryption Standard (AES)
 - B. Implementing encryption with Transport Layer Security (TLS) or IPSec
 - C. Implementing whole-memory encryption with the storage of keys in CPU registers
 - D. Requiring the use of next-generation firewalls (NGFWs) and/or network-based intrusion prevention systems (NIPSSs)
25. When protecting information assets, which of the following security controls is most effective for data at rest?
- A. Requiring whole-disk encryption for all devices with the Advanced Encryption Standard (AES)
 - B. Implementing encryption with Transport Layer Security (TLS) or IPSec
 - C. Implementing whole-memory encryption with the storage of keys in CPU registers
 - D. Requiring the use of next-generation firewalls (NGFWs) and/or network-based intrusion prevention systems (NIPSSs)
26. Which of the following is the LEAST effective security control regarding sensitive data stored on mobile devices?
- A. Back up all devices to an organizationally managed repository.
 - B. Implement full-volume encryption on all mobile devices.
 - C. Require that all mobile devices be wipeable remotely if stolen or misplaced.
 - D. Enact a policy prohibiting the access or storage of sensitive corporate data on personal mobile devices.
27. In the modern era, are paper records still a significant concern in the protection of enterprise data assets? If so, why? If not, why not?
- A. Yes, because the most sensitive data is usually only stored in printed form
 - B. Yes, because printed copies are still commonly produced, are more difficult to track, and are commonly not disposed of properly
 - C. No, because the amount of sensitive data that is ever printed out is

exceptionally small by comparison

- D. No, because sensitive data that is printed out is the easiest to properly destroy
- 28.** When selecting and implementing information asset protection standards, the process of scoping refers to which of the following?
- A. Choosing the standard that most closely provides for regulatory compliance within your organization's industry
 - B. Altering provisions of the chosen standard so that they are more relevant to your organization's environment
 - C. Eliminating from implementation the parts of the chosen standard that are not relevant to your organization's environment
 - D. Making decisions with respect to internal penalties for noncompliance with the chosen standard
- 29.** When selecting and implementing information asset protection standards, why is tailoring an important process?
- A. Because the penalties for noncompliance provided for by the chosen standard may be too severe and unrealistic
 - B. Because some of the provisions of the chosen standard might not apply to your organization's environment
 - C. Because some of the provisions of the chosen standard might better address your organization's environment if modified slightly
 - D. Because not all standards are a good fit for your organization, and so it is important to choose the best one
- 30.** When implementing data leak prevention (DLP), which is the first, most critical step?
- A. Examine the flow of sensitive data in your organization to better understand what is proper, and what should not be allowed.
 - B. Conduct a risk assessment to determine what the best data protection strategy will be for your organization.
 - C. Evaluate the features of the available products in order to determine which fits best in your organization's infrastructure.
 - D. Conduct an inventory of all the data in your organization in order to characterize and prioritize its sensitivity.

QUICK ANSWER KEY

1. C

2. C

3. D

4. C

5. A

6. C

7. B

8. B

9. D

10. C

11. D

12. B

13. C

14. A

15. C

16. B

17. A

18. C

19. A

20. D

21. B

22. B

23. D

24. B

25. A

26. D

27. B

28. C

29. C

1. As head of sales, Jim is the data owner for the sales department. Which of the following is not Jim's responsibility as data owner?
- A. Assigning information classifications
 - B. Dictating how data should be protected
 - C. Verifying the availability of data
 - D. Determining how long to retain data
- C. The responsibility of verifying the availability of data is the only responsibility listed that does not belong to the data (information) owner. Rather, it is the responsibility of the data (information) custodian. The data custodian is also responsible for maintaining and protecting data as dictated by the data owner. This includes performing regular backups of data, restoring data from backup media, retaining records of activity, and fulfilling information security and data protection requirements in the company's policies, guidelines, and standards. Data owners work at a higher level than the data custodians. The data owners basically state, "This is the level of integrity, availability, and confidentiality that needs to be provided—now go do it." The data custodian must then carry out these mandates and follow up with the installed controls to make sure they are working properly.
- A is incorrect because, as data owner, Jim is responsible for assigning information classifications. (The question asked which of the following Jim is not responsible for.)
- B is incorrect because data owners such as Jim are responsible for dictating how information should be protected. The data owner has the organizational responsibility for data protection and is liable for any negligence when it comes to protecting the organization's information assets. This means that Jim must make decisions regarding how information is protected and ensure that the data custodian (a role usually filled by IT or security) is carrying out these decisions.
- D is incorrect because determining how long to retain data is the responsibility of the data owner. The data owner is also responsible for determining who can access the information and ensuring that proper access rights are being used. He can approve access requests himself or delegate the function to business unit managers, who will

approve requests based on user access criteria defined by the data owner.

2. Assigning data classification levels can help with all of the following except:

- A.** The grouping of classified information with hierarchical and restrictive security
 - B.** Ensuring that nonsensitive data is not being protected by unnecessary controls
 - C.** Extracting data from a database
 - D.** Lowering the costs of protecting data
- C.** Data classification does not involve the extraction of data from a database. However, data classification can be used to dictate who has access to read and write data that is stored in a database. Each classification should have separate handling requirements and procedures pertaining to how that data is accessed, used, and destroyed. For example, in a corporation, confidential information may only be accessed by senior management. Auditing could be very detailed and its results monitored daily, and degaussing or overwriting procedures may be required to erase the data. On the other hand, information classified as public may be accessed by all employees, with no special auditing or destruction methods required.
- A** is incorrect because assigning data classification levels can help with the grouping of classified information with hierarchical and restrictive security. Data that shares the same classification, for example, can be grouped together and assigned the same handling requirements and procedures pertaining to how it is accessed, used, and destroyed.
- B** is incorrect because assigning data classification levels can help ensure that nonsensitive data is being protected by the necessary controls. Data classification directly deals with ensuring that the different levels of sensitive data are being protected by the necessary controls. This answer is very tricky because of all the negatives, so make sure to read such questions and answers carefully.
- D** is incorrect because data classification helps ensure data is protected in the most cost-effective manner. Protecting and maintaining data costs money, but it is important to spend this

money for the information that actually requires protection. For example, data that is classified confidential may require additional access controls (as compared to public data) to restrict access. It may also require additional auditing and monitoring. This may be appropriate for a soda company's proprietary recipe, but it would be a waste of resources if those same measures were implemented for the soda company's employee directory.

3. Susan, an attorney, has been hired to fill a new position at Widgets, Inc.: chief privacy officer (CPO). What is the primary function of her new role?
 - A. Ensuring the protection of partner data
 - B. Ensuring the accuracy and protection of company financial information
 - C. Ensuring that security policies are defined and enforced
 - D. Ensuring the protection of customer, company, and employee data

D. The chief privacy officer (CPO) position is being created by companies in response to the increasing demands on organizations to protect myriad types of data. The CPO is responsible for ensuring the security of customer, company, and employee data, which keeps the company free from legal prosecution and—hopefully—out of the headlines. Thus, the CPO is directly involved with setting policies on how data is collected, protected, and distributed to third parties. The CPO is usually an attorney and reports to the chief security officer (CSO).

A is incorrect because protecting partner data is just a small subset of all the data the CPO is responsible for protecting. CPOs are responsible for ensuring the protection of customer, company, and employee data. Partner data is among the various types of data that the CPO is responsible for protecting. In addition, the CPO is responsible for knowing how the company's suppliers, partners, and other third parties are protecting its sensitive information. Many times, companies will need to review these other parties (which have copies of data needing protection).

B is incorrect because the accuracy of financial information is the responsibility of its data owner—the chief financial officer (CFO). The CFO is responsible for the corporation's account and financial activities, and the overall financial structure of the organization. The CPO is responsible for helping to ensure the secrecy of this

data, but not the accuracy of the data. The financial information is also a small subset of all the data types the CPO is responsible for protecting.

- C** is incorrect because the definition and enforcement of security policies is the responsibility of senior management, commonly delegated to the chief information security officer (CISO) or CSO—not the CPO. A security policy is an overall general statement that dictates what role security plays within the organization. The CPO's responsibilities as they relate to policies are to contribute to the setting of data protection policies, including how data is collected, protected, and distributed to third parties.
- 4.** Jared plays a role in his company's data classification system. In this role, he must practice due care when accessing data and ensure that the data is used only in accordance with allowed policy while abiding by the rules set for the classification of the data. He does not determine, maintain, or evaluate controls, so what is Jared's role?
 - A.** Data owner
 - B.** Data custodian
 - C.** Data user
 - D.** Information systems auditor
 - C.** Any individual who uses data for work-related tasks is a data user. Users must have the necessary level of access to the data to perform the duties within their position and are responsible for following operational security procedures to ensure the data's confidentiality, integrity, and availability to others. This means that users must practice due care and act in accordance with both security policy and data classification rules.
 - A** is incorrect because the data owner has a greater level of responsibility in the protection of the data. Data owners are responsible for classifying the data, regularly reviewing classification levels, and delegating the responsibility of the data protection duties to the data custodian. The data owner is typically a manager or executive in the organization and is held responsible when it comes to protecting the company's information assets.
 - B** is incorrect because the data custodian is responsible for the implementation and maintenance of security controls as dictated by the data owner. In other words, the data custodian is the technical caretaker of the controls that protect the data. Her duties include

making backups, restoring data, implementing and maintaining countermeasures, and administering controls.

- D** is incorrect because an information systems auditor is responsible for evaluating controls. After evaluating the controls, the auditor provides reports to management, illustrating the mapping between the set acceptable risk level of the organization and her findings. This does not have to do with using the data or practicing due care with the use of data.
- 5. Michael is charged with developing a data classification program for his company. Which of the following should he do first?
 - A. Understand the different levels of protection that must be provided.
 - B. Specify data classification criteria.
 - C. Identify the data custodians.
 - D. Determine protection mechanisms for each classification level.
- A. Before Michael begins developing his company's classification program, he must understand the different levels of protection that must be provided. Only then can he develop the necessary classification levels and their criteria. One company may choose to use only two layers of classification, whereas another may choose to use more. Regardless, when developing classification levels, he should keep in mind that too many or too few classification levels will render the classification ineffective; there should be no overlap in the criteria definitions between classification levels, and classification levels should be developed for both data and software.
- B is incorrect because data classification criteria cannot be established until the classification levels themselves have been defined. The classification criteria are used by data owners to know what classification should be assigned to specific data. Basically, the classifications are defined buckets and the criteria help data owners determine what bucket each data set should be put into.
- C is incorrect because there is no need to identify the data custodians until classification levels are defined, criteria are determined for how data is classified, and the data owner has indicated the classification of the data she is responsible for. Remember, the data custodian is responsible for implementing and maintaining the controls specified by the data owner.
- D is incorrect because protection mechanisms for each classification

level cannot be determined until the classification levels themselves are defined based on the different levels of protection that are required. The types of controls implemented per classification will depend upon the level of protection that management and the security team have determined is needed.

6. Which of the following is NOT a factor in determining the sensitivity of data?
 - A. Who should be accessing the data
 - B. The value of the data
 - C. How the data will be used
 - D. The level of damage that could be caused should the data be exposed

C. How the data will be used has no bearing on how sensitive it is. In other words, the data is sensitive no matter how it will be used—even if it is not used at all.

A is incorrect because data classification criteria must consider very directly *who* will need access to the data and their level of clearance to see sensitive data. If the data is classified at too high a level, then its users will not be able to access it. If it is classified at too low a level, then unauthorized users may have access to it.

B is incorrect because the inherent value of the data also directly drives the degree of protection it must be afforded, and this is determined by its classification. This is true regardless of whether the prioritization must be confidentiality, integrity, or availability.

D is incorrect because the degree of damage that disclosure, alteration, or destruction of the data would cause is directly related to the level of protection it must be provided.
7. What is the chief security responsibility of a data owner?
 - A. Determining how the data should be preserved
 - B. Determining the data classification
 - C. Determining the data value
 - D. Determining how the data will be used

B. Setting the classification for the data drives all other decisions about the data. Determining how the data will be used and determining who should use it are responsibilities within the scope

of the data owner, but they are functional rather than security responsibilities. The owner may participate in determining the value of the data, but since its value is a measure relative to all other corporate data assets, it is not usually something the data owner is solely responsible for. Determining how the data will be preserved falls to the role of the data custodian.

- A** is incorrect because the preservation countermeasures are determined by mandatory access controls based on the classification of the data, not the other way around.
 - C** is incorrect because although assessment of the data's value is a critical component of determining its classification, it is just one component of the overall goal of the data owner.
 - D** is incorrect because how the data is to be used is not a factor in its classification. How data is used may change over time, but its sensitivity to the enterprise must determine who can access it regardless.
- 8.** Which is the most valuable technique when determining if a specific security control should be implemented?
- A.** Risk analysis
 - B.** Cost/benefit analysis
 - C.** ALE results
 - D.** Identifying the vulnerabilities and threats causing the risk
- B.** Once a risk has been identified to be real, sufficiently likely, and sufficiently impactful to require a control to be put in place to reduce the risk within a tolerable range, a countermeasure must be selected. Only an analysis of each possible measure's cost and benefit can determine which course of action should be taken.
 - A** is incorrect because the determination of risk is only the first step in identifying that a countermeasure might be required to control the risk within an acceptable threshold.
 - C** is incorrect because the ALE tells the company how much it could lose if a specific threat became real. The ALE value will go into the cost/benefit analysis, but the ALE does not address the cost of the countermeasure and the benefit of a countermeasure.
 - D** is incorrect because although the assessment of vulnerabilities and threats drives the recognition of a need for a countermeasure, that assessment alone cannot determine what the likely cost

effectiveness will be among competing countermeasures.

9. Which of the following is the LEAST important stage in the life-cycle management of information?

- A. Data specification and classification
 - B. Continuous monitoring and auditing of data access
 - C. Data archival
 - D. Database migration
- D. The movement of accessible data from one repository to another may be required over its lifespan, but typically is not as important as the other phases offered as answers to this question.
- A is incorrect because the determination of *what* the data is, and its classification, is the first essential phase of being able to provide it with the appropriate level of protection.
- B is incorrect because without continuous monitoring and auditing of accesses to sensitive data, breaches cannot be identified, and no assurance of security can be attained.
- C is incorrect because even the most sensitive data will be subject to retention requirements, which means that it will have to be archived for the appropriate period of time, but with the same level of security as when it is in live use.

10. Which of the following are effective methods of preventing data remanence on solid-state devices (SSDs)?

- i. Clearing
- ii. Purging
- iii. Degaussing
- iv. Destruction

- A. i, ii
- B. i, iii, iv
- C. iv
- D. All of the above

- C. Among the options given, physical destruction of the device is the only effective way to ensure no data remains on an SSD.
- A is incorrect because of the way that SSDs write bits to the solid-

state storage. Clearing media is usually no more effective than deletion and will not remove the data. Purging media is usually an attempt to overwrite all bits, which also may not remove the data because of the unique properties of SSDs that differ from those of hard disk devices (HDDs).

- B** is incorrect because degaussing only works by destroying the magnetization of storage devices that rely on it for persistent storage, which SSDs do not.
 - D** is incorrect for all the reasons stated.
- 11.** The requirement of erasure is the end of the media life cycle if the media contains sensitive information. Which of the following best describes purging?
- A.** Changing the polarization of the atoms on the media.
 - B.** It is unacceptable when media are to be reused in the same physical environment for the same purposes.
 - C.** Data formerly on the media is made unrecoverable by overwriting it with a pattern.
 - D.** Information is made unrecoverable, even with extraordinary effort.
- D.** Purging is the removal of sensitive data from a system, storage device, or peripheral device with storage capacity at the end of a processing period. This action is performed in such a way that there is assurance proportional to the sensitivity of the data that the data cannot be reconstructed. Deleting files on a medium does not actually make the data disappear; it only deletes the pointers to where the data in those files still lives on the medium. This is how companies that specialize in restoration can recover the deleted files intact after they have been apparently/accidentally destroyed. Even simply overwriting media with new information may not eliminate the possibility of recovering the previously written information. This is why secure overwriting algorithms are required. And, if any part of a medium containing highly sensitive information cannot be cleared or purged, then physical destruction must take place.
 - A** is incorrect because it describes degaussing, which is an example of purging. A device that performs degaussing generates a coercive magnetic force that reduces the magnetic flux density of the storage media to zero. This magnetic force is what properly erases data from media. Data is stored on magnetic media by the representation of the polarization of the atoms. Degaussing changes this

polarization by using a type of large magnet to bring it back to its original flux (magnetic alignment).

- B** is incorrect because purging is required when media will be repurposed to a different compartment. When media are erased (cleared of their contents), they are said to be sanitized. This means erasing information so that it is not readily retrieved using routine operating system commands or commercially available forensic/data recovery software.
 - C** is incorrect because it describes zeroization, which is an example of purging but does not describe purging itself. Media holding sensitive data must be properly purged, which can be accomplished through zeroization, degaussing, or media destruction.
12. Sam plans to establish mobile phone service using the personal information he has stolen from his former boss. What type of identity theft is this?
- A. Phishing
 - B. True name
 - C. Pharming
 - D. Account takeover
- B.** Identity theft refers to a situation where someone obtains key pieces of personal information, such as a driver's license number, bank account number, credentials, or Social Security number, and then uses that information to impersonate someone else. Typically, identity thieves will use the personal information to obtain credit, merchandise, or services in the name of the victim. This can result in such things as ruining the victim's credit rating, generating false criminal records, and issuing arrest warrants for the wrong individuals. Identity theft is categorized in two ways: true name and account takeover. True name identity theft means the thief uses personal information to open new accounts. The thief might open a new credit card account, establish mobile phone service like Sam, or open a new checking account in order to obtain blank checks.
 - A** is incorrect because phishing is a type of social engineering attack with the goal of obtaining personal information, credentials, credit card numbers, or financial data. The attackers lure, or fish, for sensitive data through various methods. While the goal of phishing is to dupe a victim into handing over his personal information, the goal of identity theft is to use that personal information for personal

or financial gain. An attacker can employ a phishing attack as a means to carry out identity theft.

- C** is incorrect because pharming is a technical attack that is carried out to trick victims into sending their personal information to an attacker via an illegitimate website. The victim types in a web address, such as www.nicebank.com, into his browser. The victim's system sends a request to a poisoned DNS server, which points the victim to a website that is under the attacker's control. Because the site looks and feels like the requested website, the user enters his personal information, which the attacker can then use to commit identity theft.
- D** is incorrect because account takeover identity theft means the imposter uses personal information to gain access to the person's existing accounts, rather than opening a new account. Typically, the thief will change the mailing address on an account and run up a huge bill before the person, whose identity has been stolen, realizes there is a problem. The Internet has made it easier for an identity thief to use the information they've stolen because transactions can be made without any personal interaction.

- 13.** Which of the following are common military categories of data classification?
- A.** Top Secret, Secret, Classified, Unclassified
 - B.** Top Secret, Secret, Confidential, Private
 - C.** Top Secret, Secret, Confidential, Unclassified
 - D.** Classified, Unclassified, Public
- C.** Within the U.S. military complex and national security apparatus, the most common designations for data classification are Unclassified vs. Classified. Within the classifications for "classified" information are Confidential, Secret, and Top Secret. They are defined as follows: Confidential data is that which, if improperly disclosed, could cause harm to national security. Secret data is that which, if improperly disclosed, could cause "serious" harm to national security. And finally Top Secret data is that, which if improperly disclosed, could cause "grave" harm to national security.
 - A** is incorrect because both Top Secret and Secret data are officially Classified.

- B** is incorrect because “Private” is not an official category commonly used by the military. Top Secret, Secret, and Confidential are commonly used categories for classified information in a national security context, and categories such as “For Official Use Only (FOUO)” are commonly designated to protect privacy. But they are not uniformly used.
 - D** is incorrect because although data is commonly designated as one of these three, it is less granular an answer than C.
- 14.** Joan needs to document a data classification scheme for her organization. Which criteria should she use to guide her decisions?
- A.** The value of the data and the age of the data
 - B.** Legal responsibilities based on ISO regulations
 - C.** Who will be responsible for protecting the data and how
 - D.** How an adverse data breach would be handled
- A.** The value of the data—both currently and for some period of time into the future—should be the most critical metric when evaluating data classification. That value should consider both the value of the data to the organization over time and the value of the data to an adversary. The age of the data and its usefulness to both the organization and any other organization must be taken into account as well.
 - B** is incorrect because although any organization may be subject to legal regulatory responsibilities with respect to data classification, either within the United States or internationally, the ISO merely defines standards, not requirements or regulations.
 - C** is incorrect because the designation of the roles and responsibilities as to how any data must be protected should not be determined by the operators of the scheme. Those responsible for the protection of the data must not perform those duties at their own discretion.
 - D** is incorrect because, once again, the reliability of the staff in handling an adverse event should not be a question of the discretion of their superiors or those who hired them.
- 15.** Which of the following means of data removal makes the data unrecoverable even with extraordinary effort, such as with physical forensics in a laboratory?
- A.** Deletion of the data

- B.** Sanitization of the media
- C.** Purging via overwriting
- D.** None of these will work

- C.** Purging means making data unavailable even by physical forensic efforts. This is typically achieved via overwriting each and every sector of the media upon which the data had been stored.
- A** is incorrect. Mere deletion of data with operating system commands typically leaves the data present on the storage media while marking the clusters or blocks that still store it available for later reuse.
- B** is incorrect. Although a stronger method than merely deleting data with operating system commands, sanitization usually refers to making storage media reusable within the same security context. With magnetic media, this is commonly done via degaussing.
- D** is incorrect. With appropriate diligence, data remanence can be dealt with successfully via purging techniques.

- 16.** When classifying information, its sensitivity refers to:
- A.** The magnitude of damage or loss an organization would sustain if the information was lost or made unavailable
 - B.** The magnitude of damage or loss an organization would sustain if the information was revealed to unauthorized individuals
 - C.** The ways in which an organization protects its information from third parties
 - D.** The ways in which an organization protects its information from internal abuse
- B.** Sensitivity refers to the confidentiality of data and the need to control who has access to learn its contents. If an unauthorized person gaining this sort of access would potentially damage the organization it is deemed sensitive. The magnitude of damage or loss such a breach would incur determines the degree of sensitivity of that data.
 - A** is incorrect because this describes the information's criticality, not sensitivity.
 - C** is incorrect because the means by which an organization protects the confidentiality of its data refers to security controls. The types

of controls put in place are determined by levels of sensitivity.

- D** is incorrect for most of the same reasons as C, but also because mere “internal abuse” is a relatively narrow scope for the consideration of the protection of sensitive data.

17. When classifying information, its criticality refers to:

- A.** The magnitude of damage or loss an organization would sustain if the information was lost or made unavailable
 - B.** The magnitude of damage or loss an organization would sustain if the information was revealed to unauthorized individuals
 - C.** The ways in which an organization protects its information from third parties
 - D.** The ways in which an organization protects its information from internal abuse
- A.** Data is considered critical to a business operation if key business processes depend on that data being available at all necessary times. If the loss of that availability would damage the business’s ability to function, the magnitude of the resulting disruption determines that data’s criticality.
 - B** is incorrect because it describes data sensitivity, not criticality.
 - C** is incorrect because the means by which an organization protects the availability of its data refers to security controls. The types of controls put in place are determined by levels of criticality.
 - D** is incorrect for most of the same reasons as C, but also because mere “internal abuse” is a relatively narrow scope for the consideration of the protection of critical data.

18. Which of the following classification levels are most commonly used in commercial industry?

- A.** Confidential, Secret, Top Secret
 - B.** Unclassified, Sensitive but unclassified
 - C.** Private, Proprietary, Sensitive
 - D.** Unrestricted, For government use only
- C.** Private, Proprietary, and Sensitive are common labels used in private industry, and describe decreasing levels of data sensitivity. The last, not listed, would be Public.

- A** is incorrect because these labels are the most commonly used designations in government organizations, specifically for military and national security data.
 - B** is incorrect because these labels are most commonly used in civilian government organizations to designate data not officially classified for military or national security purposes.
 - D** is incorrect because neither of these terms is common parlance in any environment.
- 19.** Which of the following classification levels are most commonly used in military environments?
- A.** Confidential, Secret, Top Secret
 - B.** Unclassified, Sensitive but unclassified
 - C.** Private, Proprietary, Sensitive
 - D.** Unrestricted, For government use only
- A.** These classifications are the most commonly used official classification levels within military and national security oriented government organizations, specifying sensitivity from least to most in the order presented.
 - B** is incorrect because these labels are more commonly used to describe the sensitivity of data within civilian governmental agencies, outside the sphere of military or national security operations.
 - C** is incorrect because these labels are most commonly associated with use in private industry.
 - D** is incorrect because neither of these terms is common parlance in any environment.
- 20.** Which of the following is true regarding data retention requirements?
- A.** Legal requirements for data retention are uniform across all regulated business sectors, and must be followed to reduce risk of criminal litigation.
 - B.** To comply with various data retention regulations, it is best to retain all data to the lengthiest legal requirement.
 - C.** Retaining the largest amount of data possible makes responding to electronic discovery (e-discovery) orders easier and more straightforward.

- D.** A well-documented policy for the retention of data is a minimum but necessary component of regulatory compliance.
- D.** Such a policy is certainly a necessary component for regulatory compliance, as no organization can hope to satisfy such requirements without an overt statement from executive management as to what exactly will be done. It is also a bare minimum, as enforced procedures must also be in place to satisfy the policy directives.
- A** is incorrect because it's simply not true for several reasons. First, such requirements are not at all uniform, neither between regulations nor across business sectors. Second, failure to adhere to them, whatever they may be, opens up the door for civil litigation risks in addition to criminal ones.
- B** is a common fallacy, but completely false. Retaining data in this manner is likely to result in too much data being retained for too long a period, which is unnecessarily burdensome at a minimum, and could potentially increase legal liability.
- C** is incorrect because retaining larger amounts of data than necessary makes responding to e-discovery orders more rather than less difficult, as there is more data to search through to find the data required.

21. Why is the issue of data remanence sometimes problematic?

- A.** Data retention policies don't usually specify when data should be deleted.
- B.** With most file systems, deleting data doesn't ensure that it cannot be recovered.
- C.** With most modern file systems, accidentally overwriting a small part of a file makes the remaining remnants unrecoverable.
- D.** Physical destruction is the only way to ensure data cannot be recovered, and this is usually too prohibitively expensive.
- B.** With most file systems, the operating system's action of deleting a file merely marks the blocks or clusters that are used to store the file's contents as "unused" and so available to be used subsequently to store other files. Unless the blocks or clusters are actually used subsequently, the data that they contain remains, and can be recovered forensically.
- A** is incorrect because one of the main purposes of data retention

policies is to specify exactly when data can and should be expunged.

- C** is incorrect because overwriting a few blocks or clusters in use by a file, either accidentally or on purpose, will leave the remaining file storage untouched, and likely recoverable at least in part.
 - D** is incorrect, because while physical destruction is often the surest way to completely eradicate all trace of data (as with burning to ash), there are other methods that can reasonably ensure that it cannot be recovered.
- 22.** For which of the following physical media is degaussing a relatively cheap and effective means of eradicating data?
- A.** Optical disks (CDs/DVDs)
 - B.** Backup tapes
 - C.** USB thumb drives
 - D.** Hard disk drives (HDDs)
- B.** Degaussing only works with magnetic media, and is relatively inexpensively performed on tapes, whose magnetic fields are relatively weak and not well shielded from external disruption.
 - A** is incorrect because optical disks are entirely unaffected by magnetic fields. Indeed, “write once read many” (WORM) disks can be effectively disposed of only through physical destruction.
 - C** is incorrect because USB thumb drives use solid-state storage, which is not easily affected by magnetic fields.
 - D** is incorrect because, although HDDs do use magnetic storage and so can be degaussed, the devices required to produce the magnetic fields necessary to disrupt their much stronger storage and shielding are relatively cost prohibitive compared to tape degaussers.
- 23.** Which of the following approaches is the most effective way for an organization to reduce its liability regarding the protection of private data?
- A.** Collect any and all data that has business utility, but ensure that the legal team has reviewed and approved all policies with respect to its protection.
 - B.** Never collect or store any privacy-protected data.
 - C.** Limit the amount of private data collected to that which is legally

allowed.

- D.** Limit the amount of private data collected to that which is required for business functions.
- D.** Some amount of private data is almost certainly required for necessary business functions, if only for human resources management. Limiting the collection of such data as much as is possible is certainly the best practice, as an organization doesn't have to protect what it doesn't possess.
- A** is incorrect because the wanton collection of any and all data that has business utility, without the evaluation of the risk that its possession imposes, is a recipe for disaster regardless of its legality.
- B** is incorrect because never collecting or storing any privacy-protected data is certainly impractical and probably impossible. By necessity, even payroll data contains private information about an organization's employees.
- C** is incorrect because, as with option A, the legality of the collection of private data is not the only concern, or where unnecessary risks can be identified. Legally collected data is routinely breached to ill effect.
- 24.** When protecting information assets, which of the following security controls is most effective for data in motion?
- A.** Requiring whole-disk encryption for all devices with the Advanced Encryption Standard (AES)
- B.** Implementing encryption with Transport Layer Security (TLS) or IPSec
- C.** Implementing whole-memory encryption with the storage of keys in CPU registers
- D.** Requiring the use of next-generation firewalls (NGFWs) and/or network-based intrusion prevention systems (NIPSSs)
- B.** Using either strong levels of encryption with TLS or employing encrypted IPSec tunnels is the best way to protect the confidentiality of data as it is being transmitted over the network, potentially in the presence of adversaries who may be capable of intercepting it.
- A** is incorrect because it is an implementation of protection for data at rest. Data that is being transmitted over the network is likely to have been decrypted from its resting state for processing prior to

transmission, so whole-disk encryption with AES is no guarantee that the data in motion cannot be easily intercepted in its cleartext form.

- C** is incorrect because it describes what may become a means of encrypting data in use during processing, though which has yet to be more than experimentally implemented.
 - D** is incorrect because these security measures are designed to protect networks and endpoints from malicious, intrusive activities rather than to protect the confidentiality of data in transit.
- 25.** When protecting information assets, which of the following security controls is most effective for data at rest?
- A.** Requiring whole-disk encryption for all devices with the Advanced Encryption Standard (AES)
 - B.** Implementing encryption with Transport Layer Security (TLS) or IPSec
 - C.** Implementing whole-memory encryption with the storage of keys in CPU registers
 - D.** Requiring the use of next-generation firewalls (NGFWs) and/or network-based intrusion prevention systems (NIPSSs)
- A.** The best method for protecting the confidentiality of data at rest, when it is being neither processed nor transmitted, is to encrypt it prior to storage. Whole-disk encryption seeks to achieve this for all stored data, and AES is the most commonly trusted algorithm for this use.
 - B** is incorrect because TLS and IPSec are algorithms for protecting data in transit, and they provide no mechanism for the protection of data prior to or after transmission.
 - C** is incorrect because it describes what may become a means of encrypting data in use during processing, though which has yet to be more than experimentally implemented.
 - D** is incorrect because these security measures are designed to protect networks and endpoints from malicious, intrusive activities rather than to protect the confidentiality of data at rest.
- 26.** Which of the following is the LEAST effective security control regarding sensitive data stored on mobile devices?
- A.** Back up all devices to an organizationally managed repository.

- B. Implement full-volume encryption on all mobile devices.
 - C. Require that all mobile devices be wipeable remotely if stolen or misplaced.
 - D. Enact a policy prohibiting the access or storage of sensitive corporate data on personal mobile devices.
- D.** Merely enacting a policy does not guarantee that it will be followed to good effect, particularly if it is one that is both difficult to enforce technically and unpopular among users. The use of personal devices to store and process corporate data such as e-mails and office documents is extremely popular and widespread. Consequently, realistic technical measures must be brought to bear.
- A** is incorrect because backing up all devices to an organizationally managed repository is an extremely important measure to protect corporate data, and one that is unlikely to result in intentional user circumvention.
- B** is also incorrect for the exact same reasons as A.
- C** is incorrect because, although some users will likely resist agreeing to what they perceive as a draconian measure, requiring remote wiping capability is a legitimate and effective security control, and users' agreement to it can be made a condition to the use of even personally owned devices in the corporate environment. Consent can and should be documented as part of a signed employee agreement, and the approved device should be inventoried as a corporate asset.

- 27.** In the modern era, are paper records still a significant concern in the protection of enterprise data assets? If so, why? If not, why not?
- A. Yes, because the most sensitive data is usually only stored in printed form
 - B. Yes, because printed copies are still commonly produced, are more difficult to track, and are commonly not disposed of properly
 - C. No, because the amount of sensitive data that is ever printed out is exceptionally small by comparison
 - D. No, because sensitive data that is printed out is the easiest to properly destroy
- B.** Any media that may contain sensitive enterprise data should be a concern when developing policies and procedures for its protection. This is especially true considering the ease with which copies can

be made and disposed of, and the near impossibility of tracking these actions in most environments.

- A** is incorrect because it inaccurately explains why paper records are still a significant concern in the protection of enterprise data assets. It is not true that the most sensitive data is usually only stored as hard copies. Printed data most commonly originates in digital form.
 - C** is incorrect because, even assuming that only a small amount of sensitive data is ever printed to paper, printed copies are nearly impossible to track and protect and thus still are a significant concern in the protection of enterprise data assets.
 - D** is incorrect because although printed data may be the easiest to physically destroy, via highly granular cross-cut shredders or burning, it is the hardest medium to ensure it is disposed of properly.
- 28.** When selecting and implementing information asset protection standards, the process of scoping refers to which of the following?
- A.** Choosing the standard that most closely provides for regulatory compliance within your organization's industry
 - B.** Altering provisions of the chosen standard so that they are more relevant to your organization's environment
 - C.** Eliminating from implementation the parts of the chosen standard that are not relevant to your organization's environment
 - D.** Making decisions with respect to internal penalties for noncompliance with the chosen standard
- C.** Comprehensive data security standards are likely to include considerations that do not apply to all organizations. Consequently, identifying and eliminating the measures that are irrelevant to the enterprise (*scoping*) simplifies compliance efforts.
 - A** is incorrect because selecting the data security standard that is most appropriate to the organization's business operations is a critical first step, but scoping that standard to the enterprise's needs comes later.
 - B** is incorrect because it describes tailoring the standard for enterprise use, rather than scoping.
 - D** is incorrect because, while making these decisions is important when implementing standards, they are not necessarily part of scoping activities.

- 29.** When selecting and implementing information asset protection standards, why is tailoring an important process?
- A. Because the penalties for noncompliance provided for by the chosen standard may be too severe and unrealistic
 - B. Because some of the provisions of the chosen standard might not apply to your organization's environment
 - C. Because some of the provisions of the chosen standard might better address your organization's environment if modified slightly
 - D. Because not all standards are a good fit for your organization, and so it is important to choose the best one
- C. Comprehensive data security standards are likely to include provisions that are fairly generic. Consequently, it can be useful to tailor them to be more specific to your enterprise's use of IT systems and networks, and the data they contain.
- A is incorrect because data security standards are rarely so specific that they describe specific penalties for noncompliance. This is commonly an enterprise-specific decision regardless of the standards adopted.
- B is incorrect because scoping, not tailoring, deals with inapplicable provisions. Tailoring applies to the provisions of the standard that remain after scoping occurs.
- D is incorrect because selecting the data security standard that is most appropriate to the organization's business operations is a critical first step, but tailoring that standard to the enterprise's needs comes later.
- 30.** When implementing data leak prevention (DLP), which is the first, most critical step?
- A. Examine the flow of sensitive data in your organization to better understand what is proper, and what should not be allowed.
 - B. Conduct a risk assessment to determine what the best data protection strategy will be for your organization.
 - C. Evaluate the features of the available products in order to determine which fits best in your organization's infrastructure.
 - D. Conduct an inventory of all the data in your organization in order to characterize and prioritize its sensitivity.

- D.** It is impossible to design and implement a strategy for the prevention of data leakage without first identifying the data that requires protection and categorizing it for prioritization of protection mechanisms. This is the necessary first step.
- A** is incorrect because, although examining data flow is an extremely useful approach to identifying risks to sensitive data, identifying and categorizing the data with respect to its sensitivity is a necessary prior step.
- B** is incorrect because, like A, although conducting a risk assessment is a necessary step in the implementation of any DLP strategy, it can be performed only after the data requiring protection has been identified and categorized as to priority.
- C** is incorrect because, again, although evaluating product features will likely be part of the DLP deployment strategy, particularly where commercial or other off-the-shelf implementations are an important component of the proposed solution, this should only follow the steps previously described.

Security Architecture and Engineering

This domain includes questions from the following topics:

- System architecture
 - Trusted computing base and security mechanisms
 - Information security software models
 - Assurance evaluation criteria and ratings
 - Certification and accreditation processes
 - Distributed systems security
 - Cryptography components and their relationships
 - Steganography
 - Public key infrastructure (PKI)
 - Site and facility design considerations
 - Physical security risks, threats, and countermeasures
 - Electric power issues and countermeasures
 - Fire prevention, detection, and suppression
-

As the complexity of computer systems increases, so, too, does security. Architectures, frameworks, and models have been developed to incorporate security and protection mechanisms in systems and hardware. In addition, system and hardware manufacturers seek evaluation, certification, and accreditation to assure buyers that their products are secure. As a CISSP, you need to understand these architectures and models as a foundation for the attacks that are committed against them and also how to protect them. Knowledge of assurance evaluation criteria and ratings and certification and accreditation processes will help you be an educated buyer of enterprise

QUESTION

1. Lacy's manager has tasked her with researching an intrusion detection system for a new dispatching center. Lacy identifies the top five products and compares their ratings. Which of the following is the evaluation criteria framework most in use today for these types of

purposes?

- A.** ITSEC
 - B.** Common Criteria
 - C.** Red Book
 - D.** Orange Book
- 2.** Certain types of attacks have been made more potent by which of the following advances to microprocessor technology?
- A.** Increased circuits, cache memory, and multiprogramming
 - B.** Dual mode computation
 - C.** Direct memory access I/O
 - D.** Increases in processing power
- 3.** CPUs and operating systems can work in two main types of multitasking modes. What controls access and the use of system resources in preemptive multitasking mode?
- A.** The user and application
 - B.** The program that is loaded into memory
 - C.** The operating system
 - D.** The CPU and user
- 4.** Virtual storage combines RAM and secondary storage for system memory. Which of the following is a security concern pertaining to virtual storage?
- A.** More than one process uses the same resource.
 - B.** It allows cookies to remain persistent in memory.
 - C.** It allows for side-channel attacks to take place.
 - D.** Two processes can carry out a denial of service.
- 5.** Which of the following is a common association of the Clark-Wilson access model?
- A.** Chinese Wall
 - B.** Access tuple
 - C.** Read up and write down rule
 - D.** Well-formed transactions

6. Which of the following correctly describes the relationship between the reference monitor and the security kernel?

 - A. The security kernel implements and enforces the reference monitor.
 - B. The reference monitor is the core of the trusted computing base, which is made up of the security kernel.
 - C. The reference monitor implements and enforces the security kernel.
 - D. The security kernel, aka abstract machine, implements the reference monitor concept.
7. The trusted computing base (TCB) ensures security within a system when a process in one domain must access another domain in order to retrieve sensitive information. What function does the TCB initiate to ensure that this is done in a secure manner?

 - A. I/O operational execution
 - B. Process deactivation
 - C. Execution domain switching
 - D. Virtual memory to real memory mapping
8. Which of the following best defines a virtual machine?

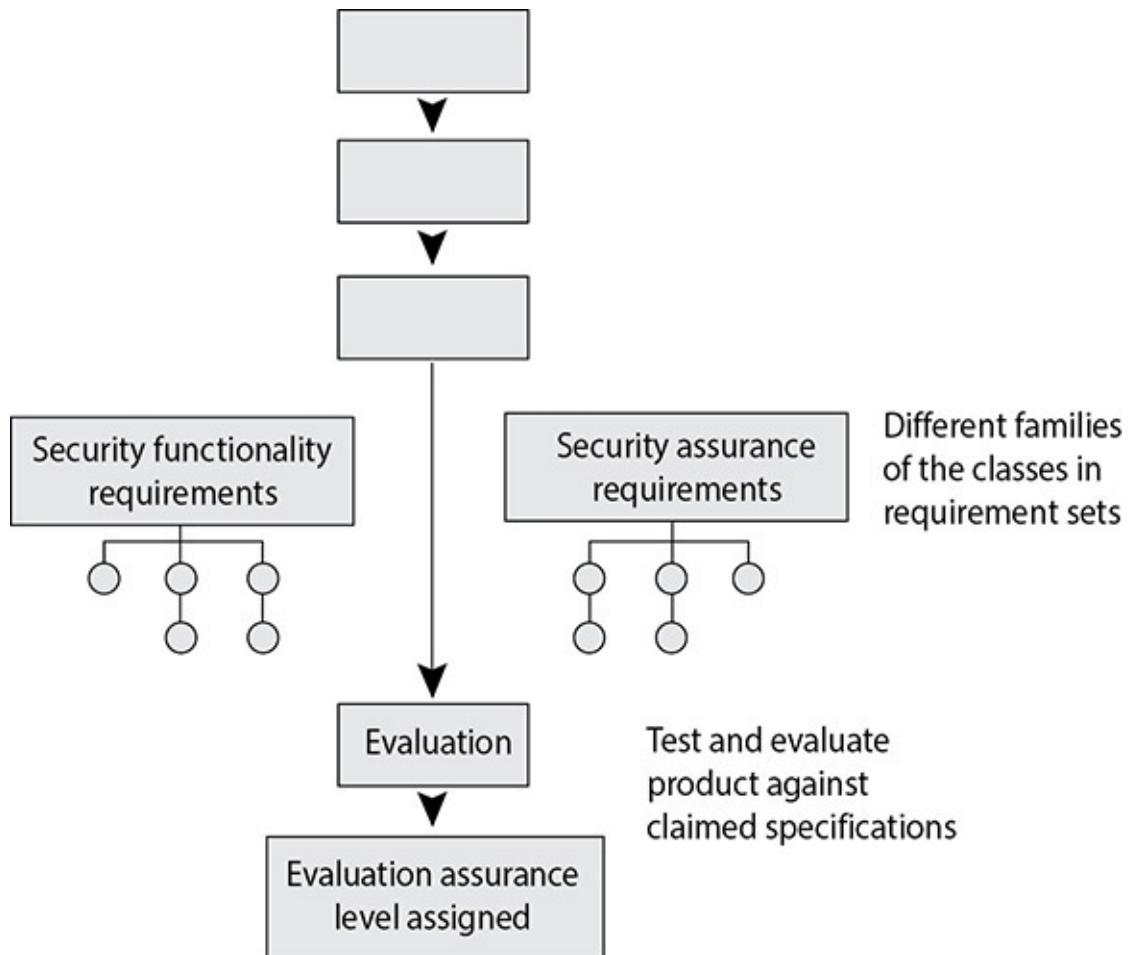
 - A. A virtual instance of an operating system
 - B. A piece of hardware that runs multiple operating system environments simultaneously
 - C. A physical environment for multiple guests
 - D. An environment that can be fully utilized while running legacy applications
9. Virtualization offers many benefits. Which of the following incorrectly describes virtualization?

 - A. Virtualization simplifies operating system patching.
 - B. Virtualization can be used to build a secure computing platform.
 - C. Virtualization can provide fault and error containment.
 - D. Virtual machines offer powerful debugging capabilities.
10. Which security architecture model defines how to securely develop access rights between subjects and objects?

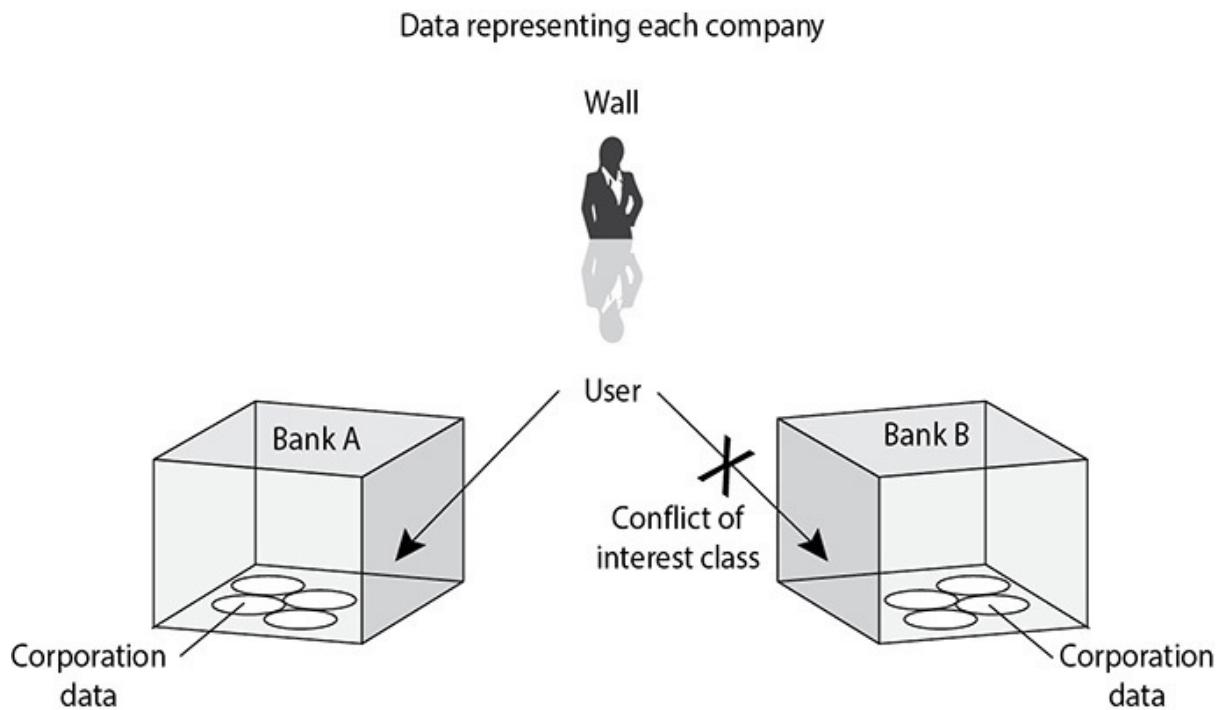
 - A. Brewer-Nash

- B.** Clark-Wilson
 - C.** Graham-Denning
 - D.** Bell-LaPadula
- 11.** Operating systems can be programmed to carry out different methods for process isolation. Which of the following refers to a method in which an interface defines how communication can take place between two processes and no process can interact with the other's internal programming code?
- A.** Virtual mapping
 - B.** Encapsulation of objects
 - C.** Time multiplexing
 - D.** Naming distinctions
- 12.** Which of the following is not a responsibility of the memory manager?
- A.** Use complex controls to ensure integrity and confidentiality when processes need to use the same shared memory segments.
 - B.** Limit processes to interact only with the memory segments assigned to them.
 - C.** Swap contents from RAM to the hard drive as needed.
 - D.** Run an algorithm to identify unused committed memory and inform the operating system that the memory is available.
- 13.** Frank is responsible for the security of his company's online applications, web servers, and web-based activities. The web applications have the capability of being dynamically "locked" so that multiple users cannot edit a web page at the same time and overwrite each other's work. An audit uncovered that although this software-locking capability was properly configured, multiple users were still able to modify the same web page at the same time. Which of the following best describes what is taking place in this situation?
- A.** Buffer overflow
 - B.** Blind SQL injection
 - C.** Cross-site request forgery
 - D.** Time-of-check/time-of-use attack
- 14.** There are several different important pieces to the Common Criteria. Which of the following best describes the first of the missing

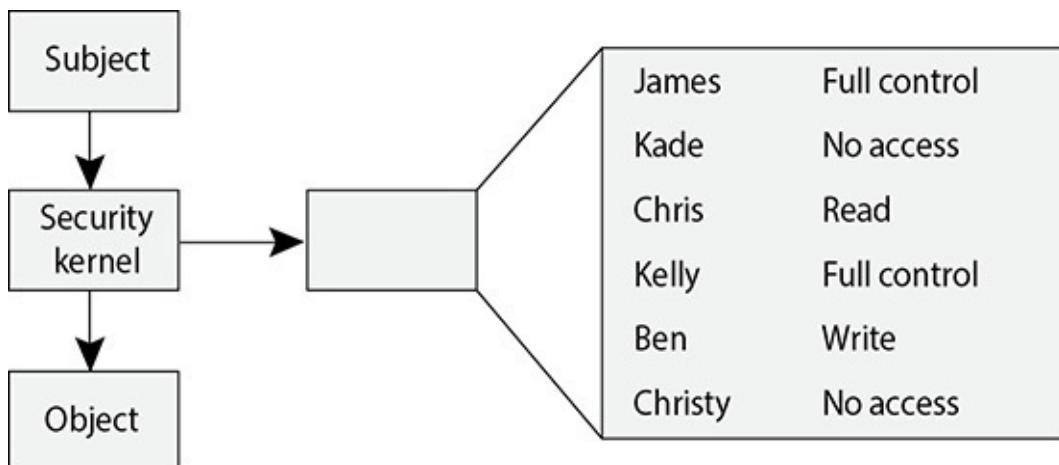
components?



- A. Target of evaluation
 - B. Protection profile
 - C. Security target
 - D. EALs
15. Different access control models provide specific types of security measures and functionality in applications and operating systems. What model is being expressed in the graphic that follows?

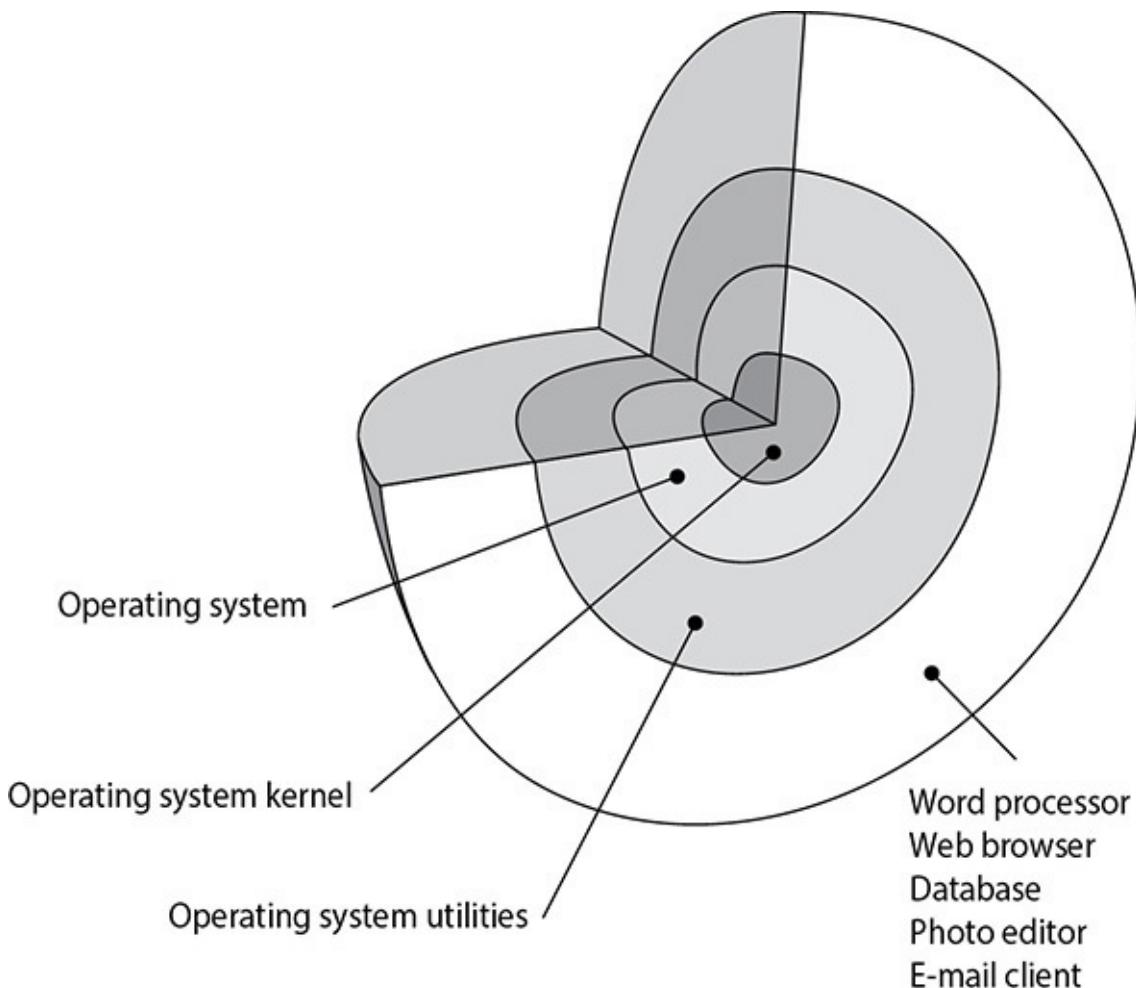


- A. Noninterference
 - B. Biba
 - C. Bell-LaPadula
 - D. Chinese Wall
- 16.** There are many different types of access control mechanisms that are commonly embedded into all operating systems. Which of the following is the mechanism that is missing in this graphic?

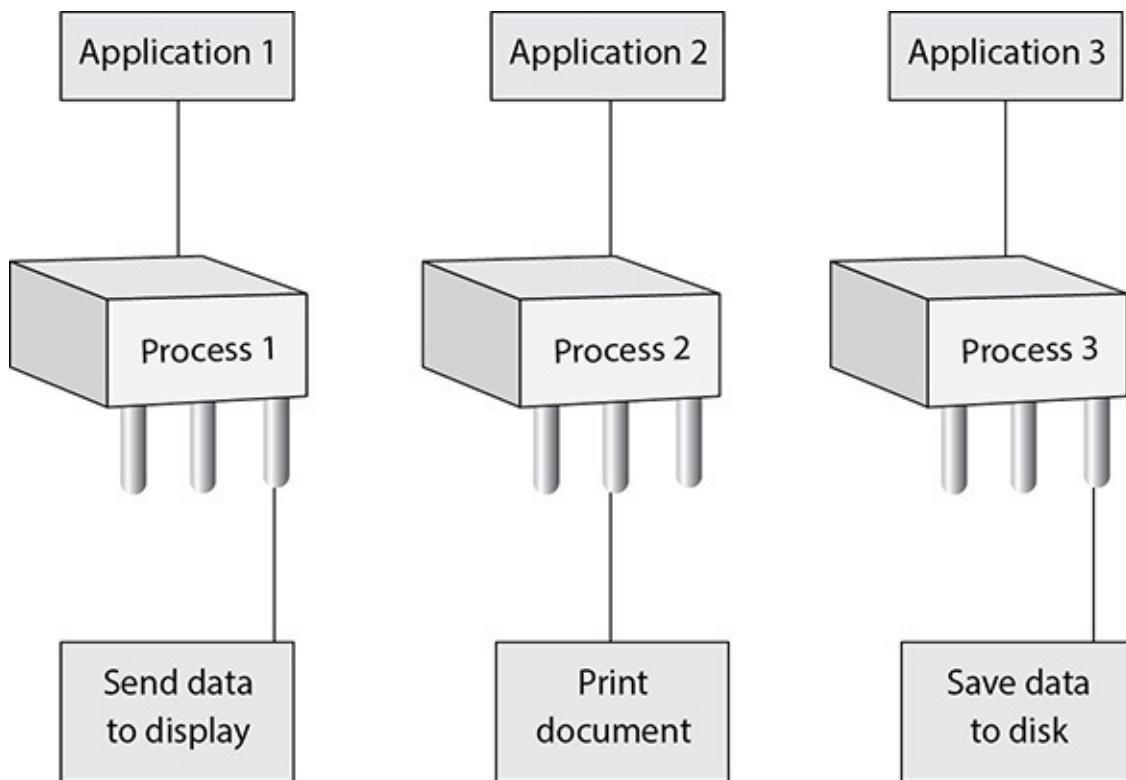


- A. Trusted computing base
- B. Security perimeter
- C. Reference monitor
- D. Domain

- 17.** There are several security enforcement components that are commonly built into operating systems. Which component is illustrated in the graphic that follows?



- A. Virtual machines
 - B. Interrupt
 - C. Cache memory
 - D. Protection rings
- 18.** A multitasking operating system can have several processes running at the same time. What are the components within the processes that are shown in the graphic that follows?



- A. Threads
- B. Registers
- C. Address buses
- D. Process tables

The following scenario applies to questions 19 and 20.

Charlie is a new security manager at a textile company that develops its own proprietary software for internal business processes. Charlie has been told that the new application his team needs to develop must comply with the ISO/IEC 42010 standard. He has found out that many of the critical applications have been developed in the C programming language and has asked for these applications to be reviewed for a specific class of security vulnerabilities.

- 19.** Which of the following best describes the standard Charlie's team needs to comply with?
- A. International standard on system design to allow for better quality, interoperability, extensibility, portability, and security
 - B. International standard on system security to allow for better threat modeling
 - C. International standard on system architecture to allow for better quality, interoperability, extensibility, portability, and security

- D. International standard on system architecture to allow for better quality, extensibility, portability, and security
- 20.** Which of the following is Charlie most likely concerned with in this situation?
 - A. Injection attacks
 - B. Memory block
 - C. Buffer overflows
 - D. Browsing attacks

The following scenario applies to questions 21 and 22.

Tim's development team is designing a new operating system. One of the requirements of the new product is that critical memory segments need to be categorized as nonexecutable, with the goal of reducing malicious code from being able to execute instructions in privileged mode. The team also wants to make sure that attackers will have a difficult time predicting execution target addresses.

- 21.** Which of the following best describes the type of protection that needs to be provided by this product?
 - A. Hardware isolation
 - B. Memory induction application
 - C. Data execution prevention
 - D. Domain isolation protection
- 22.** Which of the following best describes the type of technology the team should implement to increase the work effort of buffer overflow attacks?
 - A. Address space layout randomization
 - B. Memory induction application
 - C. Input memory isolation
 - D. Read-only memory integrity checks

The following scenario applies to questions 23, 24, and 25.

Operating systems have evolved and changed over the years. The earlier operating systems were monolithic and did not segregate critical processes from noncritical processes. As time went on, operating system vendors started to reduce the amount of programming code that ran in kernel mode. Only the

absolutely necessary code ran in kernel mode, and the remaining operating system code ran in user mode. This architecture introduced performance issues, which required the operating system vendors to reduce the critical operating system functionality to microkernels and allow the remaining operating system functionality to run in client/server models within kernel mode.

- 23.** Which of the following best describes the second operating system architecture described in the scenario?
 - A.** Layered
 - B.** Microkernel
 - C.** Monolithic
 - D.** Kernel based
- 24.** Which of the following best describes why there was a performance issue in the context of the scenario?
 - A.** Bloated programming code
 - B.** I/O and memory location procedures
 - C.** Mode transitions
 - D.** Data and address bus architecture
- 25.** Which of the following best describes the last architecture described in this scenario?
 - A.** Hybrid microkernel
 - B.** Layered
 - C.** Monolithic
 - D.** Hardened and embedded
- 26.** As with logical access controls, audit logs should be produced and monitored for physical access controls. Which of the following statements is correct about auditing physical access?
 - A.** Unsuccessful access attempts should be logged but only need to be reviewed by a security guard.
 - B.** Only successful access attempts should be logged and reviewed.
 - C.** Only unsuccessful access attempts during unauthorized hours should be logged and reviewed.
 - D.** All unsuccessful access attempts should be logged and reviewed.

- 27.** An outline for a physical security design should include program categories and the necessary countermeasures for each. What category do locks and access controls belong to?
- A. Assessment
 - B. Deterrence
 - C. Response
 - D. Delay
- 28.** What discipline combines the physical environment and the sociology issues that surround it to reduce crime rates and the fear of crime?
- A. Layered defense model
 - B. Target hardening
 - C. Crime Prevention Through Environmental Design
 - D. Natural access control
- 29.** David is preparing a server room at a new branch office. What locking mechanisms should he use for the primary and secondary server room entry doors?
- A. The primary and secondary entrance doors should have access controlled through a swipe card or cipher lock.
 - B. The primary entrance door should have access controlled through a security guard. The secondary doors should be secured from the inside and allow no entry.
 - C. The primary entrance door should have access controlled through a swipe card or cipher lock. The secondary doors should have a security guard.
 - D. The primary entrance door should have access controlled through a swipe card or cipher lock. Secondary doors should be secured from the inside and allow no entry.
- 30.** Before an effective physical security program can be rolled out, a number of steps must be taken. Which of the following steps comes first in the process of rolling out a security program?
- A. Create countermeasure performance metrics.
 - B. Conduct a risk analysis.
 - C. Design the program.

- D.** Implement countermeasures.
- 31.** A number of measures should be taken to help protect devices and the environment from electric power issues. Which of the following is best to keep voltage steady and power clean?
- A.** Power line monitor
 - B.** Surge protector
 - C.** Shielded cabling
 - D.** Regulator
- 32.** Crime Prevention Through Environmental Design (CPTED) is a discipline that outlines how the proper design of a physical environment can reduce crime by directly affecting human behavior. Of CPTED's three main components, what is illustrated in the following photo?
- 
- A.** Natural surveillance
 - B.** Target hardening
 - C.** Natural access control
 - D.** Territorial reinforcement
- 33.** There are five different classes of fire. Each depends upon what is on fire. Which of the following is the proper mapping for the items missing in the provided table?

Fire Class	Type of Fire	Elements of Fire	Suppression Method
Class A			Water, soda acid
Class B			CO ₂ , FM-200
Class C			Gas (Halon) or CO ₂ , nonconductive extinguishing agent
Class D			Dry chemicals
Class K			A wet chemical

- A. Class D—combustible metals
- B. Class C—liquid
- C. Class B—electrical
- D. Class A—electrical
34. Electrical power is being provided more through smart grids, which allow for self-healing, resistance to physical and cyberattacks, increased efficiency, and better integration of renewable energy sources. Countries want their grids to be more reliable, resilient, flexible, and efficient. Why does this type of evolution in power infrastructure concern many security professionals?
- A. Allows for direct attacks through Power over Ethernet
- B. Increased embedded software and computing capabilities
- C. Does not have proper protection against common web-based attacks
- D. Power fluctuation and outages directly affect computing systems

The following scenario applies to questions 35, 36, and 37.

Mike is the new CSO of a large pharmaceutical company. He has been asked to revamp the company's physical security program and better align it with the company's information security practices. Mike knows that the new physical security program should be made up of controls and processes that support the following categories: deterrent, delaying, detection, assessment, and response.

35. Mike's team has decided to implement new perimeter fences and warning signs against trespassing around the company's facility. Which of the categories listed in the scenario do these countermeasures map to?
- A. Deterrent

- B.** Delaying
 - C.** Detection
 - D.** Assessment
- 36.** Mike's team has decided to implement stronger locks on the exterior doors of the new company's facility. Which of the categories listed in the scenario does this countermeasure map to?
- A.** Deterrent
 - B.** Delaying
 - C.** Detection
 - D.** Assessment
- 37.** Mike's team has decided to hire and deploy security guards to monitor activities within the company's facility. Which of the categories listed in the scenario does this countermeasure map to?
- A.** Delaying
 - B.** Detection
 - C.** Assessment
 - D.** Recall

The following scenario applies to questions 38, 39, and 40.

Greg is the security facility officer of a financial institution. His boss has told him that visitors need a secondary screening before they are allowed into sensitive areas within the building. Greg has also been told by the network administrators that after the new HVAC system was installed throughout the facility, they have noticed that power voltage to the systems in the data center sags.

- 38.** Which of the following is the best control that Greg should ensure is implemented to deal with his boss's concern?
- A.** Access and audit logs
 - B.** Mantrap
 - C.** Proximity readers
 - D.** Smart card readers
- 39.** Which of the following best describes the situation that the network administrators are experiencing?
- A.** Brownouts

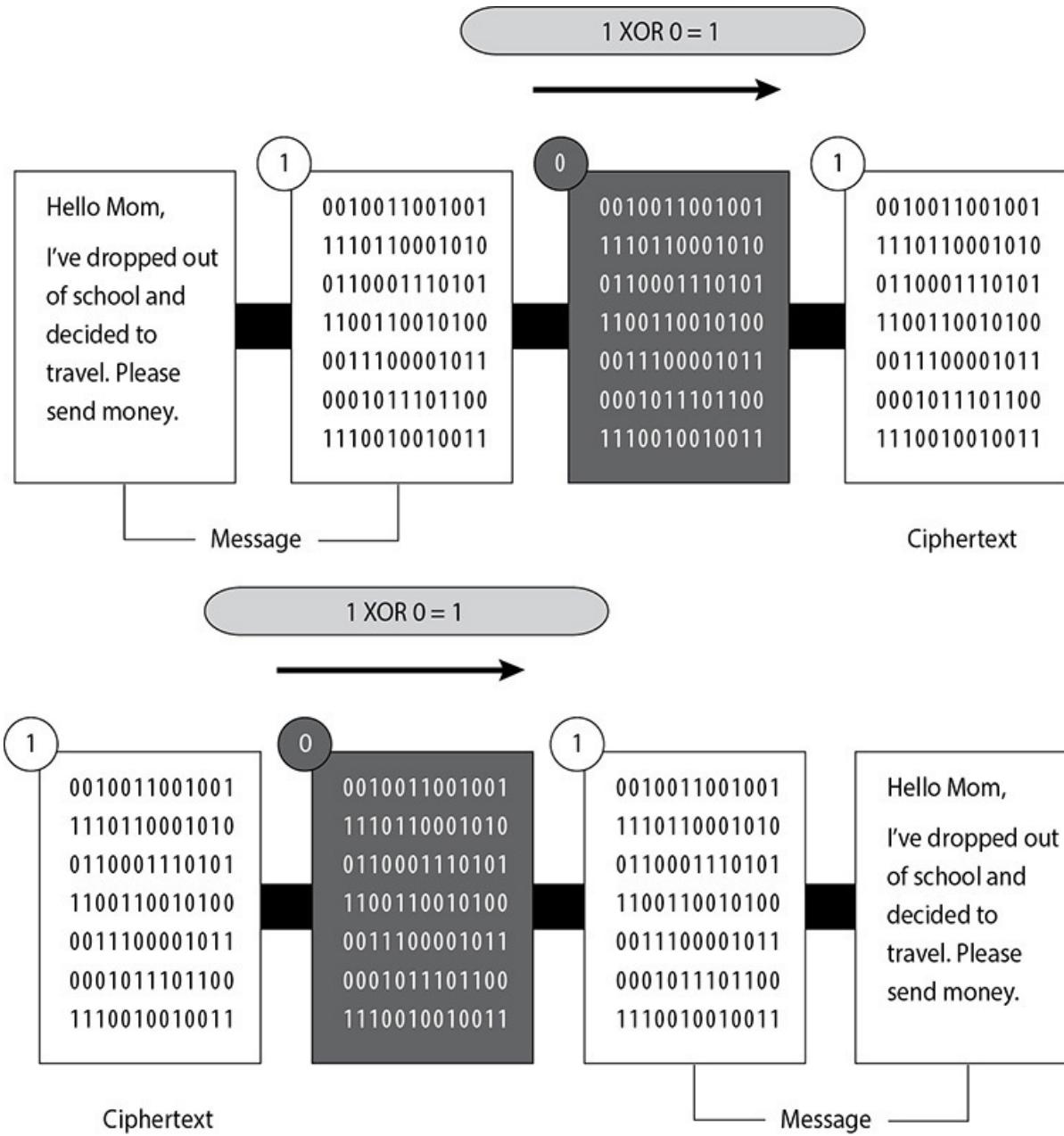
- B.** Surges
 - C.** In-rush current
 - D.** Power line interference
- 40.** Which of the following is a control that Greg's team could implement to address the network administrators' issue?
- A.** Secondary feeder line
 - B.** Insulated grounded wiring
 - C.** Line conditioner
 - D.** Generator
- 41.** There are several components involved with steganography. Which of the following refers to a file that has hidden information in it?
- A.** Stegomedium
 - B.** Concealment cipher
 - C.** Carrier
 - D.** Payload
- 42.** Which of the following incorrectly describes steganography?
- A.** It is a type of security through obscurity.
 - B.** Modifying the most significant bit is the most common method used.
 - C.** Steganography does not draw attention to itself like encryption does.
 - D.** Media files are ideal for steganographic transmission because of their large size.
- 43.** Which of the following correctly describes a drawback of symmetric key systems?
- A.** Computationally less intensive than asymmetric systems
 - B.** Work much more slowly than asymmetric systems
 - C.** Carry out mathematically intensive tasks
 - D.** Key must be delivered via secure courier
- 44.** Which of the following occurs in a PKI environment?
- A.** The RA creates the certificate, and the CA signs it.

- B. The CA signs the certificate.
 - C. The RA signs the certificate.
 - D. The user signs the certificate.
45. Which of the following correctly describes the difference between public key cryptography and public key infrastructure?
- A. Public key cryptography is the use of an asymmetric algorithm, while public key infrastructure is the use of a symmetric algorithm.
 - B. Public key cryptography is used to create public/private key pairs, and public key infrastructure is used to perform key exchange and agreement.
 - C. Public key cryptography provides authentication and nonrepudiation, while public key infrastructure provides confidentiality and integrity.
 - D. Public key cryptography is another name for asymmetric cryptography, while public key infrastructure consists of public key cryptographic mechanisms.
46. Which of the following best describes Key Derivation Functions (KDFs)?
- A. Keys are generated from a master key.
 - B. Session keys are generated from each other.
 - C. Asymmetric cryptography is used to encrypt symmetric keys.
 - D. A master key is generated from a session key.
47. An elliptic curve cryptosystem is an asymmetric algorithm. What sets it apart from other asymmetric algorithms?
- A. It provides digital signatures, secure key distribution, and encryption.
 - B. It computes discrete logarithms in a finite field.
 - C. It uses a larger percentage of resources to carry out encryption.
 - D. It is more efficient.
48. If implemented properly, a one-time pad is a perfect encryption scheme. Which of the following incorrectly describes a requirement for implementation?
- A. The pad must be securely distributed and protected at its

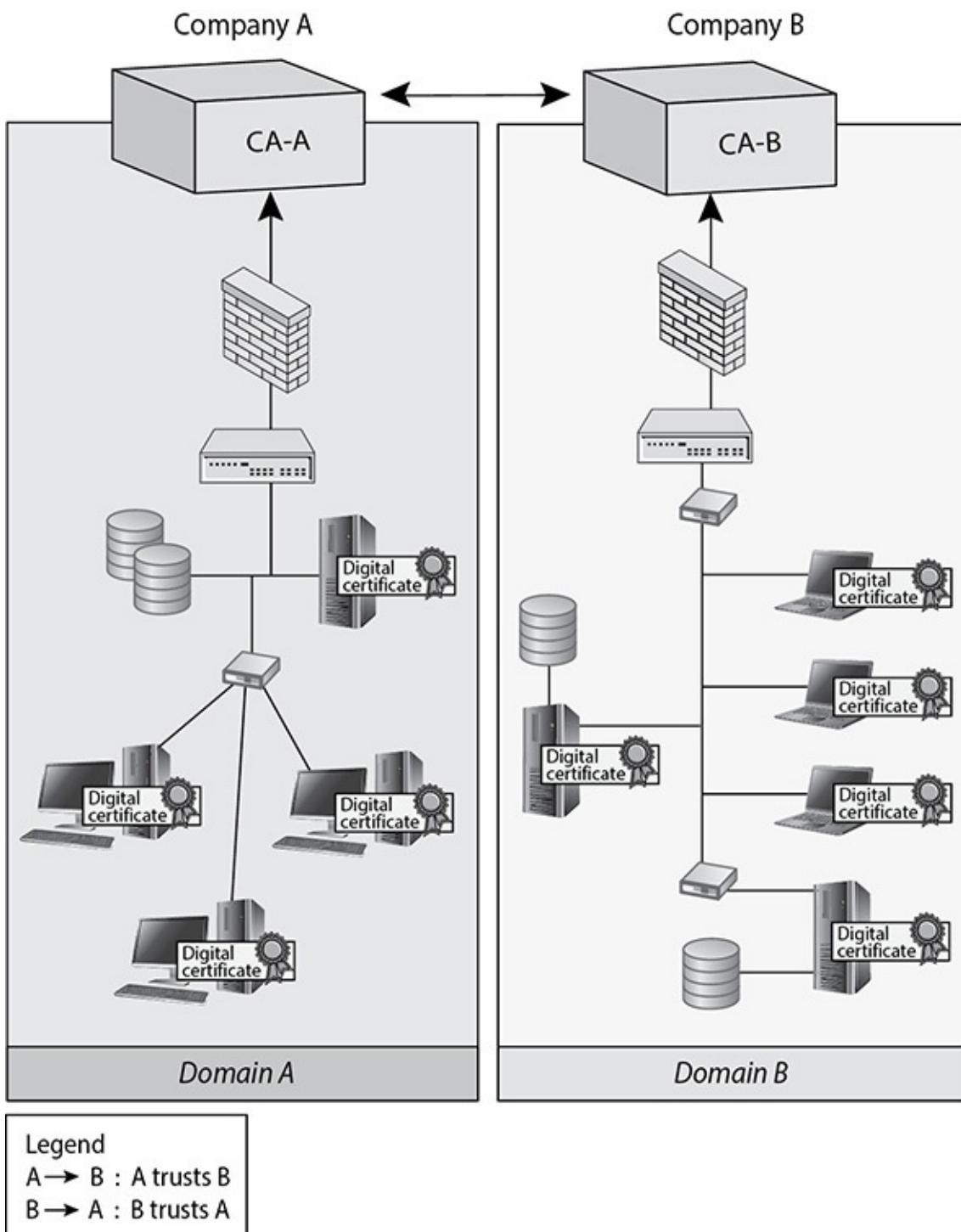
- destination.
- B. The pad must be made up of truly random values.
 - C. The pad must always be the same length.
 - D. The pad must be used only one time.
49. Sally is responsible for key management within her organization. Which of the following incorrectly describes a principle of secure key management?
- A. Keys should be backed up or escrowed in case of emergencies.
 - B. The more a key is used, the shorter its lifetime should be.
 - C. Less secure data allows for a shorter key lifetime.
 - D. Keys should be stored and transmitted by secure means.
50. Mandy needs to calculate how many keys must be generated for the 260 employees using the company's PKI asymmetric algorithm. How many keys are required?
- A. 33,670
 - B. 520
 - C. 67,340
 - D. 260
51. Which of the following works similarly to stream ciphers?
- A. One-time pad
 - B. AES
 - C. Block
 - D. RSA
52. There are two main types of symmetric ciphers: stream and block. Which of the following is not an attribute of a good stream cipher?
- A. Statistically unbiased keystream
 - B. Statistically predictable
 - C. Long periods of no repeating patterns
 - D. Keystream not linearly related to key
53. Which of the following best describes how a digital signature is created?

- A. The sender encrypts a message digest with his private key.
 - B. The sender encrypts a message digest with his public key.
 - C. The receiver encrypts a message digest with his private key.
 - D. The receiver encrypts a message digest with his public key.
54. In cryptography, different steps and algorithms provide different types of security services. Which of the following provides only authentication, nonrepudiation, and integrity?
- A. Encryption algorithm
 - B. Hash algorithm
 - C. Digital signature
 - D. Encryption paired with a digital signature
55. Advanced Encryption Standard is an algorithm used for which of the following?
- A. Data integrity
 - B. Bulk data encryption
 - C. Key recovery
 - D. Distribution of symmetric keys
56. SSL is a protocol used for securing transactions that occur over untrusted networks. Which of the following best describes what takes place during a SSL connection setup process?
- A. The server creates a session key and encrypts it with a public key.
 - B. The server creates a session key and encrypts it with a private key.
 - C. The client creates a session key and encrypts it with a private key.
 - D. The client creates a session key and encrypts it with a public key.
57. The CA is responsible for revoking certificates when necessary. Which of the following correctly describes a CRL and OCSP?
- A. The CRL was developed as a more streamlined approach to OCSP.
 - B. OCSP is a protocol that submits revoked certificates to the CRL.
 - C. OCSP is a protocol developed specifically to check the CRL during a certificate validation process.
 - D. CRL carries out real-time validation of a certificate and reports to the OCSP.

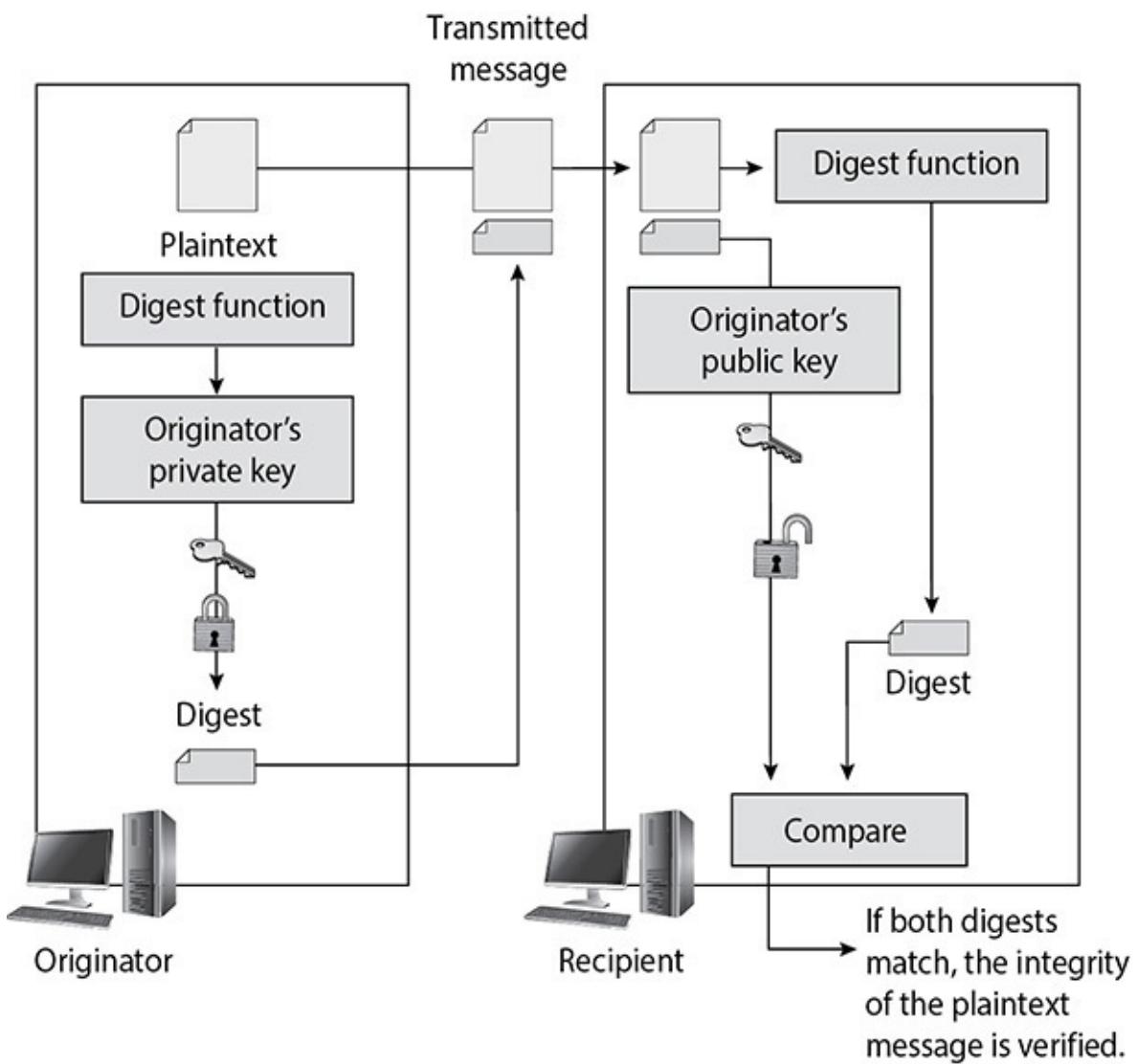
58. There are several different types of technologies within cryptography that provide confidentiality. What is represented in the graphic that follows?



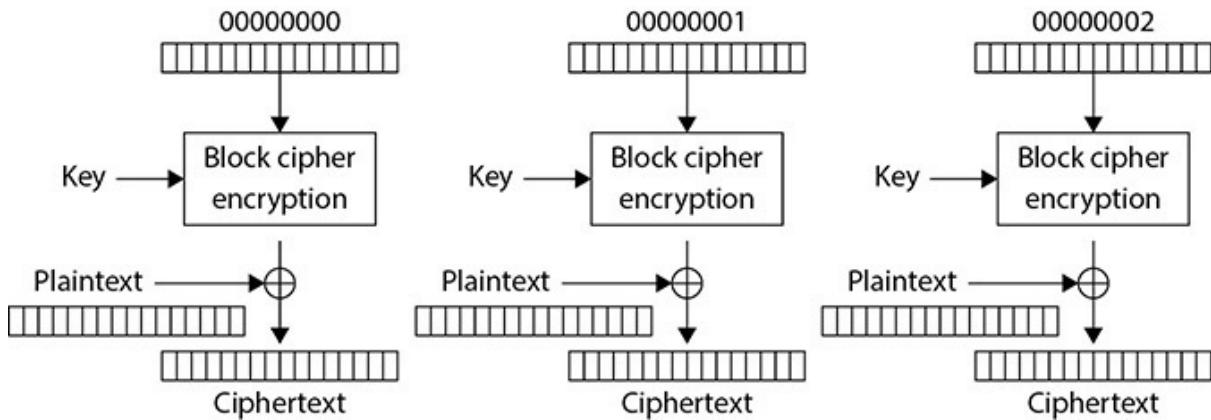
- A. Running key cipher
 B. Concealment cipher
 C. Steganography
 D. One-time pad
59. There are several different types of important architectures within public key infrastructures. Which architecture does the graphic that follows represent?



- A. Cross-certification
- B. Cross-revocation list
- C. Online Certificate Status Protocol
- D. Registration authority
60. There are different ways of providing integrity and authentication within cryptography. What type of technology is shown in the graphic that follows?



- A. One-way hash
- B. Digital signature
- C. Birthday attack
- D. Collision
61. A widely used family of symmetric algorithms is called block ciphers. When these types of algorithms are being used, a message that needs to be encrypted is segmented into individual blocks and each block is encrypted. These algorithms work in different modes, and each mode has a specific use case. Which mode is being represented in the graphic and what is its most common use case?



- A. Electronic Code Book mode is used when individual and unique keys are needed to encrypt each block.
- B. Counter mode is used when encryption and decryption need to take place in parallel and independent block recovery is available.
- C. Cipher Block Chaining mode is used when added complexity is required by incorporating subkeys for each block encryption function.
- D. Output Feedback mode is used when segmented ciphertext blocks are required for inline encryption functionality.
62. If Marge uses her private key to create a digital signature on a message she is sending to George, but she does not show or share her private key with George, what is it an example of?
- Key clustering
 - Avoiding a birthday attack
 - Providing data confidentiality
 - Zero knowledge proof
63. There are two main functions that Trusted Platform Modules (TPMs) carry out within systems today. Which of the following best describes these two functions?
- Sealing a hard disk drive is when the decryption key that can be used to decrypt data on the drive is stored on the TPM. Binding is when data pertaining to the system's state is hashed and stored on the TPM.
 - Binding a hard disk drive is when whole-disk encryption is enabled through the use of the TPM. Sealing is when a digital certificate is sealed within a TPM and the system cannot boot up without this certificate being validated.

- C. Sealing a hard disk drive is when whole-disk encryption is enabled through the use of the TPM. Binding is when a digital certificate is sealed within a TPM and the system cannot boot up without this certificate being validated.
- D. Binding a hard disk drive is when the decryption key that can be used to decrypt data on the drive is stored on the TPM. Sealing is when data pertaining to the system's state is hashed and stored on the TPM.

The following scenario applies to questions 64 and 65.

Jack has been told that successful attacks have been taking place and data that has been encrypted by his company's software systems has leaked to the company's competitors. Through Jack's investigation he has discovered that the lack of randomness in the seeding values used by the encryption algorithms in the company's software exposed patterns and allowed for successful reverse engineering.

- 64.** Which of the following is most likely the item that is the root of the problem when it comes to the necessary randomness explained in the scenario?
 - A. Asymmetric algorithm
 - B. Out-of-band communication compromise
 - C. Number generator
 - D. Symmetric algorithm
- 65.** Which of the following best describes the role of the values that is allowing for patterns as described in the scenario?
 - A. Initialization vector
 - B. One-time password
 - C. Master symmetric key
 - D. Subkey
- 66.** Sometimes when studying for an industry certification exam like the CISSP, people do not fully appreciate that the concepts and technologies that they need to learn to pass the test directly relate to real-world security issues. To enforce how exam-oriented theoretical concepts directly relate to the practical world of security, choose the correct answer that best describes the Heartbleed SSL/TLS vulnerability, which is considered to be one of the most critical attack vectors in the history of the Internet.

- A. Digital certificates were stolen through a tunneled attack within the SSL and TLS protocols.
 - B. Certificate authorities were compromised when their SSL and TLS connections were hijacked through the use of TCP hijacking sessions.
 - C. Bounds checking was not implemented, allowing sensitive data to be obtained by attackers from memory segments on web servers.
 - D. Cross-site scripting was allowed to take place on web servers that ran a vulnerable version of Java.
- 67.** What type of exploited vulnerability allows more input than the program has allocated space to store it?
- A. Symbolic links
 - B. File descriptors
 - C. Kernel flaws
 - D. Buffer overflows
- 68.** There are common cloud computing service models.
_____ usually requires companies to deploy their own operating systems, applications, and software onto the provided infrastructure. _____ is the software environment that runs on top of the infrastructure. In the _____ model the provider commonly gives the customers network-based access to a single copy of an application.
- A. Platform as a Service, Infrastructure as a Service, Software as a Service
 - B. Platform as a Service, Platform as Software, Application as a Service
 - C. Infrastructure as a Service, Application as a Service, Software as a Service
 - D. Infrastructure as a Service, Platform as a Service, Software as a Service
- 69.** A company has decided that it no longer wants to maintain its own servers and network environment because of increasing costs and liabilities. The company wants to move to a cloud-based solution, but needs to determine which type of solution best fits its needs. Which of the following provides a correct definition and mapping of a typical cloud-based solution?

- A.** Infrastructure as a Service is provided when a cloud provider delivers a computing platform that includes operating system, database, and web servers.
 - B.** Software as a Service is provided when a cloud provider delivers an infrastructure environment similar to a traditional data center.
 - C.** Platform as a Service is provided when a cloud provider delivers a computing platform that can include operating system, database, and web servers.
 - D.** Software as a Service is provided when a cloud provider delivers a software environment in the form of a computing platform.
- 70.** Sally is carrying out a software analysis on her company's proprietary application. She has found out that it is possible for an attacker to force an authorization step to take place before the authentication step is completed successfully. What type of issue would allow for this type of compromise to take place?
- A.** Back door
 - B.** Maintenance hook
 - C.** Race condition
 - D.** Data validation error
- 71.** Which of the following is true about information flow models?
- A.** The simple security rule of Bell-LaPadula dictates that a subject may not read data from a higher security level, in order to implement data integrity.
 - B.** The *-integrity rule of Biba dictates that a subject may not write data to an object at a higher integrity level, in order to implement confidentiality.
 - C.** The simple integrity rule of Biba dictates that a subject cannot write data to a lower integrity level, in order to implement integrity.
 - D.** The *-property rule of Bell-LaPadula dictates that a subject cannot write data to a lower security level, in order to implement confidentiality.
- 72.** Which of the following is true with respect to distributed systems?
- A.** A client/server system is a special case of a distributed system with only two tiers.
 - B.** Distributed systems are easier to secure than non-distributed

systems, because there are more components that can contribute to the security solution.

- C. A client/server system is distinct from distributed systems, because there are only two tiers.
 - D. Distributed systems reduce the complexity of security solutions.
73. What is the difference between generating a message authentication code (MAC) and generating a hash MAC (HMAC)?
- A. There is no difference; they are the same thing.
 - B. They are two different hashing algorithms that are used the same way but produce different message digests (MDs).
 - C. MACs are a result of hashing a message, whereas HMACs are a result of hashing both the message and a public key.
 - D. MACs are a result of hashing a message, whereas HMACs are a result of hashing both the message and a shared secret key.
74. Why is it important to understand the life cycle of cryptography and your cryptographic needs?
- A. Major new forms of cryptography are constantly being invented, which may replace your use of hashing, symmetric, or asymmetric encryption methods.
 - B. The available key space for any given algorithm (or your choice of keys within it) will inevitably “go stale” over time.
 - C. Symmetric systems like AES are continuously being upgraded to include more rounds of transforms, so it is important to be using the latest version.
 - D. Revolutionary advances in blockchains will replace old cryptography techniques.
75. Which of the following are services that cryptosystems can provide?
- A. Confidentiality, integrity, and availability
 - B. Computation, authentication, and authorization
 - C. Integrity, authentication, and accounting
 - D. Confidentiality, integrity, and authentication
76. Which of the following statements is true with respect to the physical security of distribution and storage facilities?

- A.** Smaller intermediate distribution facilities (IDFs) and storage facilities tend not to contain data as critical as the data in main distribution facilities (MDFs) and data centers, so they require less physical protection.
 - B.** Although smaller IDFs and storage facilities contain data as critical as the data in MDFs and data centers, they are commonly less well protected physically.
 - C.** All distribution and storage facilities are typically afforded the same level of physical protection in practice.
 - D.** Distribution and storage facilities don't require the same level of physical access controls as the production data centers.
-
-

QUICK ANSWER KEY

- 1.** B
- 2.** D
- 3.** C
- 4.** A
- 5.** D
- 6.** A
- 7.** C
- 8.** A
- 9.** A
- 10.** C
- 11.** B
- 12.** D
- 13.** D
- 14.** B
- 15.** D
- 16.** C
- 17.** D
- 18.** A
- 19.** C

20. C

21. C

22. A

23. B

24. C

25. A

26. D

27. D

28. C

29. D

30. B

31. D

32. A

33. A

34. B

35. A

36. B

37. C

38. B

39. C

40. C

41. C

42. B

43. D

44. B

45. D

46. A

47. D

48. C

49. C

50. B

51. A

52. B

53. A

54. C

55. B

56. D

57. C

58. D

59. A

60. B

61. B

62. D

63. D

64. C

65. A

66. C

67. D

68. D

69. C

70. C

71. D

72. A

73. D

74. B

75. D

76. B

ANSWERS A

- 1.** Lacy's manager has tasked her with researching an intrusion detection system for a new dispatching center. Lacy identifies the top five products and compares their ratings. Which of the following is the evaluation criteria framework most in use today for these types of purposes?
- A. ITSEC
- B. Common Criteria
- C. Red Book
- D. Orange Book
- B.** The Common Criteria was created in the early 1990s as a way of combining the strengths of both the Trusted Computer System Evaluation Criteria (TCSEC) and Information Technology Security Evaluation Criteria (ITSEC) while eliminating their weaknesses. The Common Criteria is more flexible than TCSEC and more straightforward than ITSEC. Because it is recognized globally, the Common Criteria helps consumers by reducing the complexity of the ratings and eliminating the need to understand the definition and meaning of different ratings within various evaluation schemes. This also helps manufacturers because now they can build to one specific set of requirements if they want to sell their products internationally instead of having to meet several different ratings with varying rules and requirements.
- A** is incorrect because ITSEC, or the Information Technology Security Evaluation Criteria, is not the most widely used. ITSEC was the first attempt at establishing a single standard for evaluating security attributes of computer systems and products by many European countries. Furthermore, ITSEC separates functionality and assurance in its evaluation, giving each a separate rating. It was developed to provide more flexibility than TCSEC and addresses integrity, availability, and confidentiality in networked systems. While the goal of the ITSEC was to become the worldwide criteria for product evaluation, it did not meet that goal and has been replaced with the Common Criteria.
- C** is incorrect because the Red Book is a U.S. government publication that addresses security evaluation topics for networks and network components. Officially titled the Trusted Network Interpretation, the book provides a framework for securing different types of networks. Subjects accessing objects on the network need to be controlled, monitored, and audited.

- D** is incorrect because the Orange Book is a U.S. government publication that primarily addresses government and military requirements and expectations for operating systems. The Orange Book is used to evaluate whether a product contains the security properties the vendor claims it does and whether the product is appropriate for a specific application or function. The Orange Book is used to review the functionality, effectiveness, and assurance of a product during its evaluation, and it uses classes that were devised to address typical patterns of security requirements. It provides a broad framework for building and evaluating trusted systems with great emphasis on controlling which users can access a system. The other name for the Orange Book is the Trusted Computer System Evaluation Criteria (TCSEC).
- 2. Certain types of attacks have been made more potent by which of the following advances to microprocessor technology?
 - A. Increased circuits, cache memory, and multiprogramming
 - B. Dual mode computation
 - C. Direct memory access I/O
 - D. Increases in processing power
- D. Due to the increase of personal computer and server processing power, it is now possible to be more successful in brute-force and cracking attacks against security mechanisms that would not have been possible a few years ago. Today's processors can execute an amazing number of instructions per second. These instructions can be used to attempt to crack passwords or encryption keys or instructions to send nefarious packets to victim systems.
- A is incorrect because increased circuits, cache memory, and multiprogramming do not make certain types of attacks more potent. Multiprogramming means that more than one program or process can be loaded into memory at the same time. This is what allows you to run your antivirus software, word processor, firewall, and e-mail client simultaneously. Cache memory is a type of memory used for high-speed writing and reading activities. When the system assumes (through its programmatic logic) that it will need to access specific information many times throughout its processing activities, it will store the information in cache memory so that it is easily and quickly accessible.
- B is incorrect because the answer is a distracter. There is no real

dual-mode computation when examining the advances in microprocessors.

- C** is incorrect because direct memory access (DMA) is a way of transferring instructions and data between I/O (input/output) devices and the system's memory without using the CPU. This speeds up data transfer rates significantly. DMA basically offloads work from the CPU by ensuring that more simple instructions are interpreted and executed through other processing capabilities within the computer system. This is not an advancement to microprocessor technology.
- 3.** CPUs and operating systems can work in two main types of multitasking modes. What controls access and the use of system resources in preemptive multitasking mode?
 - A.** The user and application
 - B.** The program that is loaded into memory
 - C.** The operating system
 - D.** The CPU and user
- C.** Operating systems started out as cooperative and then evolved into preemptive multitasking. With preemptive multitasking, used in Windows 9x and later versions and in Unix systems, the operating system controls how long a process can use a resource. The system can suspend a process that is using the CPU (or other system resources) and allow another process access to it through the use of time sharing. Thus, operating systems that use preemptive multitasking run the show, and one application does not negatively affect another application if it behaves badly. In operating systems that used cooperative multitasking, the processes had too much control over resource release, and when an application hung, it usually affected all the other applications and sometimes the operating system itself.
- A** is incorrect because the user and application do not control access and the use of system resources in preemptive multitasking mode. The application, however, has more control over the use of system resources in cooperative multitasking mode. The operating system itself works in either preemptive or cooperative multitasking modes, not the applications or users.
- B** is incorrect because, as described in answer A, a program does not run in a specific multitasking mode—the operating system does.

Cooperative multitasking, used in Windows 3.1 and early Macintosh systems, required the processes to voluntarily release resources that they were using. This was not necessarily a stable environment because if a programmer did not write his code properly to release a resource when his application was done using it, the resource would be committed indefinitely to his application and thus unavailable to other processes.

- D** is incorrect because the user and CPU do not control access and the use of system resources. Instead, the operating system controls the processor time slices that different processes can be allocated. Multitasking is the way that the operating system uses access to the CPU, which can be either cooperative or preemptive.
- 4.** Virtual storage combines RAM and secondary storage for system memory. Which of the following is a security concern pertaining to virtual storage?
 - A.** More than one process uses the same resource.
 - B.** It allows cookies to remain persistent in memory.
 - C.** It allows for side-channel attacks to take place.
 - D.** Two processes can carry out a denial of service.
- A.** When RAM and secondary storage are combined, the result is virtual memory. The system uses hard drive space—called *swap space*—that is reserved for the purpose of extending its RAM memory space. When a system fills up its volatile memory space, it writes data from memory onto the hard drive. When a program requests access to this data, it is brought from the hard drive back into memory in specific units, called page frames. Accessing data that is kept in pages on the hard drive takes more time than accessing data kept in memory because physical disk read/write access has to take place. There are internal control blocks, maintained by the operating system, to keep track of what page frames are residing in RAM, and what is available “offline,” ready to be called into RAM for execution or processing, if needed. The payoff is that it seems as though the system can hold an incredible amount of information and program instructions in memory. A security issue with using virtual swap space is that two or more processes use the same resource and the data could be corrupted or compromised.
- B** is incorrect because virtual storage is not related to cookies.

Virtual storage uses hard drive space to extend its RAM memory space. Cookies are small text files used mainly by web browsers. The cookies can contain credentials for websites, site preference settings, or shopping histories. Cookies are also commonly used to maintain web server-based sessions.

- C** is incorrect because a side-channel attack is a nonintrusive attack. In this type of attack, the attacker gathers information about how a mechanism (such as a smart card or encryption processor) works from the radiation that is given off, time taken to carry out processing, power consumed to carry out tasks, etc. This information is used to reverse-engineer the mechanism to uncover how it carries out its security tasks. This is not related to virtual storage.
 - D** is incorrect because the biggest threat within a system that has shared resources between processes, as operating systems have to share memory between all resources, is that one process will negatively interfere with the other process's resource. This is especially true with memory, since all data and instructions are stored there, whether they are sensitive or not. While it is possible for two processes to work together to carry out a denial-of-service attack, this is only one type of attack that can be carried out with or without the use of virtual storage.
5. Which of the following is a common association of the Clark-Wilson access model?
- A. Chinese Wall
 - B. Access tuple
 - C. Read up and write down rule
 - D. Well-formed transactions
- D.** In the Clark-Wilson model, a subject cannot access an object without going through some type of application or program that controls how this access can take place. The subject (usually a user) is bound to the application and then is allowed access to the necessary objects based on the access rules within the application software that are defined as "well-formed transactions." For example, when Kathy needs to update information held within her company's database, she will not be allowed to do so without a piece of software controlling these activities. First, Kathy must authenticate to the software, which is acting as a front end for the

database, and then the program will control what Kathy can and cannot do to the information in the database, based on very well-defined rules in a step-by-step manner.

- A** is incorrect because the Chinese Wall model is another name for the Brewer and Nash model, which was created to provide access controls that can change dynamically, depending upon a user's previous actions, in an effort to protect against conflicts of interest by users' access attempts. No information can flow between subjects and objects in a way that would result in a conflict of interest. The model states that a subject can write to an object if, and only if, the subject cannot read another object that is in a different dataset.
 - B** is incorrect because the Clark-Wilson model uses access *triple*, not access *tuple*. The access triple is subject-program-object. It ensures that subjects can only access objects through authorized programs.
 - C** is incorrect because the Clark-Wilson model does not have read up and write down rules. These rules are associated with the Bell-LaPadula and Biba models. The Bell-LaPadula model includes the simple security rule, which is no read up, and the star property rule, which is no write down. The Biba model includes the simple integrity axiom, which is no read down, and the star-integrity axiom, which is no write up.
6. Which of the following correctly describes the relationship between the reference monitor and the security kernel?
- A.** The security kernel implements and enforces the reference monitor.
 - B.** The reference monitor is the core of the trusted computing base, which is made up of the security kernel.
 - C.** The reference monitor implements and enforces the security kernel.
 - D.** The security kernel, aka abstract machine, implements the reference monitor concept.
- A.** The trusted computing base (TCB) is the total combination of a system's protection mechanisms. These are in the form of hardware, software, and firmware. These same components also comprise the security kernel. The reference monitor is an access control concept that is implemented and enforced by the security kernel via the hardware, software, and firmware. In doing so, the security kernel ensures that subjects have the appropriate authorization to access the objects they are requesting. The subject, be it a program, user, or

process, should not be able to access a file, program, or resource it is requesting until it has proven that it has the appropriate access rights.

- B** is incorrect because the reference monitor is not the core of the TCB. The core of the TCB is the security kernel, and the security kernel carries out the reference monitor concept. The reference monitor is a concept pertaining to access control. Since it is not a physical component, it is often referred to as an “abstract machine.” The reference monitor mediates access between subjects and objects in an effort to ensure that subjects have the necessary rights to access objects and to protect objects from unauthorized access and destructive changes.
 - C** is incorrect because the reference monitor does not implement and enforce the security kernel. Rather, the security kernel implements and enforces the reference monitor. The reference monitor is an abstract concept, while the security kernel is a combination of hardware, software, and firmware within the trusted computing base. The security kernel has three requirements, which are also the requirements of the reference monitor. The security kernel must be tamperproof and isolate the processes executing the reference monitor concept. Likewise, the security kernel must be implemented so that it is invoked for every access attempt and cannot be circumvented. Finally, the security kernel must be small enough to enable its comprehensive testing and verification.
 - D** is incorrect because abstract machine is not another name for the security kernel. Abstract machine is another name for the reference monitor, which can also be referred to as the reference monitor concept. The concept states that an abstract machine serves as the mediator between subjects and objects to ensure that the subjects have the necessary rights to access the objects they are requesting and to protect the objects from unauthorized access and modification. The security kernel is responsible for carrying out these activities.
7. The trusted computing base (TCB) ensures security within a system when a process in one domain must access another domain in order to retrieve sensitive information. What function does the TCB initiate to ensure that this is done in a secure manner?
- A. I/O operational execution
 - B. Process deactivation

C. Execution domain switching

D. Virtual memory to real memory mapping

- C.** Execution domain switching takes place when a CPU needs to move between executing instructions for a highly trusted process to a less trusted process or vice versa. The trusted computing base (TCB) allows processes to switch domains in a secure manner in order to access different levels of information based on their sensitivity. Execution domain switching takes place when a process needs to call upon a process in a higher protection ring. The CPU goes from executing instructions in user mode to privileged mode and back.
- A** is incorrect because input/output (I/O) operations are not initiated to ensure security when a process in one domain must access another domain in order to retrieve sensitive information. I/O operations include control of all input/output devices. I/O operations are functions within an operating system that allow input devices (such as a mouse or keyboard) and output devices (such as a monitor or printer) to interact with applications and with itself.
- B** is incorrect because process deactivation takes place when a process's instructions are completely executed by the CPU or when another process with a higher priority calls upon the CPU. When a process is deactivated, the CPU's registers must be filled with new information about the new requesting process. The data that is getting switched in and out of the registers may be sensitive, so the TCB components must make sure this takes place securely.
- D** is incorrect because memory mapping takes place when a process needs its instructions and data processed by the CPU. The memory manager maps the logical address to the physical address so that the CPU knows where the data is located. This is the responsibility of the operating system's memory manager.

8. Which of the following best defines a virtual machine?

- A.** A virtual instance of an operating system
- B.** A piece of hardware that runs multiple operating system environments simultaneously
- C.** A physical environment for multiple guests
- D.** An environment that can be fully utilized while running legacy applications

- A.** A virtual machine is a virtual instance of an operating system. A virtual machine can also be called a guest, which runs in a host environment. The host environment—usually an operating system—can run multiple guests simultaneously. The virtual machines pool resources such as RAM, processors, and storage from the host environment. This offers many benefits, including enhanced processing power utilization. Other benefits include the ability to run legacy applications. For example, an organization may choose to run its legacy applications on an instance (virtual machine) of Windows 7 long after it has rolled out Windows 10.
 - B** is incorrect because a virtual machine is not a piece of hardware. A virtual machine is an instance of an operating system that runs on hardware. The host can run multiple virtual machines. So, basically, you can have one computer running different operating systems at the same time. One benefit of this is consolidation. Using virtual machines, you can consolidate the workloads of several underutilized servers on to one host, thereby saving money on hardware and administrative management tasks.
 - C** is incorrect because virtual machines provide and work within software emulation. The host provides the resources, such as memory, processor, buses, RAM, and storage for the virtual machines. The virtual machines share these resources but do not access them directly. The host environment, which is responsible for managing the system resources, acts as an intermediary between the resources and the virtual machines.
 - D** is incorrect because many legacy applications are not compatible with specific hardware and newer operating systems. Because of this, the application commonly underutilizes the server software and components. The virtual machines emulate an environment that allows legacy, and other, applications to fully use the resources available to them. This is a reason to use a virtual machine, but the answer does not provide its definition.
9. Virtualization offers many benefits. Which of the following incorrectly describes virtualization?
- A.** Virtualization simplifies operating system patching.
 - B.** Virtualization can be used to build a secure computing platform.
 - C.** Virtualization can provide fault and error containment.
 - D.** Virtual machines offer powerful debugging capabilities.

- A.** Virtualization does not simplify operating system patching. In fact, it makes it more complex because it adds at least an operating system. Each operating system commonly varies in version and configurations—increasing the complexity of patching. The operating systems for the servers themselves run as guests within the host environment. Not only do you have to patch and maintain the traditional server operating systems, but now you also have to patch and maintain the virtualization software itself.
- B** is incorrect because virtualization can be used to build a secure computing platform. Untrusted applications can be run in secure, isolated sandboxes within a virtual machine. The virtualization software “compartmentalizes” the individual guest operating systems and ensures that the processes for each guest do not interact with the other guest processes in an unauthorized manner.
- C** is incorrect because virtual machines can provide fault and error containment by isolating what is run within the specific guest operating systems. Developers and security researchers can proactively inject faults into software to study its behavior without impacting other virtual machines. For this reason, virtual machines are useful tools for research and academic experiments.
- D** is incorrect because virtual machines enable powerful debugging, as well as performance monitoring, by allowing you to put debugging and performance monitoring tools in the virtual machine monitor. There’s no need to set up complex debugging scenarios, and the operating systems can be debugged without impacting productivity.

10. Which security architecture model defines how to securely develop access rights between subjects and objects?

- A.** Brewer-Nash
 - B.** Clark-Wilson
 - C.** Graham-Denning
 - D.** Bell-LaPadula
- C.** The Graham-Denning model addresses how access rights between subjects and objects are defined, developed, and integrated. It defines a set of basic rights in terms of commands that a specific subject can execute on an object. This model has eight primitive protection rights, or rules, on how these types of functionalities should take place securely. They are as follows: how to securely

create an object; how to securely create a subject; how to securely delete an object; how to securely delete a subject; how to securely provide the read access right; how to securely provide the grant access right; how to securely provide the delete access right; and how to securely provide transfer access rights. These things may sound insignificant, but when we are talking about building a secure system, they are very critical.

- ☒ **A** is incorrect because the Brewer-Nash model (also called the Chinese Wall model) is intended to provide access controls that can change dynamically depending upon a user's previous actions. The main goal is to protect against conflicts of interest by users' access attempts. For example, if a large marketing company provides marketing promotions and materials for two banks, an employee working on a project for Bank A should not be able to look at the information the marketing company has on its other bank customer, Bank B. Such action could create a conflict of interest because the banks are competitors. If the marketing company's project manager for the Bank A project could view information on Bank B's new marketing campaign, he may try to trump its promotion to please his more direct customer. The marketing company would get a bad reputation if it allowed its internal employees to behave so irresponsibly.
- ☒ **B** is incorrect because the Clark-Wilson model is implemented to protect the integrity of data and to ensure that properly formatted transactions take place within applications. It works on the following premises: subjects can access objects only through authorized programs; separation of duties is enforced; auditing is required. The Clark-Wilson model addresses all three integrity goals: prevent unauthorized users from making modifications, prevent authorized users from making improper modifications, and maintain internal and external consistency.
- ☒ **D** is incorrect because the Bell-LaPadula model was developed to address the U.S. military's concern with the security of its systems and the leakage of classified information. The model's main goal is to prevent sensitive information from being accessed in an unauthorized manner. It is a state machine model that enforces the confidentiality aspects of access control. A matrix and security levels are used to determine if subjects can access different objects. The subject's clearance is compared to the object's classification and then specific rules are applied to control how subject-to-object

interactions take place.

- 11.** Operating systems can be programmed to carry out different methods for process isolation. Which of the following refers to a method in which an interface defines how communication can take place between two processes and no process can interact with the other's internal programming code?
- A. Virtual mapping
 - B. Encapsulation of objects
 - C. Time multiplexing
 - D. Naming distinctions
- B.** When a process is properly encapsulated, no other process understands or interacts with its internal programming code. When process A needs to communicate with process B, process A just needs to know how to communicate with process B's interface. An interface defines how communication must take place between two processes. As an analogy, think back to how you had to communicate with your third-grade teacher. You had to call her Mrs. SoandSo, say please and thank you, and speak respectfully to get whatever it was you needed. The same thing is true for software components that need to communicate with each other. They have to know how to communicate properly with each other's interfaces. The interfaces dictate the type of requests that a process will accept and the type of output that will be provided. So, two processes can communicate with each other, even if they are written in different programming languages, as long as they know how to communicate with each other's interface. Encapsulation provides data hiding, which means that outside software components will not know how a process works and will not be able to manipulate the process's internal code. This is an integrity mechanism and enforces modularity in programming code.
- A** is incorrect because virtual mapping refers to how virtual to physical memory mapping takes place within an operating system. When an application needs memory to work with, it tells the operating system's memory manager how much memory it needs. The operating system carves out that amount of memory and assigns it to the requesting application. The application uses its own address scheme, which usually starts at 0, but in reality, the application does not work in the physical address space that it thinks it is working in. Rather, it works in the address space that the

memory manager assigns to it. The physical memory is the RAM chips in the system. The operating system chops up this memory and assigns portions of it to the requesting processes. Once the process is assigned its own memory space, then it can address this portion however it needs to, which is called virtual address mapping. Virtual address mapping allows the different processes to have their own memory space; the memory manager ensures that no processes improperly interact with another process's memory. This provides integrity and confidentiality.

- C** is incorrect because time multiplexing is a technology that allows processes to use the same resources through an interleaved method. A CPU has to be shared among many processes. Although it seems as though all applications are executing their instructions simultaneously, the operating system is splitting up time shares between each process. Multiplexing means that there are several data sources and the individual data pieces are piped into one communication channel. In this instance, the operating system is coordinating the different requests from the different processes and piping them through the one shared CPU. An operating system has to provide proper time multiplexing (resource sharing) to ensure that a stable working environment exists for software and users.
- D** is incorrect because naming distinctions just means that the different processes have their own name or identification value. Processes are usually assigned process identification (PID) values, which the operating system and other processes use to call upon them. If each process is isolated, that means that each process has its own unique PID value.

- 12.** Which of the following is not a responsibility of the memory manager?
- A.** Use complex controls to ensure integrity and confidentiality when processes need to use the same shared memory segments.
 - B.** Limit processes to interact only with the memory segments assigned to them.
 - C.** Swap contents from RAM to the hard drive as needed.
 - D.** Run an algorithm to identify unused committed memory and inform the operating system that the memory is available.
- D.** This answer describes the function of a garbage collector. A garbage collector is a countermeasure against memory leaks. It is software that runs an algorithm to identify unused committed

memory and then tells the operating system to mark that memory as “available.” Different types of garbage collectors work with different operating systems, programming languages, and algorithms. The portion of the operating system that keeps track of how different types of memory are used is called the memory manager. Its jobs are to allocate and deallocate different memory segments, enforce access control to ensure that processes are interacting only with their own memory segments, and swap memory contents from RAM to the hard drive. The memory manager has five basic responsibilities: relocation, protection, sharing, local organization, and physical organization.

- A** is incorrect because as part of its sharing responsibilities, the memory manager uses complex controls to ensure integrity and confidentiality when processes need to use the same shared memory segments. This is critical to protecting memory and the data in it, since two or more processes can share access to the same segment with potentially different access rights. The memory manager is also responsible for allowing many users with different levels of access to interact with the same application running in one memory segment.
- B** is incorrect because the memory manager is responsible for limiting process interactions to only those memory segments assigned to them. This responsibility falls under the protection category and helps prevent processes from gaining access to unpermitted segments. Another protection responsibility of the memory manager is to provide access control to memory segments.
- C** is incorrect because swapping contents from RAM to the hard drive as needed is a responsibility of the memory manager that falls under the relocation category. When RAM and secondary storage are combined, the result is virtual memory. The system uses hard drive space to extend its RAM memory space. Another relocation responsibility is to provide pointers for applications if their instructions and memory segment have been moved to different location in main memory.

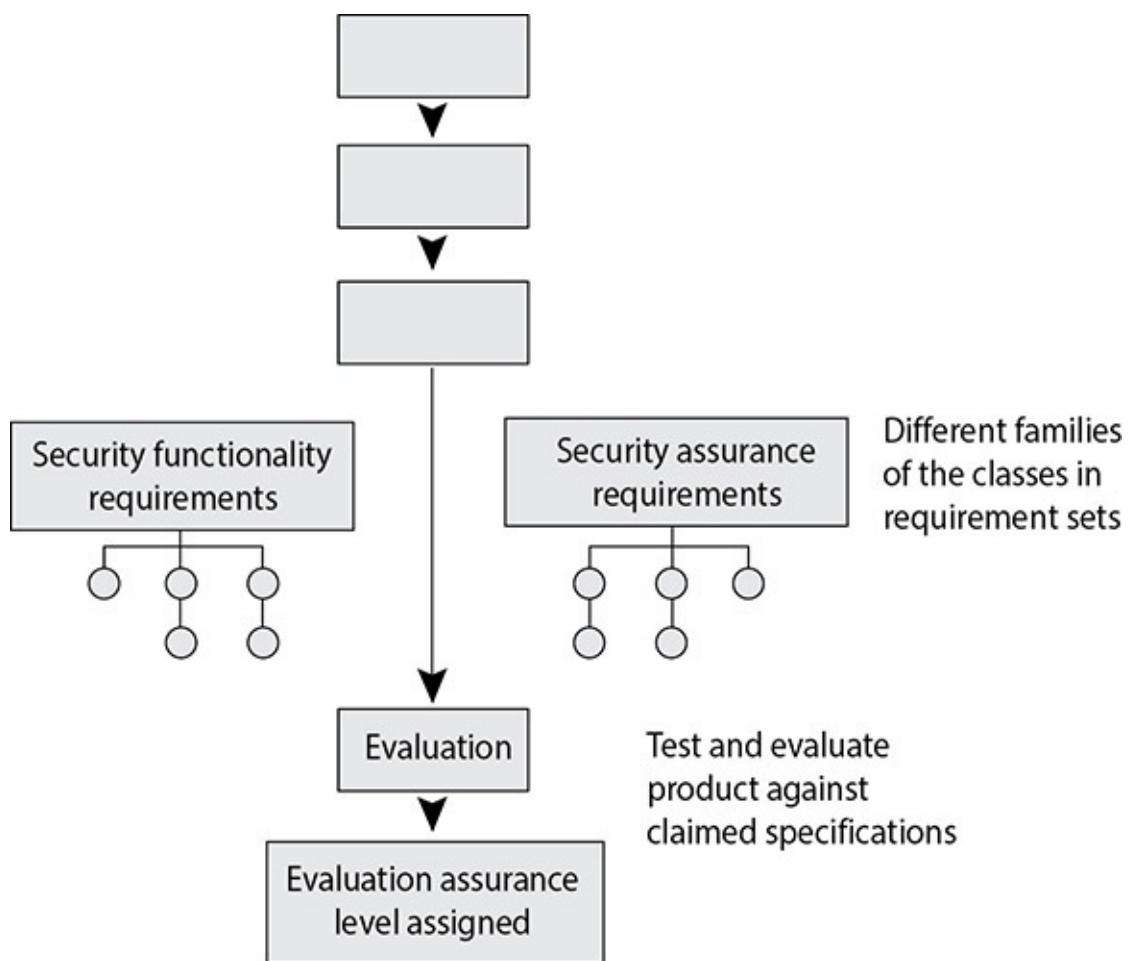
- 13.** Frank is responsible for the security of his company’s online applications, web servers, and web-based activities. The web applications have the capability of being dynamically “locked” so that multiple users cannot edit a web page at the same time and overwrite each other’s work. An audit uncovered that although this software-locking capability was properly configured, multiple users were still

able to modify the same web page at the same time. Which of the following best describes what is taking place in this situation?

- A. Buffer overflow
 - B. Blind SQL injection
 - C. Cross-site request forgery
 - D. Time-of-check/time-of-use attack
- D.** Specific attacks can take advantage of the way a system processes requests and performs tasks. A time-of-check/time-of-use (TOC/TOU) attack deals with the sequence of steps a system uses to complete a task. This type of attack takes advantage of the dependency on the timing of events that take place in a multitasking operating system. TOC/TOU is a class of software vulnerability that allows the checking of a condition (i.e., verifying a credential) and the use of the result from that condition-checking function. In the scenario of this question, the fact that the web application was most likely properly configured indicates that the programming code of this application has this type of vulnerability embedded in the code itself.
- A** is incorrect because a buffer overflow takes place when too much data is accepted as input to a specific process. A buffer is an allocated segment of memory. A buffer can be overflowed arbitrarily with too much data, but for it to be of any use to an attacker, the code inserted into the buffer must be of a specific length, followed up by commands the attacker wants executed. These types of attacks commonly result in exceptions, segmentation of faults, or sensitive data being provided to the attacker. This type of attack is not being described in this question.
- B** is incorrect because a blind SQL injection attack is a type of SQL injection attack that sends a true-or-false question to a database. In a basic SQL injection, an attacker sends specific instructions in the SQL format to interrogate the associated database. In a blind SQL attack, the attacker is limited to only sending a series of true-or-false questions to the database with the hope of gleaning sensitive information from analyzing the database's responses. This type of attack is not described in this question.
- C** is incorrect because cross-site request forgery (CSRF) is an attack type that attempts to trick the victim into loading a web page that contains a malicious request or operation. The operation is carried

out within the context of the victim's access rights. The request inherits the identity of the victim and performs an undesired function on the behalf of the victim. In this type of attack, the attacker can make the victim's system carry out an unintended activity, such as changing account information, retrieving account data, or logging out. While this type of attack could be involved with the scenario described in the question, the question is focusing on how a user is able to bypass the lock mechanism built into a web application. The lock function is being bypassed because the logic of the programming code was developed incorrectly and does not follow a strict series of check and use sequences properly.

14. There are several different important pieces to the Common Criteria. Which of the following best describes the first of the missing components?

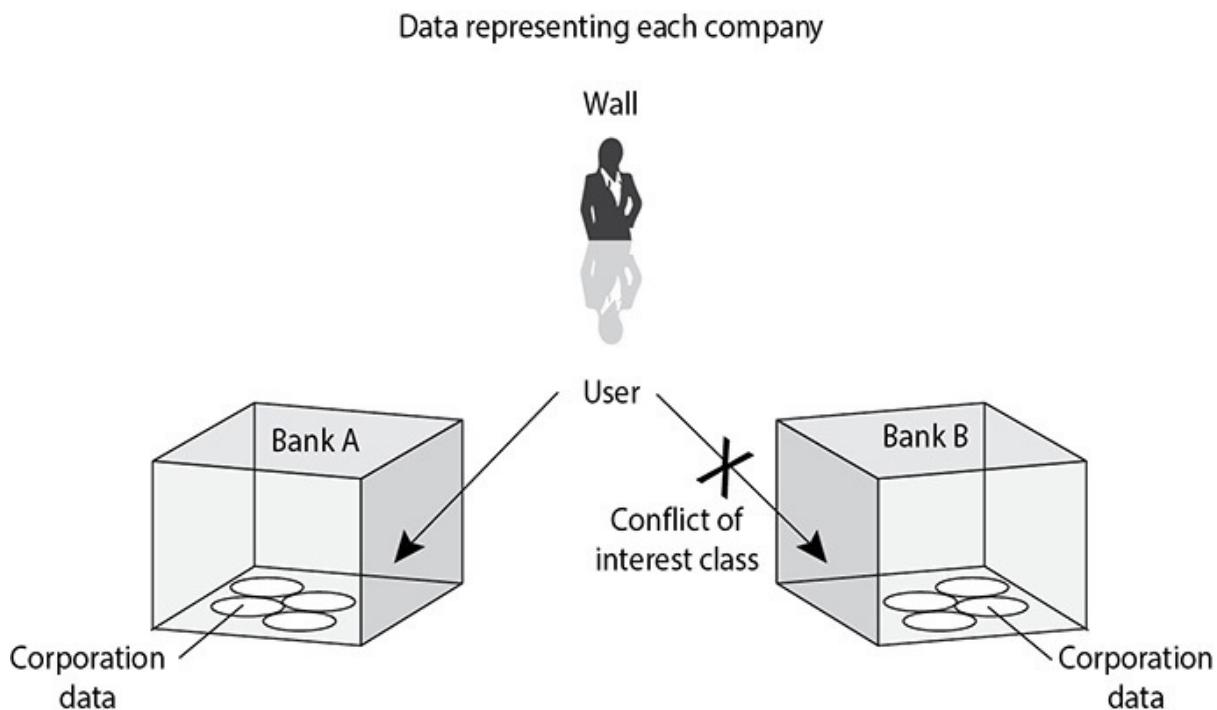


- A. Target of evaluation
- B. Protection profile
- C. Security target
- D. EALs

- B.** The Common Criteria uses protection profiles in its evaluation process. This is a mechanism used to describe a real-world need of a product that is not currently on the market. The protection profile contains the set of security requirements, their meaning and reasoning, and the corresponding EAL rating that the intended product will require. The protection profile describes the environmental assumptions, the objectives, and the functional and assurance-level expectations. Each relevant threat is listed, along with how it is to be controlled by specific objectives. The protection profile also justifies the assurance level and requirements for the strength of each protection mechanism that is expected to be in the new product. The protection profile basically says, “This is what we need out of a new product.”
- A** is incorrect because the target of evaluation (ToE), the second of the three missing pieces in the graphic, is the actual product that is being evaluated against the Common Criteria. Where the protection profile states, “This is what we need out of a new product,” the ToE is the product that a vendor creates to meet the requirements outlined in the protection profile. When there is a need in the industry for a new product that provides specific functionality and security, someone develops the protection profile to outline this need. A vendor fulfills the need by creating a new product, referred to as the ToE.
- C** is incorrect because the security target, the third piece missing in the graphic, is the vendor’s written explanation of the security functionality and assurance mechanisms that meet the needed solution outlined in the protection profile and fulfilled by the ToE. Where the protection profile outlines, “This is what we need,” the ToE is the product that fulfills this need, and the security target is the explanation on how this ToE is mapped to the protection profile. The evaluators compare the ToE with these three constructs, along with the actual requirements of the Common Criteria before assigning it an evaluation assurance level.
- D** is incorrect because evaluation assurance levels (EALs) outline the assurance ratings used in the Common Criteria. EALs are basically the grading system used in these criteria to describe the assurance and security required by a specific product. When an evaluator evaluates a product, after all of her tests she will assign an EAL value. This value is basically the grade that the product receives after all of the tests it is put through. The Common Criteria

uses a different assurance rating system than the previously used criteria. It has packages of specifications that must be met for a product to obtain the corresponding rating. These ratings and packages are collectively called the EALs.

15. Different access control models provide specific types of security measures and functionality in applications and operating systems. What model is being expressed in the graphic that follows?



A. Noninterference

B. Biba

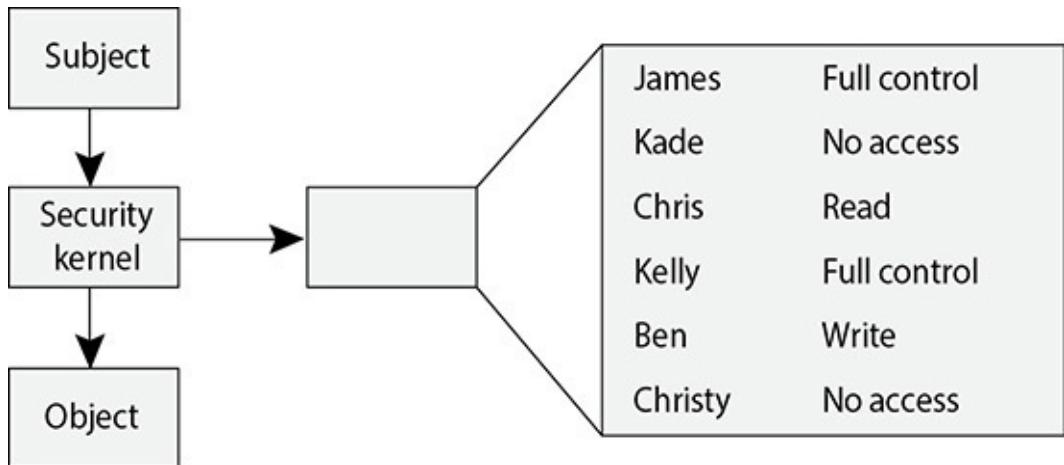
C. Bell-LaPadula

D. Chinese Wall

- D. The Chinese Wall model (also called the Brewer and Nash model) was created to provide access controls that can change dynamically depending upon a user's previous actions. The main goal of the model is to protect against conflicts of interest by users' access attempts. Suppose Maria is a broker at an investment firm that also provides other services to Acme Corporation. If Maria were able to access Acme information from the other service areas, she could learn of a phenomenal earnings report that is about to be released. Armed with that information, she could encourage her clients to buy shares of Acme, confident that the price will go up shortly. The Brewer and Nash Model is designed to mitigate the risk of this situation happening.

- A** is incorrect because multilevel security properties can be expressed in many ways, one being noninterference. The Chinese Wall model does not focus on multilevel security properties and the Noninterference model does not focus on conflicts of interest. The concept of noninterference is implemented to ensure any actions that take place at a higher security level do not affect, or interfere with, actions that take place at a lower level and vice versa. This type of model does not concern itself with conflicts of interest, but rather with what a subject knows about the state of the system. So, if an entity at a higher security level performs an action, it cannot change the state for the entity at the lower level. The Noninterference model is also focused on confidentiality. It works to ensure that subjects at a lower clearance level cannot access data or objects at a higher clearance level.
- B** is incorrect because Biba is a state machine model that addresses the integrity of data within applications without the use of a wall construct. Although the Biba model is very similar to the Bell-LaPadula model, the Bell-LaPadula model uses a lattice of security levels (Top Secret, Secret, Sensitive, and so on). These security levels were developed mainly to ensure that sensitive data is only available to authorized individuals. The Biba model is not concerned with security levels and confidentiality, so it does not base access decisions upon this type of lattice. The Biba model uses a lattice of integrity levels. Biba compartmentalizes data based on integrity levels. It is an information flow model that controls information flow in a way that is intended to protect the integrity of the most trusted information. The Biba model was not built to address conflicts of interest.
- C** is incorrect because a system that employs the Bell-LaPadula model is called a multilevel security system, meaning users with different clearances use the system, and the system processes data at different classification levels. The level at which data is classified determines the handling procedures that should be used. The Bell-LaPadula model is a state machine model that enforces the confidentiality aspects of access control. A matrix and security levels are used to determine if subjects can access different objects. The subject's clearance is compared to the object's classification and then specific rules are applied to control how subject-to-object interactions can take place. The Bell-LaPadula model was not developed to address conflicts of interest.

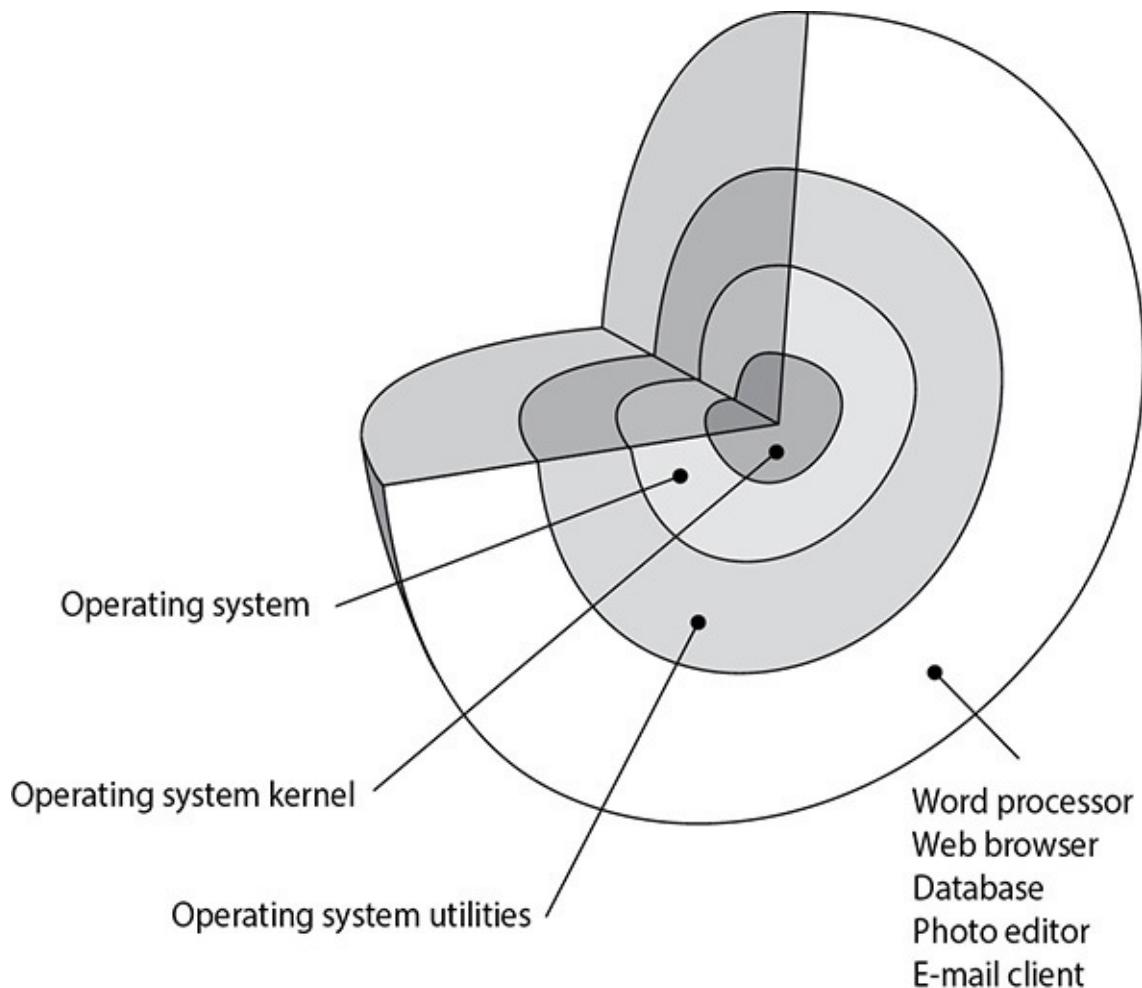
16. There are many different types of access control mechanisms that are commonly embedded into all operating systems. Which of the following is the mechanism that is missing in this graphic?



- A. Trusted computing base
 - B. Security perimeter
 - C. Reference monitor
 - D. Domain
- C. The reference monitor is an abstract machine that mediates all access subjects have to objects, both to ensure that the subjects have the necessary access rights and to protect the objects from unauthorized access and destructive modification. For a system to achieve a high level of trust, it must require subjects (programs, users, or processes) to be fully authorized prior to accessing an object (file, program, or resource). A subject must not be allowed to use a requested resource until the subject has proven it has been granted access privileges to use the requested object. The reference monitor is an access control concept, not an actual physical component, which is why it is normally referred to as the “reference monitor concept” or an “abstract machine.” The reference monitor is the access control concept, and the code that actually enforces this concept is the security kernel.
- A is incorrect because a security perimeter is a boundary that divides the trusted from the untrusted process access requests within software. The trusted processes within a system are referred to as being within the trusted computing base (TCB). The TCB is defined as the total combination of protection mechanisms within a computer system. The TCB includes hardware, software, and firmware. These are part of the TCB because the system is sure

these components will enforce the security policy and not violate it. Not all components need to be trusted, and therefore not all components fall within the TCB. The security perimeter is the demarcation between what is within the TCB, the trusted processes, and what is not, the untrusted processes.

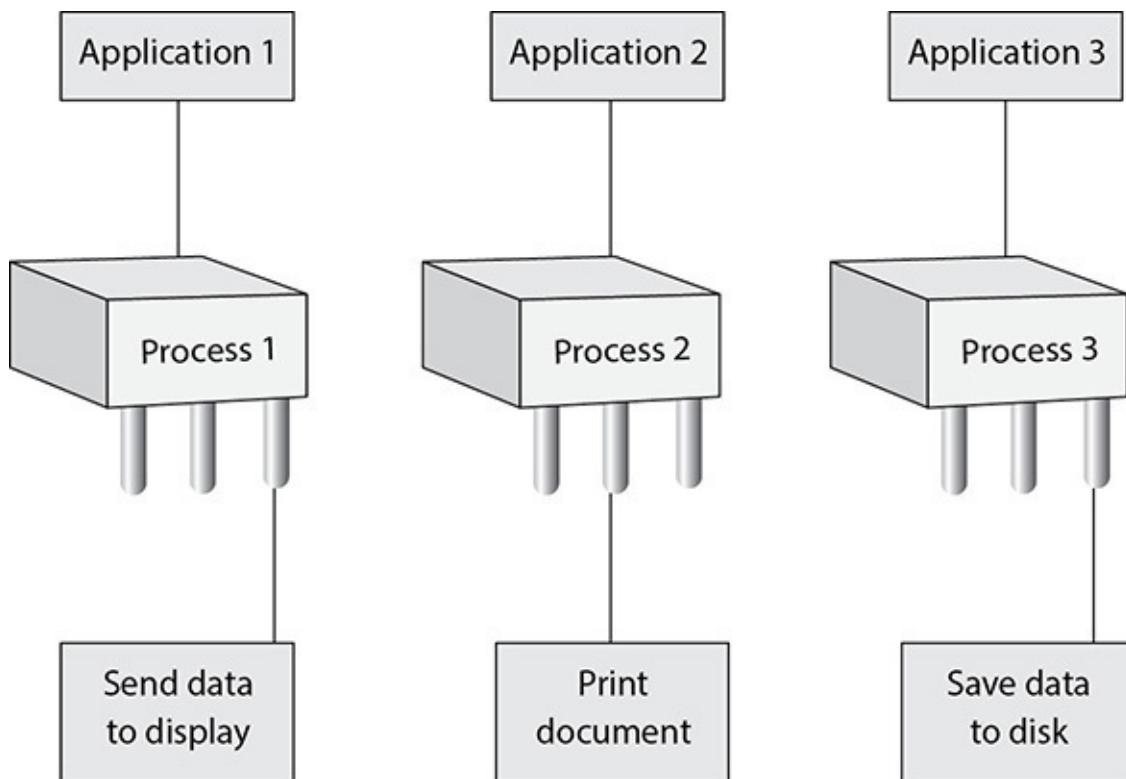
- B** is incorrect because not every process and resource falls within the TCB, so some of these components fall outside of an imaginary boundary referred to as the security perimeter. A security perimeter is a boundary that divides the trusted from the untrusted. For the system to stay in a secure and trusted state, precise communication standards must be developed to ensure that when a component within the TCB needs to communicate with a component outside the TCB, the communication cannot expose the system to unexpected security compromises. This type of communication is handled and controlled through interfaces. The security perimeter is a concept that helps enforce this type of security.
 - D** is incorrect because a domain is defined as a set of objects that a subject is able to access. This domain can be all the resources a user can access, all the files available to a program, the memory segments available to a process, or the services and processes available to an application. A subject needs to be able to access and use objects (resources) to perform tasks, and the domain defines which objects are available to the subject and which objects are untouchable and therefore unusable by the subject. A common implementation of a domain is a networked Windows environment. Resources are logically partitioned within the network to ensure subjects can only access these resources.
17. There are several security enforcement components that are commonly built into operating systems. Which component is illustrated in the graphic that follows?



- A. Virtual machines
 - B. Interrupt
 - C. Cache memory
 - D. Protection rings
- D. An operating system has several protection mechanisms to ensure processes do not negatively affect each other or the critical components. One security mechanism commonly used in operating systems is protection rings. These rings provide strict boundaries and definitions for what the processes that work within each ring can access and what operations they can successfully and securely execute. The processes that operate within the inner rings have more privileges than the processes operating in the outer rings, because the inner rings only permit the most trusted components and processes to operate within them. Protection rings support the availability, integrity, and confidentiality requirements of multitasking operating systems. The most commonly used architecture provides four protection rings:

- **Ring 0** Operating system kernel
 - **Ring 1** Remaining parts of the operating system
 - **Ring 2** I/O drivers and utilities
 - **Ring 3** Applications and user activity
- A** is incorrect because a virtual instance of an operating system is known as a virtual machine. A virtual machine is commonly referred to as a guest that is executed in the host environment. Virtualization allows a single host environment to execute multiple guests at once, with multiple virtual machines dynamically pooling resources from a common physical system. Computer resources such as RAM, processors, and storage are emulated through the host environment. The virtual machines do not directly access these resources; instead, they communicate with the host environment responsible for managing system resources. Virtual machines do not work in a circular framework as shown in the graphic.
- B** is incorrect because an interrupt is a function used in operating systems that allows for slots of the CPU to be used. The most basic CPUs can do only one thing at a time. So the system has hardware and software interrupts. When a device needs to communicate with the CPU, it has to wait for its interrupt to be called upon. The same thing happens in software. Each process has an interrupt assigned to it. It is like pulling a number at a customer service department in a store. You can't go up to the counter until your number has been called out. When a process is interacting with the CPU and an interrupt takes place (another process has requested access to the CPU), the current process's information is stored in the process table, and the next process gets its time to interact with the CPU.
- C** is incorrect because cache memory is a type of memory used for high-speed writing and reading activities and it is not necessarily a security mechanism. When the system assumes (through its programmatic logic) that it will need to access specific information many times throughout its processing activities, it will store the information in cache memory so it is easily and quickly accessible. Data in cache can be accessed much more quickly than data stored in real memory. Therefore, any information needed by the CPU very quickly, and very often, is usually stored in cache memory, thereby improving the overall speed of the computer system. Cache memory also does not work in a circular framework as illustrated in the graphic.

18. A multitasking operating system can have several processes running at the same time. What are the components within the processes that are shown in the graphic that follows?



- A. Threads
- B. Registers
- C. Address buses
- D. Process tables

- A. A process is a program in memory. More precisely, a process is the program's instructions and all the resources assigned to the process by the operating system. It is just easier to group all of these instructions and resources together and control them as one entity, which is a process. When a process needs to send something to the CPU for processing, it generates a thread. A thread is made up of an individual instruction set and the data that must be worked on by the CPU. Most applications have several different functions. Word processors can open files, save files, open other programs (such as an e-mail client), and print documents. Each one of these functions requires a thread (instruction set) to be dynamically generated. So, for example, if Tom chooses to print his document, the word processor process generates a thread that contains the instructions of how this document should be printed (font, colors, text, margins, and so on). If he chooses to send a document via e-mail through this

program, another thread is created that tells the e-mail client to open and what file needs to be sent. Threads are dynamically created and destroyed as needed. Once Tom is done printing his document, the thread that was generated for this functionality is destroyed.

- ☒ **B** is incorrect because a register is a temporary storage location. Processing chips within the CPU cover only a couple of square inches but contain millions of transistors. All operations within the CPU are performed by electrical signals at different voltages in different combinations, and each transistor holds this voltage, which represents 0's and 1's to the computer. The CPU contains registers that point to memory locations that contain the next instructions to be executed and that enable the CPU to keep status information of the data that needs to be processed. While a register can hold the instructions that make up the thread before it is fed into the CPU, it is not a component of the processes themselves.
- ☒ **C** is incorrect because an address bus is a hardwired connection to RAM chips and the individual input/output (I/O) devices in a computer system. In a computer, memory addresses of the instructions and data to be processed are held in registers until needed by the CPU. The CPU is connected to the address bus. Memory is cut up into sections that have individual addresses associated with them. I/O devices (optical discs, USB device, hard drive, and so on) are also allocated specific unique addresses. If the CPU needs to access some data, either from memory or from an I/O device, it sends down the address of where the needed data is located. The circuitry associated with the memory or I/O device recognizes the address the CPU sent down the address bus and instructs the memory or device to read the requested data and put it on the data bus. So the address bus is used by the CPU to indicate the location of the instructions to be processed, and the memory or I/O device responds by sending the data that resides at that memory location through the data bus.
- ☒ **D** is incorrect because a process table is a way for an operating system to keep track of processes that are running. An operating system is responsible for creating new processes, assigning them resources, synchronizing their communication, and making sure nothing insecure is taking place. The operating system keeps a process table, which has one entry per process. The table contains each individual process's state, stack pointer, memory allocation, program counter, and status of open files in use. The reason the

operating system documents all of this status information is that the CPU needs all of it loaded into its registers when it needs to interact with, for example, process 1. When process 1's CPU time slice is over, all of the current status information on process 1 is stored in the process table so that when its time slice is open again, all of this status information can be put back into the CPU registers. So, when it is process 2's time with the CPU, its status information is transferred from the process table to the CPU registers; it is transferred back again when the time slice is over.

The following scenario applies to questions 19 and 20.

Charlie is a new security manager at a textile company that develops its own proprietary software for internal business processes. Charlie has been told that the new application his team needs to develop must comply with the ISO/IEC 42010 standard. He has found out that many of the critical applications have been developed in the C programming language and has asked for these applications to be reviewed for a specific class of security vulnerabilities.

- 19.** Which of the following best describes the standard Charlie's team needs to comply with?
- A. International standard on system design to allow for better quality, interoperability, extensibility, portability, and security
 - B. International standard on system security to allow for better threat modeling
 - C. International standard on system architecture to allow for better quality, interoperability, extensibility, portability, and security
 - D. International standard on system architecture to allow for better quality, extensibility, portability, and security
- C. ISO/IEC 42010 has the goal of internationally standardizing the use of system architecture so that product developers don't have to improvise and come up with their own individual approaches. A disciplined approach to system architecture allows for better quality, interoperability, extensibility, portability, and security.
- A is incorrect because the answer specifically states “design” instead of “architecture.” Some people mistakenly think that these are the same things, but architecture takes place before design. Architecture works at a higher, more strategic level compared to design. Software development is becoming a more disciplined industry and it is moving toward formal architecture requirements.

- B** is incorrect because the standard identified in the question does not deal with threat modeling. ISO/IEC 42010 addresses system architecture requirements and guidelines.
 - D** is incorrect because it is not as complete as answer C; therefore, it is not the best answer. This standard does address interoperability issues, which is not listed in this answer.
- 20.** Which of the following is Charlie most likely concerned with in this situation?
- A.** Injection attacks
 - B.** Memory block
 - C.** Buffer overflows
 - D.** Browsing attacks
- C.** The C programming language is susceptible to buffer overflow attacks because some of its commands allow for direct pointer manipulations to take place. Specific commands can provide access to low-level memory addresses without carrying out bounds checking.
 - A** is incorrect because the C programming language does not have any more vulnerabilities pertaining to injection attacks than other languages. Injection attacks usually do not take place at the code level, but happen because an interface accepts data that is not properly filtered and validated.
 - B** is incorrect because this is a distracter answer. There is no official programming language vulnerability referred to as “memory block.”
 - D** is incorrect because a browsing attack is when someone is reviewing various assets for sensitive data. This does not relate to a programming language, but how access control is implemented.

The following scenario applies to questions 21 and 22.

Tim’s development team is designing a new operating system. One of the requirements of the new product is that critical memory segments need to be categorized as nonexecutable, with the goal of reducing malicious code from being able to execute instructions in privileged mode. The team also wants to make sure that attackers will have a difficult time predicting execution target addresses.

- 21.** Which of the following best describes the type of protection that needs

to be provided by this product?

- A. Hardware isolation
 - B. Memory induction application
 - C. Data execution prevention
 - D. Domain isolation protection
- C. Data execution prevention (DEP) is a security feature included in modern operating systems. It is intended to prevent a process from executing code from a nonexecutable memory region. This helps prevent certain exploits that store code via a buffer overflow, for example. DEP can mark certain memory locations as “off limits,” with the goal of reducing the “playing field” for hackers and malware.
- A is incorrect because memory hardware isolation has to be done at the hardware level, not just in an operating system. Some systems that require a high level of security can be designed to ensure that memory is not shared in any fashion. This requires hardware design, and the operating system (or other software) has to then be designed to use that specific hardware environment.
- B is incorrect because this is a distracter answer. This is not an official term or security issue.
- D is incorrect because domain isolation does not deal specifically with memory protection as does DEP. Domain isolation is not a specific technology, but a goal that operating systems attempt to accomplish. A domain is a set of resources that is available to an entity. Most people think of network domains in the Microsoft world, but a domain is just a set of resources. It is a general and old term. Domain isolation just means isolating one set of resources from another set of resources. This is commonly done so that one process cannot compromise another process’s resources.
22. Which of the following best describes the type of technology the team should implement to increase the work effort of buffer overflow attacks?
- A. Address space layout randomization
 - B. Memory induction application
 - C. Input memory isolation
 - D. Read-only memory integrity checks

- A.** Address space layout randomization (ASLR) is a control that involves randomly arranging the positions of a process's address space and other memory segments. It randomly arranges the positions of key data areas, usually including the base of the executable and position of system libraries, memory heap, and memory stacks, in a process's address space. ASLR makes it more difficult for an attacker to predict target addresses for specific memory attacks.
- B** is incorrect because this is a distracter answer. This is not an official term or security item.
- C** is incorrect because while memory isolation may help in protecting against buffer overflows, that is not the specific reason for its existence. Memory isolation is carried out to protect against many different memory attacks. ASLR has been specifically designed to try and outwit attackers and to make it more difficult for them to know a system's memory address scheme for exploitation purposes.
- D** is incorrect because this is a distracter answer. This is not an official term or security item.

The following scenario applies to questions 23, 24, and 25.

Operating systems have evolved and changed over the years. The earlier operating systems were monolithic and did not segregate critical processes from noncritical processes. As time went on, operating system vendors started to reduce the amount of programming code that ran in kernel mode. Only the absolutely necessary code ran in kernel mode, and the remaining operating system code ran in user mode. This architecture introduced performance issues, which required the operating system vendors to reduce the critical operating system functionality to microkernels and allow the remaining operating system functionality to run in client/server models within kernel mode.

- 23.** Which of the following best describes the second operating system architecture described in the scenario?
- A.** Layered
 - B.** Microkernel
 - C.** Monolithic
 - D.** Kernel based
- B.** In the microkernel architecture, a reduced amount of code is

running in kernel mode carrying out critical operating system functionality. Only the absolutely necessary code runs in kernel mode, and the remaining operating system code runs in user mode. Traditional operating system functions, such as device drivers, protocol stacks, and file systems, are removed from the microkernel to run in user space.

- A** is incorrect because a layered operating system architecture focuses on constructing the functions of the operating system into hierarchical layers. This architecture does not focus on what is or is not running in kernel mode.
- C** is incorrect because the industry started with monolithic operating systems and evolved from there. A monolithic operating system does not segregate privileged and nonprivileged processes and does not use a kernel. MS-DOS is an example of a monolithic operating system.
- D** is incorrect because while there is no official architecture called “kernel based,” this answer does not actually properly address the concept of reducing the amount of code that runs in kernel mode. The microkernel architecture specifically addressed this issue. A microkernel is the near-minimum amount of software that can provide the mechanisms needed to implement an operating system.

24. Which of the following best describes why there was a performance issue in the context of the scenario?

- A.** Bloated programming code
 - B.** I/O and memory location procedures
 - C.** Mode transitions
 - D.** Data and address bus architecture
- C.** A mode transition is when the CPU has to change from processing code in user mode to kernel mode. This is a protection measure, but it causes a performance hit because all of the information on the new process has to be loaded into the registers for the CPU to work with. Transitions between modes are at the discretion of the executing thread when the transition is from a level of high privilege to one of low privilege (kernel to user mode), but transitions from lower to higher levels of privilege can take place only through secure, hardware-controlled “gates” that are carried out by executing special instructions or when external interrupts are received.

- A** is incorrect. While bloated (extra) programming code can cause performance issues in many situations, that is not what this question is focusing on. When comparing operating system architectures and associated performance issues, the focus comes down to how specific functions are carried out and how efficient those procedures are—not the amount of code needed to carry out the function.
 - B** is incorrect because I/O and memory location do not have a direct correlation to operating system kernel architecture. The specific reason that many operating system vendors changed their products' architecture had to do with the performance issues of mode transitions the CPU had to continually carry out.
 - D** is incorrect because data and address bus architecture was not the specific reason that vendors moved to a microkernel architecture. This question is zeroing in on how much code ran in kernel versus user mode and how transitions took place, which has nothing to do with the bus architectures.
- 25.** Which of the following best describes the last architecture described in this scenario?
- A.** Hybrid microkernel
 - B.** Layered
 - C.** Monolithic
 - D.** Hardened and embedded
- A.** The hybrid microkernel architecture is a combination of monolithic and microkernel architectures. The critical operating system functionality is carried out in a microkernel construct, and the remaining functionality is carried out in a client/server model running within kernel mode. This architecture allows for the critical operating system functions to run in kernel mode and not experience the performance issues with previous architectures.
 - B** is incorrect because a layered operating system architecture focuses on constructing the functions of the operating system into hierarchical layers. This architecture does not focus on what is or is not running in kernel mode.
 - C** is incorrect because the industry started with monolithic operating systems and evolved from there. A monolithic operating system does not segregate privileged and nonprivileged processes and does not use a kernel. MS-DOS is an example of a monolithic operating

system.

- D** is incorrect because an operating system that is hardened and embedded is not a major architecture. The term “hardened” just means secured, and “embedded” means that the operating system’s functionalities are stripped down to only provide the basic and necessary functions required of the hardware the software is installed upon. Mobile phones and specialized hardware commonly have embedded operating systems.
- 26.** As with logical access controls, audit logs should be produced and monitored for physical access controls. Which of the following statements is correct about auditing physical access?
- A.** Unsuccessful access attempts should be logged but only need to be reviewed by a security guard.
 - B.** Only successful access attempts should be logged and reviewed.
 - C.** Only unsuccessful access attempts during unauthorized hours should be logged and reviewed.
 - D.** All unsuccessful access attempts should be logged and reviewed.
- D.** Physical access control systems can use software and auditing features to produce audit trails or access logs pertaining to access attempts. The following information should be logged and reviewed: the date and time of the access attempt, the entry point at which access was attempted, the user ID employed when access was attempted, and any unsuccessful access attempts, especially if they occur during unauthorized hours.
 - A** is incorrect because as with audit logs produced by computers, access logs are useless unless someone actually reviews them. A security guard may be required to review these logs, but a security professional or a facility manager should also review these logs periodically. Management needs to know where entry points into the facility exist and who attempts to use them. Audit and access logs are detective controls, not preventive. They are used to piece together a situation after the fact instead of attempting to prevent an access attempt in the first place.
 - B** is incorrect because unsuccessful access attempts should be logged and reviewed. Even though auditing is not an activity that will deny an entity access to a network, computer, or location, it will track activities so that a security professional can be warned of suspicious activity. This information can be used to point out

weaknesses of other controls and help security personnel understand where changes must be made to preserve the necessary level of security in the environment.

- C** is incorrect because all unauthorized access attempts should be logged and reviewed, regardless of when they occurred. Attempted break-ins can occur at any time. Operating parameters can be set up for some physical access controls to allow a certain number of failed access attempts to be accepted before a user is locked out; this is a type of clipping level. An audit trail of this information can alert security personnel to a possible intrusion.
- 27.** An outline for a physical security design should include program categories and the necessary countermeasures for each. What category do locks and access controls belong to?
 - A.** Assessment
 - B.** Deterrence
 - C.** Response
 - D.** Delay
- D.** The physical security program design phase should begin with a structured outline that lists each category of the program: deterrence, delaying, detection, assessment, and response. The outline evolves into a framework, which is fleshed out with the necessary controls and countermeasures. The intent behind the delay category is to stall intruders to help ensure they get caught. Examples of countermeasures that belong to this category are locks, defense-in-depth measures, and access controls. Other types of delaying mechanisms include reinforced walls and rebar. The idea is that it will take a bad guy longer to get through two reinforced walls, which gives the response force sufficient time to arrive at the scene and stop the attacker. Of the categories listed in the answer options, detection is missing. Detection refers to the determination or awareness that an intrusion has occurred. Examples of detection controls include external intruder sensors and internal intruder sensors.
- A** is incorrect because assessment countermeasures include security guard procedures and communication structure (calling tree). When an incident occurs, the assessment team (or security guard) is first on the scene to determine what has taken place and what needs to happen next: for example, a call to the police or fire station,

management, a security service, etc. The assessment determines what type of response is needed.

- B** is incorrect because deterrence refers to those controls that will discourage potential intruders from conducting criminal activity. Examples include fences, warning signs, security guards, and dogs. Another example found in residential areas is a “Neighborhood Crime Watch” sign that is erected in neighborhoods or even in home windows. The idea is that a casual intruder will be less likely to attempt an intrusion if he thinks that the neighborhood is making a concerted effort to watch for criminals and that he may be caught.
 - C** is incorrect because response refers to an organization’s processes and the personnel it assigns to react to intrusions and disruptions. Controls in this category include a response force, emergency response procedures, and police, fire, and medical personnel.
- 28.** What discipline combines the physical environment and the sociology issues that surround it to reduce crime rates and the fear of crime?
- A.** Layered defense model
 - B.** Target hardening
 - C.** Crime Prevention Through Environmental Design
 - D.** Natural access control
- C.** Crime Prevention Through Environmental Design (CPTED) is a discipline that outlines how the proper design of a physical environment can reduce crime by directly affecting human behavior. It provides guidance in loss and crime prevention through proper facility construction and environmental components and procedures. The crux of CPTED is that the physical environment can be manipulated to create behavioral effects that will reduce crime and the fear of crime. It looks at the components that make up the relationship between humans and their environment. This encompasses the physical, social, and psychological needs of the users of different types of environments and predictable behaviors of these users and offenders. For example, CCTV cameras should be mounted in full view so that criminals know their activities will be captured and other people know the environment is well monitored and thus safer.
 - A** is incorrect because a layered defense model is a tiered architecture of physical, logical, and administrative security controls. The concept is that if one layer fails, other layers will

protect the valuable asset. Layers should be implemented moving from the perimeter toward the asset. For example, you would have a fence, then your facility walls, then an access control card device, then a guard, then an IDS, and then locked computer cases and safes. This series of layers will protect the company's most sensitive assets, which would be placed in the innermost control zone of the environment. So if the bad guy were able to climb over your fence and outsmart the security guard, he would still have to circumvent several layers of controls before getting to your precious resources and systems.

- B** is incorrect because target hardening focuses on denying access through physical and artificial barriers (alarms, locks, fences, and so on). Traditional target hardening can lead to restrictions on the use, enjoyment, and aesthetics of an environment. Remember that security entails maintaining a delicate balance between ease of use and protection. A Parks and Recreation department could implement fences, intimidating signs, and barriers around its parks and green areas to discourage gangs from congregating, but who would want to play or have a picnic there? The same goes for an office building. You must provide the necessary levels of protection, but your protection mechanisms should be more subtle and unobtrusive.
 - D** is incorrect because natural access control is the guidance of people entering and leaving a space by the placement of doors, fences, lighting, and even landscaping. For example, an office building may have external bollards with lights in them. These bollards carry out different safety and security services. The bollards themselves protect the facility from physical destruction by preventing people from driving their cars into the building. The light emitted helps ensure that criminals do not have a dark place to hide. And the lights and bollard placement guides people along the sidewalk to the entrance, instead of using signs or railings.
- 29.** David is preparing a server room at a new branch office. What locking mechanisms should he use for the primary and secondary server room entry doors?
- A.** The primary and secondary entrance doors should have access controlled through a swipe card or cipher lock.
 - B.** The primary entrance door should have access controlled through a security guard. The secondary doors should be secured from the inside and allow no entry.

- C. The primary entrance door should have access controlled through a swipe card or cipher lock. The secondary doors should have a security guard.
 - D. The primary entrance door should have access controlled through a swipe card or cipher lock. Secondary doors should be secured from the inside and allow no entry.
- D.** Data centers, server rooms, and wiring closets should be located in the core areas of a facility, near wiring distribution centers. Strict access control mechanisms and procedures should be implemented for these areas. The access control mechanisms may be smart card readers, biometric readers, or combination locks. These restricted areas should have only one access door, but fire code requirements typically dictate there must be at least two doors to most data centers and server rooms. Only one door should be used for daily entry and exit, and the other door should be used only in emergency situations. This second door should not be an access door, which means people should not be able to come in through this door. It should be locked, but it should have a panic bar that will release the lock if pressed from inside and used as an exit.
- A** is incorrect because entrance should not be permitted through the secondary door—even with identification, authentication, and authorization processes. There should only be one entry point into a server room. Other doors should not provide entrance but can be used for emergency exits. Thus, the secondary doors should be secured from the inside to prevent entry.
- B** is incorrect because the primary entrance door to a server room needs to carry out identification, authentication, and authorization processes. A swipe card or cipher lock fulfills these functions. A server room, ideally, should not be directly accessible from public areas like stairways, corridors, loading docks, elevators, and restrooms. This helps prevent foot traffic from casual passersby. Those who are by the doors to secured areas should have a legitimate reason for being there, as opposed to being on their way to a meeting room, for example.
- C** is incorrect because the secondary door should not have a security guard. The door should simply be secured from the inside so that it cannot be used as an entry. The secondary door should serve as an emergency exit.

30. Before an effective physical security program can be rolled out, a

number of steps must be taken. Which of the following steps comes first in the process of rolling out a security program?

- A. Create countermeasure performance metrics.
 - B. Conduct a risk analysis.
 - C. Design the program.
 - D. Implement countermeasures.
- B.** Of the steps listed, the first in the process of rolling out an effective physical security program is to carry out a risk analysis to identify the vulnerabilities and threats, and calculate the business impact of each threat. But before this is done, a team of internal employees and/or external consultants needs to be identified to build the physical security program. The team presents the risk analysis findings to management and works with them to define an acceptable risk level for the physical security program. From there, the team must develop baselines and metrics in order to evaluate and determine if the baselines are being met by the implemented countermeasures. Once the team identifies and implements the countermeasures, the performance of these countermeasures should be continually evaluated and expressed in the previously created metrics. These performance values are compared to the set baselines. If the baselines are continually maintained, then the security program is successful because the company's acceptable risk level is not being exceeded.
- A** is incorrect because of the steps listed, creating countermeasure performance metrics is not the first step in creating a physical security program. It is, however, a very important one because it is only possible to determine how beneficial and effective the program is if it is monitored through a performance-based approach. This means you should devise measurements and metrics to measure the effectiveness of the chosen countermeasures. This enables management to make informed business decisions when investing in the protection of the organization's physical security. The goal is to increase the performance of the physical security program and decrease the risk to the company in a cost-effective manner. You should establish a baseline of performance and thereafter continually evaluate performance to make sure that the company's protection objectives are being met. Examples of possible performance metrics include number of successful crimes, number of successful disruptions, and the time it took for a criminal to

defeat a control.

- C** is incorrect because designing the program should take place after the risk analysis. Once the level of risk is understood then the design phase can take place to protect from the threats identified in the risk analysis. The design will incorporate the controls required for each category of the program: deterrence, delaying, detection, assessment, and response.
- D** is incorrect because implementing countermeasures is one of the last steps in the process of rolling out a physical security program. Before countermeasures can be identified and implemented, it is important to conduct a risk analysis and work with management to define an acceptable level of risk. From the acceptable risk level, the team should derive the required performance baselines, and then create countermeasure performance metrics. Next, the team should develop criteria from the results of the analysis, outlining the level of protection and performance required for deterrence, delaying, detection, assessment, and response. Only after these steps are completed should the team identify and implement countermeasures for each of these categories.

31. A number of measures should be taken to help protect devices and the environment from electric power issues. Which of the following is best to keep voltage steady and power clean?

- A.** Power line monitor
 - B.** Surge protector
 - C.** Shielded cabling
 - D.** Regulator
- D.** When clean power is being provided, the power supply contains no interference or voltage fluctuation. Mechanisms should be in place to detect unwanted power fluctuations and protect the integrity of your data processing environment. Voltage regulators and line conditioners can be used to ensure a clean and smooth distribution of power. The primary power runs through a regulator or conditioner. They have the capability to absorb extra current if there is a spike, and to store energy to add current to the line if there is a sag. The goal is to keep the current flowing at a nice, steady level so neither motherboard components nor employees get fried.
 - A** is incorrect because power line monitors are employed to detect frequency and voltage amplitude changes. Interference interrupts

the flow of an electrical current, and fluctuations can actually deliver a different level of voltage than what was expected. Each fluctuation can be damaging to devices and people. In order to effectively monitor frequency and voltage amplitude changes, you should understand what they are. Power excess can be described as a spike, which is momentary high voltage, or a surge, which is prolonged high voltage. Power loss can be experienced as a fault (momentary power outage) or a blackout (prolonged, complete loss of electric power). A sag or dip is a momentary low voltage condition, from one cycle to a few seconds. A brownout, also a type of power degradation, is a prolonged power supply that is below normal voltage. Finally, an in-rush current is an initial surge of current required to start a load.

- ☒ **B** is incorrect because a surge protector is used to move excess voltage to ground when a surge occurs. A surge is a prolonged rise in voltage from a power source. Surges can cause a lot of damage very quickly. A surge is one of the most common power problems and is controlled with surge protectors. A surge can come from a strong lightning strike, a power plant going online or offline, a shift in the commercial utility power grid, and electrical equipment within a business starting and stopping. Most computers have a built-in surge protector in their power supplies, but these are small surge protectors and cannot provide protection against the damage that larger surges (say, from storms) can cause. So, you need to ensure all devices are properly plugged into larger surge protectors, whose only job is to absorb any extra current before it is passed to electrical devices.
- ☒ **C** is incorrect because shielded cabling should be used for long cable runs and cables that run in buildings with fluorescent lighting or other interference mechanisms. Fluorescent lighting gives off radio frequency interference (RFI), which is disturbance to the flow of electric power while it travels across a power line. We could rip out all the fluorescent lighting in our buildings—or we can use shielded cabling where fluorescent lighting could cause a problem. If you were to climb up into your office's dropped ceiling and look around, you would probably see wires bundled and tied up to the true ceiling. If your office is using fluorescent lighting, the power and data lines should not be running over, or on top of, the fluorescent lights. This is because the radio frequencies being given off can interfere with the data or power current as it travels through these wires.

- 32.** Crime Prevention Through Environmental Design (CPTED) is a discipline that outlines how the proper design of a physical environment can reduce crime by directly affecting human behavior. Of CPTED's three main components, what is illustrated in the following photo?



- A. Natural surveillance
 - B. Target hardening
 - C. Natural access control
 - D. Territorial reinforcement
- A. CPTED provides three main strategies to bring together the physical environment and social behavior to increase overall protection: natural access control, natural surveillance, and territorial reinforcement. Surveillance can take place through organized means (security guards), mechanical means (CCTV), and natural strategies (straight lines of sight, low landscaping, raised entrances). The goal of natural surveillance is to make criminals feel uncomfortable by providing many ways observers could potentially see them and to make all other people feel safe and comfortable, by providing an open and well-designed environment. Natural surveillance is the use and placement of physical environmental features, personnel walkways, and activity areas in ways that maximize visibility. This photo shows a stairway in a building designed to be open and allow easy observation.

- B** is incorrect because target hardening focuses on denying access through physical and artificial barriers (alarms, locks, fences, and so on). Target hardening is not a component of CPTED. Traditional target hardening can lead to restrictions on the use, enjoyment, and aesthetics of an environment. If your environment is a prison, this look might be just what you need. But if your environment is an office building, you're not looking for Fort Knox décor. Nevertheless, you still must provide the necessary levels of protection, but your protection mechanisms should be more subtle and unobtrusive. Let's say your organization's team needs to protect a side door at your facility. The traditional target-hardening approach would be to put locks, alarms, and cameras on the door; install an access control mechanism, such as a proximity reader; and instruct security guards to monitor this door.
- C** is incorrect because natural access control is the guidance of people entering and leaving a space by the placement of doors, fences, lighting, and even landscaping. For example, an office building may have external bollards with lights in them. These bollards actually carry out different safety and security services. The bollards themselves protect the facility from physical destruction by preventing people from driving their cars into the building. The light emitted helps ensure that criminals do not have a dark place to hide. And the lights and bollard placement guides people along the sidewalk to the entrance, instead of using signs or railings. They work together to give individuals a feeling of being in a safe environment and help dissuade criminals by working as deterrents.
- D** is incorrect because the third CPTED strategy is territorial reinforcement, which creates physical designs that emphasize or extend the company's physical sphere of influence so legitimate users feel a sense of ownership of that space. Territorial reinforcement can be implemented through the use of walls, fences, landscaping, light fixtures, flags, clearly marked addresses, and decorative sidewalks. The goal of territorial reinforcement is to create a sense of a dedicated community. Companies implement these elements so employees feel proud of their environment and have a sense of belonging, which they will defend if required to do so. These elements are also implemented to give potential offenders the impression that they do not belong there, that their activities are at risk of being observed, and that their illegal activities will not be tolerated or ignored.

- 33.** There are five different classes of fire. Each depends upon what is on fire. Which of the following is the proper mapping for the items missing in the provided table?

Fire Class	Type of Fire	Elements of Fire	Suppression Method
Class A			Water, soda acid
Class B			CO ₂ , FM-200
Class C			Gas (Halon) or CO ₂ , nonconductive extinguishing agent
Class D			Dry chemicals
Class K			A wet chemical

- A.** Class D—combustible metals
 - B.** Class C—liquid
 - C.** Class B—electrical
 - D.** Class A—electrical
- A.** There are five classes of fire (A, B, C, D, and K). You need to know the differences among the types of fire so that you know how to properly extinguish each type. Portable fire extinguishers have markings that indicate what type of fire they should be used on. A fire is a Class D if there are combustible metals on fire. These metals can be magnesium, sodium, or potassium. These types of fires should be suppressed and extinguished with dry chemicals.
- B** is incorrect because a fire is a Class C if there is something electrical on fire. This can be computers or any other type of device that runs on electricity. These types of fires should be suppressed and extinguished with a type of gas as in Halon or CO₂.
- C** is incorrect because a fire is a Class B if there is something liquid on fire. This can be petroleum, tars, or oils. These types of fires should be suppressed and extinguished with a type of gas, such as FM-200 or CO₂.
- D** is incorrect because a fire is a Class A if there is a type of common combustible material on fire. This can be wood, paper, or cloth. These types of fires should be suppressed and extinguished with water or soda acid.

- 34.** Electrical power is being provided more through smart grids, which

allow for self-healing, resistance to physical and cyberattacks, increased efficiency, and better integration of renewable energy sources. Countries want their grids to be more reliable, resilient, flexible, and efficient. Why does this type of evolution in power infrastructure concern many security professionals?

- A. Allows for direct attacks through Power over Ethernet
 - B. Increased embedded software and computing capabilities
 - C. Does not have proper protection against common web-based attacks
 - D. Power fluctuation and outages directly affect computing systems
- B.** We are moving to smart grids, which means that there is a lot more computing software and technology embedded into the grids and the items that make up the grids to optimize and automate these functions. This in turn means that almost every component of the new power grid has to be computerized in some manner; thus, it can be vulnerable to digital-based attacks. Power grids are considered critical infrastructures to countries, and a power grid disruption can have negative consequences for a country.
- A** is incorrect because smart grids do not directly deal with providing Power over Ethernet (PoE). PoE provides both data and power connections on one cable. This means that a company does not need to have one cable for Ethernet and one for power—the power and network data can be converged onto one cable. For equipment that does not already have a power or data connection, PoE can be attractive when the power demand is low.
- C** is incorrect because implementing computing capabilities in various power grid components does not have a direct correlation to web-based attacks. Power grid components are not going to necessarily have direct access to web servers and websites. The general term for infrastructure types of systems is SCADA (supervisory control and data acquisition) and generally refers to industrial control systems (ICS). These systems monitor and control industrial, infrastructure, or facility-based processes. An attacker needs to know how to specifically exploit vulnerabilities in these types of systems, which would be different from common website vulnerabilities.
- D** is incorrect because power fluctuations and outages are not necessarily security issues, and these are not the most critical topics most security professionals would be concerned with as the

traditional power grid moves to a smart grid. A smart grid is made up of many embedded systems, which contain software that can have vulnerabilities for exploitation.

The following scenario applies to questions 35, 36, and 37.

Mike is the new CSO of a large pharmaceutical company. He has been asked to revamp the company's physical security program and better align it with the company's information security practices. Mike knows that the new physical security program should be made up of controls and processes that support the following categories: deterrent, delaying, detection, assessment, and response.

- 35.** Mike's team has decided to implement new perimeter fences and warning signs against trespassing around the company's facility. Which of the categories listed in the scenario do these countermeasures map to?
- A.** Deterrent
 - B.** Delaying
 - C.** Detection
 - D.** Assessment
- A.** Fences, warning signs, and security guards are examples of countermeasures that can be put into place to deter unauthorized entry. A physical security program should contain controls in each of the following categories: deterrent, delaying, detection, assessment, and response.
- B** is incorrect because reinforced walls, rebar, locks, and the use of double walls can be used as delaying mechanisms. The idea is that it will take the bad guy longer to get through these types of controls, which gives the response force sufficient time to arrive at the scene and stop the attacker. Deterrent controls reduce the likelihood of a vulnerability being exploited; a delaying control tries to ensure that if a bad thing happens, it will slow down the intruder.
- C** is incorrect because detection tools are implemented not to deter malicious individuals but to detect their activities. Detection tools can be intrusion detection systems, sensors, and PIDAS fencing.
- D** is incorrect because assessment controls pertain to how different situations will be identified and assessed. The most common control in this category is a security guard because he can connect the pieces of a situation together and determine what next steps should

take place. It is important that there are controls in place that will carry out incident assessment and procedures that will be followed depending upon the outcome of the assessment.

- 36.** Mike's team has decided to implement stronger locks on the exterior doors of the new company's facility. Which of the categories listed in the scenario does this countermeasure map to?
- A. Deterrent
 - B. Delaying
 - C. Detection
 - D. Assessment
- B.** Locks, defense-in-depth measures, and access controls are commonly used to delay potential intruders. A physical security program should contain controls in each of the following categories: deterrent, delaying, detection, assessment, and response.
- A** is incorrect because fences, warning signs, and security guards are examples of countermeasures that can be put into place to deter unauthorized entry. The goal of these types of controls is for a potential attacker to not carry out his activities in the first place.
- C** is incorrect because detection tools are implemented not to deter malicious individuals but to detect their activities. Detection tools can be intrusion detection systems, sensors, and PIDAS fencing.
- D** is incorrect because assessment controls pertain to how different situations will be identified and assessed. The most common control in this category is a security guard because he can connect the pieces of a situation together and determine what next steps should take place. It is important that there are controls in place that will carry out incident assessment and procedures that will be followed depending upon the outcome of the assessment.
- 37.** Mike's team has decided to hire and deploy security guards to monitor activities within the company's facility. Which of the categories listed in the scenario does this countermeasure map to?
- A. Delaying
 - B. Detection
 - C. Assessment
 - D. Recall

- C.** The assessment requirement of a physical security program pertains to how various situations will be assessed, triaged, and dealt with. The most common countermeasure to meet this need is the use of security guards.
- A** is incorrect because locks, defense-in-depth measures, and access controls are commonly used to delay potential intruders. A physical security program should contain controls in each of the following categories: deterrent, delaying, detection, assessment, and response.
- B** is incorrect because detection tools are implemented not to deter malicious individuals but to detect their activities. Detection tools can be intrusion detection systems, sensors, and PIDAS fencing.
- D** is incorrect because it is a distracter answer.

The following scenario applies to questions 38, 39, and 40.

Greg is the security facility officer of a financial institution. His boss has told him that visitors need a secondary screening before they are allowed into sensitive areas within the building. Greg has also been told by the network administrators that after the new HVAC system was installed throughout the facility, they have noticed that power voltage to the systems in the data center sags.

- 38.** Which of the following is the best control that Greg should ensure is implemented to deal with his boss's concern?
- A.** Access and audit logs
 - B.** Mantrap
 - C.** Proximity readers
 - D.** Smart card readers
- B.** A mantrap can be used so unauthorized individuals entering a facility cannot get in or out if the mantrap is activated. A mantrap is a small room with two doors. The first door is locked; a person is identified and authenticated by a security guard, biometric system, smart card reader, or swipe card reader. Once the person is authenticated and access is authorized, the first door opens and allows the person into the mantrap. The first door locks and the person is trapped. The person must be authenticated again before the second door unlocks and allows him into the facility. This requires two different authentication and authorization processes to complete successfully before someone is allowed entrance.
 - A** is incorrect because access and audit logs are not controls that can

be used to carry out secondary screening activities. These are detective controls that are commonly reviewed after an incident has occurred.

- C** is incorrect because it is not necessarily the best answer to this question. Proximity cards are most commonly used to gain physical access to a facility or location. The question specifically points out a requirement of secondary authentication to take place before someone can enter a sensitive area within a facility, and this is the reason that mantraps exist.
 - D** is incorrect because it is not necessarily the best answer to this question. Smart cards can be used for authentication purposes in many different situations. The question specifically points out a requirement of secondary authentication to take place before someone can enter a sensitive area within a facility, and this is the reason that mantraps exist. The mantrap might use smart cards as one of its authentication steps.
- 39.** Which of the following best describes the situation that the network administrators are experiencing?
- A.** Brownouts
 - B.** Surges
 - C.** In-rush current
 - D.** Power line interference
- C.** When a heavy electrical device is turned on, it can draw a large amount of current, which is referred to as in-rush current. If the device sucks up enough current, it can cause a sag in the available power for surrounding devices. This could negatively affect their performance. It is a good idea to have the data processing center and devices on a different electrical wiring segment from that of the rest of the facility, if possible, so the devices will not be affected by these issues.
 - A** is incorrect because when power companies are experiencing high demand, they frequently reduce the voltage in an electrical grid, which is referred to as a brownout. Constant-voltage transformers can be used to regulate this fluctuation of power. They can use different ranges of voltage and only release the expected 120 volts of alternating current to devices. Brownouts are not usually associated with HVAC systems.

- B** is incorrect because a surge is a quick rise in voltage from a power source. Surges can cause a lot of damage very quickly. A surge is one of the most common power problems and is controlled with surge protectors. These protectors use a device called a metal oxide varistor, which moves the excess voltage to ground when a surge occurs.
 - D** is incorrect because when clean power is being provided, the power supply contains no interference or voltage fluctuation. The possible types of interference (line noise) are electromagnetic interference (EMI) and radio frequency interference (RFI), which is disturbance to the flow of electric power while it travels across a power line. This question does not address interference issues like these.
- 40.** Which of the following is a control that Greg's team could implement to address the network administrators' issue?
- A.** Secondary feeder line
 - B.** Insulated grounded wiring
 - C.** Line conditioner
 - D.** Generator
- C.** Because these and other occurrences are common, mechanisms should be in place to detect unwanted power fluctuations and protect the integrity of data processing environments. Voltage regulators and line conditioners can be used to ensure a clean and smooth distribution of power. The primary power runs through a regulator or conditioner. They have the capability to absorb extra current if there is a spike, and to store energy to add current to the line if there is a sag.
 - A** is incorrect because a secondary feeder line from a transformer does not address the issue outlined in this scenario. A secondary line would be put into place for redundancy and failover purposes.
 - B** is incorrect because an insulated grounded wire does not address the issue outlined in the scenario. The issue in the scenario has to do with in-rush currents, which means that the voltage of the power supply is uneven and potentially damaging. Wires are grounded to ensure that an excessive current goes to the ground and not to a piece of equipment or person. Grounding wires does not address voltage and current fluctuation.

- D** is incorrect because a generator is implemented in case there is a power outage. A generator does not have any effect on power voltage changes.
- 41.** There are several components involved with steganography. Which of the following refers to a file that has hidden information in it?
- A.** Stegomedium
 - B.** Concealment cipher
 - C.** Carrier
 - D.** Payload
- C.** Steganography is a method of hiding data in another media type so that the very existence of the data is concealed. Only the sender and receiver are supposed to be able to see the message because it is secretly hidden in a graphic, WAV file, document, or other type of media. The message is not necessarily encrypted, just hidden. Encrypted messages can draw attention because it tells the bad guy, “This is something sensitive.” A message hidden in a picture would not attract this type of attention, even though the exact same secret message can be embedded into this image. Steganography is a type of security through obscurity. The components involved with steganography are the carrier, stegomedium, and payload. The carrier is a signal, data stream, or file that has hidden information inside of it. In other words, it carries the payload.
 - A** is incorrect because the stegomedium is the medium in which the information is hidden in steganography. If the message were held within a graphic, the stegomedium could be JPEG or TIFF. If the message were embedded within a file, the stegomedium could be a Word document. A stegomedium can be a graphic type, WAV file type, document type, or other type of media.
 - B** is incorrect because a concealment cipher is a type of steganography method that involves putting a message within a message. It is a way to hide a secret message within something familiar from the world around us. This answer does not specify a specific component of steganography but is a specific type of steganography.
 - D** is incorrect because the payload is the information that is to be concealed and transported through the use of steganography. The payload is the actual information that the sender wants to keep secret.

- 42.** Which of the following incorrectly describes steganography?
- A. It is a type of security through obscurity.
 - B. Modifying the most significant bit is the most common method used.
 - C. Steganography does not draw attention to itself like encryption does.
 - D. Media files are ideal for steganographic transmission because of their large size.
- B.** Steganography is the method of hiding data in another media type so that the very existence of the data is concealed. One of the most common methods of embedding the message into some type of medium is using the least significant bit (LSB)—not the most significant bit. Many types of files have some bits that can be modified and not affect the file they are in, which is where secret data can be hidden without altering the file in a visible manner. In the LSB approach, graphics with a high resolution or an audio file that has many different types of sounds (high bit rate) are the most successful in hiding information within. There is commonly no noticeable distortion, and the file is usually not increased to a size that can be detected. A 24-bit bitmap file will have 8 bits representing each of the three color values, which are red, green, and blue. These 8 bits are within each pixel. If we consider just the blue, there will be 2^8 different values of blue. The difference between 11111111 and 11111110 in the value for blue intensity is likely to be undetectable by the human eye.
- A** is incorrect because steganography is a type of security through obscurity. Security through obscurity means that instead of actually securing something with a countermeasure, someone uses secrecy as the way to protect the asset. An example of security through obscurity is if a network administrator changes his HTTP port from 80 to 8080 with the hopes that no one will figure this out. Security through obscurity means that you are trying to fool the potential attacker and you assume that the attacker will not be clever enough to figure out your trickery.
- C** is incorrect because it is true that steganography does not draw attention to itself as does encryption. An encrypted message can draw attention because it tells the bad guy that the encrypted information is sensitive (otherwise, it wouldn't be encrypted in the first place). An attacker may then be motivated to break the

encryption and uncover the information. The goal of steganography is that the attacker not even know that the sensitive information exists and thus will not attempt to capture it.

- D** is incorrect because it is true that larger media files are ideal for steganographic transmission because there are more bits to manipulate with a lower chance that anyone will notice. As a simple example, a sender might start with an innocuous image file and adjust the color of every hundredth pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it. The larger the file, the more obscurity can be accomplished because there are more bits to work with and manipulate.
- 43.** Which of the following correctly describes a drawback of symmetric key systems?
 - A.** Computationally less intensive than asymmetric systems
 - B.** Work much more slowly than asymmetric systems
 - C.** Carry out mathematically intensive tasks
 - B.** Key must be delivered via secure courier
 - D.** In order for two users to exchange messages encrypted with a symmetric algorithm, they must first figure out how to distribute the key. If a key is compromised, then all messages encrypted with that key can be decrypted and read by an intruder. It is not safe to simply send the key in an e-mail message, because the key is not protected and can be easily intercepted and used by attackers. Thus, one user must send the key to the other using an out-of-band method. The user can save the key on a thumb drive and walk it over to the other person's desk or have a secure courier deliver it. This is a disadvantage of symmetric cryptography because distribution is a hassle, as well as clumsy and insecure.
 - A** is incorrect because it describes an advantage of symmetric algorithms. Because they are less computationally intensive than asymmetric algorithms, symmetric algorithms tend to be much faster. They can encrypt and decrypt relatively quickly large amounts of data that would take an unacceptable amount of time to encrypt and decrypt with an asymmetric algorithm.
 - B** is incorrect because asymmetric systems work much more slowly than symmetric systems. The speed with which symmetric algorithms work is an advantage. Asymmetric algorithms are slower

than symmetric algorithms because they use much more complex mathematics to carry out their functions, which requires more processing time. However, asymmetric algorithms can provide authentication and nonrepudiation, whereas symmetric algorithms cannot. Because both users employ the same key to encrypt and decrypt messages, symmetric cryptosystems can provide confidentiality but they cannot provide authentication or nonrepudiation. There is no way to prove through cryptography who actually sent a message if two people are using the same key.

- C** is incorrect because asymmetric algorithms carry out mathematically intensive tasks. Symmetric algorithms, on the other hand, carry out relatively simplistic mathematical functions on the bits during the encryption and decryption processes. They substitute and scramble (transpose) bits, which is not overly difficult or processor intensive. The reason it is hard to break this type of encryption is that the symmetric algorithms carry out this type of functionality over and over again. So a set of bits will go through a long series of being substituted and transposed.

- 44.** Which of the following occurs in a PKI environment?
- A.** The RA creates the certificate, and the CA signs it.
 - B.** The CA signs the certificate.
 - C.** The RA signs the certificate.
 - D.** The user signs the certificate.
- B.** A certificate authority (CA) is a trusted organization (or server) that maintains and issues digital certificates. When a person requests a certificate, the registration authority (RA) verifies that individual's identity and passes the certificate request off to the CA. The CA constructs the certificate, digitally signs it, sends it to the requester, and maintains the certificate over its lifetime. The CA digitally signs it so that the receiver can verify that the certificate came from that specific CA. The CA digitally signs the certificate with its private key, and the receiver verifies this signature with the CA's public key.
 - A** is incorrect because the RA does not create the certificate; the CA creates it and signs it. The RA performs the certification registration duties. The RA establishes and confirms the identity of the individual requesting the certificate, initiates the certification process with a CA on behalf of an end user, and can perform

certificate life-cycle management functions. The RA cannot issue certificates but can act as a broker between the user and the CA. When users need new certificates, they make requests to the RA, and the RA verifies all necessary identification information before allowing a request to go to the CA.

- C** is incorrect because the RA does not sign the certificate. The CA signs the certificate. The RA validates the user's identity and then sends the request for a certificate to the CA.
 - D** is incorrect because the user does not sign the certificate. In a PKI environment, a user's certificate is created and signed by the CA. The CA is a trusted third party that generates and maintains user certificates, which hold their public keys. The certificate is digitally signed to provide confidence to others that the certificate was created by that specific CA.
- 45.** Which of the following correctly describes the difference between public key cryptography and public key infrastructure?
- A.** Public key cryptography is the use of an asymmetric algorithm, while public key infrastructure is the use of a symmetric algorithm.
 - B.** Public key cryptography is used to create public/private key pairs, and public key infrastructure is used to perform key exchange and agreement.
 - C.** Public key cryptography provides authentication and nonrepudiation, while public key infrastructure provides confidentiality and integrity.
 - D.** Public key cryptography is another name for asymmetric cryptography, while public key infrastructure consists of public key cryptographic mechanisms.
- D.** Public key cryptography is asymmetric cryptography; the terms are used interchangeably. Public key cryptography is one piece in a public key infrastructure (PKI), which is made up of many different parts, including certificate authorities, registration authorities, certificates, keys, programs, and users. The infrastructure contains the pieces that will identify users, create and distribute certificates, maintain and revoke certificates, distribute and maintain encryption keys, and enable all technologies to communicate and work together for the purpose of encrypted communication and authentication.
 - A** is incorrect because PKI uses a hybrid system of symmetric and

asymmetric key algorithms and methods. Public key cryptography is the use of an asymmetric algorithm. Thus, the terms asymmetric cryptography and public key cryptography are interchangeable and mean the same thing. Examples of asymmetric algorithms are RSA, elliptic curve cryptosystem (ECC), Diffie-Hellman, and El Gamal.

- B** is incorrect because public key cryptography is the use of asymmetric algorithms, which are used to create public/private key pairs, perform key exchange or agreement, and generate and verify digital signatures. Public key infrastructure, on the other hand, is not an algorithm, a protocol, or an application—it is an infrastructure based on symmetric and asymmetric cryptography.
- C** is incorrect because a PKI does not provide authentication, nonrepudiation, confidentiality, and integrity directly—it can use algorithms that provide these security services. A PKI uses asymmetric, symmetric, and hashing algorithms. Symmetric algorithms provide confidentiality, asymmetric algorithms provide authentication and nonrepudiation, and hashing algorithms provide integrity.

46. Which of the following best describes Key Derivation Functions (KDFs)?

- A.** Keys are generated from a master key.
- B.** Session keys are generated from each other.
- C.** Asymmetric cryptography is used to encrypt symmetric keys.
- D.** A master key is generated from a session key.
- A.** For complex keys to be generated, commonly a master key is created and then symmetric keys (subkeys) are generated from it. Key Derivation Functions (KDFs) derive encryption keys from a secret value. The secret value can be a master key, passphrase, or password. KDFs are used to help ensure the randomness of the key values to make it harder for the attacker to uncover them. The KDF commonly uses a pseudorandom number generator with the secret value to make each encryption key unique.
- B** is incorrect because session keys are commonly generated from the master key—not from each other. For example, if an application is responsible for creating a session key for each subject that requests one, it should not be giving out the same instance of that one key. Different systems need to have different symmetric keys to ensure that the window for the bad guy to capture and uncover that

key is smaller than if the same key is used over and over again. When two or more keys are created from a master key, they are called subkeys.

- C** is incorrect because the encryption of keys has nothing to do with KDFs. Use of KDFs pertains to the procedures of creating unique and strong encryption keys. KDFs help to ensure that enough randomness is involved when generating new keys so that the attacker has a harder time uncovering them.
 - D** is incorrect because the statement is backward. A session key is commonly generated from a master key. When keys are generated from an original value, as in a master key, the resulting keys are referred to as subkeys or subsession keys.
- 47.** An elliptic curve cryptosystem is an asymmetric algorithm. What sets it apart from other asymmetric algorithms?
- A.** It provides digital signatures, secure key distribution, and encryption.
 - B.** It computes discrete logarithms in a finite field.
 - C.** It uses a larger percentage of resources to carry out encryption.
 - D.** It is more efficient.
- D.** Elliptic curves are rich mathematical structures that have shown usefulness in many different types of applications. An elliptic curve cryptosystem (ECC) differs from other asymmetric algorithms due to its efficiency. ECC is more efficient than any other asymmetric algorithm because of less intensive mathematics. In most cases, the longer the key, the more protection that is provided, but ECC can provide the same level of protection with a key size that is shorter than what RSA requires. Because longer keys require more resources to perform mathematical tasks, the smaller keys used in ECC require fewer resources of the device. And fewer resources make for a more efficient algorithm.
 - A** is incorrect because ECC is not the only asymmetric algorithm that provides digital signatures, secure key distribution, and encryption. These services are also provided by RSA and other asymmetric algorithms. Using its one-way function, ECC provides encryption and signature verification, and the inverse direction performs decryption and signature generation. It can also be used as a key exchange protocol, meaning it is used to encrypt the symmetric key to get it securely to its destination.

- B** is incorrect because Diffie-Hellman and El Gamal calculate discrete logarithms in a finite field. In the field of mathematics that deals with elliptic curves, points on the curves compose a structure called a group. These points are the values used in mathematical formulas for ECC's encryption and decryption processes. The algorithm computes discrete logarithms of elliptic curves, which is different from calculating discrete logarithms in a finite field.
 - C** is incorrect because ECCs use much fewer resources when compared to other asymmetric algorithms. Some devices, like wireless devices and cellular phones, have limited processing capacity, storage, power, and bandwidth. With these types of devices, efficiency of resource use is very important.
- 48.** If implemented properly, a one-time pad is a perfect encryption scheme. Which of the following incorrectly describes a requirement for implementation?
- A.** The pad must be securely distributed and protected at its destination.
 - B.** The pad must be made up of truly random values.
 - C.** The pad must always be the same length.
 - D.** The pad must be used only one time.
- C.** A one-time pad is a perfect encryption scheme because it is considered unbreakable if implemented properly. It was invented by Gilbert Vernam in 1917, so sometimes it is referred to as the Vernam cipher. The pad must be at least as long as the message. If it is not as long as the message, the pad will need to be reused to cover the whole message. This would be the same thing as using a pad more than one time, which could introduce patterns.
 - A** is incorrect because it is true that the pad must be securely distributed and protected at its destination. This is a very cumbersome process to accomplish, because the pads are usually just individual pieces of paper that need to be delivered by a secure courier and properly guarded at each destination. Historically, one-time pads have been used to protect different types of sensitive data. Today, they are still in place for many types of militaries as a backup encryption option if current encryption processes (that require computers and a power source) are unavailable for reasons of war or attacks.
 - B** is incorrect because it is true that the pad must be made up of truly

random values. This may not seem like a difficult task, but even our computer systems today do not have truly random number generators; rather, they have pseudorandom number generators. These generators are seeded by an initial value from some component within the computer system (time, CPU cycles, etc.). Although a computer system is complex, it is a predictable environment, so if the seeding value is predictable in any way, the resulting values created are not truly random—but pseudorandom.

- D** is incorrect because it is true that the pad must be used only one time. If the pad is used more than one time, this might introduce patterns in the encryption process that will aid an evildoer in his goal of breaking the encryption. Although the one-time pad approach to encryption can provide a very high degree of security, it is impractical in most situations because of all of its different requirements. Each possible pair of entities that might want to communicate in this fashion must receive, in a secure fashion, a pad. This type of key management can be overwhelming and may require more overhead than it is worth. The distribution of the pad can be challenging, and the sender and receiver must be perfectly synchronized so that each is using the same pad.
- 49.** Sally is responsible for key management within her organization. Which of the following incorrectly describes a principle of secure key management?
 - A. Keys should be backed up or escrowed in case of emergencies.
 - B. The more a key is used, the shorter its lifetime should be.
 - C. Less secure data allows for a shorter key lifetime.
 - D. Keys should be stored and transmitted by secure means.
- C.** Key management is critical for proper protection. Part of key management is determining the lifespan of keys. The key's lifetime should correspond with the sensitivity of the data it is protecting. Less secure data may allow for a longer key lifetime, whereas more sensitive data might require a shorter key lifetime. Keys should be properly destroyed when their lifetime comes to an end. The processes of changing and destroying keys should be automated and hidden from the user. They should be integrated into software or the operating system. It only adds complexity and opens the doors for more errors when processes are done manually and depend upon end users to perform certain functions.

- A** is incorrect because it is true that keys should be backed up or escrowed in case of emergencies. Keys are at risk of being lost, destroyed, or corrupted. Backup copies should be available and easily accessible when required. If data is encrypted and then the user accidentally loses the necessary key to decrypt it, this information would be lost forever if there were not a backup key. The application being used for cryptography may have key recovery options, or it may require copies of the keys to be kept in a secure place.
 - B** is incorrect because it is true that the more a key is used, the shorter its lifetime should be. The frequency of use of a cryptographic key has a direct correlation to how often the key should be changed. The more a key is used, the more likely it is to be captured and compromised. If a key is used infrequently, then this risk drops dramatically. The necessary level of security and the frequency of use can dictate the frequency of key updates. A mom-and-pop diner might only change its cryptography keys every month, whereas an information warfare military unit might change them every day or every week.
 - D** is incorrect because it is true that keys should be stored and transmitted by secure means. Keys are stored before and after distribution. When a key is distributed to a user, it needs a secure place within the file system to be stored and used in a controlled method. The key, the algorithm that will use the key, configurations, and parameters are stored in a module that also needs to be protected. If an attacker is able to obtain these components, she could masquerade as another user and decrypt, read, and re-encrypt messages not intended for her.
50. Mandy needs to calculate how many keys must be generated for the 260 employees using the company's PKI asymmetric algorithm. How many keys are required?
- A.** 33,670
 - B.** 520
 - C.** 67,340
 - D.** 260
- B.** With asymmetric algorithms, every user must have at least one pair of keys (private and public). In public key systems, each entity has different keys, or asymmetric keys. The two different

asymmetric keys are mathematically related. If a message is encrypted by one key, the other key is required in order to decrypt the message. The formula for determining the number of keys needed in this environment is $N \times 2$, which is the number of people (N) multiplied by the number of keys each person would need (2). In a public key system, the pair of keys is made up of one public key and one private key. The public key can be known to everyone, and the private key must be known and used only by the owner.

- ☒ **A** is incorrect because 33,670 is the number of keys needed in a symmetric key cryptosystem. Each pair of users who want to exchange data using symmetric key encryption must have two instances of the same key. This means that if Dan and Bob want to communicate, both need to obtain a copy of the same key. If Dan also wants to communicate using symmetric encryption with Norm and Dave, he needs to have three separate keys, one for each friend. This might not sound like a big deal until Dan realizes that he may communicate with hundreds of people over a period of several months, and keeping track and using the correct key that corresponds to each specific receiver can become a daunting task. If 10 people needed to communicate securely with each other using symmetric keys, then 45 keys would need to be kept track of. If 100 people were going to communicate, then 4,950 keys would be involved. The equation used to calculate the number of symmetric keys needed is $N(N - 1) / 2 = \text{number of keys}$.
- ☒ **C** is incorrect because 67,340 is the total derived from $N(N - 1)$, which is part of the formula used to determine the number of keys needed in a symmetric key cryptosystem. The complete formula is $N(N - 1) / 2$. The question, however, asked for the number of keys that would be used in a public key infrastructure's asymmetric algorithms. Asymmetric—not symmetric—keys are used in a public key cryptosystem. The formula for determining the number of asymmetric keys that are needed is $N \times 2$.
- ☒ **D** is incorrect because each user in a public key infrastructure requires at least one key pair—a public key and a private key. One key cannot encrypt and decrypt the same message. So each user requires at least two keys. Thus, the formula for determining the number of asymmetric keys that are needed is $N \times 2$.

51. Which of the following works similarly to stream ciphers?

- A.** One-time pad

B. AES

C. Block

D. RSA

- A.** Stream ciphers were developed to provide the same type of protection one-time pads do, which is why they work in such a similar manner. In practice, however, stream ciphers cannot provide the level of protection one-time pads do, but because stream ciphers are implemented through software and automated means, they are much more practical. A one-time pad is a perfect encryption scheme because it is considered unbreakable if implemented properly. This cipher uses a pad made up of random values. A plaintext message that needs to be encrypted is converted into bits, and a one-time pad is made up of random bits. This encryption process uses a binary mathematical function called exclusive-OR, usually abbreviated as XOR. XOR is an operation that is applied to two bits and is a function commonly used in binary mathematics and encryption methods. Stream ciphers also encrypt at the bit level, which is how they are similar to one-time pad encryption schemes.
- B** is incorrect because AES is a symmetric block cipher. When a block cipher is used for encryption and decryption purposes, the message is divided into blocks of bits. These blocks are then put through mathematical functions, one block at a time. Stream ciphers encrypt data one bit at a time, whereas a block cipher encrypts data one block of bits at a time. Suppose you need to encrypt a message you are sending to your friend and you are using a block cipher that uses a 64-bit block size. Your message of 640 bits is chopped up into ten individual blocks of 64 bits. Each block is put through a succession of mathematical formulas, and what you end up with is ten blocks of encrypted text. You send this encrypted message to your friend. He has to have the same block cipher and key, and those ten ciphertext blocks go back through the algorithm in the reverse sequence and end up in your plaintext message.
- C** is incorrect because, as stated in the preceding answer, when a block cipher is used for encryption and decryption purposes, the message is divided into blocks of bits. These blocks are then put through mathematical functions, one block at a time.
- D** is incorrect because RSA is a public key algorithm that is the most popular when it comes to asymmetric algorithms. Asymmetric algorithms use a different type of mathematics than symmetric

algorithms and are nothing similar to one-time pad encryption schemes. The security of this algorithm comes from the difficulty of factoring large numbers into their original prime numbers.

52. There are two main types of symmetric ciphers: stream and block. Which of the following is not an attribute of a good stream cipher?
- A. Statistically unbiased keystream
 - B. Statistically predictable
 - C. Long periods of no repeating patterns
 - D. Keystream not linearly related to key
- B.** The two main types of symmetric algorithms are block ciphers and stream ciphers. A block cipher performs mathematical functions on blocks of bits at a time. A stream cipher, on the other hand, does not divide a message into blocks. Instead, a stream cipher treats the message as a stream of bits and performs mathematical functions on each bit individually. Good stream ciphers offer the following: unpredictable statistical results, long periods of no repeating patterns, a statistically unbiased keystream, and a keystream that is not linearly related to the key. If a stream cipher is statistically predictable, then it will be possible for an attacker to uncover the key and break the cipher.
- A** is incorrect because a statistically unbiased keystream is an attribute of a good stream cipher. A statistically unbiased keystream means that there are as many zeros as there are ones. There should be no dominance in the number of zeros or ones in the keystream.
- C** is incorrect because long periods of no repeating patterns within keystream values is a characteristic of a good stream cipher. The ultimate goal of any encryption is to provide a high level of randomness so that an attacker cannot reverse-engineer and uncover the key that was used during the encryption process.
- D** is incorrect because a keystream not linearly related to a key is an attribute of a good stream cipher. This means that if someone figures out the keystream values, that does not mean he now knows the key value. This is important because the key provides the randomness of the encryption process. Most encryption algorithms are public, so people know how they work. The secret to the secret sauce is the key. The key provides randomness, so that the stream of bits that is XORed to the plaintext is as random as possible.

- 53.** Which of the following best describes how a digital signature is created?
- A. The sender encrypts a message digest with his private key.
 - B. The sender encrypts a message digest with his public key.
 - C. The receiver encrypts a message digest with his private key.
 - D. The receiver encrypts a message digest with his public key.
- A. A digital signature is a hash value that has been encrypted with the sender's private key. The act of digital signing means encrypting the message's hash value with a private key. If Sam wants to ensure that the message he sends to Debbie is not modified and he wants her to be sure it came only from him, he can digitally sign the message. This means that a one-way hashing function would be run on the message, and then Sam would encrypt that hash value with his private key. When Debbie receives the message, she will perform the hashing function on the message and come up with her own hash value. Then she will decrypt the sent hash value (digital signature) with Sam's public key. She then compares the two values, and if they are the same, she can be sure the message was not altered during transmission. She is also sure the message came from Sam because the value was encrypted with his private key.
- B is incorrect because if the sender encrypts the message digest with his public key, the recipient will not be able to decrypt it. The recipient would need access to the sender's private key, which should never happen. The private key should always be kept secret.
- C is incorrect because the receiver should decrypt the message digest with the sender's public key. The message digest is encrypted with the sender's private key, which can only be decrypted with the sender's public key.
- D is incorrect because the receiver should decrypt the message digest with the sender's public key. The message digest is encrypted with the sender's private key, which can only be decrypted with the sender's public key.
- 54.** In cryptography, different steps and algorithms provide different types of security services. Which of the following provides only authentication, nonrepudiation, and integrity?
- A. Encryption algorithm
 - B. Hash algorithm

C. Digital signature

D. Encryption paired with a digital signature

- C. A digital signature is a hash value that has been encrypted with the sender's private key. The act of signing means encrypting the message's hash value with a private key. A message can be digitally signed, which provides authentication, nonrepudiation, and integrity. The hashing function ensures the integrity of the message, and the signing of the hash value provides authentication and nonrepudiation.
- A is incorrect because encryption algorithms provide confidentiality. Encryption is most commonly carried out with the use of symmetric algorithms. Symmetric algorithms can only provide confidentiality and not authentication, nonrepudiation, and integrity.
- B is incorrect because hashing algorithms provide data integrity. Hashing algorithms generate message digests (also called hash values) to detect whether modification has taken place. The sender and receiver independently generate their own digests, and the receiver compares these values. If they differ, the receiver knows the message has been altered. A hashing algorithm cannot provide authentication or nonrepudiation.
- D is incorrect because encryption and a digital signature provide confidentiality, authentication, nonrepudiation, and integrity. The encryption alone provides confidentiality. And the digital signature provides authentication, nonrepudiation, and integrity. The question asks for which can only provide authentication, nonrepudiation, and integrity.

55. Advanced Encryption Standard is an algorithm used for which of the following?

- A. Data integrity
- B. Bulk data encryption
- C. Key recovery
- D. Distribution of symmetric keys

- B. The Advanced Encryption Standard (AES) is a data encryption standard that was developed to improve upon the previous de facto standard—the Data Encryption Standard (DES). As a symmetric algorithm, AES is used to encrypt bulk data. Symmetric algorithms of any kind are used to encrypt large amounts of data (bulk), while

asymmetric algorithms are used to encrypt a small amount of data as in keys and hashing values.

- A** is incorrect because AES is an encryption algorithm and therefore provides confidentiality, not data integrity. Hashing algorithms, such as SHA-1, MD2, MD4, MD5, and HAVAL, provide data integrity.
- C** is incorrect because AES is not used for key recovery. However, AES generates and makes use of keys, which require key recovery procedures. Keys are at risk of being lost, destroyed, or corrupted. Backup copies should be available and easily accessible when required. If data is encrypted and then the user accidentally loses the necessary key to decrypt it, this information would be lost forever if there were not a backup key to save the day. The application being used for cryptography may have key recovery options, or it may require copies of the keys to be kept in a secure place.
- D** is incorrect because asymmetric algorithms are used to protect symmetric keys while being distributed. AES is a symmetric algorithm. In a hybrid system, the symmetric algorithm creates a secret key that will be used to encrypt the bulk, or the message, and the asymmetric key encrypts the secret key for transmission.

56. SSL is a protocol used for securing transactions that occur over untrusted networks. Which of the following best describes what takes place during a SSL connection setup process?

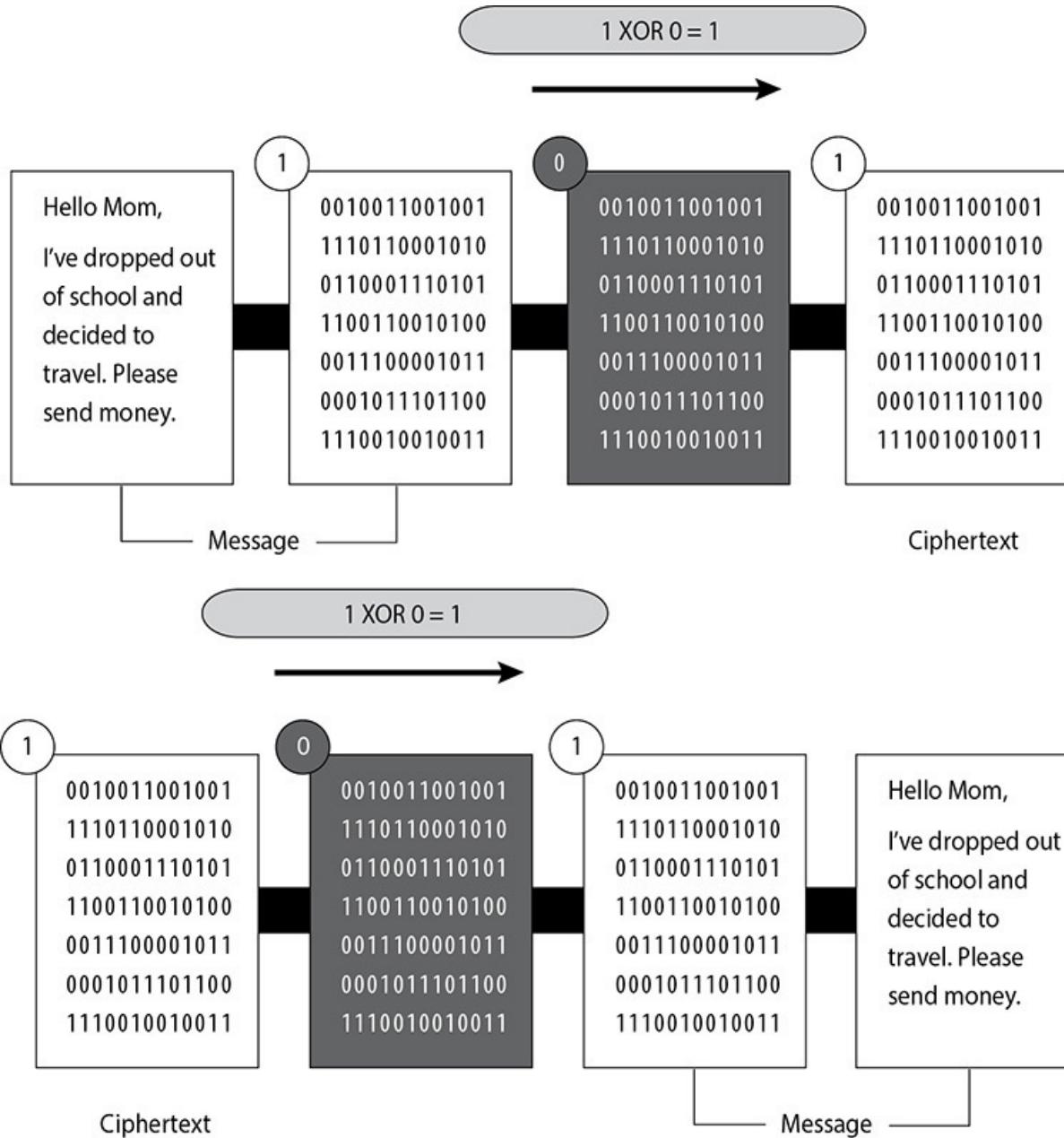
- A.** The server creates a session key and encrypts it with a public key.
 - B.** The server creates a session key and encrypts it with a private key.
 - C.** The client creates a session key and encrypts it with a private key.
 - D.** The client creates a session key and encrypts it with a public key.
- D.** Secure Sockets Layer (SSL) uses public key encryption and provides data encryption, server authentication, message integrity, and optional client authentication. When a client accesses a website, that website may have both secured and public portions. The secured portion would require the user to be authenticated in some fashion. When the client goes from a public page on the website to a secured page, the web server will start the necessary tasks to invoke SSL and protect this type of communication. The server sends a message back to the client, indicating a secure session should be established, and the client in response sends its security

parameters. The server compares those security parameters to its own until it finds a match. This is the handshaking phase. The server authenticates to the client by sending it a digital certificate, and if the client decides to trust the server, the process continues. The client generates a session key and encrypts it with the server's public key. This encrypted key is sent to the web server, and they both use this symmetric key to encrypt the data they send back and forth.

- A** is incorrect because the server does not create the session key; the client creates a session key and encrypts it with the server's public key. SSL is commonly used in web transactions and works in the following way: client creates session key, client encrypts session key with server's public key and sends it to the server, server receives session key and decrypts it with its private key.
 - B** is incorrect because the server does not create the session key, and it is not encrypted with the private key. The client creates a session key and encrypts it with the server's public key. The server receives the session key and decrypts it with its private key. The session key is then used to encrypt the data that is transmitted between the client and server.
 - C** is incorrect because the client uses the server's public key to encrypt the session key it generates. If the client encrypted the session key with the private key, then any entity that possessed the client's public key would be able to decrypt the session key. This does not provide any security. By encrypting the session key with the server's public key, only the server—which possesses the corresponding private key—can decrypt it.
57. The CA is responsible for revoking certificates when necessary. Which of the following correctly describes a CRL and OCSP?
- A. The CRL was developed as a more streamlined approach to OCSP.
 - B. OCSP is a protocol that submits revoked certificates to the CRL.
 - C. OCSP is a protocol developed specifically to check the CRL during a certificate validation process.
 - D. CRL carries out real-time validation of a certificate and reports to the OCSP.
 - C. The certificate authority (CA) is responsible for creating and handing out certificates, maintaining them, and revoking them if necessary. Revocation is handled by the CA, and the revoked

certificate information is stored on a certificate revocation list (CRL). This is a list of every certificate that has been revoked. This list is maintained and updated periodically. A certificate may be revoked because the key holder's private key was compromised or because the CA discovered the certificate was issued to the wrong person. If the certificate becomes invalid for some reason, the CRL is the mechanism for the CA to let others know this information. The Online Certificate Status Protocol (OCSP) is being used more and more rather than the cumbersome CRL approach. When using just a CRL, the user's browser must check a central CRL to find out if the certification has been revoked or the CA continually pushes out CRL values to the clients to ensure they have an updated CRL. If OCSP is implemented, it does this work automatically in the background. It carries out real-time validation of a certificate and reports back to the user whether the certificate is valid, invalid, or unknown.

- A** is incorrect because a CRL is actually a cumbersome approach to managing and validating revoked certificates. OCSP is increasingly being used to address this. OCSP does this work in the background, doing what the user's web browser would do when just using CRL. OCSP checks a central CRL to see if a certification has been revoked.
 - B** is incorrect because OCSP does not submit revoked certificates to the CRL. The CA is responsible for the creation, distribution, and maintenance of certificates. This includes revoking them when necessary and storing the information on a CRL.
 - D** is incorrect because OCSP, not the CRL, carries out real-time validation of a certificate. In addition, OCSP reports back to the user whether the certificate is valid, invalid, or unknown.
- 58.** There are several different types of technologies within cryptography that provide confidentiality. What is represented in the graphic that follows?

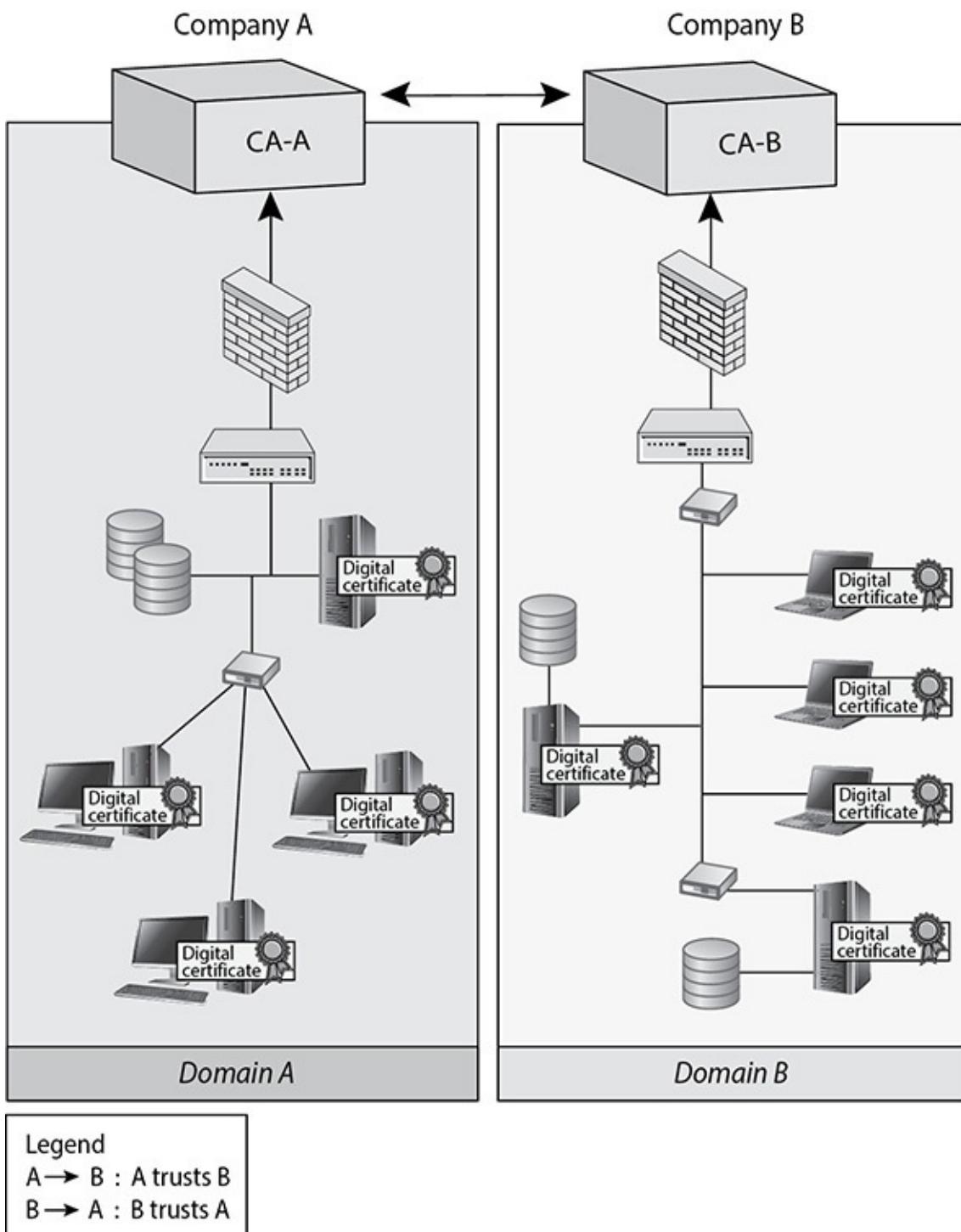


- A. Running key cipher
- B. Concealment cipher
- C. Steganography
- D. One-time pad
- D. A one-time pad is a perfect encryption scheme because it is considered unbreakable if implemented properly. A one-time pad uses a pad with random values that are XORed against the message to produce ciphertext. The plaintext message shown in the graphic that needs to be encrypted has been converted into bits, and our one-time pad is made up of random bits. This encryption process uses a binary mathematical function called exclusive-OR, usually

abbreviated as XOR. The receiver must have the same one-time pad to decrypt the message by reversing the process.

- ☒ **A** is incorrect because a running key cipher uses a key that does not require an electronic algorithm and bit alterations but cleverly uses components in the physical world around you. For instance, the algorithm could be a set of books agreed upon by the sender and receiver. The key in this type of cipher could be a book page, line number, and column count. If you get a message from your supersecret spy buddy and the message reads “149l6c7.299l3c7.911l5c8,” this could mean for you to look at the 1st book in your predetermined series of books, the 49th page, 6th line down the page, and the 7th column. So you write down the letter in that column, which is *h*. The second set of numbers starts with 2, so you go to the 2nd book, 99th page, 3rd line down, and then to the 7th column, which is *o*. The last letter you get from the 9th book, 11th page, 5th line, 8th column, which is *t*. So now you have come up with your important secret message, which is *hot*.
- ☒ **B** is incorrect because a concealment cipher is a message within a message. If your spy buddy and you decide your key value is every third word, then when you get a message from him, you will pick out every third word and write it down. Suppose he sends you a message that reads, “The saying, ‘The time is right’ is not cow language, so is now a dead subject.” Because your key is every third word, you come up with “The right cow is dead.”
- ☒ **C** is incorrect because steganography is a method of hiding data in another media type so that the very existence of the data is concealed. Only the sender and receiver are supposed to be able to see the message because it is secretly hidden in a graphic, WAV file, document, or other type of media. The message is not encrypted, just hidden. Encrypted messages can draw attention because it tells the bad guy, “This is something sensitive.” A message hidden in a picture would not attract this type of attention, even though the exact same secret message can be embedded into this image. Steganography is a type of security through obscurity.

- 59.** There are several different types of important architectures within public key infrastructures. Which architecture does the graphic that follows represent?



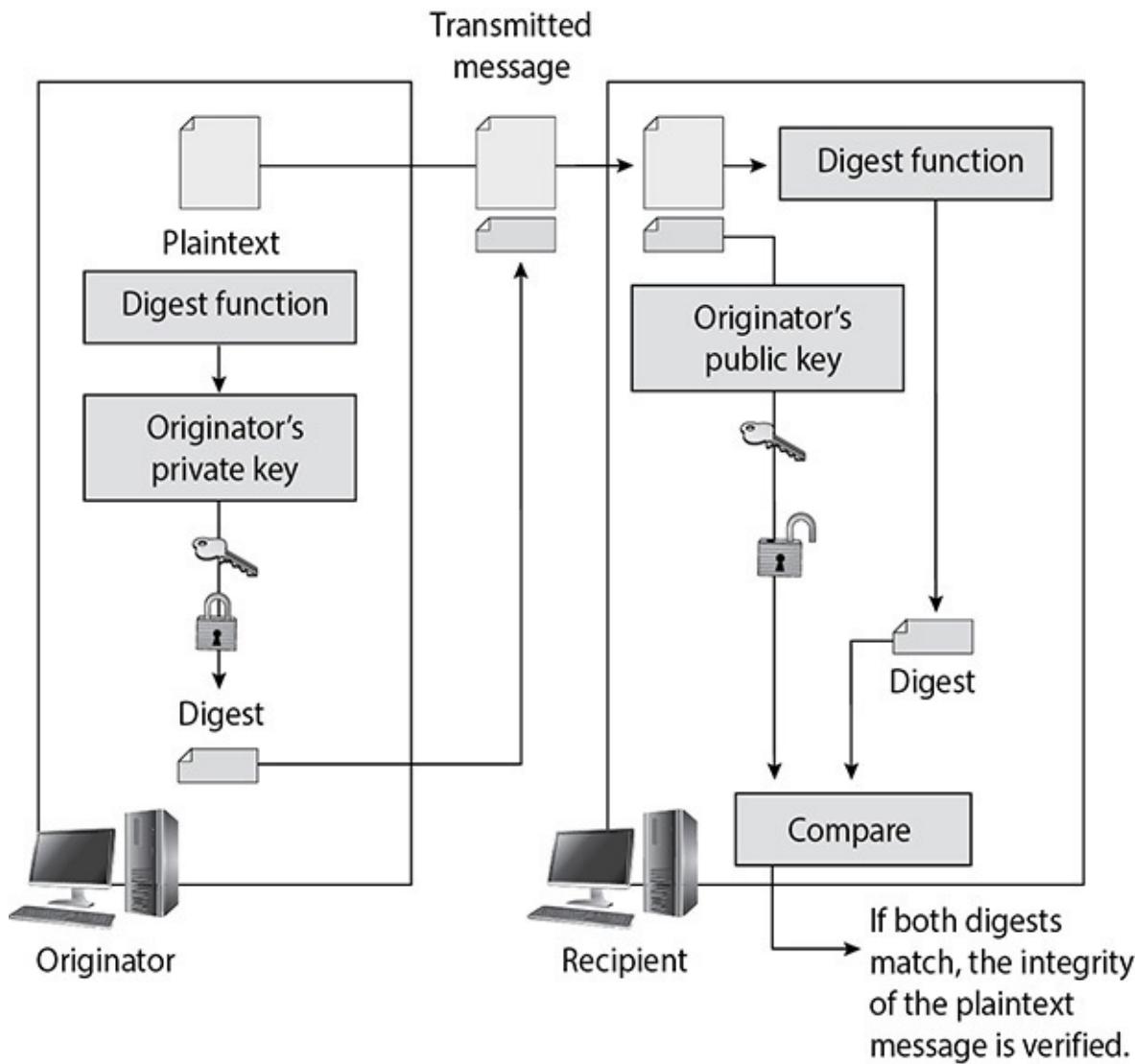
- A. Cross-certification**
- B. Cross-revocation list**
- C. Online Certificate Status Protocol**
- D. Registration authority**
- A. When independent PKIs need to interconnect to allow for secure communication to take place (either between departments or different companies), there must be a way for the two root CAs to**

trust each other. The two CAs do not have a CA above them they can both trust, so they must carry out cross-certification. A cross-certification is the process undertaken by CAs to establish a trust relationship in which they rely upon each other's digital certificates and public keys as if they had issued them themselves. When this is set up, a CA for one company can validate digital certificates from the other company and vice versa.

- B** is incorrect because a certificate revocation list (CRL) contains all of the revoked certifications within a PKI. The CA is responsible for creating and handing out certificates, maintaining them, and revoking them if necessary. Revocation is handled by the CA, and the revoked certificate information is stored on a CRL. This is a list of every certificate that has been revoked. This list is maintained and updated periodically. A certificate may be revoked because the key holder's private key was compromised or because the CA discovered the certificate was issued to the wrong person. An analogy for the use of a CRL is how a driver's license is used by a police officer. If an officer pulls over Sean for speeding, the officer will ask to see Sean's license. The officer will then run a check on the license to find out if Sean is wanted for any other infractions of the law and to verify the license has not expired. The same thing happens when a person compares a certificate to a CRL. If the certificate became invalid for some reason, the CRL is the mechanism for the CA to let others know this information.
- C** is incorrect because the Online Certificate Status Protocol (OCSP) carries out real-time validation of a certificate and reports back to the user whether the certificate is valid, invalid, or unknown. When using just a CRL, the user's browser must either check a central CRL to find out if the certification has been revoked or a CA must continually push out CRL values to the clients to ensure they have an updated CRL. If OCSP is implemented, it does this work automatically in the background. OCSP checks the CRL that is maintained by the CA. So the CRL is still being used, but now we have a protocol developed specifically to check the CRL during a certificate validation process.
- D** is incorrect because the registration authority (RA) performs the certification registration duties. The RA establishes and confirms the identity of an individual and initiates the certification process with a CA on behalf of an end user. The RA cannot issue certificates but can act as a broker between the user and the CA. When users

need new certificates, they make requests to the RA, and the RA verifies all necessary identification information before allowing a request to go to the CA.

60. There are different ways of providing integrity and authentication within cryptography. What type of technology is shown in the graphic that follows?



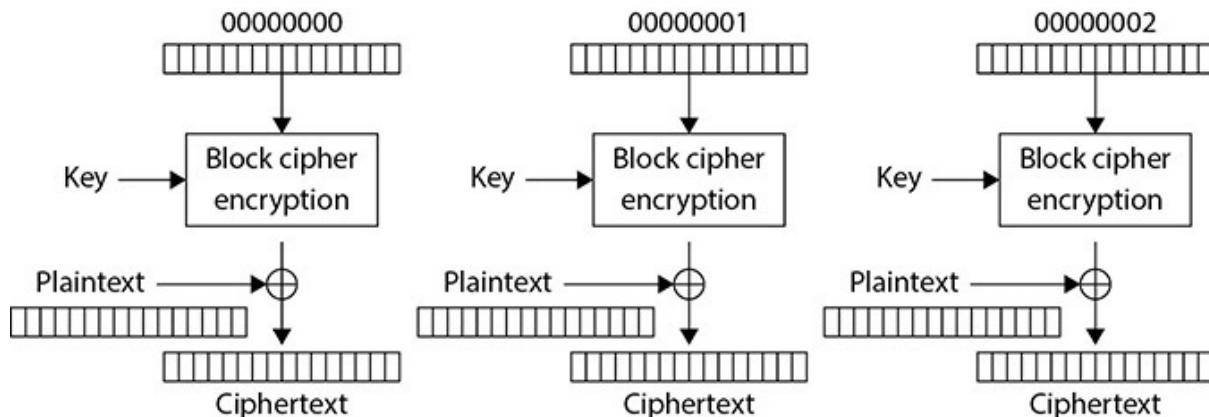
- A. One-way hash
 - B. Digital signature
 - C. Birthday attack
 - D. Collision
- B. When a hash algorithm is applied to a message, it produces a message digest, and this value is signed with a private key to produce a digital signature. It provides authentication, data integrity, and nonrepudiation. The act of signing is the actual encryption of

the value with the private key. When Maureen receives the message, she will perform the hashing function on the message and come up with her own hash value. Then she will decrypt the sent hash value (digital signature) with Kevin's public key. She then compares the two values, and if they are the same, she can be sure the message was not altered during transmission. She is also sure the message came from Kevin because the value was encrypted with his private key.

- ☒ **A** is incorrect because a one-way hash is a function that takes a variable-length string and a message and produces a fixed-length value called a hash value. For example, if Kevin wants to send a message to Maureen and he wants to ensure the message does not get altered in an unauthorized fashion while it is being transmitted, he would calculate a hash value for the message and append it to the message itself. When Maureen receives the message, she performs the same hashing function Kevin used and then compares her result with the hash value sent with the message. If the two values are the same, Maureen can be sure the message was not altered during transmission. If the two values are different, Maureen knows the message was altered, either intentionally or unintentionally, and she discards the message.
- ☒ **C** is incorrect because a birthday attack is an attack on hashing functions through brute force. The attacker tries to create two messages with the same hashing value. A good hashing algorithm should not produce the same hash value for two different messages. If the algorithm does produce the same value for two distinctly different messages, this is called a collision. An attacker can attempt to force a collision, which is referred to as a birthday attack. Hash algorithms usually use message digest sizes (the value of n) that are large enough to make collisions difficult to accomplish, but they are still possible. An algorithm that has 160-bit output, like SHA-1, may require approximately 2^{80} computations to break. This means there is a less than 1 in 2^{80} chance that someone could carry out a successful birthday attack. A hashing algorithm that has a larger bit output is less vulnerable to brute-force attacks such as a birthday attack.
- ☒ **D** is incorrect because a collision is when two hashed messages result in the same value. A strong one-hash function should not provide the same hash value for two or more different messages. If a hashing algorithm takes steps to ensure it does not create the same

hash value for two or more messages, it is said to be collision free. If a hashing algorithm generates a message digest of 60 bits, there is a high likelihood that an adversary can find a collision using only 2^{30} inputs.

- 61.** A widely used family of symmetric algorithms is called block ciphers. When these types of algorithms are being used, a message that needs to be encrypted is segmented into individual blocks and each block is encrypted. These algorithms work in different modes, and each mode has a specific use case. Which mode is being represented in the graphic and what is its most common use case?



- A. Electronic Code Book mode is used when individual and unique keys are needed to encrypt each block.
 - B. Counter mode is used when encryption and decryption need to take place in parallel and independent block recovery is available.
 - C. Cipher Block Chaining mode is used when added complexity is required by incorporating subkeys for each block encryption function.
 - D. Output Feedback mode is used when segmented ciphertext blocks are required for inline encryption functionality.
- B. Unlike most of the other block cipher modes, Counter (CTR) mode does not incorporate any chaining between blocks that are being encrypted. This means that the receiving end does not have to wait and receive all of the message blocks before starting to decrypt the message. The individual blocks are not coupled or dependent upon each other. Since the receiving end can decrypt the blocks as soon as they are received, the decryption process happens faster compared to other modes. Since the blocks are not chained and dependent upon each other, the individual message blocks can be independently recovered if necessary. Encryption modes that chain

the blocks together do not allow for independent recovery—if one block gets corrupted, subsequent blocks become irrecoverable. For these reasons, CTR is most commonly used in newer versions of protocols such as IPSec and in technologies such as Wi-Fi. CTR mode is used when data within multiple packets needs to be transmitted between two systems over a network connection; thus, it is used by networking protocols. Other block modes, such as Electronic Code Book, are most often used within applications, not protocols.

- ☒ **A** is incorrect because Electronic Code Book (ECB) is not being represented in the graphic and this mode is not used for the stated reason of requiring unique keys per block. ECB mode is commonly used when a small amount of data (e.g., PIN value) needs to be encrypted. CTR mode is used when larger amounts of data need to be encrypted (e.g., e-mail, document) and transmitted over a network. CTR uses incremental counters, as shown in the top of the graphic (00000000, 00000001, 00000002). These counter values are used in conjunction with a key to carry out encryption and decryption. ECB does not use any counter values because the amount of data that is being encrypted is smaller and not optimized for network-based transmission.
- ☒ **C** is incorrect because Cipher Block Chaining (CBC) mode is not being represented in the graphic and the stated use case for CBC is not correct. CBC mode is used when large amounts of data need to be encrypted. The chaining effect adds more randomness to the encryption process because each block is used to encrypt the next block. (One block of bits is used to scramble the next block of bits to make it harder to reverse engineer.) CTR does not incorporate this chaining property; instead, it uses sequence counter values (1, 2, 3, etc.). The sequence counter values do not provide as much randomness as the chaining function, but these are used when data needs to be decrypted quickly. So CBC mode is commonly used within applications that will reside on one system, and CTR mode is used by protocols that need to transmit encrypted data to different nodes on a network.
- ☒ **D** is incorrect because Output Feedback (OFB) mode is not being represented in the graphic and the stated use case for OFB is not correct. OFB mode is used when a block cipher needs to emulate a stream cipher. This means that an encryption algorithm (e.g., DES, AES) is being used to encrypt blocks of data one bit at a time

(stream) instead of one block at a time. OFB mode is used when the amount of data that needs to be encrypted is small (e.g., 8 bits) and the data needs to be transmitted (e.g., synchronous link). While all of these modes might sound confusing, each exists for a specific purpose. ECB mode is used to encrypt small data sets, such as a PIN value on the magnetic strip of your credit card. CBC mode is used when encrypting items such as Word documents on your laptop. CTR mode is used when a transmission protocol such as VPN needs to transmit encrypted data over a network. OFB mode is used when data sets such as keystrokes need to be encrypted and transmitted to a back-end system. When a programmer develops software that uses block algorithms, these modes are configurations for the algorithm and are passed into the block algorithm (e.g., AES) as parameters. This is how a developer “configures” an algorithm. For example, if a developer is using AES in a VPN, she would configure the algorithm to use CTR mode. If a developer is using AES to encrypt a PIN for a credit card, she would configure the algorithm to work in ECB mode.

62. If Marge uses her private key to create a digital signature on a message she is sending to George, but she does not show or share her private key with George, what is it an example of?
- A. Key clustering
 - B. Avoiding a birthday attack
 - C. Providing data confidentiality
 - D. Zero knowledge proof
- D.** Zero knowledge proof means that someone can tell you something without telling you more information than you need to know. In cryptography, it means proving that you have a specific key without sharing that key or showing it to anyone. A zero knowledge proof is an interactive method for one party to prove to another that a (usually mathematical) statement is true without revealing anything sensitive.
- A** is incorrect because key clustering is an instance when two different keys generate the same ciphertext from the same plaintext. This is caused by a logical flaw in an algorithm.
- B** is incorrect because if the algorithm does produce the same value for two distinctly different messages, this is called a collision. An attacker can attempt to force a collision, which is referred to as a

birthday attack. This attack is based on the mathematical birthday paradox that exists in standard statistics. It is a cryptographic attack that exploits the mathematics behind the birthday problem in the probability theory. This is not what is being addressed in the question.

- C** is incorrect because confidentiality provided through cryptography is usually in place when data is encrypted with a key. If the data is considered bulk data, then a symmetric key is used. Not showing others a private key keeps the private key secret, but this is not necessarily confidentiality.
- 63.** There are two main functions that Trusted Platform Modules (TPMs) carry out within systems today. Which of the following best describes these two functions?
 - A.** Sealing a hard disk drive is when the decryption key that can be used to decrypt data on the drive is stored on the TPM. Binding is when data pertaining to the system's state is hashed and stored on the TPM.
 - B.** Binding a hard disk drive is when whole-disk encryption is enabled through the use of the TPM. Sealing is when a digital certificate is sealed within a TPM and the system cannot boot up without this certificate being validated.
 - C.** Sealing a hard disk drive is when whole-disk encryption is enabled through the use of the TPM. Binding is when a digital certificate is sealed within a TPM and the system cannot boot up without this certificate being validated.
 - D.** Binding a hard disk drive is when the decryption key that can be used to decrypt data on the drive is stored on the TPM. Sealing is when data pertaining to the system's state is hashed and stored on the TPM.
- D.** The essence of the TPM lies in a protected and encapsulated microcontroller security chip that provides a safe haven for storing and processing security-intensive data such as keys, passwords, and digital certificates. “Binding” a hard disk drive is the most common usage scenario of the TPM—where the content of a given hard disk drive is affixed with a particular computing system. Another application of the TPM is “sealing” a system’s state to a particular hardware and software configuration.
- A** is incorrect because binding a hard disk drive is when the

decryption key that can be used to decrypt data on the drive is stored on the TPM. Sealing is when data pertaining to the system's state is hashed and stored on the TPM.

- ☒ **B** is incorrect because binding a hard disk drive is when the decryption key that can be used to decrypt data on the drive is stored on the TPM. Sealing is when data pertaining to the system's state is hashed and stored on the TPM. The content of the hard disk drive is encrypted, and the decryption key is stored away in the TPM chip. To ensure safe storage of the decryption key, it is further "wrapped" with another encryption key. Binding a hard disk drive makes its content basically inaccessible to other systems, and any attempt to retrieve the drive's content by attaching it to another system will be very difficult.
- ☒ **C** is incorrect because sealing a system is fairly straightforward. The TPM generates hash values based on the system's configuration files and is stored. A sealed system will only be activated once the TPM verifies the integrity of the system's configuration by comparing it with the original "sealing" value.

The following scenario applies to questions 64 and 65.

Jack has been told that successful attacks have been taking place and data that has been encrypted by his company's software systems has leaked to the company's competitors. Through Jack's investigation he has discovered that the lack of randomness in the seeding values used by the encryption algorithms in the company's software exposed patterns and allowed for successful reverse engineering.

- 64.** Which of the following is most likely the item that is the root of the problem when it comes to the necessary randomness explained in the scenario?
- A.** Asymmetric algorithm
 - B.** Out-of-band communication compromise
 - C.** Number generator
 - D.** Symmetric algorithm
- C.** A number generator is used to create a stream of random values and must be seeded by an initial value. This piece of software obtains its seeding value from some component within the computer system (time, CPU cycles, etc.). Although a computer system is complex, it is a predictable environment, so if the seeding value is predictable in any way, the resulting values created are not truly random, but pseudorandom. If the values from a number generator illustrate patterns and those patterns are recognizable during cryptographic processes, this weakness could allow an attacker to reverse-engineer the algorithm and gain access to confidential data.
- A** is incorrect because an asymmetric algorithm carries out cryptographic functions through the use of two different key types, public and private. This is also called public key cryptography. Components, as in number generators, can be used with asymmetric algorithms, but they are a class of algorithms and do not necessarily integrate randomness issues.
- B** is incorrect because out-of-band communication just means that communication data is being sent through a channel that is different from the encrypted data that is traveling. It does not have any direct correlation with randomness issues.
- D** is incorrect because a symmetric algorithm carries out cryptographic functions through the use of two instances of the same key. Components, as in number generators, can be used with

symmetric algorithms, but they are a class of algorithms and do not necessarily cause randomness issues.

- 65.** Which of the following best describes the role of the values that is allowing for patterns as described in the scenario?
- A.** Initialization vector
 - B.** One-time password
 - C.** Master symmetric key
 - D.** Subkey
- A.** Initialization vectors (IVs) are random values that are used with algorithms to ensure patterns are not created during the encryption process. They are used with keys and do not need to be encrypted when being sent to the destination. If IVs are not used, then two identical plaintext values that are encrypted with the same key will create the same ciphertext. Providing attackers with these types of patterns can make their job easier in breaking the encryption method and uncovering the key.
- B** is incorrect because a one-time pad is an encryption method created by Gilbert Vernam that is considered impossible to crack if carried out properly. A one-time pad uses a pad with random values that are XORed against the message to produce ciphertext. The pad is at least as long as the message itself and is used once and then discarded. This technology is not addressed in this scenario.
- C** is incorrect because for complex keys to be generated, commonly a master key is created, and then symmetric keys are generated from it. For example, if an application is responsible for creating a session key for each subject that requests one, it should not be giving out the same instance of that one key. Different subjects need to have different symmetric keys to ensure that the window for the attack to capture and uncover that key is smaller than if the same key were to be used over and over again. When two or more keys are created from a master key, they are called subkeys. This is not a component of the randomness issue addressed in the scenario.
- D** is incorrect because when two or more keys are created from a master key, they are called subkeys. This is not a component of the randomness issue addressed in the scenario.
- 66.** Sometimes when studying for an industry certification exam like the CISSP, people do not fully appreciate that the concepts and

technologies that they need to learn to pass the test directly relate to real-world security issues. To enforce how exam-oriented theoretical concepts directly relate to the practical world of security, choose the correct answer that best describes the Heartbleed SSL/TLS vulnerability, which is considered to be one of the most critical attack vectors in the history of the Internet.

- A. Digital certificates were stolen through a tunneled attack within the SSL and TLS protocols.
 - B. Certificate authorities were compromised when their SSL and TLS connections were hijacked through the use of TCP hijacking sessions.
 - C. Bounds checking was not implemented, allowing sensitive data to be obtained by attackers from memory segments on web servers.
 - D. Cross-site scripting was allowed to take place on web servers that ran a vulnerable version of Java.
- C. OpenSSL implemented an SSL/TLS extension outlined by the IETF in RFP 6520 that allows a connection to remain active between two systems communicating over this security protocol. The way that OpenSSL implemented this extension allows the sending system to request data that it is not authorized to access—such as web server private keys. When an attacker obtains a web server's private key, this circumvents all of the security provided by a public key infrastructure (PKI) environment that the SSL/TLS protocol is based upon. The point is that if you do not really understand how a PKI works and how private and public keys work, the role of digital certificates in security protocols—such as SSL/TLS, bounds checking, and buffer over-reads—you won't understand straightforward vulnerabilities such as Heartbleed. While you will not be asked about a specific vulnerability on the CISSP exam, you will be expected to understand all of the components and technologies involved that allow for this vulnerability to be so dangerous and powerful.
- A is incorrect because this vulnerability did not involve the stealing of digital certificates and there is actually no security issue involved with digital certificates being "stolen." Digital certificates commonly reside in open and accessible directories and are shared between entities that participate in a PKI, so there is no threat of them being stolen. Digital certificates are created by certificate authorities, which generate a hash and a digital signature on each

individual digital certificate. This digital signature protects the integrity of the certificate and allows a receiver to detect if a certificate has been modified. It is the fact that each digital certificate is protected with a digital signature created by the originating certificate authority that allows us to store these certificates in locations that do not require controls against theft.

- B** is incorrect because this vulnerability does not have anything to do with a certificate authority being compromised, and TCP hijacking is not a successful way of compromising any SSL/TLS connection. TCP hijacking is an attack that takes advantage of the fact that TCP packet sequence numbers can be predicted, which allows an attacker to insert himself within an active TCP session and take over the connection and use it for his nefarious purposes. SSL/TLS works at a higher level of the network stack compared to TCP, and the hijacking of a TCP session does not equate to compromising a secure connection using this security protocol. It is important to understand not only how attacks such as TCP hijacking take place, but also what attack types can and cannot accomplish.
- D** is incorrect because the Heartbleed vulnerability does not have anything to do with cross-site scripting or Java. Rather, it is a vulnerability within the implementation of the SSL/TLS protocol. Cross-site scripting (XSS) is a vulnerability within a web application that allows an attacker to compromise the web application and then have the capability of injecting malicious client-side scripts into web pages viewed by potential victims. XSS relates to a vulnerability within a web app running on a web server, not the SSL/TLS protocol. As a security professional, it is important to understand where specific vulnerabilities reside and what they are able to accomplish. An XSS vulnerability cannot lead to a compromise that a Heartbleed attack can accomplish, and the Heartbleed vulnerability cannot accomplish the same outcome as a compromised XSS vulnerability.

67. What type of exploited vulnerability allows more input than the program has allocated space to store it?

- A.** Symbolic links
- B.** File descriptors
- C.** Kernel flaws
- D.** Buffer overflows

- D.** Poor programming practices allow more input than the software has allocated space to store it. This overwrites data or program memory after the end of the allocated buffer, and sometimes it allows the attacker to inject program code and then cause the processor to execute it in what is called a buffer overflow. This gives the attacker the same level of access as that held by the software that was successfully attacked. If the program was run as an administrative user or by the system itself, this can mean complete access to the system. Good programming practice, automated source code scanners, enhanced programming libraries, and strongly typed languages that disallow buffer overflows are all ways of reducing this type of vulnerability.
- A** is incorrect because a symbolic link is a stub file that redirects access to system files or data to another place. If an attacker can compromise the symbolic link, then the attacker may be able to gain unauthorized access. (Symbolic links are used in Unix- and Linux-type systems.) This may allow the attacker to damage important data and/or gain privileged access to the system. A historical example of this was to use a symbolic link to cause a program to delete a password database, or replace a line in the password database with characters that, in essence, created an password-less root-equivalent account. Programs, and especially scripts, must be written to assure that the full path to the file cannot be circumvented.
- B** is incorrect because file descriptors are exploited if a program makes unsafe use of a file descriptor and an attacker is able to cause unexpected input to be provided to the program, or cause output to go to an unexpected place with the privileges of the executing program. File descriptors are numbers many operating systems use to represent open files in a process. Certain file descriptor numbers are universal, meaning the same thing to all programs. Good programming practices, automated source code scanners, and application security testing are all ways of reducing file descriptor attacks.
- C** is incorrect because kernel flaws are problems that occur below the level of the user interface, deep inside the operating system. Flaws in the kernel that can be reached by an attacker, if exploitable, give the attacker the most powerful level of control over the system. It is important to ensure that security patches to operating systems—after sufficient testing—are promptly deployed

in the environment to keep the window of vulnerability as small as possible.

68. There are common cloud computing service models.

_____ usually requires companies to deploy their own operating systems, applications, and software onto the provided infrastructure. _____ is the software environment that runs on top of the infrastructure. In the _____ model the provider commonly gives the customers network-based access to a single copy of an application.

- A. Platform as a Service, Infrastructure as a Service, Software as a Service
 - B. Platform as a Service, Platform as Software, Application as a Service
 - C. Infrastructure as a Service, Application as a Service, Software as a Service
 - D. Infrastructure as a Service, Platform as a Service, Software as a Service
- D. The most common cloud service models are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).
- A is incorrect because these items are not in the correct order.
Infrastructure as a Service (IaaS) is when cloud providers offer the infrastructure environment of a traditional data center in an on-demand delivery method. Companies deploy their own operating systems, applications, and software onto this provided infrastructure and are responsible for maintaining them.
- B is incorrect because the most common cloud service models are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). There are no models called Platform as Software or Application as a Service. These are distracters.
Platform as a Service (PaaS) is when cloud providers deliver a computing platform, which can include an operating system, database, and web server as a holistic execution environment. Where IaaS is the “raw IT network,” PaaS is the software environment that runs on top of the IT network.
- C is incorrect because the most common cloud service models are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). There is no model called Application

as a Service. With Software as a Service (SaaS), the provider gives users access to specific application software (CRM, e-mail, games). The provider gives the customers network-based access to a single copy of an application created specifically for SaaS distribution and use.

- 69.** A company has decided that it no longer wants to maintain its own servers and network environment because of increasing costs and liabilities. The company wants to move to a cloud-based solution, but needs to determine which type of solution best fits its needs. Which of the following provides a correct definition and mapping of a typical cloud-based solution?
- A. Infrastructure as a Service is provided when a cloud provider delivers a computing platform that includes operating system, database, and web servers.
 - B. Software as a Service is provided when a cloud provider delivers an infrastructure environment similar to a traditional data center.
 - C. Platform as a Service is provided when a cloud provider delivers a computing platform that can include operating system, database, and web servers.
 - D. Software as a Service is provided when a cloud provider delivers a software environment in the form of a computing platform.
- C. Cloud computing is a general term that describes how network and server technology can be aggregated and virtualized and then partitioned to provide individual customers specific computing environments. This centralized aggregation and centralized control provides end users with on-demand self-service, broad access across multiple devices, resource pooling, rapid elasticity, and service metering capability. There are different types of cloud computing offerings. Platform as a Service (PaaS) is in place when a cloud provider delivers a computing platform, such as an operating system, database, and web server, as a holistic execution environment. Where Infrastructure as a Service (IaaS) is the “raw IT network,” PaaS is the software environment that runs on top of the IT network.
- A is incorrect because Infrastructure as a Service (IaaS) is in place when a cloud provider offers the infrastructure environment of a traditional data center in an on-demand delivery method. Companies deploy their own operating systems, applications, and software onto this provided infrastructure and are responsible for

maintaining them. IaaS cloud solutions often include additional resources, such as storage, firewalls, VLANs, load balancing, and other traditional network functionality.

- B** is incorrect because Software as a Service (SaaS) is in place when a cloud provider gives users access to specific application software (CRM, e-mail, games). The provider gives the customers network-based access to a specified number of copies of an application created specifically for SaaS distribution and use. In this type of offering, the cloud provider manages the infrastructure and platforms that the applications run within. Access to applications is commonly sold in an on-demand and subscription fee model. Cloud providers install and maintain the application, and end users access the software remotely from cloud clients. Cloud end users do not manage the cloud infrastructure and platform where the application runs.
 - D** is incorrect because Software as a Service (SaaS) is in place when a cloud provider gives users access to specific application software (CRM, e-mail, games) as described earlier. Software applications that are offered through a cloud provider are commonly virtualized to allow them to be scalable to meet high demands and run times. If the company in the question has business requirements for commonly used applications, then SaaS might be the best solution. In this type of situation, each employee would be provided credentials to interact with an instance of the needed application, and the cloud provider would carry out all of the “behind the scenes” maintenance and operation responsibilities.
- 70.** Sally is carrying out a software analysis on her company’s proprietary application. She has found out that it is possible for an attacker to force an authorization step to take place before the authentication step is completed successfully. What type of issue would allow for this type of compromise to take place?
- A.** Back door
 - B.** Maintenance hook
 - C.** Race condition
 - D.** Data validation error
- C.** A race condition is when processes carry out their tasks on a shared resource and there is a potential that the sequence is carried out in the wrong order. A race condition is possible when two or

more processes use a shared resource, as in data within a variable. It is important that the processes carry out their functionality in the correct sequence. If process 2 carried out its task on the data before process 1, the result will be much different than if process 1 carried out its tasks on the data before process 2. If authentication and authorization steps are split into two functions, there is a possibility an attacker could use a race condition to force the authorization step to be completed before the authentication step.

- A** is incorrect because a back door is a service that is available and “listening” on a specific port. Back doors are implemented by attackers so that they can gain easy access to compromised systems without having to authenticate as a regular system user.
- B** is incorrect because a maintenance hook is specific software code that allows easy and unauthorized access to sensitive components of a software product. Software programmers commonly use maintenance hooks to allow them to get quick access to a product’s code so that fixes can be carried out, but this is dangerous. If an attacker uncovered this type of access, compromises could take place that would most likely not require authentication and would probably not be logged.
- D** is incorrect because data validation errors do not commonly allow an attacker to manipulate process execution sequences. An attacker would enter invalid data through a specific interface, with the goals of having their code execute on the victim machine or carry out a buffer overflow.

71. Which of the following is true about information flow models?

- A.** The simple security rule of Bell-LaPadula dictates that a subject may not read data from a higher security level, in order to implement data integrity.
 - B.** The *-integrity rule of Biba dictates that a subject may not write data to an object at a higher integrity level, in order to implement confidentiality.
 - C.** The simple integrity rule of Biba dictates that a subject cannot write data to a lower integrity level, in order to implement integrity.
 - D.** The *-property rule of Bell-LaPadula dictates that a subject cannot write data to a lower security level, in order to implement confidentiality.
- D.** The Bell-LaPadula model is concerned with confidentiality, and

the *-property rule dictates “no write down” in order to avoid declassifying data.

- A** is incorrect because, although the simple security rule of Bell-LaPadula does state that data may not be read from a higher level (“no read up”), the model is designed to implement data confidentiality, not data integrity.
- B** is incorrect because, although the *-integrity rule of Biba does state that data may not be written to a security layer above the current one (“no write up”), the model is designed to implement data integrity, not confidentiality.
- C** is incorrect because the simple integrity rule of Biba states that data cannot be *read from* (not *written to*) a lower integrity level (“no read down”).

72. Which of the following is true with respect to distributed systems?

- A.** A client/server system is a special case of a distributed system with only two tiers.
 - B.** Distributed systems are easier to secure than non-distributed systems, because there are more components that can contribute to the security solution.
 - C.** A client/server system is distinct from distributed systems, because there are only two tiers.
 - D.** Distributed systems reduce the complexity of security solutions.
- A.** A distributed system is any system with multiple computing nodes, and this includes simple two-node client/server systems.
 - B** is incorrect because the reverse is true. Distributed systems are far harder to secure, because failures can occur within any of the many components.
 - C** is incorrect because simple client/server systems are merely two-node distributed systems.
 - D** is incorrect because the reverse is true. Distributed systems invariably increase the complexity of security solutions, though often necessarily. In any case, complexity is anathema to security.

73. What is the difference between generating a message authentication code (MAC) and generating a hash MAC (HMAC)?

- A.** There is no difference; they are the same thing.

- B. They are two different hashing algorithms that are used the same way but produce different message digests (MDs).
- C. MACs are a result of hashing a message, whereas HMACs are a result of hashing both the message and a public key.
- D. MACs are a result of hashing a message, whereas HMACs are a result of hashing both the message and a shared secret key.
- D. By hashing the message concatenated with a shared secret (symmetric) key, the resulting HMAC can be used to validate not only the integrity of the message, but also that the source possessed the proper key. A MAC can be used to validate the integrity of the message alone.
- A is incorrect because they are different, as described in the previous explanation.
- B is incorrect because hashing is used differently between the two. MAC hashes only the message. HMAC hashes the message and a symmetric key.
- C is incorrect because the key used in HMAC is not a public (asymmetric) key, but rather a shared secret (symmetric) key.
74. Why is it important to understand the life cycle of cryptography and your cryptographic needs?
- A. Major new forms of cryptography are constantly being invented, which may replace your use of hashing, symmetric, or asymmetric encryption methods.
- B. The available key space for any given algorithm (or your choice of keys within it) will inevitably “go stale” over time.
- C. Symmetric systems like AES are continuously being upgraded to include more rounds of transforms, so it is important to be using the latest version.
- D. Revolutionary advances in blockchains will replace old cryptography techniques.
- B. The historically consistent rate of advance in commercial, off-the-shelf computational power has meant that the work factor of all of our cryptographic key spaces has declined over time. This should be assumed to continue: systems that cannot be easily brute forced today may be easily brute forced tomorrow.
- A is incorrect because advances in cryptography are infrequent and

tend to be incremental. For something to come along that truly replaces hashing, symmetric, or asymmetric algorithms would be revolutionary, and not part of the usual life cycle.

- C** is incorrect because the AES algorithm is not subject to version upgrades based on the number of rounds of transforms.
- D** is incorrect because blockchains are neither a revolutionary advance in cryptography nor are they likely to supplant other more mature uses of it.

75. Which of the following are services that cryptosystems can provide?

- A.** Confidentiality, integrity, and availability
 - B.** Computation, authentication, and authorization
 - C.** Integrity, authentication, and accounting
 - D.** Confidentiality, integrity, and authentication
- D.** Cryptosystems can render data unintelligible except to authorized entities (confidentiality), can validate that data has not been altered (integrity), and can validate the identity of an entity (authentication).
 - A** is incorrect because, although confidentiality and integrity are services provided by cryptosystems, they do not address assured availability—quite the opposite. Cryptography is a common component in ransomware, which attacks data availability.
 - B** is incorrect because “computation” is meaningless in this context. Cryptosystems rely on computation, as all systems do, but they do not provide it.
 - C** is incorrect because accounting is not a service within the realm of cryptosystems. Accounting entails keeping records of accesses for historical auditing, and while cryptosystems can be used to protect the confidentiality and integrity of such records, this is not a unique use.

76. Which of the following statements is true with respect to the physical security of distribution and storage facilities?

- A.** Smaller intermediate distribution facilities (IDFs) and storage facilities tend not to contain data as critical as the data in main distribution facilities (MDFs) and data centers, so they require less physical protection.
- B.** Although smaller IDFs and storage facilities contain data as critical

as the data in MDFs and data centers, they are commonly less well protected physically.

- C. All distribution and storage facilities are typically afforded the same level of physical protection in practice.
 - D. Distribution and storage facilities don't require the same level of physical access controls as the production data centers.
- B.** Smaller IDFs and storage facilities contain data as critical as the data in MDFs and data centers but are commonly less well protected physically. For example, an IDF may be not much more than a switch on a shelf in a janitor's closet that is commonly left unlocked. Likewise, storage facilities for archived data are unlikely to have the same physical access controls as a data center.
- A** is incorrect because the data that flows through IDFs and is archived in offsite storage facilities is likely the same data flowing through the MDFs and resident in the production data center, and thus IDFs and storage facilities require the same level of physical protection.
- C** is incorrect because distribution and storage facilities are not typically afforded the same level of physical protection, as described in the explanation of the correct answer.
- D** is incorrect because storage facilities require the same level of physical access controls as the production data centers, as described in the explanation of answer A.

Communication and Network Security

This domain includes questions from the following topics:

- OSI and TCP/IP models
 - Protocol types and security issues
 - LAN, WAN, MAN, intranet, and extranet technologies
 - Transmission media
 - Wireless technologies
 - Network devices and services
 - Communications security management
 - Remote access technologies
 - Threats and attacks
 - Software-defined networks
 - Content distribution networks
 - Multilayer protocols
 - Convergent network technologies
-

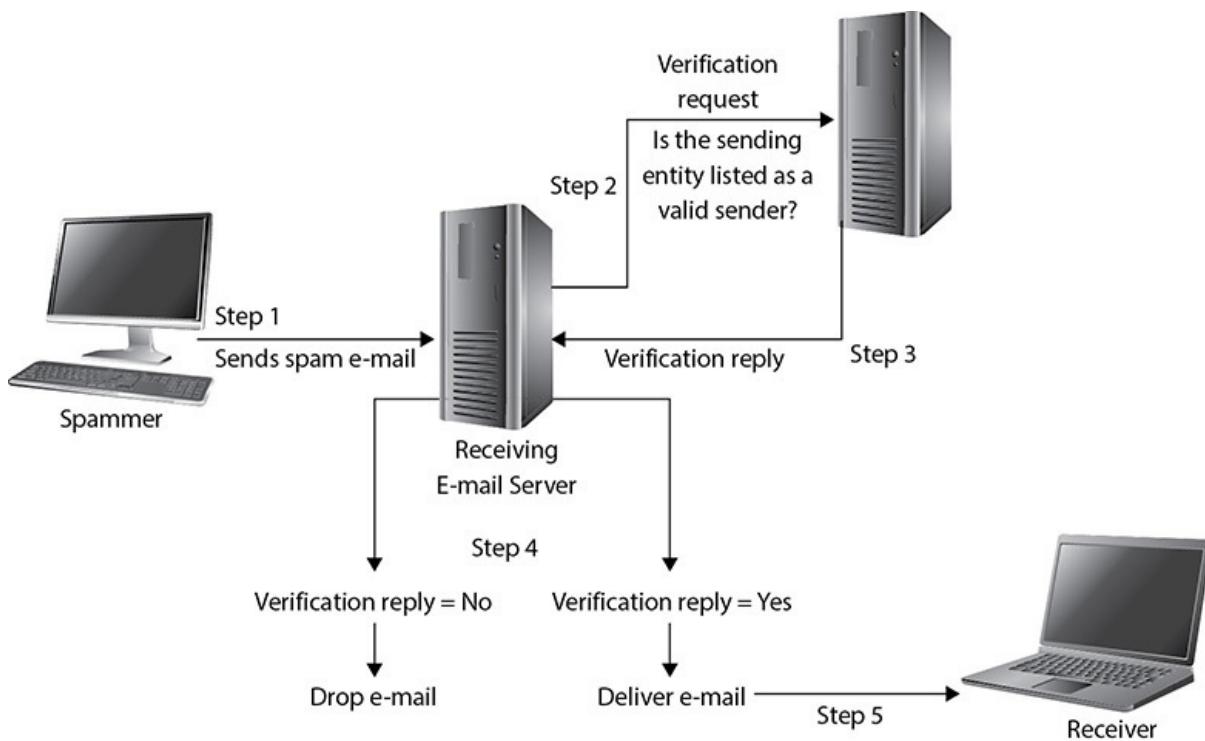
A network forms the backbone of an organization's IT infrastructure. Without it, systems couldn't communicate and users couldn't share resources in real time. Because of the myriad protocols, technologies, and concepts involved in networking, it is one of the more complex topics you need to understand for the CISSP exam and in your role as a security professional. The many different types of devices, protocols, and security mechanisms within an environment provide different functionality. You must understand how the technologies work, how they interact with each other, how they're configured,



QUESTIONS

1. Layer 2 of the OSI model has two sublayers. What are those sublayers, and what are two IEEE standards that describe technologies at that layer?

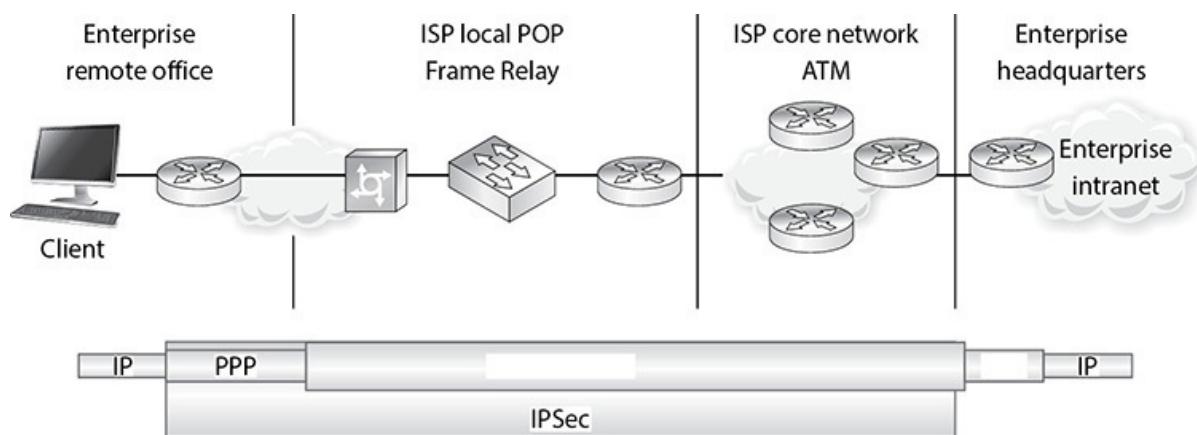
- A.** LCL and MAC; IEEE 802.2 and 802.3
 - B.** LCL and MAC; IEEE 802.1 and 802.3
 - C.** Network and MAC; IEEE 802.1 and 802.3
 - D.** LLC and MAC; IEEE 802.2 and 802.3
- 2.** Which of the following is not an effective countermeasure against spam?
- A.** Open mail relay servers
 - B.** Properly configured mail relay servers
 - C.** Filtering on an e-mail gateway
 - D.** Filtering on the client
- 3.** Robert is responsible for implementing a common architecture used when customers need to access confidential information through Internet connections. Which of the following best describes this type of architecture?
- A.** Two-tiered model
 - B.** Screened subnet
 - C.** Three-tiered model
 - D.** Public and private DNS zones
- 4.** Since sending spam (unwanted messages) has increased over the years and e-mail has become a common way of sending out malicious links and malware, the industry has developed different ways to combat these issues. One approach is to use a Sender Policy Framework, which is an e-mail validation system. In the following graphic, what type of system receives the request in step 2 and replies in step 3?



- A. DNS server
- B. E-mail server
- C. RADIUS server
- D. Authentication server
5. Which of the following indicates to a packet where to go and how to communicate with the right service or protocol on the destination computer?
- A. Socket
- B. IP address
- C. Port
- D. Frame
6. Several different tunneling protocols can be used in dial-up situations. Which of the following would be best to use as a VPN tunneling solution?
- A. L2P
- B. PPTP
- C. IPSec
- D. L2TP
7. Which of the following correctly describes Bluejacking?

- A. Bluejacking is a harmful, malicious attack.
 - B. It is the process of taking over another portable device via a Bluetooth-enabled device.
 - C. It is commonly used to send contact information.
 - D. The term was coined by the use of a Bluetooth device and the act of hijacking another device.
- 8. DNS is a popular target for attackers due to its strategic role on the Internet. What type of attack uses recursive queries to poison the cache of a DNS server?
 - A. DNS hijacking
 - B. Manipulation of the hosts file
 - C. Social engineering
 - D. Domain litigation
- 9. IP telephony networks require the same security measures as those implemented on an IP data network. Which of the following is unique to IP telephony?
 - A. Limiting IP sessions going through media gateways
 - B. Identification of rogue devices
 - C. Implementation of authentication
 - D. Encryption of packets containing sensitive information
- 10. Angela wants to group together computers by department to make it easier for them to share network resources. Which of the following will best allow her to group computers logically?
 - A. VLAN
 - B. Open network architecture
 - C. Intranet
 - D. VAN
- 11. Which of the following incorrectly describes how routing commonly takes place on the Internet?
 - A. EGP is used in the areas “between” each AS.
 - B. Regions of nodes that share characteristics and behaviors are called ASs.

- C. CAs are specific nodes that are responsible for routing to nodes outside of their region.
 - D. Each AS uses IGP to perform routing functionality.
- 12.** Both de facto and proprietary interior protocols are in use today. Which of the following is a proprietary interior protocol that chooses the best path between the source and destination?
- A. IGRP
 - B. RIP
 - C. BGP
 - D. OSPF
- 13.** When a system needs to send data to an end user, that data may have to travel over different networking protocols to get to the destination. The different protocol types depend upon how far geographically the data needs to travel, the types of intermediate devices involved, and how this data needs to be protected during transmission. In the following graphic, which two WAN protocols are missing, and what is the best reasoning for their functionality in the transmission scenario being illustrated?

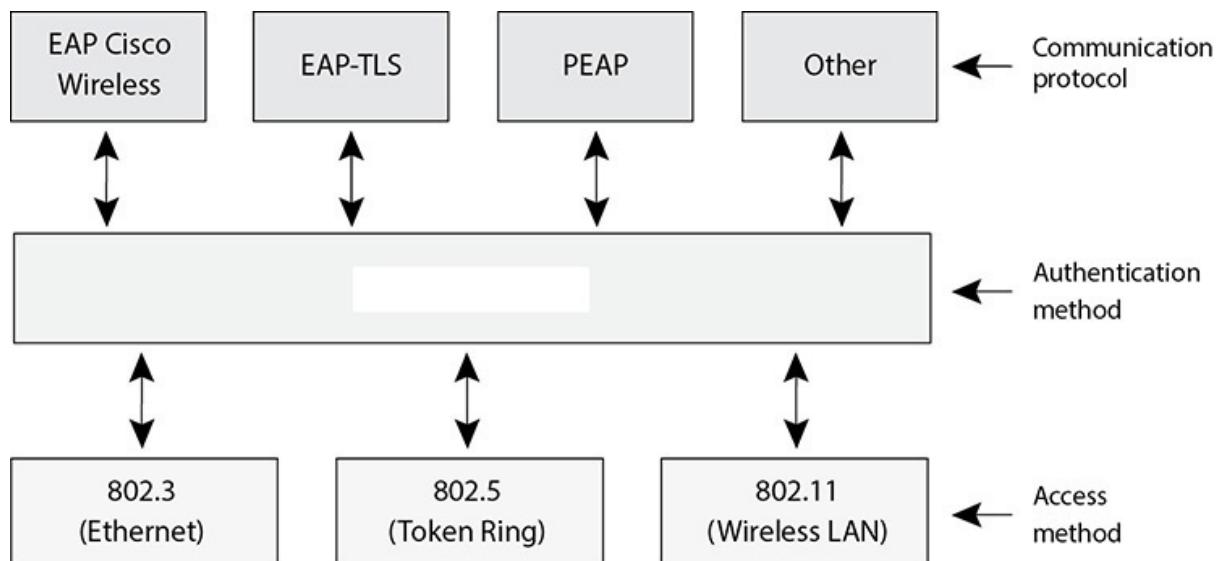


- A. PPTP is being used since the traffic needs to travel over different WAN technologies. PPP is being used because the “last leg” of the transmission is over a multiplexed telecommunication link.
- B. L2FP is being used since the traffic needs to travel over different WAN technologies. PPP is being used because the “last leg” of the transmission is over a serial telecommunication link.
- C. L2TP is being used since the traffic needs to travel over different WAN technologies. PPP is being used because the “last leg” of the transmission is over a serial telecommunication link.

- D. IPSec tunnel mode is being used since the traffic needs to travel over different WAN technologies. PPP is being used because the “last leg” of the transmission is over a multiplexed telecommunication link.
- 14.** Which of the following does NOT describe IP telephony security?
- A. VoIP networks should be protected with the same security controls used on a data network.
 - B. Softphones are more secure than IP phones.
 - C. As endpoints, IP phones can become the target of attacks.
 - D. The current Internet architecture over which voice is transmitted is less secure than physical phone lines.
- 15.** When an organization splits naming zones, the names of its hosts that are accessible only from an intranet are hidden from the Internet. Which of the following best describes why this is done?
- A. To prevent attackers from accessing servers
 - B. To prevent the manipulation of the hosts file
 - C. To avoid providing attackers with valuable information that can be used to prepare an attack
 - D. To avoid providing attackers with information needed for cyber squatting
- 16.** Which of the following best describes why e-mail spoofing is easily executed?
- A. SMTP lacks an adequate authentication mechanism.
 - B. Administrators often forget to configure an SMTP server to prevent inbound SMTP connections for domains it doesn’t serve.
 - C. Keyword filtering is technically obsolete.
 - D. Blacklists are undependable.
- 17.** Which of the following is not a benefit of VoIP?
- A. Cost
 - B. Convergence
 - C. Flexibility
 - D. Security
- 18.** Today, satellites are used to provide wireless connectivity between

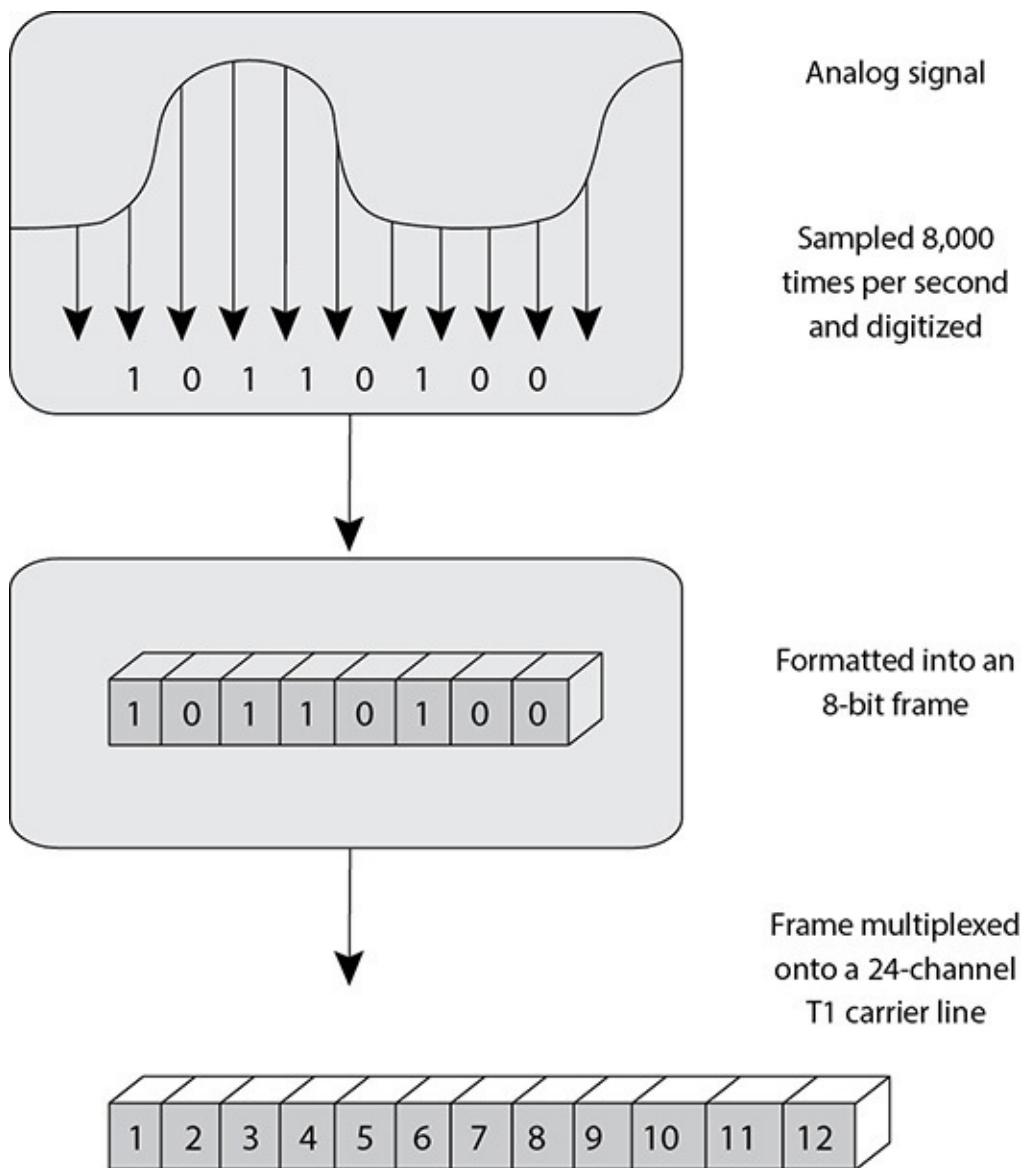
different locations. What two prerequisites are needed for two different locations to communicate via satellite links?

- A. They must be connected via a phone line and have access to a modem.
 - B. They must be within the satellite's line of sight and footprint.
 - C. They must have broadband and a satellite in low Earth orbit.
 - D. They must have a transponder and be within the satellite's footprint.
19. Brad is a security manager at Thingamabobs, Inc. He is preparing a presentation for his company's executives on the risks of using instant messaging (IM) and his reasons for wanting to prohibit its use on the company network. Which of the following should not be included in his presentation?
- A. Sensitive data and files can be transferred from system to system over IM.
 - B. Users can receive information—including malware—from an attacker posing as a legitimate sender.
 - C. IM use can be stopped by simply blocking specific ports on the network firewalls.
 - D. A security policy is needed specifying IM usage restrictions.
20. There are several different types of authentication technologies. Which type is being shown in the graphic that follows?

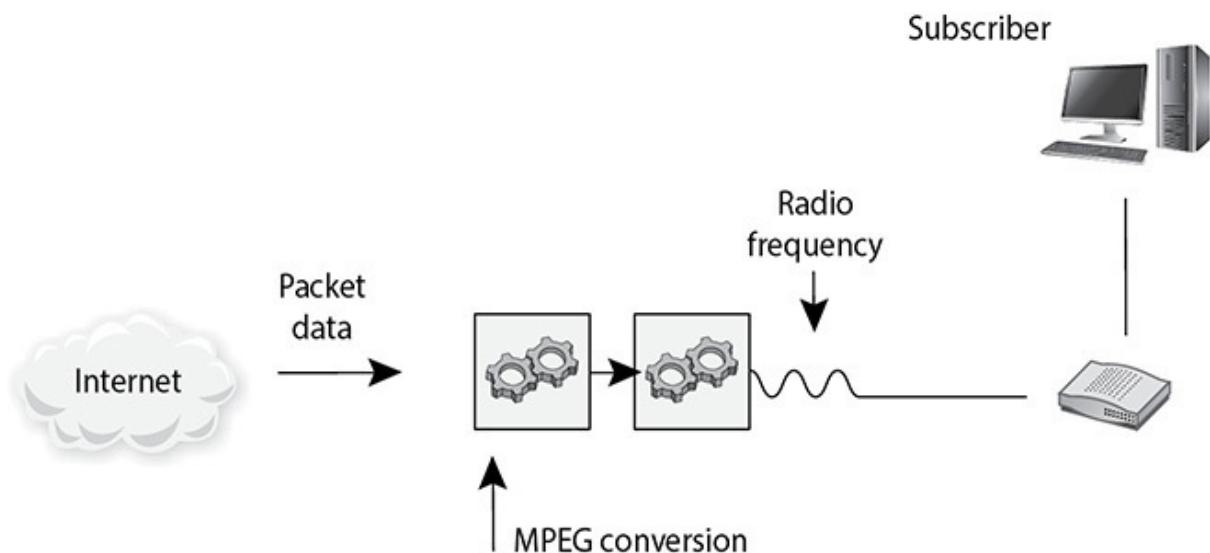


- A. 802.1X
- B. Extensible Authentication Protocol

- C. Frequency hopping spread spectrum
 - D. Orthogonal frequency-division multiplexing
- 21.** What type of security encryption component is missing from the table that follows?
- | | 802.1X Dynamic WEP | Wi-Fi Protected Access | Robust Security Network |
|----------------|---------------------------|-------------------------------|--------------------------------|
| Access Control | 802.1X | 802.1X or preshared key | 802.1X or preshared key |
| Authentication | EAP methods | EAP methods or preshared key | EAP methods or preshared key |
| Encryption | WEP | | CCMP (AES Counter Mode) |
| Integrity | None | Michael MIC | CCMP (AES CBC-MAC) |
- A. Service Set ID
 - B. Temporal Key Integrity Protocol
 - C. Ad hoc WLAN
 - D. Open system authentication
- 22.** What type of technology is represented in the graphic that follows?



- A. Asynchronous Transfer Mode
- B. Synchronous Optical Networks
- C. Frequency-division multiplexing
- D. Multiplexing
23. What type of telecommunication technology is illustrated in the graphic that follows?



- A. Digital Subscriber Line
 - B. Integrated Services Digital Network
 - C. BRI ISDN
 - D. Cable modem
- 24.** Which type of WAN tunneling protocol is missing from the right table in the graphic that follows?

PPTP	
Internet Must Be IP Based	Internet Can Be IP Frame Relay, x.25, or ATM Based
No Header Compression	Header Compression
No Tunnel Authentication	Tunnel Authentication
Built-In PPP Encryption	Uses IPSec Encryption



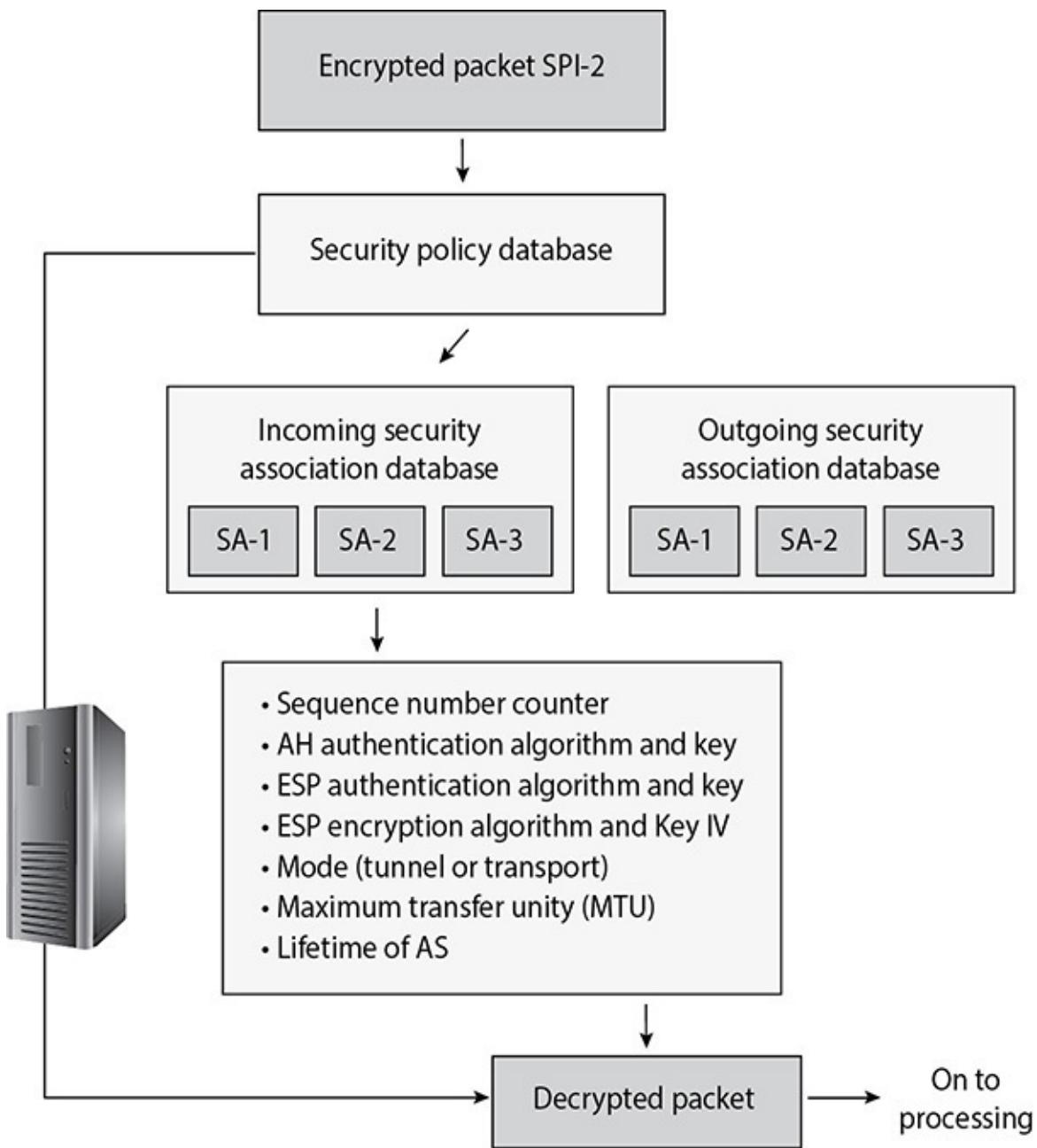
- A.** IPSec
 - B.** FDDI
 - C.** L2TP
 - D.** CSMA/CD
- 25.** IPv6 has many new and different characteristics and functionality compared to IPv4. Which of the following is an incorrect functionality or characteristic of IPv6?
- i.** IPv6 allows for nonscoped addresses, which enables an administrator to restrict specific addresses for specific servers or file and print sharing, for example.
 - ii.** IPv6 has IPSec integrated into the protocol stack, which provides application-based secure transmission and authentication.
 - iii.** IPv6 has more flexibility and routing capabilities compared to IPv4 and allows for Quality of Service (QoS) priority values to be assigned to time-sensitive transmissions.
 - iv.** The protocol offers autoconfiguration, which makes administration much easier compared to IPv4, and it does not require network address translation (NAT) to extend its address space.
- A.** i, iii
 - B.** i, ii
 - C.** ii, iii
 - D.** ii, iv
- 26.** Hanna is a new security manager for a computer consulting company. She has found out that the company has lost intellectual property in the past because malicious employees installed rogue devices on the network, which were used to capture sensitive traffic. Hanna needs to implement a solution that ensures only authorized devices are allowed access to the company network. Which of the following IEEE standards was developed for this type of protection?
- A.** IEEE 802.1AR
 - B.** IEEE 802.1AE
 - C.** IEEE 802.1AF
 - D.** IEEE 802.1XR
- 27.** _____ is a set of extensions to DNS that provides to

DNS clients (resolvers) origin authentication of DNS data to reduce the threat of DNS poisoning, spoofing, and similar attack types.

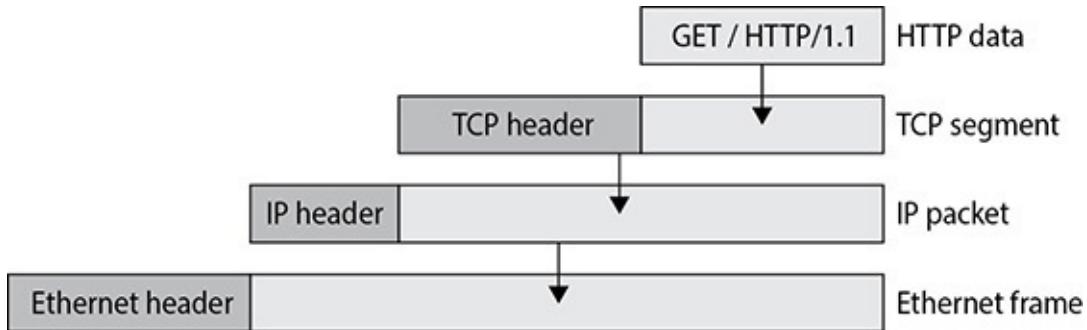
- A. Resource records
 - B. Zone transfer
 - C. DNSSEC
 - D. Resource transfer
28. Which of the following best describes the difference between a virtual firewall that works in bridge mode versus one that is embedded into a hypervisor?
- A. Bridge-mode virtual firewall allows the firewall to monitor individual traffic links, and hypervisor integration allows the firewall to monitor all activities taking place within a host system.
 - B. Bridge-mode virtual firewall allows the firewall to monitor individual network links, and hypervisor integration allows the firewall to monitor all activities taking place within a guest system.
 - C. Bridge-mode virtual firewall allows the firewall to monitor individual traffic links, and hypervisor integration allows the firewall to monitor all activities taking place within a guest system.
 - D. Bridge-mode virtual firewall allows the firewall to monitor individual guest systems, and hypervisor integration allows the firewall to monitor all activities taking place within a network system.
29. Which of the following does software-defined networking (SDN) technology specify?
- A. The mapping between MAC addresses and IP addresses in software
 - B. The end nodes' static routing tables in a dynamic way
 - C. How routers communicate their routing tables to each other as events occur
 - D. How routers move packets based on a centrally managed controller's instructions
30. Determining the geographic location of a client IP address in order to route it toward the most proximal topological source of web content is an example of what technology?
- A. Content distribution network (CDN)

- B. Distributed name service (DNS)
 - C. Distributed web service (DWS)
 - D. Content domain distribution (CDD)
- 31. Which of the following protocols or set of protocols is used in Voice over IP (VoIP) for caller identification?
 - A. Real-time Transport Protocol (RTP) and/or Secure Real-time Transport Protocol (SRTP)
 - B. Real-time Transport Protocol (RTP) and Real-time Transport Control Protocol (RTCP)
 - C. Session Initiation Protocol (SIP)
 - D. Public Switched Telephony/Phone Branch Exchange (PSTN/PBX)
- 32. Encryption can happen at different layers of an operating system and network stack. Where does PPTP encryption take place?
 - A. Data link layer
 - B. Within applications
 - C. Transport layer
 - D. Data link and physical layers
- 33. Which of the following INCORRECTLY describes IP spoofing and session hijacking?
 - A. Address spoofing helps an attacker to hijack sessions between two users without being noticed.
 - B. IP spoofing makes it harder to track down an attacker.
 - C. Session hijacking can be prevented with mutual authentication.
 - D. IP spoofing is used to hijack SSL and IPSec secure communications.
- 34. A small medical institution's IT security team has become overwhelmed with having to operate and maintain IDSSs, firewalls, enterprise-wide antimalware solutions, data leak prevention technologies, and centralized log management. Which of the following best describes what type of solution this organization should implement to allow for standardized and streamlined security operations?
 - A. Unified threat management
 - B. Continuous monitoring technology

- C. Centralized access control systems
 - D. Cloud-based security solution
35. Which of the following protocols blurs the lines between the OSI model layers, performing the tasks of several at once?
- A. Distributed Network Protocol 3 (DNP3)
 - B. File Transfer Protocol (FTP)
 - C. Transmission Control Protocol (TCP)
 - D. Domain Name System (DNS)
36. Which of the following correctly describes the relationship between SSL and TLS?
- A. TLS is the open-community version of SSL.
 - B. SSL can be modified by developers to expand the protocol's capabilities.
 - C. TLS is a proprietary protocol, while SSL is an open-community protocol.
 - D. SSL is more extensible and backward compatible with TLS.
37. End-to-end encryption is used by users, and link encryption is used by service providers. Which of the following correctly describes these technologies?
- A. Link encryption does not encrypt headers and trailers.
 - B. Link encryption encrypts everything but data link messaging.
 - C. End-to-end encryption requires headers to be decrypted at each hop.
 - D. End-to-end encryption encrypts all headers and trailers.
38. What do the SA values in the graphic of IPSec that follows represent?



- A. Security parameter index
 B. Security ability
 C. Security association
 D. Security assistant
39. What is the process depicted in the illustration below referred to as?



- A.** TCP/IP model
- B.** Layering
- C.** Encapsulation
- D.** OSI model
- 40.** Which of the following is a purpose of the transport layer?
- The hop-by-hop delivery of packets from one network to another
 - Representing data in a structure that can be understood by processes at the endpoints
 - Encapsulating the IP packet for transport
 - Ensuring reliable data transfer
- 41.** Which of the following statements is NOT true about the IPv4 address 192.168.10.129\25?
- It is an RFC 1918–specified private address.
 - The netmask for this address is 255.255.255.0.
 - The network address for the network it specifies is 192.168.10.128\25.
 - The host portion of this 32-bit address is the low-order 7 bits.
- 42.** Which of the following statements describes a “converged” protocol?
- It is a term used to describe a situation where two otherwise independent protocols—often functioning at the same layer—become one, as with Fibre Channel (FC) over Ethernet (FCoE).
 - It is any situation where one protocol is encapsulated with another, as with TCP inside of IP (TCP/IP).
 - It refers to when two protocols at the same layer begin to do essentially the same thing, such as HTTP and HTTPS.
 - It is any situation where a protocol is encapsulated within another

protocol in a way that bends or breaks the OSI model, as with IPv6 over generic routing encapsulation (GRE) over IPv4.

- 43.** Ethernet uses a shared medium for all stations on a LAN to communicate, and uses a carrier sense multiple access with collision detection (CSMA/CD) approach to managing communications between stations. Which of the following statements about this protocol best explains how it works?
- A. A control frame is passed from station to station, granting permission for that station to transmit once it is received.
 - B. Each station is required to monitor the medium for transmissions and only transmit when all other stations are silent. Each station is also responsible for alerting all other stations if it observes more than one station transmitting at the same time.
 - C. Each station is required to monitor the medium for transmissions and only transmit when all other stations are silent. Each station is also responsible for signaling its intent to transmit before doing so.
 - D. A primary station is responsible for determining which of the other stations is due to transmit, by polling each of them at regular intervals to determine which station has data to transmit.
- 44.** Within the realm of network components, what are “endpoints” and why do they pose such difficult security challenges?
- A. Endpoints are the client systems on a network. Because they establish connections to both internal and external servers, their activities can be difficult to monitor and control, and downloads of malicious software into the environment are commonplace.
 - B. Endpoints are the servers to which all the clients connect for authentication, file sharing, and other services. Due to the high volume of connections they support, it can be difficult to monitor and detect malicious activity directed at them, buried among the normal activities.
 - C. Endpoints are everything except the network communication devices, including desktops, servers, mobile devices, and other embedded systems. The management challenges they pose include intermittent connectivity, lack of management infrastructure for some platforms, and the unavailability of software updates for others.
 - D. Endpoints are primarily desktop and mobile systems, which may or

may not exist statically on the network. As a result, keeping track of them in order to maintain up-to-date patching and proper configuration can be difficult.

- 45.** Which of the following describes the best use of Network Access Control (NAC)?
- A. The use of IEEE 802.1X Extensible Authentication Protocol (EAP) to authenticate endpoints prior to allowing them to join a network
 - B. The combined use of a public key infrastructure (PKI) and a hardware Trusted Platform Module (TPM) to conduct certificate-based endpoint authentication and establish a secure link through symmetric key exchange
 - C. The combination of EAP for endpoint authentication and multifactor user authentication for highly granular control
 - D. The use of EAP both for endpoint authentication and for inspection of endpoint OS patch levels and antimalware updates, with the goal of placing untrusted systems into a quarantined VLAN segment
- 46.** What is the greatest weakness, and hence concern, with virtualized networks?
- A. Because network interface cards (NICs) are virtualized (vNICs), the data traveling between them is merely copied from one memory location to another by the hypervisor layer on a single physical host.
 - B. The absence of a physical network makes it impossible to deploy firewalls or intrusion detection systems to regulate and monitor traffic between the virtual systems.
 - C. Virtual networks are essentially clouds with no well-defined topologies. This makes the network paths between virtual systems impossible to know.
 - D. Virtual NICs have much higher throughputs than physical ones. As a result, modern network-based intrusion detection systems (NIDSs) cannot inspect their traffic at real-time speeds.

QUICK ANSWER KEY

- 1. D
- 2. A
- 3. C

4. A

5. A

6. B

7. C

8. A

9. A

10. A

11. C

12. A

13. C

14. B

15. C

16. A

17. D

18. B

19. C

20. A

21. B

22. D

23. D

24. C

25. B

26. A

27. C

28. A

29. D

30. A

31. C

32. A

33. D

34. A

35. A

36. A

37. B

38. C

39. C

40. D

41. B

42. A

43. B

44. C

45. D

46. A

ANSWERS A

- 1.** Layer 2 of the OSI model has two sublayers. What are those sublayers, and what are two IEEE standards that describe technologies at that layer?

 - A.** LCL and MAC; IEEE 802.2 and 802.3
 - B.** LCL and MAC; IEEE 802.1 and 802.3
 - C.** Network and MAC; IEEE 802.1 and 802.3
 - D.** LLC and MAC; IEEE 802.2 and 802.3
- D.** The data link layer, or Layer 2, of the OSI model is responsible for adding a header and a trailer to a packet to prepare the packet for the local area network or wide area network technology binary format for proper line transmission. Layer 2 is divided into two functional sublayers. The upper sublayer is the Logical Link Control (LLC) and is defined in the IEEE 802.2 specification. It communicates with the network layer, which is immediately above the data link layer. Below the LLC is the Media Access Control (MAC) sublayer, which specifies the interface with the protocol requirements of the physical layer. Thus, the specification for this layer depends on the technology of the physical layer. The IEEE

MAC specification for Ethernet is 802.3, Token Ring is 802.5, wireless LAN is 802.11, and so on. When you see a reference to an IEEE standard, such as 802.11 or 802.16, it refers to the protocol working at the MAC sublayer of the data link layer of the protocol stack.

- A** is incorrect because LCL is a distracter. The correct acronym for the upper sublayer of the data link layer is LLC. It stands for the Logical Link Control. By providing multiplexing and flow control mechanisms, the LLC enables the coexistence of network protocols within a multipoint network and their transportation over the same network media.
 - B** is incorrect because LCL is a distracter. The sublayers of the data link layer are the Logical Link Control (LLC) and the Media Access Control (MAC). Furthermore, the LLC is defined in the IEEE 802.2 specification, not 802.1. The IEEE 802.1 specifications are concerned with protocol layers above the MAC and LLC layers. It addresses LAN/MAN architecture, network management, internetworking between LANs and WANs, and link security.
 - C** is incorrect because network is not a sublayer of the data link layer. The sublayers of the data link layer are the Logical Link Control (LLC) and the Media Access Control (MAC). The LLC sits between the network layer (the layer immediately above the data link layer) and the MAC sublayer. Also, the LLC is defined in the IEEE 802.2 specification, not IEEE 802.1. As just explained, 802.1 standards address areas of LAN/MAN architecture, network management, internetworking between LANs and WANs, and link security.
2. Which of the following is not an effective countermeasure against spam?
- A. Open mail relay servers
 - B. Properly configured mail relay servers
 - C. Filtering on an e-mail gateway
 - D. Filtering on the client
- A. An open mail relay server is not an effective countermeasure against spam; in fact, spammers often use them to distribute spam, as they allow an attacker to mask their identity. An open mail relay is an SMTP server that is configured to allow inbound SMTP connections from anyone and to anyone on the Internet. This is how

the Internet was originally set up, but many relays are now properly configured to prevent attackers from using them to distribute spam or pornography.

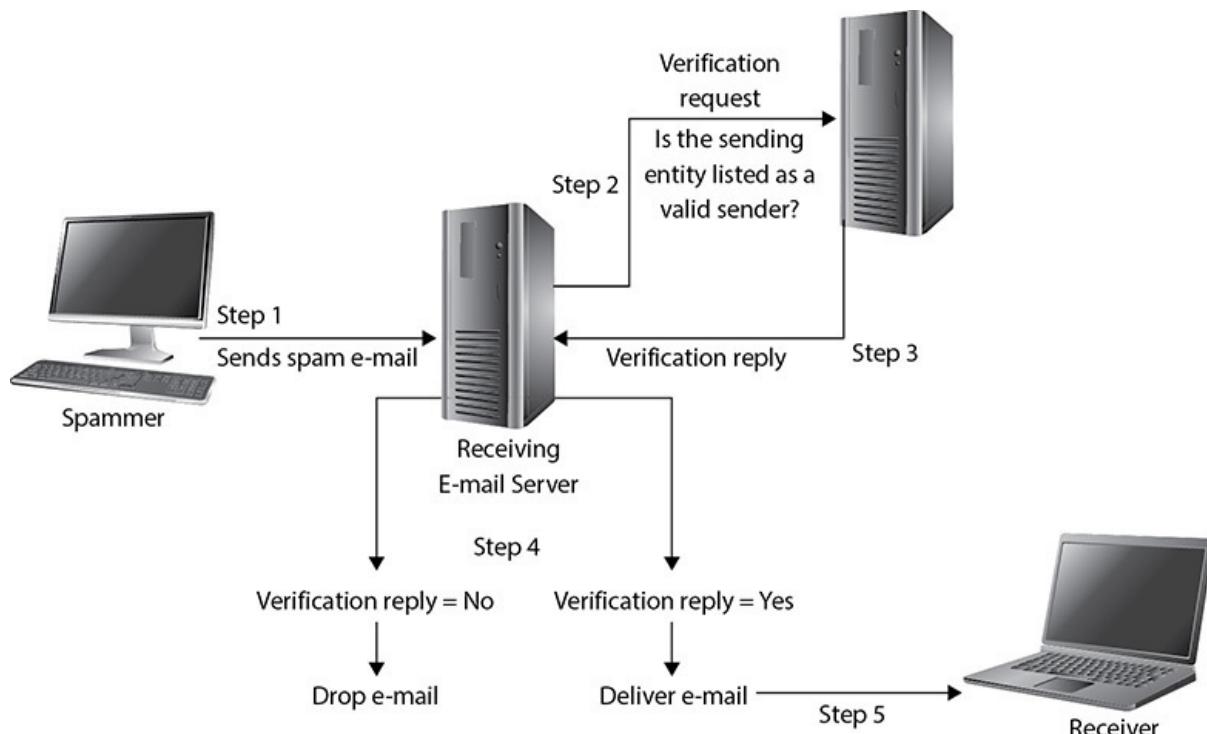
- B** is incorrect because a properly configured mail relay server only allows e-mail that is destined for or originating from known users to pass through it. In this way, a closed mail relay server helps prevent the distribution of spam. In order to be considered closed, an SMTP server should be configured to accept and forward messages from local IP addresses to local mailboxes, from local IP addresses to nonlocal mailboxes, from known and trusted IP addresses to local mailboxes, and from clients that are authenticated and authorized. Servers that are left open are considered to be the result of poor systems administration.
 - C** is incorrect because implementing spam filters on an e-mail gateway is the most common countermeasure against spam. Doing so helps protect network and server capacity, reduces the risk of legitimate e-mail being discarded, and saves users time. A number of commercial spam filters based on a variety of algorithms are available. The filtering software accepts e-mail as its input and either forwards the message unchanged to the recipient, redirects the message for delivery elsewhere, or discards the message.
 - D** is incorrect because filtering on the client is a countermeasure against spam. In fact, filtering can take place at the gateway, which is the most popular method, on the e-mail server, or on the client. There are also different methods of filtering. Filtering based on keywords was once a popular method but has since become obsolete because it is prone to false positives and can be bypassed easily by spammers. Now more sophisticated filters are used. These are based on statistical analysis or analysis of e-mail traffic patterns.
3. Robert is responsible for implementing a common architecture used when customers need to access confidential information through Internet connections. Which of the following best describes this type of architecture?
- A. Two-tiered model
 - B. Screened subnet
 - C. Three-tiered model
 - D. Public and private DNS zones
- C. Many of today's e-commerce architectures use a three-tiered

architecture approach. The three-tier architecture is a client/server architecture in which the user interface, functional process logic, and data storage run as independent components that are developed and maintained, often on separate platforms. The three-tier architecture allows for any one of the tiers to be upgraded or modified as needed without affecting the other two tiers because of its modularity. In the case of e-commerce, the presentation layer is a front-end web server that users interact with. It can serve both static and cached dynamic content. The business logic layer is where the request is reformatted and processed. This is commonly a dynamic content processing and generation-level application server. The data storage is where the sensitive data is held. It is a back-end database that holds both the data and the database management system software that is used to manage and provide access to the data. The separate tiers may be connected with middleware and run on separate physical servers.

- A** is incorrect because two-tiered, or client/server, describes an architecture in which a server provides services to one or more clients that request those services. Many of today's business applications and Internet protocols use the client/server model. This architecture uses two systems: a client and a server. The client is one tier and the server is another tier, hence the two-tier architecture. Each instance of the client software is connected to one or more servers. The client sends its information request to a server, which processes the request and returns the data to the client. A three-tier architecture is a better approach for protecting sensitive information when requests are coming in from the Internet. It provides one extra tier that an attacker must exploit to gain access to the sensitive data being held on the back-end server.
- B** is incorrect because a screened-host architecture means that one firewall is in place to protect one server, which is basically a one-tier architecture. An external, public-facing firewall screens the requests coming in from an untrusted network as in the Internet. If the one tier, the only firewall, is compromised, then the attacker can gain access to the sensitive data that resides on the server relatively easily.
- D** is incorrect because while separating DNS servers into public and private servers provides protection, it is not an actual architecture used for the purpose requested in the question. Organizations should implement split DNS (public and private facing), which

means a DNS server in the DMZ handles external resolution requests, while an internal DNS server handles only internal requests. This helps ensure that the internal DNS has layers of protection and is not exposed to Internet connections.

4. Since sending spam (unwanted messages) has increased over the years and e-mail has become a common way of sending out malicious links and malware, the industry has developed different ways to combat these issues. One approach is to use a Sender Policy Framework, which is an e-mail validation system. In the following graphic, what type of system receives the request in step 2 and replies in step 3?



- A. DNS server
B. E-mail server
C. RADIUS server
D. Authentication server
- A. Sender Policy Framework (SPF) is an e-mail validation system designed to prevent spam and malicious e-mail by detecting e-mail spoofing. Attackers commonly spoof e-mail addresses to try and fool the receiver into thinking that the message came from a known and trusted source. SPF allows network administrators to specify which hosts are allowed to send mail from a given domain by implementing an SPF record in the Domain Name System (DNS). The e-mail server is configured to check with the DNS server to

verify that an e-mail coming from a specific domain was sent from an IP address that has been sanctioned by the sending domain's administrator. In the graphic, step 2 is the e-mail server sending this validation request to a DNS server, and step 4 illustrates the resulting validation process that is followed.

- ☒ **B** is incorrect because the e-mail server is being represented between steps 1 and 2. The graphic shows how an e-mail is sent to an e-mail server on a specific domain. The e-mail server is configured to verify that the message comes from a host that is allowed to send it by checking with the source domain's DNS server. If the DNS server has a record that indicates that e-mail from the sending host is allowed, then the e-mail server will forward the message onto the intended destination. The sender's address is sent at the beginning of a Simple Mail Transfer Protocol (SMTP) transmission. If the e-mail server rejects e-mail from that specific address, the sending client will receive a rejection message. If the client is relaying the message on behalf of another entity (message transfer agent), then a bounced message is sent to the original sending address. SPF deals with e-mail spoofing and cannot detect or prevent e-mail address forgery. Attackers commonly use e-mail spoofing to carry out phishing attacks with the goal of obtaining private or sensitive information from the victim.
- ☒ **C** is incorrect because RADIUS is not involved with this type of verification. Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized authentication, authorization, and accounting (AAA) functionality for individual end users that need to connect to a remote system or a network. RADIUS is an authentication framework used to authenticate users, not domain names or e-mail–sending entities. RADIUS is a client/server protocol that is commonly used with network access servers (NAS), remote access servers (RAS), and 802.1X port authentication.
- ☒ **D** is incorrect because the graphic is illustrating how a DNS server is part of the SPF validation process. The DNS server is not an authentication server. A DNS server contains records that mainly contain IP-to-hostname mappings. In an SPF setup, the DNS server would have a record indicating which sending servers the receiving e-mail server is allowed to accept e-mail from, which is configured by the network administrator. SPF is necessary because the Simple Mail Transfer Protocol (SMTP) does not have inherent security.

functionality to detect spoofed messages. An attacker could spoof an e-mail address and essentially claim to be any source address, and there is nothing within SMTP to identify this activity. Attackers commonly carry out this type of spoofing attack with the goal of tricking an end user into accepting the message and clicking a malicious link or a malicious attachment.

5. Which of the following indicates to a packet where to go and how to communicate with the right service or protocol on the destination computer?

A. Socket

B. IP address

C. Port

D. Frame

A. User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) are transport protocols that applications use to get their data across a network. They both use ports to communicate with upper OSI layers and to keep track of various conversations that take place simultaneously. The ports are also the mechanism used to identify how other computers access services. When a TCP or UDP message is formed, a source and a destination port are contained within the header information along with the source and destination IP addresses. This makes up a socket, which is how packets know where to go—by the address—and how to communicate with the right service or protocol on the other computer—by the port number. The IP address acts as the doorway to a computer, and the port acts as the doorway to the actual protocol or service. To communicate properly, the packet needs to know these doors.

B is incorrect because an IP address does not tell a packet how to communicate with a service or protocol. The purpose of an IP address is host or network interface identification and location addressing. Each node in a network has a unique IP address. This information, along with the source and destination ports, makes up a socket. The IP address tells the packet where to go, and the port indicates how to communicate with the right service or protocol.

C is incorrect because the port only tells the packet how to communicate with the right service or protocol. It does not tell the packet where to go. The IP address provides this information. A

port is a communications endpoint used by IP protocols such as TCP and UDP. Ports are identified by a number. They are also associated with an IP address and a protocol used for communication.

- D** is incorrect because frame is the term used to refer to a datagram after it is given a header and trailer at the data link layer. A message is formed and passed to the application layer from a program and sent down through the protocol stack. Each protocol at each layer adds its own information (headers and trailers) to the message and passes it down to the next level. As the message is passed down the stack, it goes through a sort of evolution, and each stage has a specific name that indicates what is taking place. When an application formats data to be transmitted over the network, the data is called a message. The message is sent to the transport layer, where TCP does its magic on the data. The bundle of data is now a segment. The segment is sent to the network layer. The network layer adds routing and addressing, and now the bundle is called a datagram. The network layer passes off the datagram to the data link layer, which frames the datagram with a header and a trailer, and now it is called a frame.

- 6.** Several different tunneling protocols can be used in dial-up situations. Which of the following would be best to use as a VPN tunneling solution?

- A.** L2P
- B.** PPTP
- C.** IPSec
- D.** L2TP

- B.** A virtual private network (VPN) is a secure, private connection through a public network or an otherwise unsecure environment. It is a private connection because the encryption and tunneling protocols are used to ensure the confidentiality and integrity of the data in transit. It is important to remember that VPN technology requires a tunnel to work, and it assumes encryption. The protocols that can be used for VPNs are Point-to-Point Tunneling Protocol (PPTP), Internet Protocol Security (IPSec), and Layer 2 Tunneling Protocol (L2TP). PPTP, a Microsoft protocol, allows remote users to set up a PPP connection to a local ISP and then create a secure VPN to their destination. PPTP has been the de facto industry-standard tunneling protocol for years, but the new de facto standard

for VPNs is IPSec. PPTP is designed for client/server connectivity and establishes a single point-to-point connection between two computers. It works at the data link layer and transmits only over IP networks.

- A** is incorrect because L2P does not exist. This is a distracter answer.
- C** is incorrect because although IPSec is one of the three primary VPN tunneling protocols, it is not used over dial-up connections. It supports only IP networks and works at the network layer, providing security on top of IP. IPSec handles multiple connections at the same time, and provides secure authentication and encryption.
- D** is incorrect because L2TP is not a tunneling protocol that works over a dial-up connection. L2TP is a tunneling protocol that can extend a VPN over various WAN network types (IP, X.25, frame relay). A hybrid of L2F and PPTP, L2TP works at the data link layer and transmits over multiple types of networks, not just IP. However, it must be combined with IPSec for security, so it is not considered a VPN solution by itself.

7. Which of the following correctly describes Bluejacking?

- A.** Bluejacking is a harmful, malicious attack.
- B.** It is the process of taking over another portable device via a Bluetooth-enabled device.
- C.** It is commonly used to send contact information.
- D.** The term was coined by the use of a Bluetooth device and the act of hijacking another device.
- C.** Bluetooth is vulnerable to an attack called Bluejacking, which entails an attacker sending an unsolicited message to a device that is Bluetooth-enabled. Bluejackers look for a receiving device, such as a mobile device or laptop, and then send a message to it. Often, the Bluejacker is trying to send their business card to be added to the victim's contact list in their address book. The countermeasure is to put the Bluetooth-enabled device into nondiscoverable mode so that others cannot identify this device in the first place. If you receive some type of message this way, just look around you. Bluetooth only works within a 10-meter distance, so it is coming from someone close by.
- A** is incorrect because Bluejacking is actually a harmless nuisance rather than a malicious attack. It is the act of sending unsolicited

messages to Bluetooth-enabled devices. The first act took place in a bank in which the attacker polled the network and found an active Nokia phone. He then sent the message “Buy Ericsson.”

- B** is incorrect because Bluejacking does not involve taking over another device. It does not give the attacker control of the target device. Rather, the Bluejacker simply sends an unsolicited message to the Bluetooth-enabled device. These messages are usually text only, but it is possible to also send images or sounds. Victims are often unfamiliar with Bluejacking and may think their phone is malfunctioning or that they have been attacked by a virus or hijacked by a Trojan horse.
 - D** is incorrect because the term Bluejacking has nothing to do with hijacking, which means to take over something. The name Bluejacking was invented by a Malaysian IT consultant who sent the message “Buy Ericsson” to another Bluetooth-enabled device.
8. DNS is a popular target for attackers due to its strategic role on the Internet. What type of attack uses recursive queries to poison the cache of a DNS server?
- A. DNS hijacking
 - B. Manipulation of the hosts file
 - C. Social engineering
 - D. Domain litigation
- A. DNS plays a strategic role in the transmission of traffic on the Internet. The DNS directs traffic to the appropriate address by mapping domain names to their corresponding IP addresses. DNS queries can be classified as either recursive or iterative. In a recursive query the DNS server often forwards the query to another server and returns the proper response to the inquirer. In an iterative query, the DNS server responds with an address for another DNS server that might be able to answer the question, and the client then proceeds to ask the new DNS server. Attackers use recursive queries to poison the cache of a DNS server. In this manner, attackers can point systems to a website that they control and that contains malware or some other form of attack. Here’s how it works: An attacker sends a recursive query to a victim DNS server asking for the IP address of the domain www.logicalsecurity.com. The DNS server forwards the query to another DNS server. However, before the other DNS server responds, the attacker injects

his own IP address. The victim server accepts the IP address and stores it in its cache for a specific period of time. The next time a system queries the server to resolve www.logicalsecurity.com to its IP address, the server will direct users to the attacker's IP address. This is called DNS spoofing or DNS poisoning.

- B** is incorrect because manipulating the hosts file does not use recursive queries to poison the cache of a DNS server. A client first queries a hosts file before issuing a request to a DNS server. Some viruses add invalid IP addresses of antivirus vendors to the hosts file in order to prevent the download of virus definitions and prevent detection. This is an example of manipulating the hosts file.
 - C** is incorrect because social engineering does not involve querying a DNS server. Social engineering refers to the manipulation of individuals for the purpose of gaining unauthorized access or information. Social engineering takes advantage of people's desire to be helpful and/or trusting. It is a nontechnical attack that may use technology in its execution. For example, an attacker might pose as a user's manager and send him a spoofed e-mail asking for the password to an application. The user, wanting to help and keep his manager's favor, is likely to provide the password.
 - D** is incorrect because domain litigation does not involve poisoning a DNS server's cache. Domain names are subject to trademark risks, including the temporary unavailability or permanent loss of an established domain name. A victim company could lose its entire Internet presence as a result of domain litigation. Organizations concerned over the possibility of trademark disputes related to their domain name(s) should establish contingency plans. For example, a company may establish a second, unrelated domain that can still represent the company's name.
- 9.** IP telephony networks require the same security measures as those implemented on an IP data network. Which of the following is unique to IP telephony?
- A. Limiting IP sessions going through media gateways
 - B. Identification of rogue devices
 - C. Implementation of authentication
 - D. Encryption of packets containing sensitive information
- A. A media gateway is the translation unit between disparate telecommunications networks. VoIP media gateways perform the

conversion between time-division multiplexing (TDM) voice to Voice over Internet Protocol (VoIP). As a security measure, the number of calls via media gateways should be limited. Otherwise, media gateways are vulnerable to denial-of-service attacks, hijacking, and other types of attacks.

- B** is incorrect because it is necessary to identify rogue devices on both IP telephony and data networks. On IP telephony networks, it is necessary to look specifically for rogue IP phones and softphones. Rogue means that these devices are unauthorized. They are therefore not managed or secured by IT and can introduce additional risk to the network. A common rogue device found on data networks is wireless access points. A rogue access point can provide an entry to the network for unauthorized users.
- C** is incorrect because authentication is recommended for both data and voice networks. In both cases, authentication allows you to register users and equipment on the network so that you can verify they are who they say they are when they try to connect to the network. Authentication also allows you to deny access to users and devices that are not authorized.
- D** is incorrect because sensitive data can be transmitted on either a voice or data network and should be encrypted in both cases. Eavesdropping is a very real threat for VoIP networks. Consider all the sales meetings, management meetings, financial meetings, etc., that are conducted over the phone. Every word that is spoken in those meetings is vulnerable to eavesdropping. Encrypting voice data is one of the best ways to protect this sensitive data.

- 10.** Angela wants to group together computers by department to make it easier for them to share network resources. Which of the following will best allow her to group computers logically?
- A.** VLAN
 - B.** Open network architecture
 - C.** Intranet
 - D.** VAN
- A.** Virtual LANs (VLANs) enable the logical separation and grouping of computers based on resource requirements, security, or business needs in spite of the standard physical location of the systems. This technology allows Angela to logically place all computers within the same department on the same VLAN network

so that all users can receive the same broadcast messages and can access the same types of resources, regardless of their physical location. This means that computers can be grouped together even if they are not located on the same network.

- B** is incorrect because open network architecture describes technologies that can make up a network. It is one that no vendor owns, that is not proprietary, and that can easily integrate various technologies and vendor implementations of those technologies. The OSI model provides a framework for developing products that will work within an open network architecture. Vendors use the OSI model as a blueprint and develop their own protocols and interfaces to produce functionality that is different from that of other vendors. However, because these vendors use the OSI model as their starting place, integration of other vendor products is an easier task, and the interoperability issues are less burdensome than if the vendors had developed their own networking framework from scratch.
- C** is incorrect because an intranet is a private network that a company uses when it wants to use the Internet and web-based technologies for internal networks. The company has web servers and client machines using web browsers, and it uses the TCP/IP protocol suite. The web pages are written in HTML or XML, and are accessed via HTTP.
- D** is incorrect because a value-added network (VAN) is an electronic data interchange (EDI) infrastructure developed and maintained by a service bureau. Here's an example of how a VAN works: A retail store such as Target tracks its inventory by having employees scan bar codes on individual items. When the inventory of an item—such as garden hoses—becomes low, an employee sends a request for more garden hoses. The request goes to a mailbox at a VAN that Target pays to use, and the request is then pushed out to the garden hose supplier. Because Target deals with thousands of suppliers, using a VAN simplifies the ordering process. There is no need to manually track down the right supplier and submit a purchase order.

- 11.** Which of the following incorrectly describes how routing commonly takes place on the Internet?
- A.** EGP is used in the areas “between” each AS.
 - B.** Regions of nodes that share characteristics and behaviors are called ASs.
 - C.** CAs are specific nodes that are responsible for routing to nodes

outside of their region.

D. Each AS uses IGP to perform routing functionality.

- C. A CA, or certificate authority, is a trusted third party that provides digital certificates for use in a public key infrastructure. CAs have nothing to do with routing. A PKI environment provides a hierarchical trust model but does not deal with routing of traffic.
- A is incorrect because the statement is true. The Exterior Gateway Protocol (EGP) functions between each autonomous system (AS). The architecture of the Internet that supports these various ASs is created so that no entity that needs to connect to a specific AS has to know or understand the interior protocols that can be used. Instead, for ASs to communicate, they just have to be using the same exterior routing protocols.
- B is incorrect because the statement is true; regions of nodes (networks) that share characteristics and behaviors are called autonomous systems (ASs). These ASs are independently controlled by different corporations and organizations. An AS is made up of computers and devices, which are administered by a single entity and use a common Interior Gateway Protocol (IGP). The boundaries of these ASs are delineated by border routers. These routers connect to the border routers of other ASs and run interior and exterior routing protocols. Internal routers connect to other routers within the same AS and run interior routing protocols. So, in reality, the Internet is just a network made up of ASs and routing protocols.
- D is incorrect because an Interior Gateway Protocol (IGP) handles routing tasks within each AS. There are two categories of IGPs: distance-vector routing protocols and link-state routing protocols. Distance-vector routing protocols include Routing Information Protocol (RIP) and Interior Gateway Routing Protocol (IGRP). Routers using these protocols do not possess information about the entire network topology. Nodes using link-state routing protocols, on the other hand, possess information about the complete network topology. Examples of these protocols include Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (IS-IS).

12. Both de facto and proprietary interior protocols are in use today. Which of the following is a proprietary interior protocol that chooses the best path between the source and destination?

A. IGRP

B. RIP

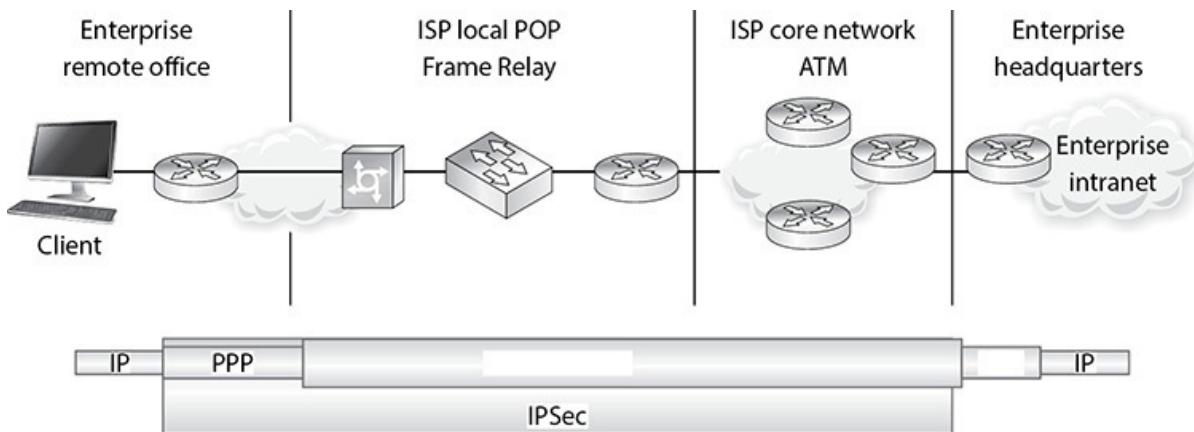
C. BGP

D. OSPF

- A.** Interior Gateway Routing Protocol (IGRP) is a distance-vector routing protocol that was developed by, and is proprietary to, Cisco Systems. Whereas Routing Information Protocol (RIP) uses one criterion to find the best path between the source and the destination, IGRP uses five criteria to make a “best route” decision. A network administrator can set weights on these different metrics so that the protocol works best in that specific environment.
- B** is incorrect because Routing Information Protocol (RIP) is not proprietary. RIP is a standard that outlines how routers exchange routing table data and is considered a distance-vector protocol, which means it calculates the shortest distance between the source and the destination. It is considered a legacy protocol, because of its slow performance and lack of functionality. It should only be used in small networks. RIP version 1 has no authentication, and RIP version 2 sends passwords in cleartext or hashed with MD5.
- C** is incorrect because the Border Gateway Protocol (BGP) is an Exterior Gateway Protocol (EGP). BGP enables routers on different ASs to share routing information to ensure effective and efficient routing between the different networks. BGP is commonly used by Internet service providers to route data from one location to the next on the Internet.
- D** is incorrect because Open Shortest Path First (OSPF) is not proprietary. OSPF uses link-state algorithms to send out routing table information. The use of these algorithms allows for smaller, more frequent routing table updates to take place. This provides a more stable network than RIP but requires more memory and CPU resources to support this extra processing. OSPF allows for a hierarchical routing network that has a backbone link connecting all subnets together. OSPF is the preferred protocol and has replaced RIP in many networks today. Authentication can take place with cleartext passwords or hashed passwords, or you can choose to configure no authentication on the routers using this protocol.

- 13.** When a system needs to send data to an end user, that data may have to travel over different networking protocols to get to the destination. The

different protocol types depend upon how far geographically the data needs to travel, the types of intermediate devices involved, and how this data needs to be protected during transmission. In the following graphic, which two WAN protocols are missing, and what is the best reasoning for their functionality in the transmission scenario being illustrated?



- A. PPTP is being used since the traffic needs to travel over different WAN technologies. PPP is being used because the “last leg” of the transmission is over a multiplexed telecommunication link.
- B. L2FP is being used since the traffic needs to travel over different WAN technologies. PPP is being used because the “last leg” of the transmission is over a serial telecommunication link.
- C. L2TP is being used since the traffic needs to travel over different WAN technologies. PPP is being used because the “last leg” of the transmission is over a serial telecommunication link.
- D. IPSec tunnel mode is being used since the traffic needs to travel over different WAN technologies. PPP is being used because the “last leg” of the transmission is over a multiplexed telecommunication link.
- C. Point-to-Point Protocol (PPP) is a data link protocol that carries out framing and encapsulation for point-to-point connections. Telecommunication devices commonly use PPP as their data link protocol, which encapsulates data to be sent over serial connection links. Layer 2 Tunneling Protocol (L2TP) is used when a PPP connection needs to be extended through a non-IP-based WAN network. L2TP tunnels PPP traffic over various network types such as ATM and Frame Relay. This means that when two networks are connected by WAN links, each network's gateway device (i.e., border router) is configured to use L2TP. When the destination gateway system receives data over the L2TP, it “unwraps” the

packets by stripping off the L2TP headers and sends the packets over the next leg of the transmission, which in this graphic is a telecommunication link using PPP.

- A** is incorrect because PPTP is used when a PPP connection needs to be extended through an IP-based network. PPTP does not work over non-IP networks such as Frame Relay and ATM. PPTP is an older protocol that is not used to transmit data over complex non-IP WAN links as shown in this graphic. PPTP uses Generic Routing Encapsulation (GRE) and TCP to encapsulate PPP packets and to extend a PPP connection through an IP network. The second part of the answer states that PPP is used for multiplexed telecommunication links, which is incorrect because multiplexing takes place at the physical layer and is carried out by devices, not at the data link layer through a protocol.
- B** is incorrect because there is no protocol called L2FP. This is a distracter answer. L2F is Cisco's Layer 2 Forwarding proprietary protocol used for tunneling PPP traffic. This protocol is used to create secure virtual private connections over the Internet. Various functionalities of the L2F and PPTP protocols were combined to create the L2TP protocol. The two endpoints of an L2TP tunnel are called the LAC (L2TP Access Concentrator) and the LNS (L2TP Network Server). Once an L2TP tunnel is established between the two ends, the network traffic between the peers is bidirectional.
- D** is incorrect because IPSec can only work over IP-based networks and is not a WAN VPN technology that extends PPP connections. For data to travel over WAN links of this type, a data link protocol needs to be used, and IPSec is a network layer protocol. IPSec is a suite of protocols developed to protect traffic traveling over an IP network, because the basic Internet Protocol (IP) does not have any type of security functionality built into it. When an L2TP connection requires the security functionality that IPSec provides (authentication, integrity, confidentiality), the L2TP and IPSec protocols are configured to work together to provide the necessary level of protection. The second part of the answer states that PPP is used for multiplexed telecommunication links, which is incorrect because multiplexing takes place at the physical layer and is carried out by devices, not at the data link layer through a protocol.

14. Which of the following does NOT describe IP telephony security?

- A.** VoIP networks should be protected with the same security controls used on a data network.

- B. Softphones are more secure than IP phones.
 - C. As endpoints, IP phones can become the target of attacks.
 - D. The current Internet architecture over which voice is transmitted is less secure than physical phone lines.
- B.** IP softphones should be used with caution. A softphone is a software application that allows the user to make phone calls via a computer over the Internet. A softphone, which replaces dedicated hardware, behaves like a traditional telephone. It can be used with a headset connected to a PC's sound card or with a USB phone. Skype is an example of a softphone application. Compared to hardware-based IP phones, softphones make an IP network more vulnerable. However, softphones are no worse than any other interactive Internet application. In addition, data-centered malware can more easily enter a network via softphones because they do not separate voice traffic from data as do IP phones.
- A** is incorrect because the statement correctly describes IP telephony network security. An IP telephony network uses the same technology as a traditional IP network, only it can support voice applications. Therefore, the IP telephony network is susceptible to the same vulnerabilities as a traditional IP network and should be protected accordingly. This means the IP telephony network should be engineered to have the proper security.
- C** is incorrect because the statement is true. IP phones on an IP telephony network are the equivalent of a workstation on a data network in terms of their vulnerability to attack. Thus, IP phones should be protected with many of the same security controls that are implemented in a traditional workstation. For example, default administrator passwords should be changed. Unnecessary remote access features should be disabled. Logging should be enabled and the firmware upgrade process should be secured.
- D** is incorrect because the statement is true. For the most part, the current Internet architecture over which voice is transmitted is less secure than physical phone lines. Physical phone lines provide point-to-point connections, which are harder to tap into than the software-based tunnels that make up most of the Internet. This is an important factor to take into consideration when securing an IP telephony network because the network is now transmitting two invaluable assets—data and voice. It is not unusual for personally identifiable information, financial information, and other sensitive

data to be spoken over the phone. Intercepting this information over an IP telephony network is as easy as intercepting regular data. Now voice traffic needs to be encrypted, too.

15. When an organization splits naming zones, the names of its hosts that are accessible only from an intranet are hidden from the Internet. Which of the following best describes why this is done?
- A. To prevent attackers from accessing servers
 - B. To prevent the manipulation of the hosts file
 - C. To avoid providing attackers with valuable information that can be used to prepare an attack
 - D. To avoid providing attackers with information needed for cyber squatting
- C. Many companies have their own internal DNS servers to resolve their internal hostnames. These companies usually also use the DNS servers at their ISPs to resolve hostnames on the Internet. An internal DNS server can be used to resolve hostnames on the entire network, but usually more than one DNS server is used so that the load can be split up and so that redundancy and fault tolerance are in place. Within DNS servers, networks are split into zones. One zone may contain all hostnames for the marketing and accounting departments, and another zone may contain hostnames for the administration, research, and legal departments. It is a good idea to split DNS zones when possible so that the names of hosts that are accessible only from an intranet are not visible from the Internet. This information is valuable to an attacker who is planning an attack because it can lead to other information, such as the network structure, organizational structure, or server operating systems.
- A is incorrect because this is not the best answer for this question. Naming zones are split up so that attackers cannot learn information about internal systems, such as names, IP addresses, functions, and so on. One of the secondary attacks after exploiting a DNS server could be accessing a server in an unauthorized manner, but ensuring unauthorized access just to servers is not the main reason to split DNS zones.
- B is incorrect because splitting naming zones has to do with how DNS servers are set up to resolve hostnames, not manipulate the hosts file. The hosts file can be manipulated for a number of reasons, both for good and bad. The hosts file always maps the

hostname localhost to the IP address 127.0.0.1 (this is the loopback network interface, which was originally defined in RFC 3330), as well as other hosts. Some viruses add invalid IP addresses of antivirus vendors to the hosts file to avoid detection. By adding frequently visited IP addresses to the hosts file, you can increase the speed of web browsing. You can also block spyware and ad networks by adding lists of spyware and ad network sites to the hosts file and mapping them to the loopback network interface. This way, these sites always point back to the user's machine and the sites cannot be reached.

- D** is incorrect because hackers do not need information on a DNS server to carry out cyber squatting. Cyber squatting occurs when an attacker purchases a well-known brand or company name, or variation thereof, as a domain name with the goal of selling it to the rightful owner. In the meantime, the company can be misrepresented to the public. The only way an organization can avoid cyber squatting is by registering adjacent domains and variations on the domain or through trademark litigation.
- 16.** Which of the following best describes why e-mail spoofing is easily executed?
 - A.** SMTP lacks an adequate authentication mechanism.
 - B.** Administrators often forget to configure an SMTP server to prevent inbound SMTP connections for domains it doesn't serve.
 - C.** Keyword filtering is technically obsolete.
 - D.** Blacklists are undependable.
- A.** E-mail spoofing is easy to execute because SMTP lacks an adequate authentication mechanism. An attacker can spoof e-mail sender addresses by sending a Telnet command to port 25 of a mail server followed by a number of SMTP commands. Spammers use e-mail spoofing to obfuscate their identity. Oftentimes, the purported sender of a spam e-mail is actually another victim of spam whose e-mail address has been sold to or harvested by a spammer.
- B** is incorrect because the answer alludes to open mail relay servers. The failure to configure an SMTP server to prevent SMTP connections for domains it doesn't serve is not a common mistake. It is well known that an open mail relay allows spammers to hide their identity and is a principal tool in the distribution of spam. Open mail relays are, therefore, considered a sign of bad system

administration. An open relay is not required for e-mail spoofing.

- C** is incorrect because keyword filtering is a countermeasure that can be used to help suppress spam. While keyword filtering by itself was popular at one time, it is no longer an effective countermeasure when used just by itself. Keyword filtering is prone to false positives and spammers have found creative ways to work around it. For example, keywords may be intentionally misspelled or one or two letters of a common word swapped with a special character.
- D** is incorrect because blacklists list open mail relay servers that are known for sending spam. Administrators can use blacklists to prevent the delivery of e-mail originating from those hosts in an effort to suppress spam. However, blacklists cannot be depended upon for complete protection because they are often managed by private organizations and individuals according to their own rules.

17. Which of the following is not a benefit of VoIP?

- A.** Cost
 - B.** Convergence
 - C.** Flexibility
 - D.** Security
- D.** Voice over Internet Protocol (VoIP) refers to transmission technologies that deliver voice communications over IP networks. IP telephony uses technologies that are similar to TCP/IP, so its vulnerabilities are also similar. The voice system is vulnerable to application manipulation (such as toll fraud and blocking), unauthorized administrative access, and poor implementation. In terms of the network and media, it is also vulnerable to denial-of-service attacks against the gateways and network resources. Eavesdropping is also a concern, since data traffic is sent in cleartext unless it is encrypted.
 - A** is incorrect because cost is a benefit of VoIP. Using VoIP means a company has to pay for and maintain only one network, instead of one network dedicated to data transmission and another network dedicated to voice transmission. Telephony features such as conference calling, call forwarding, and automatic redial are free from open-source VoIP implementations, while traditional telecommunications companies charge extra for them. And, finally, VoIP costs are lower because of the way they are billed. VoIP calls are billed per megabyte, while regular telephone calls are billed by

the minute. In general, it is cheaper to send data over the Internet for a given period of time than it is to use the regular telephone for that same amount of time.

- B** is incorrect because convergence is a benefit of VoIP.
Convergence refers to the merging of the traditional IP network with the traditional analog phone network. This is a benefit because a company no longer has to pay for and maintain separate networks for data and voice. However, while convergence saves money and administration overhead, certain security issues must be understood and dealt with.
- C** is incorrect because flexibility is a benefit of VoIP. The technology easily supports multiple telephone calls over a single Internet broadband connection without having to add extra lines. It also offers location independence. All that is needed to obtain a WAN or MAN phone connection to a VoIP provider is an adequate Internet connection. VoIP can also be integrated with other Internet services, such as video conversation, file exchange during a call, and audio conferencing.

18. Today, satellites are used to provide wireless connectivity between different locations. What two prerequisites are needed for two different locations to communicate via satellite links?

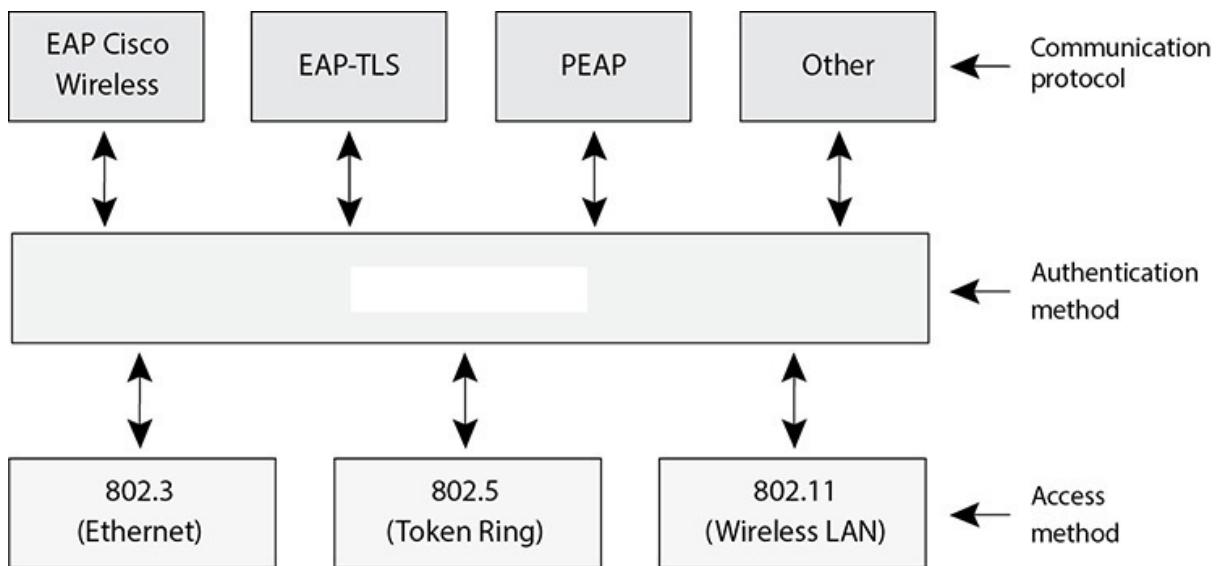
- A.** They must be connected via a phone line and have access to a modem.
- B.** They must be within the satellite's line of sight and footprint.
- C.** They must have broadband and a satellite in low Earth orbit.
- D.** They must have a transponder and be within the satellite's footprint.
- B.** For two different locations to communicate via satellite links, they must be within the satellite's line of sight and footprint (area covered by the satellite). The sender of information modulates the data onto a radio signal that is transmitted to the satellite. A transponder on the satellite receives this signal, amplifies it, and relays it to the receiver. The receiver must have a certain type of antenna, which is one of those circular, dish-like components on top of buildings. The antenna contains one or more microwave receivers, depending upon how many satellites it is accepting data from. The size of the footprint depends upon the type of satellite being used. It can be as large as a country or only a few hundred feet in circumference.

- A** is incorrect because a phone line and a modem are not wireless. However, in most cases satellite broadband is a hybrid system that uses a regular phone line and modem-like technologies for data and requests sent from the user's machine, but employs a satellite link to send data to the user.
- C** is incorrect because the satellite provides broadband transmission. It is commonly used for television channels and PC Internet access. While it is certainly necessary to have a satellite in orbit, and those in low Earth orbit are commonly used for two-way paging, international cellular communication, TV stations, and Internet use, it is not the best answer to this question.
- D** is incorrect because the two locations do not require a transponder. The transponder is on the satellite itself. The transponder receives a signal, amplifies it, and sends it to the receiver. However, it is necessary for the two locations to be within the satellite's footprint.

- 19.** Brad is a security manager at Thingamabobs, Inc. He is preparing a presentation for his company's executives on the risks of using instant messaging (IM) and his reasons for wanting to prohibit its use on the company network. Which of the following should not be included in his presentation?
- A.** Sensitive data and files can be transferred from system to system over IM.
 - B.** Users can receive information—including malware—from an attacker posing as a legitimate sender.
 - C.** IM use can be stopped by simply blocking specific ports on the network firewalls.
 - D.** A security policy is needed specifying IM usage restrictions.
- C.** Instant messaging (IM) allows people to communicate with one another through a type of real-time and personal chat room. It alerts individuals when someone who is on their "buddy list" has accessed the intranet/Internet so that they can send text messages back and forth in real time. The technology also allows for files to be transferred from system to system. The technology is made up of clients and servers. The user installs an IM client (AOL, ICQ, Yahoo Messenger, and so on) and is assigned a unique identifier. This user gives out this unique identifier to people whom she wants to communicate with via IM. Blocking specific ports on the

firewalls is not usually effective because the IM traffic may be using common ports that need to be open (HTTP port 80 and FTP port 21). Many of the IM clients autoconfigure themselves to work on another port if their default port is unavailable and blocked by the firewall.

- A** is incorrect because in addition to text messages, instant messaging allows for files to be transferred from system to system. These files could contain sensitive information, putting the company at business and legal risk. And, of course, sharing files over IM can eat up network bandwidth and impact network performance as a result.
 - B** is incorrect because the statement is true. Because of the lack of strong authentication, accounts can be spoofed so that the receiver accepts information from a malicious user instead of the legitimate sender. There have also been numerous buffer overflow and malformed packet attacks that have been successful with different IM clients. These attacks are usually carried out with the goal of obtaining unauthorized access to the victim's system.
 - D** is incorrect because Brad should include in his presentation the need for a security policy specifying IM usage restrictions. This is just one of several best practices for protecting an environment from IM-related security breaches. Other best practices include implementing an integrated antivirus/firewall product on all computers, configuring firewalls to block IM traffic, upgrading IM software to more secure versions, and implementing corporate IM servers so that internal employees communicate within the organization's network only.
- 20.** There are several different types of authentication technologies. Which type is being shown in the graphic that follows?



- A.** 802.1X
- B.** Extensible Authentication Protocol
- C.** Frequency hopping spread spectrum
- D.** Orthogonal frequency-division multiplexing
- A.** The 802.1X standard is a port-based network access control that ensures a user cannot make a full network connection until he is properly authenticated. This means a user cannot access network resources and no traffic is allowed to pass, other than authentication traffic, from the wireless device to the network until the user is properly authenticated. An analogy is having a chain on your front door that enables you to open the door slightly to identify a person who knocks before you allow him to enter your house. User authentication provides a higher degree of confidence and protection than system authentication.
- B** is incorrect because Extensible Authentication Protocol (EAP) is not a specific authentication technology; instead, it provides a framework to enable many types of authentication techniques to be used during point-to-point (PPP) connections. As the name states, it extends the authentication possibilities from the norm (PAP and CHAP) to other methods such as one-time passwords, token cards, biometrics, Kerberos, and future mechanisms. So when a user connects to an authentication server and both have EAP capabilities, they can negotiate between a longer list of possible authentication methods.
- C** is incorrect because spread spectrum means that something is distributing individual signals across the allocated frequencies in

some fashion. This is used in wireless communication and is not an authentication technology. Frequency hopping spread spectrum (FHSS) takes the total amount of bandwidth (spectrum) and splits it into smaller subchannels. The sender and receiver work at one of these channels for a specific amount of time and then move to another channel. The sender puts the first piece of data on one frequency, the second on a different frequency, and so on. The FHSS algorithm determines the individual frequencies that will be used and in what order, and this is referred to as the sender's and receiver's hop sequence.

- D** is incorrect because orthogonal frequency-division multiplexing (OFDM) is a digital multicarrier modulation scheme that compacts multiple modulated carriers tightly together, reducing the required bandwidth. The modulated signals are orthogonal (perpendicular) and do not interfere with each other. OFDM uses a composite of narrow channel bands to enhance its performance in high-frequency bands. This is used in wireless communication and is not an authentication technology.

21. What type of security encryption component is missing from the table that follows?

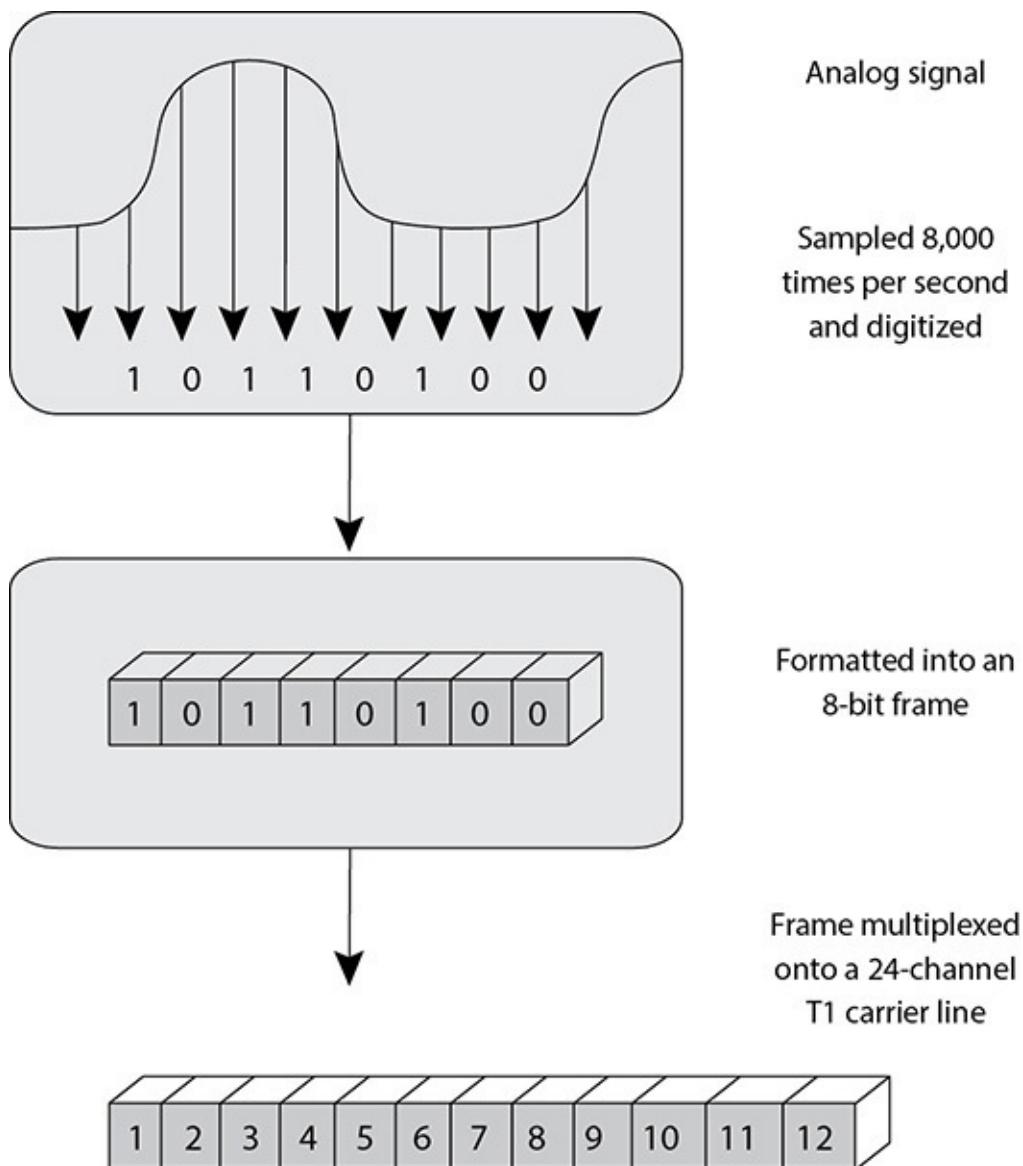
	802.1X Dynamic WEP	Wi-Fi Protected Access	Robust Security Network
Access Control	802.1X	802.1X or preshared key	802.1X or preshared key
Authentication	EAP methods	EAP methods or preshared key	EAP methods or preshared key
Encryption	WEP		CCMP (AES Counter Mode)
Integrity	None	Michael MIC	CCMP (AES CBC-MAC)

- A.** Service Set ID
 - B.** Temporal Key Integrity Protocol
 - C.** Ad hoc WLAN
 - D.** Open system authentication
- B.** The Temporal Key Integrity Protocol (TKIP) generates random values used in the encryption process, which makes it much harder for an attacker to break. To allow for an even higher level of encryption protection, the standard also includes the new Advanced Encryption Standard (AES) algorithm to be used in new WLAN implementations. TKIP actually works with the Wired Equivalent Privacy (WEP) protocol by feeding it keying material, which is data to be used for generating new dynamic keys. WEP uses the RC4

encryption algorithm, and the current implementation of the algorithm provides very little protection. More complexity is added to the key generation process with the use of TKIP, which makes it much more difficult for attackers to uncover the encryption keys. The IEEE working group developed TKIP so that customers would only need to obtain firmware or software updates instead of purchasing new equipment for this type of protection.

- A** is incorrect because when wireless devices work in infrastructure mode, the access point (AP) and wireless clients form a group referred to as a Basic Service Set (BSS). This group is assigned a name, which is the Service Set ID (SSID) value. This value has nothing to do with encryption. Any hosts that wish to participate within a particular WLAN must be configured with the proper SSID. Various hosts can be segmented into different WLANs by using different SSIDs. The reasons to segment a WLAN into portions are the same reasons wired systems are segmented on a network: the users require access to different resources, have different business functions, or have different levels of trust.
- C** is incorrect because an ad hoc WLAN has nothing to do with encryption, but rather with how wireless devices on a network are set up. An ad hoc WLAN has no access points; the wireless devices communicate with each other through their wireless NICs instead of going through a centralized device. To construct an ad hoc network, wireless client software is installed on contributing hosts and configured for peer-to-peer operation mode.
- D** is incorrect because open system authentication (OSA) just means a wireless device does not need to prove it has a specific cryptographic key for authentication. Depending upon the product and the configuration, a network administrator can also limit access to specific MAC addresses. OSA does not require the wireless device to prove to an access point it has a specific cryptographic key to allow for authentication purposes. In many cases, the wireless device needs to provide only the correct SSID value. In OSA implementations, all transactions are in cleartext because no encryption is involved. So an intruder can sniff the traffic, capture the necessary steps of authentication, and walk through the same steps to be authenticated and associated to an AP.

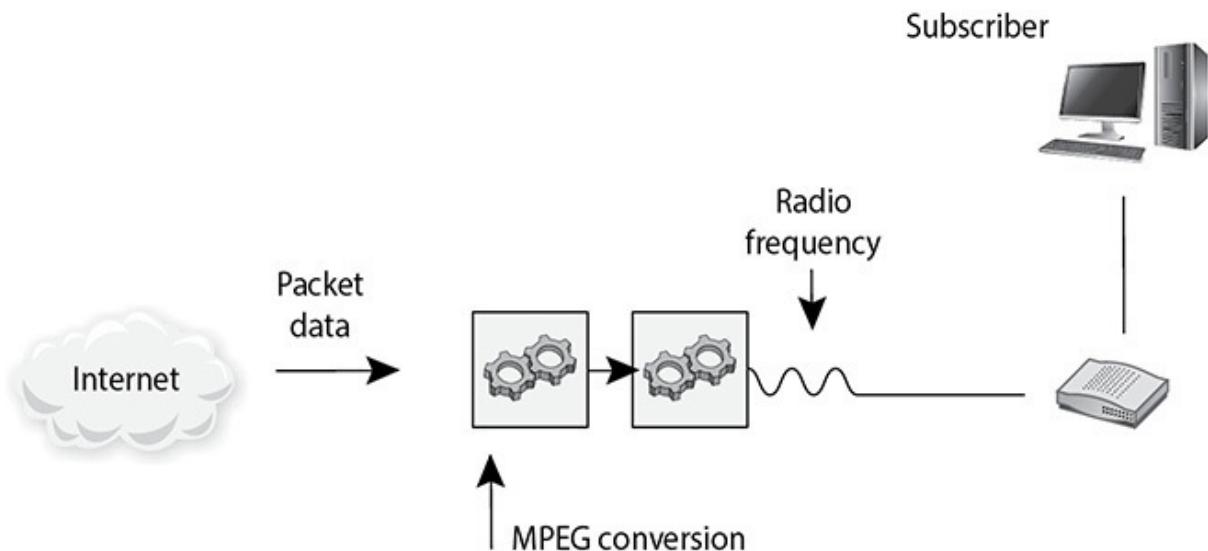
22. What type of technology is represented in the graphic that follows?



- A. Asynchronous Transfer Mode
 - B. Synchronous Optical Networks
 - C. Frequency-division multiplexing
 - D. Multiplexing
- D. Multiplexing is a method of combining multiple channels of data over a single transmission path. The transmission is so fast and efficient that the ends do not realize they are sharing a line with many other entities. The systems “think” they have the line all to themselves. Telephone systems have been around for about 100 years, and they started as copper-based analog systems. Central switching offices connected individual telephones manually (via human operators) at first, and later by using electronic switching equipment. After two telephones were connected, they had an end-

to-end connection, or an end-to-end circuit. Multiple phone calls were divided up and placed on the same wire, which is multiplexing.

- A is incorrect because Asynchronous Transfer Mode (ATM) is a high-speed network technology that is used in LAN and WAN implementations by carriers, ISPs, and telephone companies. This technology is not what is shown in the graphic. ATM encapsulates data in fixed cells and can be used to deliver data over the Synchronous Optical Networks (SONET) network. The analogy of a highway and cars is used to describe the SONET and ATM relationship. SONET is the highway that provides the foundation (or network) for the cars—the ATM packets—to travel on.
 - B is incorrect because Synchronous Optical Networks (SONET) is actually a standard for telecommunications transmissions over fiber-optic cables. Carriers and telephone companies have deployed SONET networks for North America, and if they follow the SONET standards properly, these various networks can communicate with little difficulty. A metropolitan area network (MAN) is usually a backbone that connects LANs to each other and LANs to WANs, the Internet, and telecommunications and cable networks. A majority of today's MANs are SONET or FDDI rings provided by the telecommunications service providers.
 - C is incorrect because frequency-division multiplexing is a form of signal multiplexing that involves assigning nonoverlapping frequency ranges to different signals or to each “user” of a medium. This is a type of multiplexing, but works over wireless signal spectrums instead of a time-based approach shown in the graphic. It can also be used to combine multiple signals before final modulation onto a carrier signal. In this case the carrier signals are referred to as subcarriers; each frequency within the spectrum is used as a channel to move data. An example is a stereo FM transmission.
23. What type of telecommunication technology is illustrated in the graphic that follows?



- A.** Digital Subscriber Line
 - B.** Integrated Services Digital Network
 - C.** BRI ISDN
 - D.** Cable modem
- D.** The cable television companies have been delivering television services to homes for years, and then they started delivering data transmission services for users who have cable modems and want to connect to the Internet at high speeds. Cable modems provide high-speed access, up to 50 Mbps, to the Internet through existing cable coaxial and fiber lines. The cable modem provides upstream and downstream conversions. Not all cable companies provide Internet access as a service, mainly because they have not upgraded their infrastructure to move from a one-way network to a two-way network. Once this conversion takes place, data can come down from a central point (referred to as the head) to a residential home and back up to the head and onto the Internet.
- A** is incorrect because Digital Subscriber Line (DSL) is another type of high-speed connection technology used to connect a home or business to the service provider's central office. It uses existing phone lines and provides a 24-hour connection to the Internet. This does indeed sound better than sliced bread, but only certain people can get this service because you have to be within a 2.5-mile radius of the DSL service provider's equipment. As the distance between a residence and the central office increases, the transmission rates for DSL decrease. DSL does not go through the cable TV lines and does not have to go through the conversion from analog to digital and back as illustrated in the graphic. DSL is a broadband

technology that can provide up to a 52 Mbps transmission speed without replacing the carrier's copper wire.

- B** is incorrect because Integrated Services Digital Network (ISDN) is a communications protocol provided by telephone companies and ISPs that does not need to go through the conversion process shown in the graphic. This protocol and the necessary equipment enable data, voice, and other types of traffic to travel over a medium in a digital manner previously used only for analog voice transmission. Telephone companies went all digital many years ago, except for the local loops, which consist of the copper wires that connect houses and businesses to their carrier provider's central offices. These central offices contain the telephone company's switching equipment, and it is here the analog-to-digital transformation takes place.
- C** is incorrect because ISDN breaks the telephone line into different channels and transmits data in a digital form rather than the old analog form. ISDN provides two basic home and business services: Basic Rate Interface (BRI) and Primary Rate Interface (PRI). BRI has two B channels that enable data to be transferred and one D channel that provides for call setup, connection management, error control, caller ID, and more. The bandwidth available with BRI is 144 Kbps, whereas the top modems can provide only 56 Kbps. The BRI service is common for residential use, and the PRI, which has 23 B channels and one D channel, is more commonly used in corporations.

- 24.** Which type of WAN tunneling protocol is missing from the right table in the graphic that follows?

PPTP	
Internet Must Be IP Based	Internet Can Be IP Frame Relay, x.25, or ATM Based
No Header Compression	Header Compression
No Tunnel Authentication	Tunnel Authentication
Built-In PPP Encryption	Uses IPSec Encryption



Client



Server

- A. IPSec
 - B. FDDI
 - C. L2TP
 - D. CSMA/CD
- C. Tunneling is the main ingredient to a VPN because that is how the VPN creates its connection. Three main tunneling protocols are used in VPN connections: PPTP, L2TP, and IPSec. L2TP provides the functionality of the Point-to-Point Tunneling Protocol (PPTP), but it can work over networks other than just IP, and it provides a higher level of security when combined with IPSec. L2TP does not provide any encryption or authentication services, so it needs to be combined with IPSec if those services are required. The processes that L2TP uses for encapsulation are similar to those used by PPTP. The PPP frame is encapsulated with L2TP. One limitation of PPTP is that it can work only over IP networks, so other protocols must be used to move data over frame relay, X.25, and ATM links.
- A is incorrect because the Internet Protocol Security (IPSec) protocol suite provides a method of setting up a secure channel for protected data exchange between two devices. The devices that

share this secure channel can be two servers, two routers, a workstation and a server, or two gateways between different networks. IPSec is a widely accepted standard for providing network layer protection. IPSec is commonly used with L2TP to provide protection for the data that travels over this type of communication path as shown in the graphic.

- B** is incorrect because Fiber Distributed Data Interface (FDDI) technology is a high-speed token-passing media access technology. FDDI has a data transmission speed of up to 100 Mbps and is usually used as a backbone network using fiber-optic cabling. FDDI also provides fault tolerance by offering a second counter-rotating fiber ring. The primary ring has data traveling clockwise and is used for regular data transmission. The second ring transmits data in a counterclockwise fashion and is invoked only if the primary ring goes down. Sensors watch the primary ring and, if it goes down, invoke a ring wrap so that the data will be diverted to the second ring. Each node on the FDDI network has relays that are connected to both rings, so if a break in the ring occurs, the two rings can be joined. L2TP is used for WAN connections, while FDDI is commonly used for MAN connections.
 - D** is incorrect because carrier sense multiple access with collision detection (CSMA/CD) is a network access method in which a carrier sensing scheme is used. A transmission is called a carrier, so if a computer is transmitting frames, it is performing a carrier activity. When computers use the CSMA/CD protocol, they monitor the transmission activity, or carrier activity, on the wire so they can determine when would be the best time to transmit data. Each node monitors the wire continuously and waits until the wire is free before it transmits its data. As an analogy, consider several people gathered in a group talking here and there about this and that. If a person wants to talk, she usually listens to the current conversation and waits for a break before she proceeds to talk. If she does not wait for the first person to stop talking, she will be speaking at the same time as the other person, and the people around them may not be able to understand fully what each is trying to say.
25. IPv6 has many new and different characteristics and functionality compared to IPv4. Which of the following is an incorrect functionality or characteristic of IPv6?
- i. IPv6 allows for nonscoped addresses, which enables an administrator to restrict specific addresses for specific servers or

file and print sharing, for example.

- ii. IPv6 has IPSec integrated into the protocol stack, which provides application-based secure transmission and authentication.
 - iii. IPv6 has more flexibility and routing capabilities compared to IPv4 and allows for Quality of Service (QoS) priority values to be assigned to time-sensitive transmissions.
 - iv. The protocol offers autoconfiguration, which makes administration much easier compared to IPv4, and it does not require network address translation (NAT) to extend its address space.
- A. i, iii
- B. i, ii
- C. ii, iii
- D. ii, iv

- B.** IPv6 allows for scoped addresses, which enables an administrator to restrict specific addresses for specific servers or file and print sharing, for example. IPv6 has IPSec integrated into the protocol stack, which provides end-to-end secure transmission and authentication.
- A** is incorrect. IPv6 allows for scoped addresses, which enables an administrator to restrict specific addresses for specific servers or file and print sharing, for example. IPv6 has more flexibility and routing capabilities and allows for Quality of Service (QoS) priority values to be assigned to time-sensitive transmissions.
- C** is incorrect. IPv6 has more flexibility and routing capabilities and allows for QoS priority values to be assigned to time-sensitive transmissions. IPv6 has IPSec integrated into the protocol stack, which provides end-to-end secure transmission and authentication.
- D** is incorrect because IPv6 has IPSec integrated into the protocol stack, which provides end-to-end secure transmission and authentication. The protocol offers autoconfiguration, which makes administration much easier, and it does not require network address translation (NAT) to extend its address space.

- 26.** Hanna is a new security manager for a computer consulting company. She has found out that the company has lost intellectual property in the past because malicious employees installed rogue devices on the network, which were used to capture sensitive traffic. Hanna needs to implement a solution that ensures only authorized devices are allowed

access to the company network. Which of the following IEEE standards was developed for this type of protection?

- A. IEEE 802.1AR
- B. IEEE 802.1AE
- C. IEEE 802.1AF
- D. IEEE 802.1XR

- A. The IEEE 802.1AR standard specifies unique per-device identifiers (DevID) and the management and cryptographic binding of a device (router, switch, access point) to its identifiers. A verifiable unique device identity allows establishment of the trustworthiness of devices; thus, it facilitates secure device provisioning. A secure device identifier (DevID) is cryptographically bound to a device and supports authentication of the device's identity. Locally significant identities can be securely associated with an initial manufacturer-provisioned DevID and used in provisioning and authentication protocols to allow a network administrator to establish the trustworthiness of a device and select appropriate policies for transmission and reception of data and control protocols to and from the device.
- B is incorrect because 802.1AE is the IEEE MAC Security standard (MACSec), which defines a security infrastructure to provide data confidentiality, data integrity, and data origin authentication. Where a VPN connection provides protection at the higher networking layers, MACSec provides hop-by-hop protection at layer 2.
- C is incorrect because 802.1AR provides a unique ID for a device. 802.1AE provides data encryption, integrity, and origin authentication functionality. 802.1AF carries out key agreement functions for the session keys used for data encryption. Each of these standards provides specific parameters to work within an 802.1X EAP-TLS framework.
- D is incorrect because this is a distracter answer. This is not a valid standard.

27. _____ is a set of extensions to DNS that provides to DNS clients (resolvers) origin authentication of DNS data to reduce the threat of DNS poisoning, spoofing, and similar attack types.

- A. Resource records
- B. Zone transfer

C. DNSSEC

D. Resource transfer

- C.** DNSSEC is a set of extensions to DNS that provides to DNS clients (resolvers) origin authentication of DNS data to reduce the threat of DNS poisoning, spoofing, and similar attack types.
DNSSEC is a suite of Internet Engineering Task Force (IETF) specifications for securing services provided by the DNS as used on IP networks.
- A** is incorrect because a DNS server contains records that map hostnames to IP addresses, which are referred to as resource records. When a user's computer needs to resolve a hostname to an IP address, it looks to its networking settings to find its DNS server. The computer then sends a request containing the hostname to the DNS server for resolution. The DNS server looks at its resource records and finds the record with this particular hostname, retrieves the address, and replies to the computer with the corresponding IP address.
- B** is incorrect because primary and secondary DNS servers synchronize their information through a zone transfer. After changes take place to the primary DNS server, those changes must be replicated to the secondary DNS server. It is important to configure the DNS server to allow zone transfers to take place only between the specific servers.
- D** is incorrect because it is a distracter answer.

28. Which of the following best describes the difference between a virtual firewall that works in bridge mode versus one that is embedded into a hypervisor?

- A.** Bridge-mode virtual firewall allows the firewall to monitor individual traffic links, and hypervisor integration allows the firewall to monitor all activities taking place within a host system.
- B.** Bridge-mode virtual firewall allows the firewall to monitor individual network links, and hypervisor integration allows the firewall to monitor all activities taking place within a guest system.
- C.** Bridge-mode virtual firewall allows the firewall to monitor individual traffic links, and hypervisor integration allows the firewall to monitor all activities taking place within a guest system.
- D.** Bridge-mode virtual firewall allows the firewall to monitor

individual guest systems, and hypervisor integration allows the firewall to monitor all activities taking place within a network system.

- A.** Virtual firewalls can be bridge-mode products, which monitor individual traffic links between virtual machines, or they can be integrated within the hypervisor of a virtualized environment. The hypervisor is the software component that carries out virtual machine management and oversees guest system software execution. If the firewall is embedded within the hypervisor, then it can “see” and monitor all the activities taking place within the host system.
 - B** is incorrect because bridge-mode virtual firewall allows the firewall to monitor individual traffic links between hosts, not network links. Hypervisor integration allows the firewall to monitor all activities taking place within a host system, not a guest system.
 - C** is incorrect because bridge-mode virtual firewall allows the firewall to monitor individual traffic links, and hypervisor integration allows the firewall to monitor all activities taking place within a host system, not a guest system. The hypervisor is the software component that carries out virtual machine management and oversees guest system software execution. If the firewall is embedded within the hypervisor, then it can “see” and monitor all the activities taking place within the system.
 - D** is incorrect because a bridge-mode virtual firewall allows the firewall to monitor individual traffic between guest systems, and hypervisor integration allows the firewall to monitor all activities taking place within a host system, not a network system.
- 29.** Which of the following does software-defined networking (SDN) technology specify?
- A.** The mapping between MAC addresses and IP addresses in software
 - B.** The end nodes’ static routing tables in a dynamic way
 - C.** How routers communicate their routing tables to each other as events occur
 - D.** How routers move packets based on a centrally managed controller’s instructions
- D.** Software-defined networking (SDN) is intended to decouple the router’s logical function of making routing decisions and its

mechanical function of passing data between interfaces, and to make routing decisions more centrally manageable. The SDN architecture is intended to be a standards-based way of providing control logic to routers' data planes in a scalable, programmable way.

- A** is incorrect because the mapping between Media Access Control (MAC) addresses and Internet Protocol (IP) addresses is provided by the Address Resolution Protocol (ARP). This is what allows encapsulation of OSI layer 3 packets into suitable OSI layer 2 frames for processing by switches, hubs, and wireless access points.
 - B** is incorrect because the static routing tables that most end nodes are configured with are either hard-coded by system administrators (typical in the case of servers) or provided via the Dynamic Host Configuration Protocol (DHCP) for desktop and mobile systems.
 - C** is incorrect because traditional routing table configuration exchange between routing devices is most often communicated via either a distance-vector routing protocol such as the Routing Information Protocol (RIP) or a link-state routing protocol such as Open Shortest Path First (OSPF). In these cases the routers share information between themselves within a routing domain, and then make their decisions as to how to pass packets based on internal logic.
- 30.** Determining the geographic location of a client IP address in order to route it toward the most proximal topological source of web content is an example of what technology?
- A.** Content distribution network (CDN)
 - B.** Distributed name service (DNS)
 - C.** Distributed web service (DWS)
 - D.** Content domain distribution (CDD)
- A.** Content distribution networks (CDNs) are designed to optimize the delivery of content, primarily via the Hypertext Transfer Protocol (HTTP), to clients based on their global topological position. In such a design, multiple web servers hosted at many points of presence on the Internet contain the same content in a globally synchronized manner, and so clients can be directed to the nearest source, typically via the manipulation of DNS records based on geolocation algorithms for the requester's IP address.

- B** is incorrect because distributed name service is a distracter answer, in that no such protocol exists. DNS properly refers to the Domain Name Service protocol, which is most often used in CDNs in order to direct clients to the server most geographically proximal to them for the content requested.
 - C** is incorrect because distributed web service is also a distracter answer. The concept of a distributed web service discovery architecture has been discussed by the IEEE and others, but is not a formal protocol. Its goals are orthogonal to the idea of efficient content delivery.
 - D** is incorrect because content domain distribution is provided as a distracter answer to ensure that the CISSP candidate can distinguish between concepts and generally accepted acronyms. There is no such thing as CDD in this context.
- 31.** Which of the following protocols or set of protocols is used in Voice over IP (VoIP) for caller identification?
- A.** Real-time Transport Protocol (RTP) and/or Secure Real-time Transport Protocol (SRTP)
 - B.** Real-time Transport Protocol (RTP) and Real-time Transport Control Protocol (RTCP)
 - C.** Session Initiation Protocol (SIP)
 - D.** Public Switched Telephony/Phone Branch Exchange (PSTN/PBX)
- C.** The Session Initiation Protocol is commonly used for all VoIP transactions except the actual media exchange between calling or receiving stations. This includes caller identification and location, call setup and teardown, etc. It is brokered by a mutually trusted third-party system that contains registration information for each station/user.
 - A** is incorrect because RTP/SRTP are the protocols commonly used between end nodes for direct media interaction. While the call negotiation is commonly accomplished via SIP or even H.323 (archaically) using a location server, the media exchange is typically point-to-point via these protocols.
 - B** is incorrect because as explained for answer A, RTP is a media transport protocol, not a negotiation protocol. RTCP is a further distracter, as it is a protocol for monitoring the performance of VoIP networking, measuring and reporting on such aspects as latency and

jitter.

- D** is incorrect because while PSTN/PBX technologies are important to VoIP networking, they are not central to caller identification in the way that SIP is. Rather, such an acronym typically refers to a way of building an interface between a VoIP network and publicly addressable phone numbers.
- 32.** Encryption can happen at different layers of an operating system and network stack. Where does PPTP encryption take place?
 - A.** Data link layer
 - B.** Within applications
 - C.** Transport layer
 - D.** Data link and physical layers
- A.** The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks (VPNs). It is a Microsoft-proprietary VPN protocol that works at the data link layer of the OSI model. PPTP can only provide a single connection and can only work over PPP connections.
- B** is incorrect because end-to-end encryption takes place within the applications. End-to-end encryption means that only the data payload is encrypted. If encryption works at any layer of the OSI model, then headers and trailers can also be encrypted. Since PPTP works at the data link layer, headers and trailers from the upper layers can be encrypted and protected along with the data payload.
- C** is incorrect because SSL is an example of an encryption technology that works at the transport layer, not PPTP. SSL uses public key encryption and provides data encryption, server authentication, message integrity, and optional client authentication to display secured portions of a website to a user. When HTTP runs over SSL, you have HTTP Secure (HTTPS). HTTP works at the application layer, but SSL still works at the transport layer.
- D** is incorrect because PPTP works at the data link layer, but not the physical layer. The physical layer technologies convert the bits from the data link layer into some type of transmission format. If the data transmission is taking place over a UTP connection, then the data is converted into electronic voltage at the physical layer. If data transmission is taking place over fiber lines, then the data is converted into photons. Specifications for the physical layer include

the timing of voltage changes, voltage levels, and the physical connectors for electrical, optical, and mechanical transmission.

- 33.** Which of the following INCORRECTLY describes IP spoofing and session hijacking?
- A. Address spoofing helps an attacker to hijack sessions between two users without being noticed.
 - B. IP spoofing makes it harder to track down an attacker.
 - C. Session hijacking can be prevented with mutual authentication.
 - D. IP spoofing is used to hijack SSL and IPSec secure communications.
- D.** Secure Sockets Layer (SSL) and IPSec can protect the integrity, authenticity, and confidentiality of network traffic. Even if an attacker spoofed an IP address, he would not be able to successfully manipulate or read SSL- or IPSec-encrypted traffic, as he would not have access to the keys and other cryptographic material required.
- A** is incorrect because the statement is true. Address spoofing helps an attacker to hijack sessions between two users without being noticed. If an attacker wanted to take over a session between two computers, she would need to put herself in the middle of their conversation without being detected. Tools like Juggernaut and the HUNT Project enable the attacker to spy on the TCP connection and then hijack it.
- B** is incorrect because the statement is true. Spoofing is the presentation of false information, usually within packets, to trick other systems and hide the origin of the message. This is usually done by hackers so that their identity cannot be successfully uncovered.
- C** is incorrect because the statement is true. If session hijacking is a concern on a network, the administrator can implement a protocol, such as IPSec or Kerberos, that requires mutual authentication between users or systems.
- 34.** A small medical institution's IT security team has become overwhelmed with having to operate and maintain IDSSs, firewalls, enterprise-wide antimalware solutions, data leak prevention technologies, and centralized log management. Which of the following best describes what type of solution this organization should implement to allow for standardized and streamlined security operations?

- A.** Unified threat management
 - B.** Continuous monitoring technology
 - C.** Centralized access control systems
 - D.** Cloud-based security solution
- A.** It has become very challenging to manage the long laundry list of security solutions almost every network needs to have in place. The list includes, but is not limited to, firewalls, antimalware, antispam, IDS/IPS, content filtering, data leak prevention, VPN capabilities, and continuous monitoring and reporting. Unified threat management (UTM) appliance products have been developed that provide all (or many) of these functionalities in a single network appliance. The goals of UTM are simplicity, streamlined installation and maintenance, centralized control, and the ability to understand a network's security from a holistic point of view. Each security product vendor has its own UTM solution, but each has similar goals of allowing administrators to monitor and manage a variety of security-related applications and products through a single management console.
- B** is incorrect because continuous monitoring in the security industry most commonly refers to information security continuous monitoring (ISCM), which allows companies to obtain situational awareness, ongoing awareness of information security, vulnerabilities, and threats to support business risk management decisions. Monitoring focuses on gathering data as it pertains to the health and security posture of an environment and does not combine all of the technologies mentioned in the question. Each network device and security solution (i.e., vulnerability scanners, firewalls, IDS, IPS, etc.) generates its own logs, and it is difficult to monitor these individually in order to understand what is actually taking place within an enterprise networked environment. Monitoring can take place through manual or automated processes, but when we are specifically addressing continuous monitoring, this is usually accomplished through automation. Automated continuous monitoring technologies attempt to aggregate and correlate these diverse log types to provide a single interface and holistic understanding of the environment. Continuous monitoring technologies also carry out automated scans of critical systems instead of the time-consuming and error-prone approach of manual scans and certification and accreditation processes. The Security Content Automation Protocol (SCAP) was one of the first

specifications launched that allows different security product vendors to implement continuous monitoring capabilities in a standardized manner.

- C** is incorrect because centralized access control systems do not attempt to combine all of the security products and functions mentioned in the question. Centralized access control systems are used so that access control can be practiced in a standardized manner across various systems within a networked environment. Access control commonly encompasses identification, authentication, authorization, and accountability of the users who need to access a network's resources. The network's resources are usually provided through different system types (i.e., Windows, Unix, Linux, mainframes), and it is challenging to be able to practice access control across all of these diverse systems in a standardized and predictable manner. Centralized access control allows administrators to define and maintain access control policies across a heterogeneous environment that supports various users' access needs.
 - D** is incorrect because cloud-based security solution is a distracter answer. While there are security managed services that allow an outsourced company to manage and maintain a company's security devices and solutions, this is not considered a cloud-based solution. Cloud-based solutions provide an infrastructure environment, platform, or application to a customer so that the customer does not need to spend time and money maintaining these items themselves. Some cloud providers might provide some of these security services within their Infrastructure as a Service (IaaS) offerings, but this is not the main focus of a cloud-based solution.
- 35.** Which of the following protocols blurs the lines between the OSI model layers, performing the tasks of several at once?
- A.** Distributed Network Protocol 3 (DNP3)
 - B.** File Transfer Protocol (FTP)
 - C.** Transmission Control Protocol (TCP)
 - D.** Domain Name System (DNS)
- A.** DNP3 was designed for use in SCADA systems, which were historically configured in a flat network hierarchy, with devices serially connected to each other. As such, modern routing functionality was not required. Consequently, it behaves much like

a serial link layer protocol, but also performs the function of a transport layer protocol as well.

- B** is incorrect because FTP is a bit odd in that it uses multiple ports: one that essentially provides command and control between the client and server, and others that are used for the actual data transference. However all connections are conducted via TCP at the transport layer.
 - C** is incorrect because it is most distinctly a transport layer protocol only.
 - D** is incorrect, because although DNS uses both TCP and UDP, both are transport layer protocols.
36. Which of the following correctly describes the relationship between SSL and TLS?
- A. TLS is the open-community version of SSL.
 - B. SSL can be modified by developers to expand the protocol's capabilities.
 - C. TLS is a proprietary protocol, while SSL is an open-community protocol.
 - D. SSL is more extensible and backward compatible with TLS.
- A. Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are cryptographic protocols that are used to secure communications by encrypting segments of network connections. Both protocols work at the session layer of IPv4, though (ISC)² considers them presentation layer protocols because they provide encryption. TLS is the open-community version of SSL. Because TLS is an open-community protocol, its specifications can be modified by vendors within the community to expand what it can do and what technologies it can work with. SSL is a proprietary protocol, and TLS was developed by a standards body, making it an open-community protocol.
 - B is incorrect because SSL is a proprietary protocol developed by Netscape. This means the technology community cannot easily extend SSL to interoperate and expand in its functionality. If a protocol is proprietary in nature, as SSL is, the technology community cannot directly change its specifications and functionality. The reason that TLS was developed was to standardize how data can be transmitted securely through a protocol

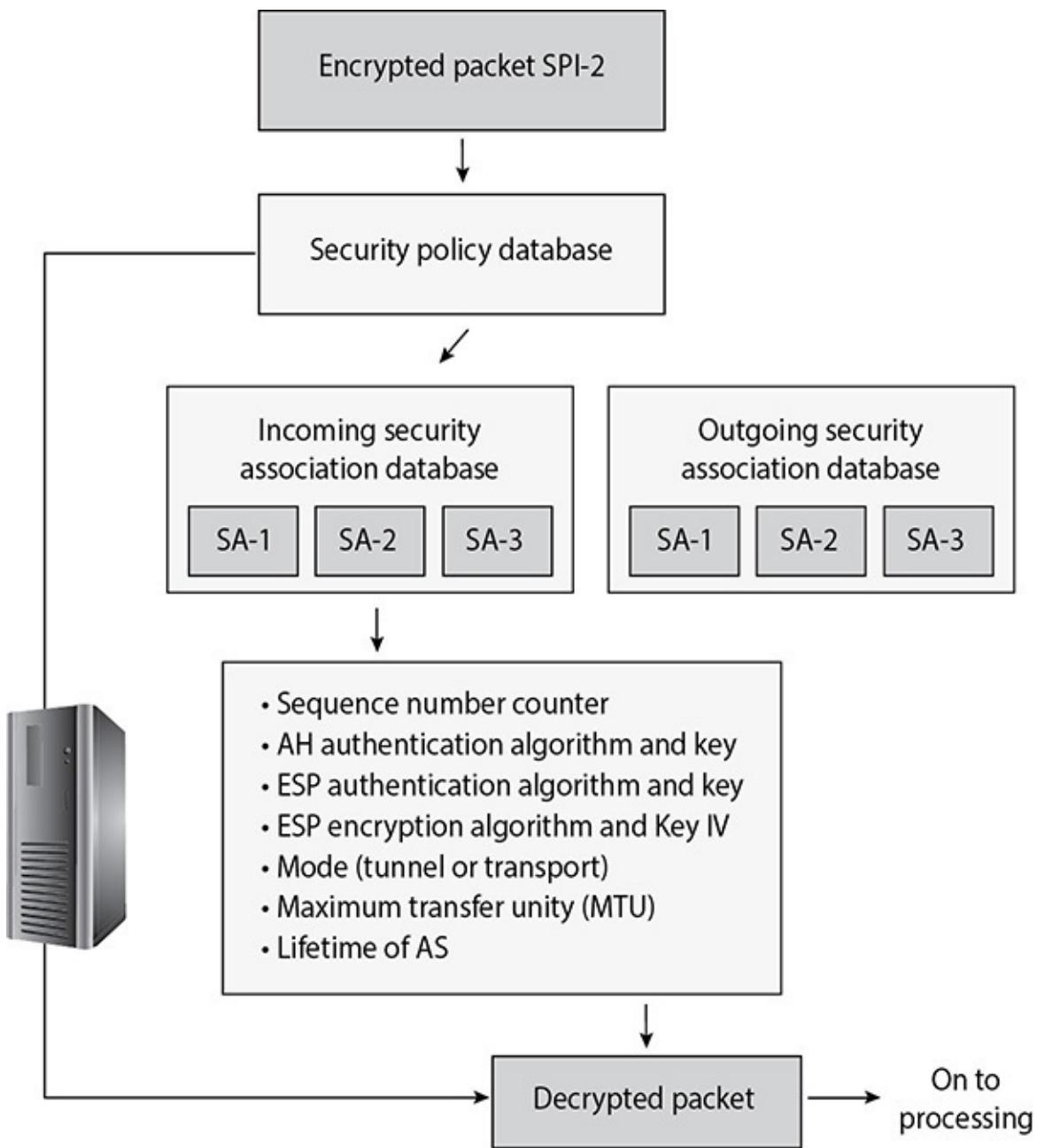
and how vendors can modify the protocol and still allow for interoperability.

- C** is incorrect because the statement is backward. TLS is not proprietary. It is the open-community version of SSL, which is proprietary.
 - D** is incorrect because TLS is actually more extensible than SSL and is not backward compatible with SSL. TLS and SSL provide the same type of functionality and are very similar, but not similar enough to work directly together. If two devices need to communicate securely, they need to be using either TLS or SSL—they cannot use a hybrid approach and still be able to communicate.
- 37.** End-to-end encryption is used by users, and link encryption is used by service providers. Which of the following correctly describes these technologies?
- A.** Link encryption does not encrypt headers and trailers.
 - B.** Link encryption encrypts everything but data link messaging.
 - C.** End-to-end encryption requires headers to be decrypted at each hop.
 - D.** End-to-end encryption encrypts all headers and trailers.
- B.** Encryption can be performed at different communication levels, each with different types of protection and implications. Two general modes of encryption implementation are link encryption and end-to-end encryption. Link encryption encrypts all the data along a specific communication path, as in a satellite link, T3 line, or telephone circuit. Not only is the user information encrypted, but the header, trailers, addresses, and routing data that are part of the packets are also encrypted. The only traffic not encrypted in this technology is the data link control messaging information, which includes instructions and parameters that the different link devices use to synchronize communication methods. Link encryption provides protection against packet sniffers and eavesdroppers. In end-to-end encryption, the headers, addresses, routing, and trailer information are not encrypted, enabling attackers to learn more about a captured packet and where it is headed. With end-to-end encryption only the data payload is encrypted.
 - A** is incorrect because link encryption does encrypt the headers and trailers. This is a major advantage to using link encryption: the headers, trailers, and data payload are encrypted except for the data link messaging. It also works seamlessly at a lower layer in the OSI

model, so users do not need to do anything to initiate it.

- C** is incorrect because the headers are not encrypted with end-to-end encryption, so there is no need to decrypt them at each hop. This is an advantage of using end-to-end encryption. Other advantages include additional flexibility for the user in choosing what gets encrypted and how, and a higher granularity of functionality because each application or user can choose specific configurations.
- D** is incorrect because end-to-end encryption does not encrypt any headers or trailers. As a result, they are not protected. This is the primary disadvantage to using end-to-end encryption. If the headers and trailers need to be protected, then link encryption should be used.

38. What do the SA values in the graphic of IPSec that follows represent?

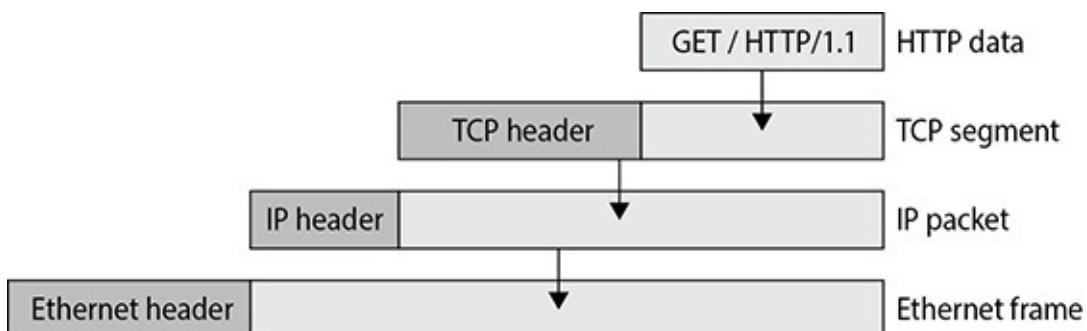


- A. Security parameter index
- B. Security ability
- C. Security association
- D. Security assistant
- C. Each IPSec VPN device will have at least one security association (SA) for each secure connection it uses. The SA, which is critical to the IPSec architecture, is a record of the configurations the device needs to support an IPSec connection over a VPN connection. When two devices complete their handshaking process, which means they have agreed upon a long list of parameters they

will use to communicate, these data must be recorded and stored somewhere, which is in the SA. The SA can contain the authentication and encryption keys, the agreed-upon algorithms, the key lifetime, the source IP address, and other information. When a device receives a packet via the IPSec protocol, it is the SA that tells the device what to do with the packet. So if device B receives a packet from device C via IPSec, device B will look to the corresponding SA to tell it how to decrypt the packet, how to properly authenticate the source of the packet, which key to use, and how to reply to the message if necessary.

- A** is incorrect because a security parameter index (SPI) keeps track of the different SAs. SAs are directional, so a device will have one SA for outbound traffic and a different SA for inbound traffic for each individual communication channel. If a device is connecting to three devices, it will have at least six SAs, one for each inbound or outbound connection per remote device. So how can a device keep all of these SAs organized and ensure that the right SA is invoked for the right connection? With the SPI, that's how. Each device has an SPI that keeps track of the different SAs and tells the device which one is appropriate to invoke for the different packets it receives.
- B** is incorrect because there is no component within IPSec officially referred to as security ability. This is a distracter answer.
- D** is incorrect because there is no component within IPSec officially referred to as security assistant. This is a distracter answer.

39. What is the process depicted in the illustration below referred to as?



- A.** TCP/IP model
- B.** Layering
- C.** Encapsulation
- D.** OSI model

- C.** The illustration depicts data moving down the layers of the stack of the TCP/IP model. Application layer data becomes the payload of a TCP segment, by prepending the TCP protocol data to it as a header. The TCP segment becomes an IP packet by prepending the IP protocol data to it as a header. The IP packet becomes an Ethernet frame by prepending the Ethernet protocol data to it as a header. (Also a small footer is attached at this layer, not depicted.) This is referred to as encapsulation.
 - A** is incorrect because, although the illustration shows the use of the TCP/IP model, the process depicted of its use is encapsulation.
 - B** is incorrect because, although layering is depicted as well, the downward processing of data passing through the layers is encapsulation.
 - D** is incorrect because the model in use in the illustration is the four-layer TCP/IP model, not the seven-layer OSI model.
- 40.** Which of the following is a purpose of the transport layer?
- A.** The hop-by-hop delivery of packets from one network to another
 - B.** Representing data in a structure that can be understood by processes at the endpoints
 - C.** Encapsulating the IP packet for transport
 - D.** Ensuring reliable data transfer
- D.** TCP, at the transport layer, provides for reliable data segment delivery, sequencing, and flow control, among other assurances.
 - A** is incorrect because the hop-by-hop delivery of packets between networks is the responsibility of the IP protocol.
 - B** is incorrect because managing the data structures passed between applications on the endpoints is the job of the presentation layer.
 - C** is incorrect because IP packets encapsulate TCP segments, not the other way around.
- 41.** Which of the following statements is NOT true about the IPv4 address 192.168.10.129\25?
- A.** It is an RFC 1918–specified private address.
 - B.** The netmask for this address is 255.255.255.0.
 - C.** The network address for the network it specifies is 192.168.10.128\25.

- D.** The host portion of this 32-bit address is the low-order 7 bits.
- B.** The \25 classless interdomain routing (CIDR) notation for this address indicates that the high-order (leftmost) 25 bits comprise the network portion, and the remaining low-order (rightmost) 7 bits are the host portion. In binary, the netmask representation would look like: 11111111 11111111 11111111 10000000. The “dotted quad” decimal notation of this netmask would then be 255.255.255.128.
- A** is incorrect because it is a true statement, as the address is within the 192.168.0.0\16 range specified by RFC 1918 as reserved for private use.
- C** is incorrect because it is a true statement, as the network address is the address where the host portion is all 0's. In binary the last byte would be 10000000, which is 128 in decimal.
- D** is incorrect because it is a true statement, as the host portion of this 32-bit address is the low-order 7 bits.
- 42.** Which of the following statements describes a “converged” protocol?
- A.** It is a term used to describe a situation where two otherwise independent protocols—often functioning at the same layer—become one, as with Fibre Channel (FC) over Ethernet (FCoE).
- B.** It is any situation where one protocol is encapsulated with another, as with TCP inside of IP (TCP/IP).
- C.** It refers to when two protocols at the same layer begin to do essentially the same thing, such as HTTP and HTTPS.
- D.** It is any situation where a protocol is encapsulated within another protocol in a way that bends or breaks the OSI model, as IPv6 over generic routing encapsulation (GRE) over IPv4.
- A.** FCoE, in allowing older Fibre Channel frames to ride over Ethernet frames, is an example of a converged protocol, as they are otherwise both data link protocols.
- B** is incorrect, as it merely describes encapsulation, not convergence. Convergence is a form of encapsulation that blurs the lines of the layering model.
- C** is incorrect because a “converged” protocol does not refer to when two protocols at the same layer begin to do essentially the same thing. The specific example of HTTP and HTTPS is not a convergent situation, but rather the use of HTTP semantics either layered over SSL/TLS or not.

- D** is incorrect because a “converged” protocol does not refer to any situation where a protocol is encapsulated within another in a way that bends or breaks the OSI model. The specific example of layering IPv6 over GRE over IPv4 bends our OSI model, but it is an example of tunneling, not convergence.
43. Ethernet uses a shared medium for all stations on a LAN to communicate, and uses a carrier sense multiple access with collision detection (CSMA/CD) approach to managing communications between stations. Which of the following statements about this protocol best explains how it works?
- A. A control frame is passed from station to station, granting permission for that station to transmit once it is received.
 - B. Each station is required to monitor the medium for transmissions and only transmit when all other stations are silent. Each station is also responsible for alerting all other stations if it observes more than one station transmitting at the same time.
 - C. Each station is required to monitor the medium for transmissions and only transmit when all other stations are silent. Each station is also responsible for signaling its intent to transmit before doing so.
 - D. A primary station is responsible for determining which of the other stations is due to transmit, by polling each of them at regular intervals to determine which station has data to transmit.
- B.** Each of the answers above describe methods for sharing a communications medium and managing collisions. With CSMA/CD, each station senses for whether another station is already transmitting before beginning to do so, but also senses whether a collision has occurred, and notifying all other stations that they need to back off before trying again.
 - A** is incorrect because it describes token passing rather than any form of CSMA.
 - C** is incorrect because, while it describes a “carrier sense multiple access” approach, it further describes “collision avoidance” or CSMA/CA. In this scheme, each station announces that it will transmit, notifying all other stations that they will have to wait. Once the transmitting station senses that the medium is quiet, it can transmit.
 - D** is incorrect because it describes a polling scheme with primary

and secondary stations, in which collisions are managed by the primary station alone.

- 44.** Within the realm of network components, what are “endpoints” and why do they pose such difficult security challenges?
- A. Endpoints are the client systems on a network. Because they establish connections to both internal and external servers, their activities can be difficult to monitor and control, and downloads of malicious software into the environment are commonplace.
 - B. Endpoints are the servers to which all the clients connect for authentication, file sharing, and other services. Due to the high volume of connections they support, it can be difficult to monitor and detect malicious activity directed at them, buried among the normal activities.
 - C. Endpoints are everything except the network communication devices, including desktops, servers, mobile devices, and other embedded systems. The management challenges they pose include intermittent connectivity, lack of management infrastructure for some platforms, and the unavailability of software updates for others.
 - D. Endpoints are primarily desktop and mobile systems, which may or may not exist statically on the network. As a result, keeping track of them in order to maintain up-to-date patching and proper configuration can be difficult.
- C. A network “endpoint” is anything and everything that is not an infrastructure device. In an Active Directory environment, both desktops and servers may have a robust management and patching regime. However, other endpoints include printers, mobile devices, point of sale (POS) systems, Internet of Things (IoT) devices, and industrial control system (ICS) devices like heating, ventilation, and air conditioning (HVAC) controllers. For many of these platforms, there may simply be no enterprise-scale management infrastructure available, and patching against known vulnerabilities may not be possible.
- A is incorrect because endpoints encompass more than client systems, as described in the preceding explanation. Further, while monitoring for client retrieval of malware can be difficult, it is within the realm of manageability.
- B is incorrect because endpoints encompass more than servers, as

described in the explanation of the correct answer. Further, systems and software designed for monitoring malicious activity directed at server-side devices are fairly mature and capable and can handle high volumes of connections.

- D** is incorrect because, again, endpoints encompass more than desktop or mobile client systems, and include an array of systems for which management platforms and patching systems may not even exist.
- 45.** Which of the following describes the best use of Network Access Control (NAC)?
 - A.** The use of IEEE 802.1X Extensible Authentication Protocol (EAP) to authenticate endpoints prior to allowing them to join a network
 - B.** The combined use of a public key infrastructure (PKI) and a hardware Trusted Platform Module (TPM) to conduct certificate-based endpoint authentication and establish a secure link through symmetric key exchange
 - C.** The combination of EAP for endpoint authentication and multifactor user authentication for highly granular control
 - D.** The use of EAP both for endpoint authentication and for inspection of endpoint OS patch levels and antimalware updates, with the goal of placing untrusted systems into a quarantined VLAN segment
- D.** NAC can and should use some form of EAP for endpoint authentication, but the common best use of it is to enable an authenticated system to be inspected as to its security posture. If the system is behind in its patch level or antimalware updates, or is generally misconfigured, it should be placed into a VLAN that gives it access only to the systems providing the necessary updates and configuration management. Once the system meets policy requirements, it can then be reassigned to the appropriate protected LAN segment.
- A** is incorrect because it doesn't go far enough. As just explained, EAP should also be used to control the access granted to an authenticated node.
- B** is incorrect because, as above, it doesn't go far enough. Authenticated systems should be examined as to the compliance of their configurations before being allowed access to protected networks.

- C** is incorrect because, while multifactor user authentication is a good idea, it is not relevant to NAC, which is oriented to the system itself, not the user logged into it.
- 46.** What is the greatest weakness, and hence concern, with virtualized networks?
 - A.** Because network interface cards (NICs) are virtualized (vNICs), the data traveling between them is merely copied from one memory location to another by the hypervisor layer on a single physical host.
 - B.** The absence of a physical network makes it impossible to deploy firewalls or intrusion detection systems to regulate and monitor traffic between the virtual systems.
 - C.** Virtual networks are essentially clouds with no well-defined topologies. This makes the network paths between virtual systems impossible to know.
 - D.** Virtual NICs have much higher throughputs than physical ones. As a result, modern network-based intrusion detection systems (NIDSs) cannot inspect their traffic at real-time speeds.
- A.** Virtualized networking means that data transmission does not cross a physical link, but is merely a memory operation within a single host upon which all the virtual systems reside. Consequently, a single compromise of the hypervisor can essentially result in a compromise of the entirety of the virtual network it provides.
- B** is incorrect because virtual firewalls and intrusion detection systems can be deployed, although they can only regulate and monitor the virtual links between the systems in the hypervisor. However, if the hypervisor itself is compromised, they can still be circumvented.
- C** is incorrect because virtual networks can and do have well-defined topologies, with the virtual paths between the virtual systems architected toward a known and defensible infrastructure. Yet they still depend on the security of the hypervisor within which they are constructed.
- D** is incorrect. While it is true that the throughput of a virtual link between systems is software-defined, and limited to CPU and memory speeds rather than the speeds of physical NIC interfaces, so are the capabilities of the virtual monitoring devices deployed.

Identity and Access Management

This domain includes questions from the following topics:

- Identification methods and technologies
 - Authentication methods, models, and technologies
 - Discretionary, mandatory, and nondiscretionary models
 - Accountability, monitoring, and auditing practices
 - Registration and proof of identity
 - Identity as a Service
 - Threats to access control practices and technologies
-
-

Controlling access to resources is a vital element of any information security program. Controlling who can access what and when helps protect information assets and company resources from unauthorized modification and disclosure. Thus, access controls address all three services in the AIC triad—availability, integrity, and confidentiality—be they technical, physical, or administrative in nature. Security professionals should understand the principles behind access controls to ensure their adequacy and proper implementation.



QUESTIONS

1. Which of the following does NOT correctly describe a directory service?
 - A. It manages objects within a directory by using namespaces.
 - B. It enforces security policy by carrying out access control and identity management functions.
 - C. It assigns namespaces to each object in databases that are based on the X.509 standard and are accessed by LDAP.
 - D. It allows an administrator to configure and manage how identification takes place within the network.
2. Hannah has been assigned the task of installing web access management (WAM) software. What is the best description for what WAM is commonly used for?

- A. Control external entities requesting access through X.500 databases
 - B. Control external entities requesting access to internal objects
 - C. Control internal entities requesting access through X.500 databases
 - D. Control internal entities requesting access to external objects
- 3. There are several types of password management approaches used by identity management systems. Which of the following reduces help-desk call volume, but is also criticized for the ease with which a hacker could gain access to multiple resources if a password is compromised?
 - A. Management password reset
 - B. Self-service password reset
 - C. Password synchronization
 - D. Assisted password reset
- 4. In the United States, federal agencies must adhere to Federal Information Processing Standard (FIPS) 201-2 “Personal Identity Verification,” which discusses technical measures of authentication for federal employees and contractors. This standard must be followed in order to ensure which of the following?
 - A. That government employees are properly cleared for the work assigned
 - B. That government employees are only allowed access to data of their clearance level
 - C. That the identity of the government employee has been appropriately verified
 - D. That the data that government employees have access to has been appropriately classified
- 5. Which of the following does NOT describe privacy-aware role-based access control?
 - A. It is an example of a discretionary access control model.
 - B. Detailed access controls indicate the type of data that users can access based on the data’s level of privacy sensitivity.
 - C. It is an extension of role-based access control.
 - D. It should be used to integrate privacy policies and access control policies.

- 6.** Security Assertion Markup Language (SAML) is an XML-based standard for exchanging authentication and authorization data between systems on different security domains. SAML allows for the sharing of authentication information, such as how authentication took place, entity attributes, and what the entity is authorized to access. SAML is most commonly used in web-based environments that require single sign-on (SSO) capability. Which of the following has a correct definition associated with the corresponding SAML component?
- A.** Two SAML assertions are used (authentication, authorization) that indicate that an SAML authority validated a specific subject.
 - B.** SAML assertions are most commonly used to allow for identity federation and distributed authorization.
 - C.** SAML binding specification describes how to embed SAML messages within the TCP and UDP protocols.
 - D.** SAML profiles define how SAML messages, assertions, and protocols are to be implemented in SSL and TLS.
- 7.** Brian has been asked to work on the virtual directory of his company's new identity management system. Which of the following best describes a virtual directory?
- A.** Meta-directory
 - B.** User attribute information stored in an HR database
 - C.** Virtual container for data from multiple sources
 - D.** A service that allows an administrator to configure and manage how identification takes place
- 8.** Which of the following accurately describes Identity as a Service (IDaaS)?
- A.** A form of single sign-on (SSO) that spans multiple entities in an enterprise
 - B.** A form of SSO that spans multiple independent enterprises
 - C.** A way to provide SSO without multiple forms of authentication
 - D.** A way to demonstrate identity without having to sign on
- 9.** Which of the following correctly describes a federated identity and its role within identity management processes?
- A.** A nonportable identity that can be used across business boundaries

- B. A portable identity that can be used across business boundaries
 - C. An identity that can be used within intranet virtual directories and identity stores
 - D. An identity specified by domain names that can be used across business boundaries
10. Security countermeasures should be transparent to users and attackers. Which of the following does NOT describe transparency?
- A. User activities are monitored and tracked without negatively affecting system performance.
 - B. User activities are monitored and tracked without the user knowing about the mechanism that is carrying this out.
 - C. Users are allowed access in a manner that does not negatively affect business processes.
 - D. Unauthorized access attempts are denied and logged without the intruder knowing about the mechanism that is carrying this out.
11. What markup language allows for the sharing of application security policies to ensure that all applications are following the same security rules?
- A. XML
 - B. SPML
 - C. XACML
 - D. GML
12. The importance of protecting audit logs generated by computers and network devices is highlighted by the fact that it is required by many of today's regulations. Which of the following does NOT explain why audit logs should be protected?
- A. If not properly protected, these logs may not be admissible during a prosecution.
 - B. Audit logs contain sensitive data and should only be accessible to a certain subset of people.
 - C. Intruders may attempt to scrub the logs to hide their activities.
 - D. The format of the logs should be unknown and unavailable to the intruder.
13. Of the following, what is the primary item that a capability table is

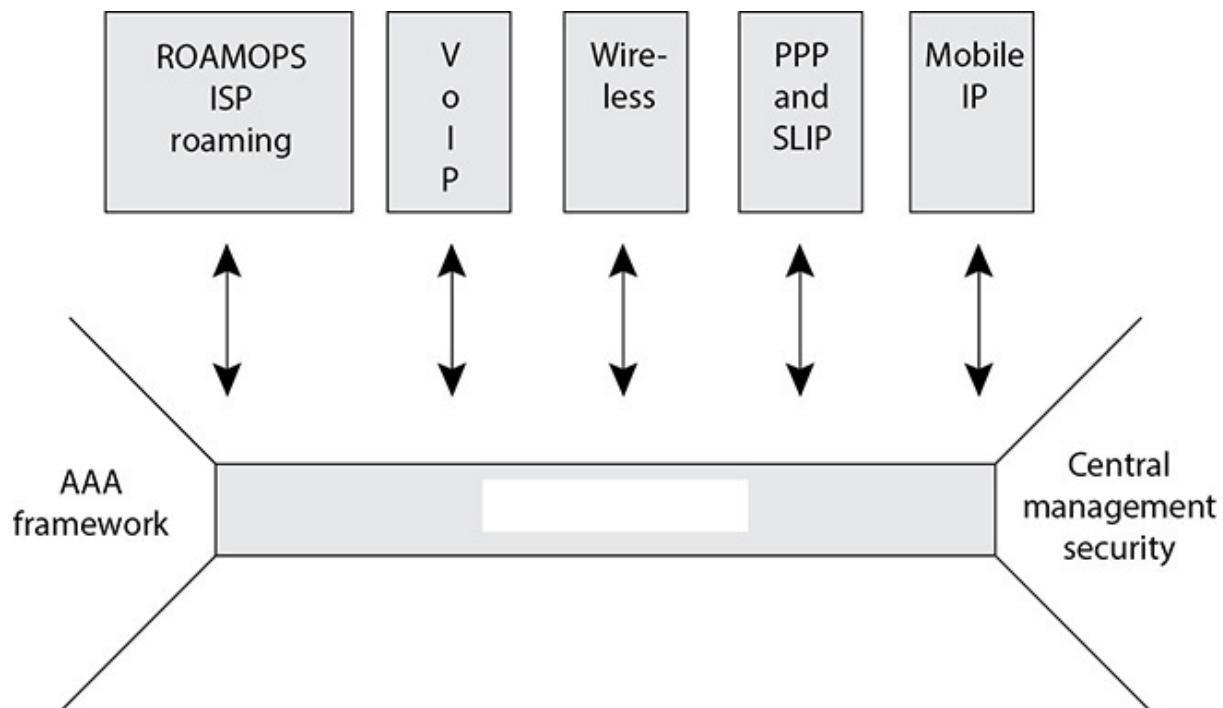
based upon?

- A. A subject
- B. An object
- C. A product
- D. An application

14. Which markup language allows a company to send service requests and the receiving company to provision access to these services?

- A. XML
- B. SPML
- C. SGML
- D. HTML

15. There are several different types of centralized access control protocols. Which of the following is illustrated in the graphic that follows?



- A. Diameter
- B. Watchdog
- C. RADIUS
- D. TACACS+

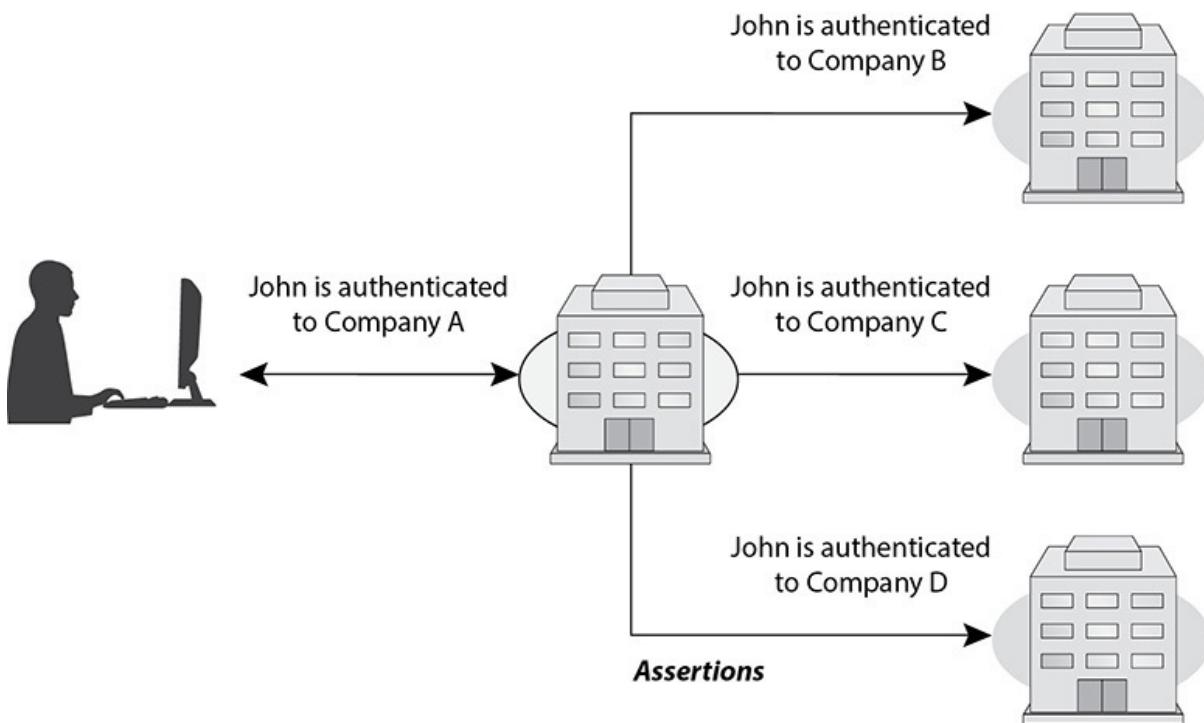
16. An access control matrix is used in many operating systems and applications to control access between subjects and objects. What is the

column in this type of matrix referred to as?

Access Control Matrix

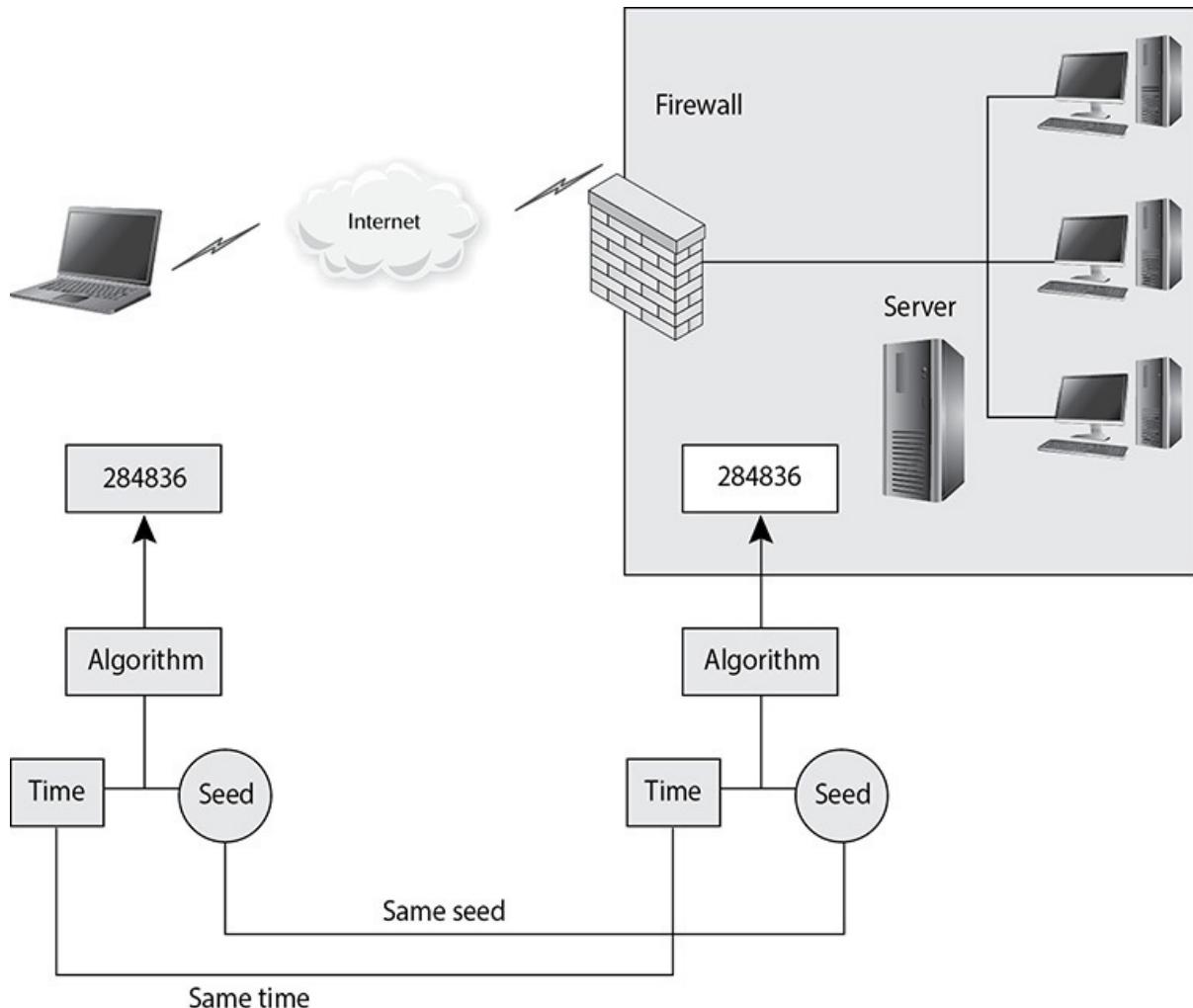
Subject	File1	File2	File3	File4
Larry	Read	Read, Write	Read	Read, Write
Curly	Full Control	No Access	Full Control	Read
Mo	Read, Write	Full Control	Read	Full Control
Bob	Full Control	Full Control	No Access	No Access

- A. Capability table
 - B. Constrained interface
 - C. Role-based value
 - D. ACL
17. What technology within identity management is illustrated in the graphic that follows?



- A. User provisioning
- B. Federated identity
- C. Directories
- D. Web access management

18. There are different ways that specific technologies can create one-time passwords for authentication purposes. What type of technology is illustrated in the graphic that follows?



- A. Counter synchronous token
- B. Asynchronous token
- C. Mandatory token
- D. Synchronous token
19. Which of the following best describes how SAML, SOAP, and HTTP commonly work together in an environment that provides web services?
- A. The security attributes are put into SAML format. The web service request and the authentication data are encrypted in a SOAP message. The message is transmitted in an HTTP connection.
- B. The security attributes are put into SAML format. The web service request and the authentication data are encapsulated in a SOAP

message. The message is transmitted in an HTTP connection over TLS.

- C. The authentication data is put into SAML format. The web service request and authentication data are encapsulated in a SOAP message. The message is transmitted in an HTTP connection.
 - D. The authentication data is put into SAML format. The HTTP request and the authentication data are encapsulated in a SOAP message. The message is transmitted in an HTTP connection.
- 20.** Jill is establishing a companywide sales program that will require different user groups with different privileges to access information on a centralized database. How should the security manager secure the database?
- A. Increase the database's security controls and provide more granularity.
 - B. Implement access controls that display each user's permissions each time they access the database.
 - C. Change the database's classification label to a higher security status.
 - D. Decrease the security so that all users can access the information as needed.
- 21.** Bethany is working on a mandatory access control (MAC) system. She has been working on a file that was classified as Secret. She can no longer access this file because it has been reclassified as Top Secret. She deduces that the project she was working on has just increased in confidentiality and she now knows more about this project than her clearance and need-to-know allows. Which of the following refers to a concept that attempts to prevent this type of scenario from occurring?
- A. Covert storage channel
 - B. Inference attack
 - C. Noninterference
 - D. Aggregation
- 22.** A number of attacks can be performed against smart cards. Side-channel is a class of attacks that doesn't try to compromise a flaw or weakness. Which of the following is NOT a side-channel attack?
- A. Differential power analysis

- B.** Microprobing analysis
 - C.** Timing analysis
 - D.** Electromagnetic analysis
- 23.** Emily is listening to network traffic and capturing passwords as they are sent to the authentication server. She plans to use the passwords as part of a future attack. What type of attack is this?
- A.** Brute-force attack
 - B.** Dictionary attack
 - C.** Social engineering attack
 - D.** Replay attack
- 24.** Which of the following is the best way to reduce brute-force attacks that allow intruders to uncover users' passwords?
- A.** Increase the clipping level.
 - B.** Lock out an account for a certain amount of time after the clipping level is reached.
 - C.** After a threshold of failed login attempts is met, the administrator must physically lock out the account.
 - D.** Choose a weaker algorithm that encrypts the password file.
- 25.** Phishing and pharming are similar. Which of the following correctly describes the difference between phishing and pharming?
- A.** Personal information is collected from victims through legitimate-looking websites in phishing attacks, while personal information is collected from victims via e-mail in pharming attacks.
 - B.** Phishing attacks point e-mail recipients to a form where victims input personal information, while pharming attacks use pop-up forms at legitimate websites to collect personal information from victims.
 - C.** Victims are pointed to a fake website with a domain name that looks similar to a legitimate site's domain name in a phishing attack, while victims are directed to a fake website as a result of a legitimate domain name being incorrectly translated by the DNS server in a pharming attack.
 - D.** Phishing is a technical attack, while pharming is a type of social engineering.

- 26.** There are several types of intrusion detection systems (IDSs). What type of IDS builds a profile of an environment's normal activities and assigns an anomaly score to packets based on the profile?
- A. State-based
 - B. Statistical anomaly-based
 - C. Misuse-detection system
 - D. Protocol signature-based
- 27.** A rule-based IDS takes a different approach than a signature-based or anomaly-based system. Which of the following is characteristic of a rule-based IDS?
- A. Uses IF/THEN programming within expert systems
 - B. Identifies protocols used outside of their common bounds
 - C. Compares patterns to several activities at once
 - D. Can detect new attacks
- 28.** Tom works at a large retail company that recently deployed radio-frequency identification (RFID) to better manage its inventory processes. Employees use scanners to gather product-related information instead of manually looking up product data. Tom has found out that malicious customers have carried out attacks on the RFID technology to reduce the amount they pay on store items. Which of the following is the most likely reason for the existence of this type of vulnerability?
- A. The company's security team does not understand how to secure this type of technology.
 - B. The cost of integrating security within RFID is cost prohibitive.
 - C. The technology has low processing capabilities and encryption is very processor intensive.
 - D. RFID is a new and emerging technology, and the industry does not currently have ways to secure it.
- 29.** Tanya is the security administrator for a large distributed retail company. The company's network has many different network devices and software appliances that generate logs and audit data. Tanya and her staff have become overwhelmed with trying to review all of the log files when attempting to identify if anything suspicious is taking place within the network. Which of the following is the best solution for this

company to implement?

- A. Security information and event management
 - B. Event correlation tools
 - C. Intrusion detection systems
 - D. Security event correlation management tools
30. The Logistics Agency of a country's department of defense is responsible for ensuring that all necessary materials get to the proper locations to support the department's day-to-day activities. The data that this agency maintains must be protected according to the three main security principles of security controls. For this agency's responsibilities, which security principle has the highest priority?
- A. Confidentiality
 - B. Integrity
 - C. Availability
 - D. Privacy
31. Claudia is the CISO for a global financial institution, overseeing the security of hundreds of millions of bank accounts. Which of the three main security principles should she consider most important when prioritizing the controls her enterprise should deploy?
- A. Confidentiality
 - B. Integrity
 - C. Availability
 - D. Authenticity
32. Which of the following is an example of a credential management system, also known as an identity management (IdM) system?
- A. A historic log of the activities performed by users once they have presented their credentials to a central authorizing system
 - B. A database of the credentials that have been registered to each individual in an enterprise, in order to correlate users with usernames and locales
 - C. A security information and event management (SIEM) system that contains the logs for various credentialing systems in the enterprise, for correlation of activities by ID

- D. A Kerberos Key Distribution Center (KDC) that contains the symmetric keys of all the entities and systems in a Kerberos realm, which can be centrally administered to ensure that it is up-to-date with respect to additions and deletions of keys
- 33.** Which of the following attributes is used to biometrically authenticate a user's identity?
- A. Something you know
 - B. Something you have
 - C. Something you are
 - D. Someplace you are
- 34.** Within biometric authentication, what is a Type II error rate?
- A. The rate of errors where the system falsely accepts the authentication of an individual who is not who they purport to be
 - B. The rate of errors where the system falsely rejects the authentication of an individual who is who they purport to be
 - C. The rate of errors that the system produces where false rejections and false acceptances are equal
 - D. The rate of errors where the system fails to either accept or reject the authentication of an individual regardless of their validity
- 35.** Which of the following criteria is the most important consideration for the selection and deployment of a biometric authentication system?
- A. False acceptance rate (FAR) or Type II error rate
 - B. False rejection rate (FRR) or Type I error rate
 - C. Crossover error rate (CER) or equal error rate (EER)
 - D. Processing speed
- 36.** Though "something you know," in the form of passwords, is the most common authentication factor still used today, it is considered one of the weakest. This is because passwords are easy for users to share, and relatively easy for adversaries to steal or guess. Which of the following measures is the best way to counter attacks on this form of authentication?
- A. Store all passwords in encrypted form only, so that recovering them requires a special key to decrypt them for authentication.
 - B. Employ a password policy to ensure that passwords are chosen in

such a way that they are neither easy for an attacker to guess nor easy for an attacker to brute force.

- C. Require that all passwords be composed of a combination of unique characters, regardless of length.
 - D. Ensure that accounts are locked out after a minimum number of incorrect guesses within a short amount of time.
- 37.** Which of the following is the correct sequence in the Kerberos authentication process with respect to passwords, Key Distribution Centers (KDCs), ticket granting servers (TGSs), ticket granting tickets (TGTs), services, and service tickets?
- A. The user provides a username/password to the workstation, the workstation obtains a TGT from the TGS, then subsequently obtains a service ticket from the KDC, which it presents to the service.
 - B. The workstation obtains a TGT from the KDC, which the user then validates with a password. The TGT is then exchanged for a service ticket from the TGS, which is presented to the service.
 - C. The user provides a username/password to the workstation, the workstation obtains a TGT from the KDC, then subsequently obtains a service ticket from the TGS, which it presents to the service.
 - D. The user obtains a service ticket from the service. The user then validates this ticket with a username/password provided to the TGS, which results in a TGT that is further validated by the KDC in a final step.
- 38.** In practical use, which of the following best describes a “session”?
- A. Any data exchange between two discrete endpoints, over any arbitrary duration
 - B. Any authenticated exchange between two parties that is used to carry on a conversation, with a discrete beginning, period of activity, and termination
 - C. Any discrete period of time that a user is logged into a workstation
 - D. The volume of data exchanged between two systems during a discrete period of time
- 39.** The use of “resource servers” and “authorization servers” to enable a “client” web service (such as LinkedIn) to access a “resource owner”

(such as Google) for federated authorization is a hallmark of what open standard?

- A. OpenID
 - B. SAML
 - C. SSO
 - D. OAuth
40. Which of the following is NOT true of OpenID Connect (OIDC)?
- A. It is mainly used as an open standards-based single sign-on (SSO) mechanism between disparate platforms within an enterprise environment.
 - B. It is layered on the OAuth protocol to allow both authentication and authorization in a transparent way for client resource requests.
 - C. It supports three flows: authorization code flow, implicit flow, and hybrid flow.
 - D. It involves browser redirections from the OpenID provider back to the relying party using authorization codes.
41. Which of the following attributes are added beyond traditional access control mechanisms (RBAC, MAC, and DAC) in order to implement ABAC?
- A. Subjects
 - B. Objects
 - C. Actions
 - D. Context

QUICK ANSWER KEY

- 1. C
- 2. B
- 3. C
- 4. C
- 5. A
- 6. B
- 7. C

8. B

9. B

10. A

11. C

12. D

13. A

14. B

15. A

16. D

17. B

18. D

19. C

20. A

21. C

22. B

23. D

24. B

25. C

26. B

27. A

28. C

29. A

30. A

31. B

32. D

33. C

34. A

35. D

36. B

37. C

38. B

39. D

40. A

41. D

ANSWERS A

- 1.** Which of the following does NOT correctly describe a directory service?

 - A.** It manages objects within a directory by using namespaces.
 - B.** It enforces security policy by carrying out access control and identity management functions.
 - C.** It assigns namespaces to each object in databases that are based on the X.509 standard and are accessed by LDAP.
 - D.** It allows an administrator to configure and manage how identification takes place within the network.
- C.** Most enterprises have some type of directory that contains information pertaining to the company's network resources and users. Most directories follow a hierarchical database format, based on the X.500 standard (not X.509), and a type of protocol, as in Lightweight Directory Access Protocol (LDAP), that allows subjects and applications to interact with the directory. Applications can request information about a particular user by making an LDAP request to the directory, and users can request information about a specific resource by using a similar request. A directory service assigns distinguished names (DNs) to each object in databases based on the X.500 standard that are accessed by LDAP. Each distinguished name represents a collection of attributes about a specific object and is stored in the directory as an entry.
- A** is incorrect because objects within hierarchical databases are managed by a directory service. The directory service allows an administrator to configure and manage how identification, authentication, authorization, and access control take place within the network. The objects within the directory are labeled and identified with namespaces, which is how the directory service keeps the objects organized.
- B** is incorrect because directory services do enforce the configured

security policy by carrying out access control and identity management functions. For example, when a user logs into a domain controller in a Windows environment, the directory service (Active Directory) determines what network resources she can and cannot access.

- D** is incorrect because directory services do allow an administrator to configure and manage how identification takes place within the network. It also allows for the configuration and management of authentication, authorization, and access control.
- 2.** Hannah has been assigned the task of installing web access management (WAM) software. What is the best description for what WAM is commonly used for?
 - A.** Control external entities requesting access through X.500 databases
 - B.** Control external entities requesting access to internal objects
 - C.** Control internal entities requesting access through X.500 databases
 - D.** Control internal entities requesting access to external objects
- B.** Web access management (WAM) software controls what users can access when using a web browser to interact with web-based enterprise assets. This type of technology is continually becoming more robust and experiencing increased deployment. This is because of the increased use of e-commerce, online banking, content providing, web services, and more. The basic components and activities in a web access control management process are as follows:
 - 1.** User sends in credentials to web server.
 - 2.** Web server requests the WAM platform to authenticate the user. WAM authenticates against the LDAP directory and retrieves authorizations from the policy database.
 - 3.** User requests to access a resource (object).
 - 4.** Web server verifies that object access is authorized and allows access to the requested resource.
- A** is incorrect because a directory service should be carrying out access control in the directory of an X.500 database—not web access management software. The directory service manages the entries and data and enforces the configured security policy by carrying out access control and identity management functions. Examples of directory services include Active Directory and NetIQ

eDirectory. While web-based access requests may be to objects held within a database, WAM mainly controls communication between web browsers and servers. The web servers should communicate to a back-end database, commonly through a directory service.

- C** is incorrect because a directory service should be carrying out access control for internal entities requesting access to an X.500 database using the LDAP. This type of database provides a hierarchical structure for the organization of objects (subjects and resources). The directory service develops unique distinguished names for each object and appends the corresponding attribute to each object as needed. The directory service enforces a security policy (configured by the administrator) to control how subjects and objects interact. While web-based access requests may be to objects held within a database, WAM mainly controls communication between web browsers and servers. WAM was developed mainly for external-to-internal communication, although it can be used for internal-to-internal communication also. Answer B is the best answer out of the four provided.
 - D** is incorrect because WAM software is most commonly used to control external entities requesting access to internal objects; not the other way around, as stated by the answer option. For example, WAM may be used by a bank to control its customers' access to back-end account data.
3. There are several types of password management approaches used by identity management systems. Which of the following reduces help-desk call volume, but is also criticized for the ease with which a hacker could gain access to multiple resources if a password is compromised?
- A.** Management password reset
 - B.** Self-service password reset
 - C.** Password synchronization
 - D.** Assisted password reset
- C.** Password synchronization is designed to reduce the complexity of keeping up with different passwords for different systems. Password synchronization technology can allow users to maintain a single password across multiple systems by transparently synchronizing the password to other systems and applications. This reduces help-desk call volume. One criticism of this approach is that since only one password is used to access different resources,

now the hacker only has to figure out one credential set to gain unauthorized access to all resources.

- A** is incorrect because there is no such thing as a management password reset. This answer is a distracter. The most common password management approaches are password synchronization, self-service password reset, and assisted password reset.
 - B** is incorrect because self-service password reset does not necessarily deal with multiple passwords. However, it does help reduce the overall volume of password-related help-desk calls. In the case of self-service password reset, users are allowed to reset their own passwords. For example, when a user forgets his password, he may be prompted to answer questions that he identified during the registration process. If the answer he gives matches the information he provided during registration, then he is granted the ability to change his password.
 - D** is incorrect because assisted password reset does not necessarily deal with multiple passwords. It reduces the resolution process for password issues by allowing the help desk to authenticate a user before resetting her password. The caller must be identified and authenticated through the password management tool before the password can be changed. Once the password is updated, the system that the user is authenticating to should require the user to change her password again. This would ensure that only she (and not she and the help-desk person) knows her password. The goal of an assisted password reset product is to reduce the cost of support calls and ensure that all calls are processed in a uniform, consistent, and secure fashion.
4. In the United States, federal agencies must adhere to Federal Information Processing Standard (FIPS) 201-2 “Personal Identity Verification,” which discusses technical measures of authentication for federal employees and contractors. This standard must be followed in order to ensure which of the following?
- A.** That government employees are properly cleared for the work assigned
 - B.** That government employees are only allowed access to data of their clearance level
 - C.** That the identity of the government employee has been appropriately verified

- D. That the data that government employees have access to has been appropriately classified
- C. FIPS 201-2 specifies the U.S. government standards for Personal Identity Verification (PIV), giving varying requirements of assurance. Access by government employees and contracted agents to restricted information hinges on their level of clearance and their need to know it, but first and foremost the government requires assurance that the individual is who they say they are.
- A is incorrect because government employees must be properly cleared for the information that they are granted access to, but prior to such access, their true identity must be available for review and affirmation.
- B is incorrect because government employees must only be allowed access to information that they are cleared to know and have a need to access. But again, this must be based on a specified level of assurance that the clearance they possess is valid.
- D is incorrect because classification of data is not directly related to Personal Identity Verification.
5. Which of the following does NOT describe privacy-aware role-based access control?
- A. It is an example of a discretionary access control model.
- B. Detailed access controls indicate the type of data that users can access based on the data's level of privacy sensitivity.
- C. It is an extension of role-based access control.
- D. It should be used to integrate privacy policies and access control policies.
- A. A system that uses discretionary access control (DAC) enables the owner of the resource to specify which subjects can access specific resources. This model is called discretionary because the control of access is based on the discretion of the owner. Many times department managers, or business unit managers, are the owners of the data within their specific department. Being the owner, they can specify who should have access and who should not. Privacy-aware role-based access control is an extension of role-based access control (RBAC). There are three main access control models: DAC, mandatory access control (MAC), and RBAC. Privacy-aware role-based access control is a type of RBAC, not

DAC.

- B** is incorrect because privacy-aware role-based access control is based on detailed access controls that indicate the type of data that users can access based on the data's level of privacy sensitivity. Other access control models, such as MAC, DAC, and RBAC, do not lend themselves to protect the level of privacy of data, but the functions that users can carry out. For example, managers may be able to access a privacy folder, but there needs to be more detailed access control that indicates, for example, that they can access customers' home addresses but not Social Security numbers. The industry has advanced to needing much more detail-oriented access control when it comes to sensitive privacy information as in Social Security numbers and credit card data, which is why privacy-aware role-based access control was developed.
 - C** is incorrect because privacy-aware role-based access control is an extension of role-based access control. Access rights are determined based on the user's role and responsibilities within the company, and the level of privacy of the data they need access to.
 - D** is incorrect because the languages used for privacy policies and access control policies should be either the same or integrated when using privacy-aware role-based access control. The goal of the use of privacy-aware role-based access control is to make access control much more detailed and focused on privacy-related data, thus it should be using the same type of terms and language as the organization's original access control policy and standards.
6. Security Assertion Markup Language (SAML) is an XML-based standard for exchanging authentication and authorization data between systems on different security domains. SAML allows for the sharing of authentication information, such as how authentication took place, entity attributes, and what the entity is authorized to access. SAML is most commonly used in web-based environments that require single sign-on (SSO) capability. Which of the following has a correct definition associated with the corresponding SAML component?
- A. Two SAML assertions are used (authentication, authorization) that indicate that an SAML authority validated a specific subject.
 - B. SAML assertions are most commonly used to allow for identity federation and distributed authorization.
 - C. SAML binding specification describes how to embed SAML messages within the TCP and UDP protocols.

- D.** SAML profiles define how SAML messages, assertions, and protocols are to be implemented in SSL and TLS.
- B.** SAML provides a model to allow two parties to share authentication information about one entity. The two parties are considered the service provider and the identity provider. The identity provider asserts information about the principal, such as whether or not the subject has been authenticated or has a particular attribute. The service provider uses the information supplied by the identity provider to make access decisions, including but not limited to, whether or not to trust the identity provider's assertion. By trusting the identity provider's information, the service provider can provide services without requiring the principal to authenticate again. This framework allows for federated identification and distributed authentication across domains.
- A** is incorrect because there are three kinds of SAML assertions (authentication, attribute, authorization) that indicate an SAML authority validated a specific subject. Authentication assertion validates that the subject was authenticated by an SAML authority through a specific manner. For example, an assertion might indicate that Sam Long was authenticated on a specific date, at a specific time, through the use of a digital certificate, and authentication is valid for 30 minutes. The asserting party sends this authentication data to the relying party so that the subject can be authenticated on the relying party's system and the subject does not need to log in again.
- C** is incorrect because the SAML binding specification describes how to embed SAML messages within communications or messaging protocols to allow for SAML request-response message exchange. SAML bindings define how these message exchanges take place in application layer protocols (e.g., SOAP, HTTP), not transport layer protocols such as TCP and UDP. The SAML specification defines the SAML protocol, which is an XML-based request and response protocol for processing SAML assertions. This means that this specification pertains to a packet's payload data, which works at the application layer of the OSI model. Transport layers are at a lower part of the network stack and have no direct interaction with this XML specification.
- D** is incorrect because SAML profiles define how SAML messages, assertions, and protocols are to be implemented in use cases. This specification does not deal with session and transport layer

protocols as in SSL and TLS. Each profile within the SAML specification outlines how SAML messages, assertions, and protocols are to be used in specific scenarios. For example, one SAML profile outlines how SAML is to be used to support a single sign-on environment across multiple web applications. This profile defines how an SAML-aware client (i.e., web browser) is to be supported and how identification data is to be managed among multiple service providers.

7. Brian has been asked to work on the virtual directory of his company's new identity management system. Which of the following best describes a virtual directory?
 - A. Meta-directory
 - B. User attribute information stored in an HR database
 - C. Virtual container for data from multiple sources
 - D. A service that allows an administrator to configure and manage how identification takes place

C. A network directory is a container for users and network resources. One directory does not contain (or know about) all of the users and resources within the enterprise, so a collection of directories must be used. A virtual directory gathers the necessary information used from sources scattered throughout the network and stores them in a central virtual directory (virtual container). This provides a unified view of all users' digital identity information throughout the enterprise. The virtual directory periodically synchronizes itself with all of the identity stores (individual network directories) to ensure the most up-to-date information is being used by all applications and identity management components within the enterprise.

A is incorrect because whereas a virtual directory is similar to a meta-directory, the meta-directory works with one directory, while a virtual directory works with multiple data sources. When an identity management component makes a call to a virtual directory, it has the capability to scan different directories throughout the enterprise, whereas a meta-directory only has the capability to scan the one directory it is associated with.

B is incorrect because it best describes an identity store. A lot of information stored in an identity management directory is scattered throughout the enterprise. User attribute information (employee

status, job description, department, and so on) is usually stored in the HR database; authentication information could be in a Kerberos server; role and group identification information might be in a SQL database; and resource-oriented authentication information can be stored in Active Directory on a domain controller. These are commonly referred to as identity stores and are located in different places on the network. Many identity management products use virtual directories to call upon the data in these identity stores.

- D** is incorrect because it describes the directory service. The directory service allows an administrator to configure and manage how identification, authentication, authorization, and access control occur within the network. It manages the objects within a directory by using namespaces and enforces the configured security policy by carrying out access control and identity management functions.
- 8.** Which of the following accurately describes Identity as a Service (IDaaS)?
- A.** A form of single sign-on (SSO) that spans multiple entities in an enterprise
 - B.** A form of SSO that spans multiple independent enterprises
 - C.** A way to provide SSO without multiple forms of authentication
 - D.** A way to demonstrate identity without having to sign on
- B.** Providers of IDaaS allow their clients to have a form of SSO that works across various otherwise independent accounts for independent vendors. A common example is the ability to use a Google account to create a Facebook page.
 - A** is incorrect because SSO that spans multiple entities within an enterprise is most commonly provisioned by a public key infrastructure (PKI) such as is provided by Active Directory in a Microsoft environment or via an 802.1X protocol for other technologies.
 - C** is incorrect because any SSO solution should provide for multifactor authentication.
 - D** is incorrect because all demonstrations of identity require authentication to be valid.
- 9.** Which of the following correctly describes a federated identity and its role within identity management processes?
- A.** A nonportable identity that can be used across business boundaries

- B. A portable identity that can be used across business boundaries
 - C. An identity that can be used within intranet virtual directories and identity stores
 - D. An identity specified by domain names that can be used across business boundaries
- B.** A federated identity is a portable identity and its associated entitlements that can be used across business boundaries. It allows a user to be authenticated across multiple IT systems and enterprises. Identity federation is based upon linking a user's otherwise distinct identities at two or more locations without the need to synchronize or consolidate directory information. Federated identity offers businesses and consumers a more convenient way of accessing distributed resources and is a key component of e-commerce.
- A** is incorrect because a federated identity is portable. It could not be used across business boundaries if it was not portable—and that's the whole point of a federated identity. The world continually gets smaller as technology brings people and companies closer together. Many times, when we are interacting with just one website, we are actually interacting with several different companies—we just don't know it. The reason we don't know it is because these companies are sharing our identity and authentication information behind the scenes. This is done to improve ease of use for the user.
- C** is incorrect because a federated identity is meant to be used across business boundaries—not within the organization. In other words, its use extends beyond the organization that owns the user data. Using federated identities, organizations with different technologies for directory services, security, and authentication can share applications, thereby allowing users to sign in to multiple applications with the same user ID, password, etc.
- D** is incorrect because a federated identity is not specified by a domain name. A federated identity is a portable identity and its associated entitlements. It includes the username, password, and other personal identification information used to sign in to an application.

10. Security countermeasures should be transparent to users and attackers. Which of the following does NOT describe transparency?

- A. User activities are monitored and tracked without negatively affecting system performance.

- B. User activities are monitored and tracked without the user knowing about the mechanism that is carrying this out.
 - C. Users are allowed access in a manner that does not negatively affect business processes.
 - D. Unauthorized access attempts are denied and logged without the intruder knowing about the mechanism that is carrying this out.
- A. Unfortunately, security components usually affect system performance in one fashion or another, although many times it is unnoticeable to the user. There is a possibility that if a system's performance is noticeably slow, this could be an indication that security countermeasures are in place. The reason that controls should be transparent is so that users and intruders do not know enough to be able to disable or bypass them. The controls should also not stand in the way of the company being able to carry out its necessary functions.
- B is incorrect because transparency is about activities being monitored and tracked without the user's knowledge of the mechanism that is doing the monitoring and the tracking. While it is a best practice to tell users if their computer use is being monitored, it is not necessary to tell them how they are being monitored. If users are aware of the mechanisms that monitor their activities, then they may attempt to disable or bypass them.
- C is incorrect because there must be a balance between security and usability. This means that users should be allowed access—where appropriate—with affecting business processes. They should have the means to get their job done.
- D is incorrect because you do not want intruders to know about the mechanisms in place to deny and log unauthorized access attempts. An intruder could use this knowledge to disable or bypass the mechanism and successfully gain unauthorized access to network resources.
11. What markup language allows for the sharing of application security policies to ensure that all applications are following the same security rules?
- A. XML
 - B. SPML
 - C. XACML

D. GML

- C.** Two or more companies can have a trust model set up to share identity, authorization, and authentication methods. This means that if Bill authenticates to his company's software, this software can pass the authentication parameters to its partner's software. This allows Bill to interact with the partner's software without having to authenticate twice. This can happen through Extensible Access Control Markup Language (XACML), which allows two or more organizations to share application security policies based upon their trust model. XACML is a markup language and processing model that is implemented in XML. It declares access control policies and describes how to interpret them.
 - A** is incorrect because XML (Extensible Markup Language) is a method for electronically coding documents and representing data structures such as those in web services. XML is not used to share security information. XML is an open standard that is more robust than its predecessor, HTML. In addition to serving as a markup language in and of itself, XML serves as the foundation for other more industry-specific XML standards. XML allows companies to use a markup language that meets their different needs while still being able to communicate with each other.
 - B** is incorrect because Service Provisioning Markup Language (SPML) is used by companies to exchange user, resource, and service provisioning information, not application security information. SPML is an XML-based framework developed by OASIS with the goal of allowing enterprise platforms (such as web portals and application servers) to generate provisioning requests across multiple companies for the purpose of the secure and quick setup of web services and applications.
 - D** is incorrect because Generalized Markup Language (GML) is a method created by IBM for formatting documents. It describes a document in terms of its parts (chapters, paragraphs, lists, etc.) and their relationship (heading levels). GML was a predecessor to Standard Generalized Markup Language (SGML) and Hypertext Markup Language (HTML).
- 12.** The importance of protecting audit logs generated by computers and network devices is highlighted by the fact that it is required by many of today's regulations. Which of the following does NOT explain why audit logs should be protected?

- A.** If not properly protected, these logs may not be admissible during a prosecution.
 - B.** Audit logs contain sensitive data and should only be accessible to a certain subset of people.
 - C.** Intruders may attempt to scrub the logs to hide their activities.
 - D.** The format of the logs should be unknown and unavailable to the intruder.
- D.** Auditing tools are technical controls that track activity within a network, on a network device, or on a specific computer. Even though auditing is not an activity that will deny an entity access to a network or computer, it will track activities so that a security administrator can understand the types of access that took place, identify a security breach, or warn the administrator of suspicious activity. This information can be used to point out weaknesses of other technical controls and help the administrator understand where changes must be made to preserve the necessary security level within the environment. Intruders can also use this information to exploit those weaknesses, so audit logs should be protected through permissions, rights, and integrity controls, as in hashing algorithms. However, the format of systems logs is commonly standardized with all like systems. Hiding log formats is not a usual countermeasure and is not a reason to protect audit log files.
- A** is incorrect because due care must be taken to protect audit logs in order for them to be admissible in court. Audit trails can be used to provide alerts about any suspicious activities that can be investigated at a later time. In addition, they can be valuable in determining exactly how far an attack has gone and the extent of the damage that may have been caused. It is important to make sure a proper chain of custody is maintained to ensure any data collected can be properly and accurately represented in case it needs to be used for later events such as criminal proceedings or investigations.
- B** is incorrect because only the administrator and security personnel should be able to view, modify, and delete audit trail information. No other individuals should be able to view this data, much less modify or delete it. The integrity of the data can be ensured with the use of digital signatures, message digest tools, and strong access controls. Its confidentiality can be protected with encryption and access controls, if necessary, and it can be stored on write-once

media to prevent loss or modification of the data. Unauthorized access attempts to audit logs should be captured and reported.

- C** is incorrect because the statement is true. If an intruder breaks into your house, he will do his best to cover his tracks by not leaving fingerprints or any other clues that can be used to tie him to the criminal activity. The same is true in computer fraud and illegal activity. The intruder will work to cover his tracks. Attackers often delete audit logs that hold this incriminating information. (Deleting such data within audit logs is called *scrubbing*.) Deleting this information can cause the administrator to not be alerted or aware of the security breach, and can destroy valuable data. Therefore, audit logs should be protected by strict access control.

13. Of the following, what is the primary item that a capability table is based upon?

- A.** A subject
- B.** An object
- C.** A product
- D.** An application

- A.** A capability table specifies the access rights a certain subject possesses pertaining to specific objects. A capability list (also referred to as a capability table) is different from an access control list (ACL) because the subject is bound to the capability table, whereas the object is bound to the ACL. A capability can be in the form of a token, ticket, or key. When a subject presents a capability component, the operating system (or application) will review the access rights and operations outlined in the capability component and allow the subject to carry out just those functions. A capability component is a data structure that contains a unique object identifier and the access rights the subject has to that object. The object may be a file, array, memory segment, or port.
- B.** is incorrect because an object is bound to an access control list (ACL), not a capability component. ACLs are used in several operating systems, applications, and router configurations. They are lists of subjects that are authorized to access a specific object, and they define what level of authorization is granted. Authorization can be specified to an individual or group. ACLs map values from the access control matrix to the object. Whereas a capability corresponds to a row in the access control matrix, the ACL

corresponds to a column of the matrix.

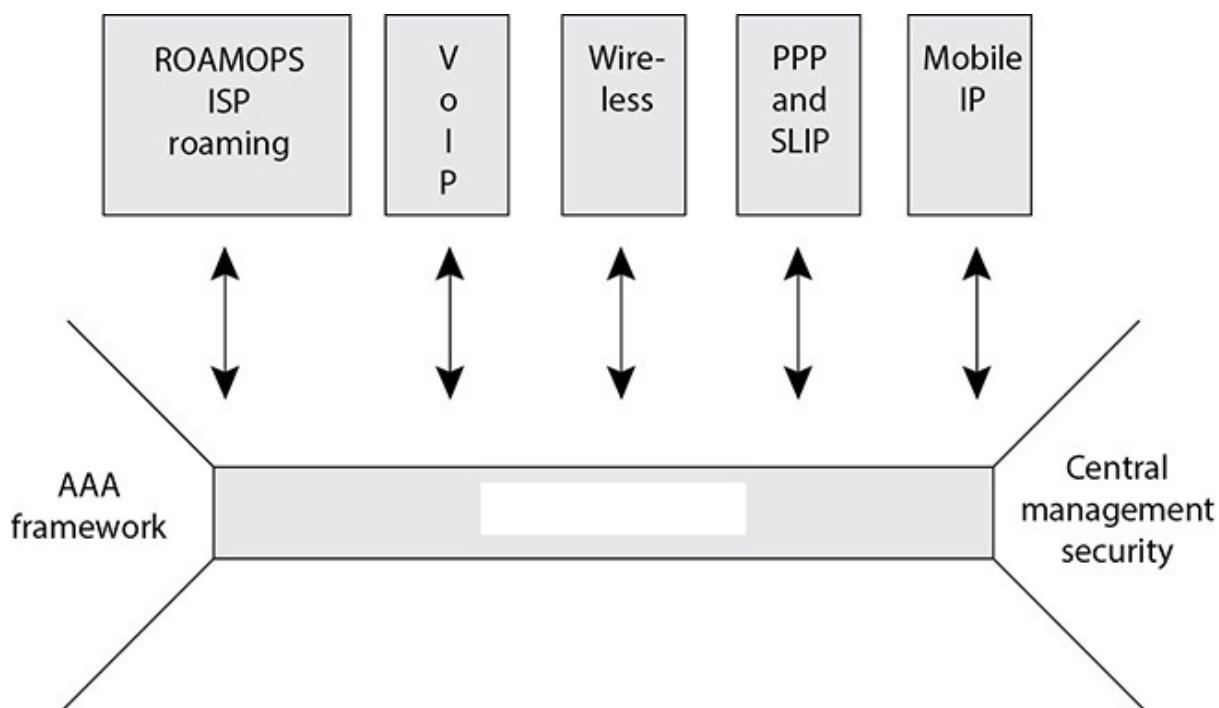
- C** is incorrect because a product can be an object or subject. If a user attempts to access a product (such as a program), the user is the subject and the product is the object. If a product attempts to access a database, the product is the subject and the database is the object. While a product could be a subject in a capability list for example, the best answer is A. A capability list indicates what objects a subject can access and the operations that can be carried out on those objects.
- D** is incorrect because this is similar to answer C. If a user attempts to access an application, the user is the subject and the application is the object. If an application attempts to access a database, the application is the subject and the database is the object. While an application could be a subject in a capability list for example, the best answer is A. A capability list indicates what objects a subject can access and the operations that can be carried out on those objects.

14. Which markup language allows a company to send service requests and the receiving company to provision access to these services?

- A.** XML
 - B.** SPML
 - C.** SGML
 - D.** HTML
- B.** Service Provisioning Markup Language (SPML) is a markup language, built on the Extensible Markup Language (XML) framework, that exchanges information about which users should get access to what resources and services. So let's say that an automobile company and a tire company only allow inventory managers within the automobile company to order tires. If Bob logs in to the automobile company's inventory software and orders 40 tires, how does the tire company know that this request is coming from an authorized vendor and user with the Inventory Managers group? The automobile company's software can pass user and group identity information to the tire company's software. The tire company uses this identity information to make an authorization decision that then allows Bob's request for 40 tires to be filled. Since both the sending and receiving companies are following one standard (XML), this type of interoperability can take place.

- A is incorrect because it is not the best answer to the question.
SPML—which is based on XML—allows company interfaces to pass service requests and the receiving company to provision access to these services. This interoperability is made possible because the companies are both using XML, which is a set of rules for electronically encoding documents and web-based communication. XML is also used to encode arbitrary data structures, as in web services. It allows groups or companies to create information formats, like SPML, that enable a consistent means of sharing data.
- C is incorrect because Standard Generalized Markup Language (SGML) was one of the first markup languages developed. It does not provide user access or provisioning functionality. SGML was a standard that defines generalized markup tags for documents. It is a successor to Generalized Markup Language and came long before XML or SPML.
- D is incorrect because Hypertext Markup Language (HTML) was developed to annotate web pages. HTML is a precursor to XML and SGML. HTML provides a means of denoting structural semantics for text and other elements found on a web page. It can be used to embed images and objects and create interactive forms. However, it cannot allow company interfaces to pass service requests and the receiving company to provision access to these services.

15. There are several different types of centralized access control protocols. Which of the following is illustrated in the graphic that follows?



- A.** Diameter
- B.** Watchdog
- C.** RADIUS
- D.** TACACS+

- A.** Diameter is an authentication, authorization, and auditing (AAA) protocol that provides the same type of functionality as RADIUS and TACACS+ but also provides more flexibility and capabilities to meet the new demands of today's complex and diverse networks. At one time, all remote communication took place over Point-to-Point Protocol (PPP) and Serial Line Internet Protocol (SLIP) connections, and users authenticated themselves through Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). Technology has become much more complicated and there are more devices and protocols to choose from than ever before. The Diameter protocol allows wireless devices, smart phones, and other devices to be able to authenticate themselves to networks using roaming protocols, Mobile IP, Ethernet over PPP, Voice over IP (VoIP), and others.
- B** is incorrect because watchdog timers are commonly used to detect software faults, such as a process ending abnormally or hanging. The watchdog functionality sends out a type of "heartbeat" packet to determine whether a service is responding. If it is not, the process can be terminated or reset. These packets help prevent against software deadlocks, infinite loops, and process prioritization problems. This functionality can be used in AAA protocols to determine whether packets need to be re-sent and whether connections experiencing problems should be closed and reopened, but it is not an access control protocol itself.
- C** is incorrect because Remote Authentication Dial-In User Service (RADIUS) is a network protocol and provides client/server authentication, authorization, and audit for remote users. A network may have access servers, DSL, ISDN, or a T1 line dedicated for remote users to communicate through. The access server requests the remote user's logon credentials and passes them back to a RADIUS server, which houses the usernames and password values. The remote user is a client to the access server, and the access server is a client to the RADIUS server.
- D** is incorrect because Terminal Access Controller Access Control System Plus (TACACS+) provides basically the same functionality

as RADIUS. The RADIUS protocol combines the authentication and authorization functionality. TACACS+ uses a true AAA architecture, which separates each function out. This gives a network administrator more flexibility in how remote users are authenticated. Neither TACACS+ nor RADIUS can carry out these services for devices that need to communicate over VoIP, mobile IP, or other similar types of protocols.

- 16.** An access control matrix is used in many operating systems and applications to control access between subjects and objects. What is the column in this type of matrix referred to as?

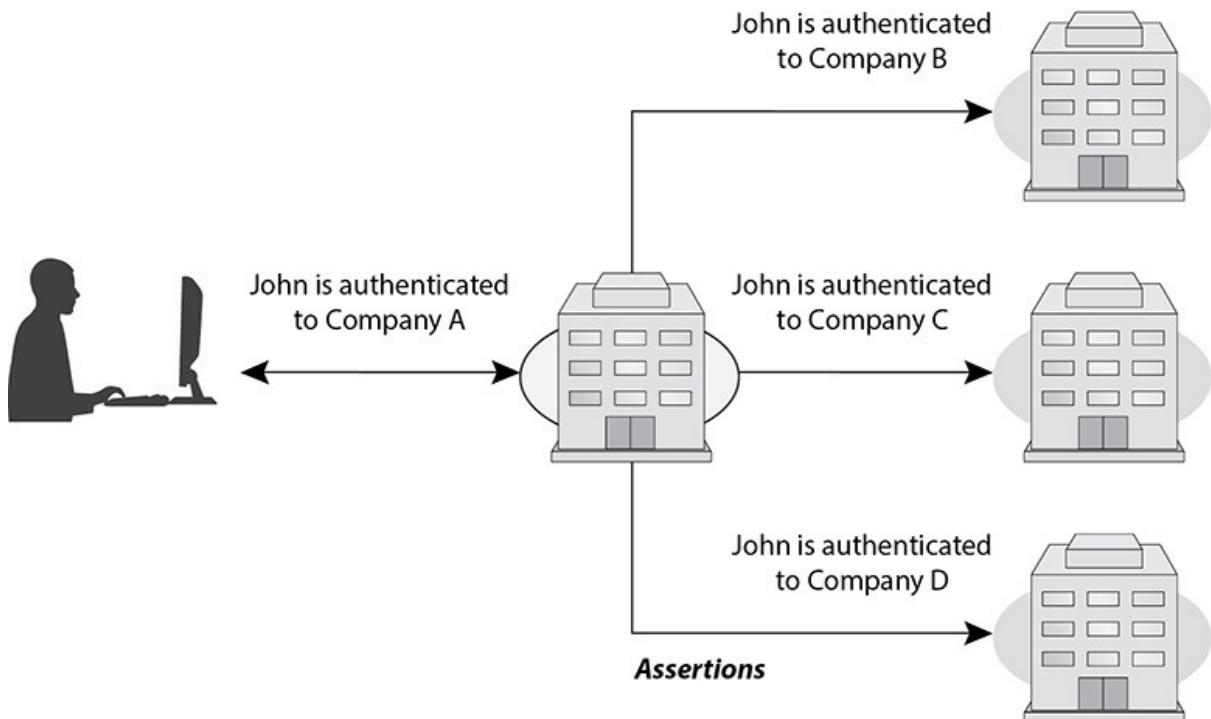
Access Control Matrix

Subject	File1	File2	File3	File4
Larry	Read	Read, Write	Read	Read, Write
Curly	Full Control	No Access	Full Control	Read
Mo	Read, Write	Full Control	Read	Full Control
Bob	Full Control	Full Control	No Access	No Access

- A. Capability table
B. Constrained interface
C. Role-based value
D. ACL
- D. Access control lists (ACLs) map values from the access control matrix to the object. Whereas a capability corresponds to a row in the access control matrix, the ACL corresponds to a column of the matrix. ACLs are used in several operating systems, applications, and router configurations. They are lists of subjects that are authorized to access specific objects, and they define what level of authorization is granted. Authorization can be specified to an individual or group. So the ACL is bound to an object and indicates which subjects can access it, and a capability table is bound to a subject and indicates which objects that subject can access.
- A is incorrect because a capability can be in the form of a token, ticket, or key and is a row within an access control matrix. When a subject presents a capability component, the operating system (or application) will review the access rights and operations outlined in

the capability component and allow the subject to carry out just those functions. A capability component is a data structure that contains a unique object identifier and the access rights the subject has to that object. The object may be a file, array, memory segment, or port. Each user, process, and application in a capability system has a list of capabilities it can carry out.

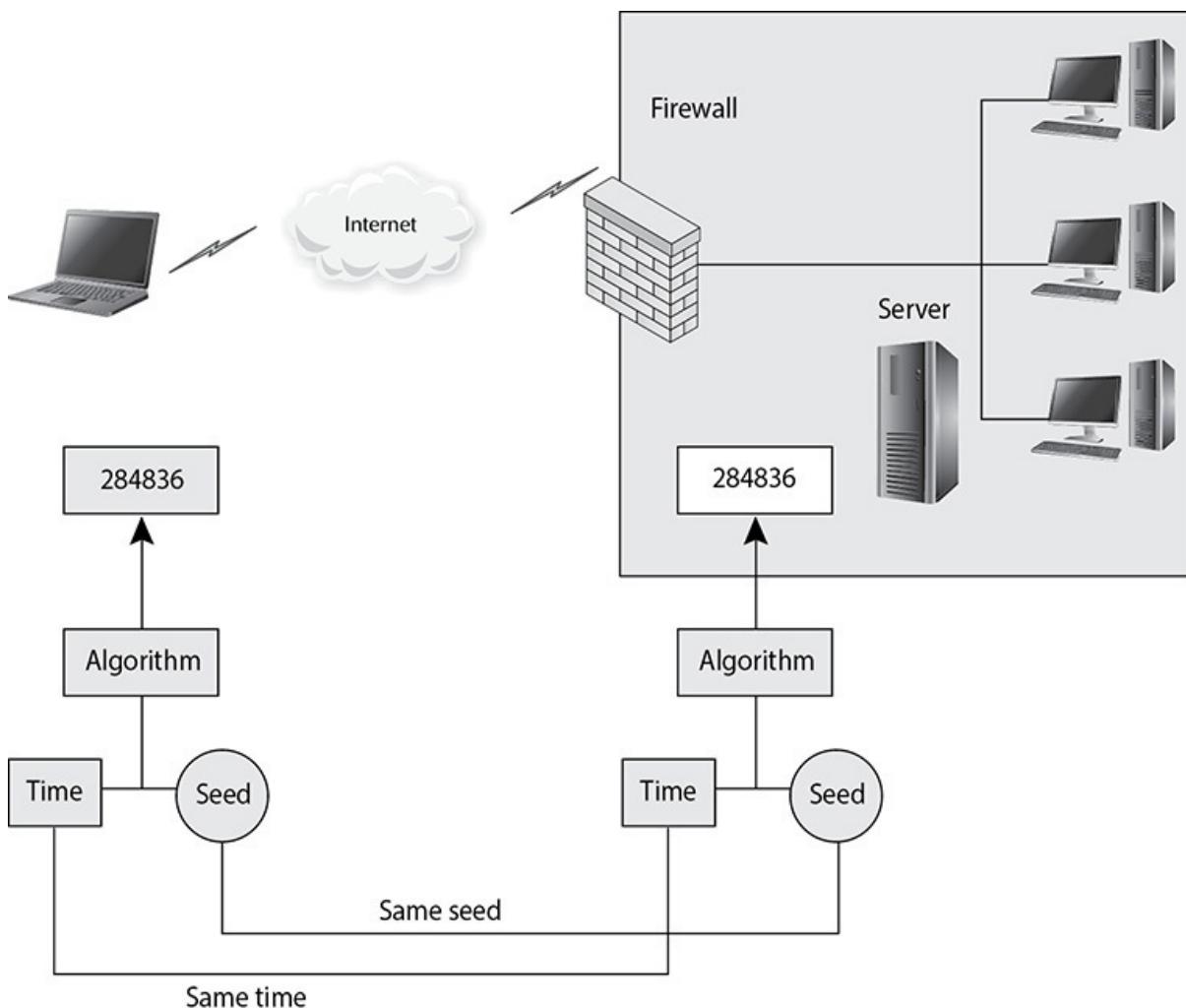
- B** is incorrect because constrained user interfaces restrict users' access abilities by not allowing them to request certain functions or information or to have access to specific system resources. Three major types of restricted interfaces exist: menus and shells, database views, and physically constrained interfaces. When menu and shell restrictions are used, the options users are given are the commands they can execute. For example, if an administrator wants users to be able to execute only one program, that program would be the only choice available on the menu. If restricted shells were used, the shell would contain only the commands the administrator wants the users to be able to execute.
 - C** is incorrect because a role-based access control (RBAC) model, also called nondiscretionary access control, uses a centrally administered set of controls to determine how subjects and objects interact. This type of model lets access to resources be based on the role the user holds within the company. It is referred to as nondiscretionary because assigning a user to a role is unavoidably imposed. This means that if you are assigned only to the Contractor role in a company, there is nothing you can do about it. You don't have the discretion to determine what role you will be assigned.
- 17.** What technology within identity management is illustrated in the graphic that follows?



- A. User provisioning
 - B. Federated identity
 - C. Directories
 - D. Web access management
- B.** A federated identity is a portable identity and its associated entitlements that can be used across business boundaries. It allows a user to be authenticated across multiple IT systems and enterprises. Identity federation is based upon linking a user's otherwise distinct identities at two or more locations without the need to synchronize or consolidate directory information. Federated identity offers businesses and consumers a more convenient way of accessing distributed resources and is a key component of e-commerce.
- A** is incorrect because user provisioning refers to the creation, maintenance, and deactivation of user objects and attributes as they exist in one or more systems, directories, or applications in response to business processes. User provisioning software may include one or more of the following components: change propagation, self-service workflow, consolidated user administration, delegated user administration, and federated change control. User objects may represent employees, contractors, vendors, partners, customers, or other recipients of a service. Services may include e-mail, access to a database, access to a file server or mainframe, and so on. User provisioning can be a function with federation identification, but

this is not what the graphic illustrates.

- C** is incorrect because while most enterprises have some type of directory that contains information pertaining to the company's network resources and users, those directories do not commonly spread across different businesses. Most directories follow a hierarchical database format, based on the X.500 standard, and a type of protocol, as in Lightweight Directory Access Protocol (LDAP), that allows subjects and applications to interact with the directory. Applications can request information about a particular user by making an LDAP request to the directory, and users can request information about a specific resource by using a similar request. While directories can work within a federated framework, this is not what the graphic shows.
 - D** is incorrect because web access management (WAM) software controls what users can access when using a web browser to interact with web-based enterprise assets. This type of technology is continually becoming more robust and experiencing increased deployment. This is because of the increased use of e-commerce, online banking, content providing, web services, and more. More complexity comes in with all the different ways a user can authenticate (password, digital certificate, token, and others), the resources and services that may be available to the user (transfer funds, purchase product, update profile, and so forth), and the necessary infrastructure components. The infrastructure is usually made up of a web server farm (many servers), a directory that contains the users' accounts and attributes, a database, a couple of firewalls, and some routers, all laid out in a tiered architecture.
- 18.** There are different ways that specific technologies can create one-time passwords for authentication purposes. What type of technology is illustrated in the graphic that follows?



- A. Counter synchronous token
 - B. Asynchronous token
 - C. Mandatory token
 - D. Synchronous token
- D. A synchronous token device synchronizes with the authentication service by using time or a counter as the core piece of the authentication process. If the synchronization is time based, as shown in this graphic, the token device and the authentication service must hold the same time within their internal clocks. The time value on the token device and a secret key are used to create the one-time password, which is displayed to the user. The user enters this value and a user ID into the computer, which then passes them to the server running the authentication service. The authentication service decrypts this value and compares it to the value it expected. If the two match, the user is authenticated and allowed to use the computer and resources.

- A** is incorrect because if the token device and authentication service use counter-synchronization, it is not based on time as shown in the graphic. When using a counter-synchronization token device, the user will need to initiate the creation of the one-time password by pushing a button on the token device. This causes the token device and the authentication service to advance to the next authentication value. This value and a base secret are hashed and displayed to the user. The user enters this resulting value along with a user ID to be authenticated. In either time- or counter-based synchronization, the token device and authentication service must share the same secret base key used for encryption and decryption.
 - B** is incorrect because a token device using an asynchronous token-generating method employs a challenge/response scheme to authenticate the user. This technology does not use synchronization but instead uses discrete steps in its authentication process. In this situation, the authentication server sends the user a challenge, a random value also called a nonce. The user enters this random value into the token device, which encrypts it and returns a value the user uses as a one-time password. The user sends this value, along with a username, to the authentication server. If the authentication server can decrypt the value and it is the same challenge value sent earlier, the user is authenticated.
 - C** is incorrect because there is no such thing as a mandatory token. This is a distracter answer.
- 19.** Which of the following best describes how SAML, SOAP, and HTTP commonly work together in an environment that provides web services?
- A.** The security attributes are put into SAML format. The web service request and the authentication data are encrypted in a SOAP message. The message is transmitted in an HTTP connection.
 - B.** The security attributes are put into SAML format. The web service request and the authentication data are encapsulated in a SOAP message. The message is transmitted in an HTTP connection over TLS.
 - C.** The authentication data is put into SAML format. The web service request and authentication data are encapsulated in a SOAP message. The message is transmitted in an HTTP connection.
 - D.** The authentication data is put into SAML format. The HTTP request and the authentication data are encapsulated in a SOAP

message. The message is transmitted in an HTTP connection.

- C.** As an example, when you log in to your company's portal and double-click a link (e.g., Salesforce), your company's portal will take this request and your authentication data and package them up in an Security Assertion Markup Language (SAML) format and encapsulate that data into a Simple Object Access Protocol (SOAP) message. This message would be transmitted over an HTTP connection to the Salesforce vendor site, and once you are authenticated you can interact with the vendor software. SAML packages up authentication data, SOAP packages up web service requests and SAML data, and the request is transmitted over an HTTP connection.
 - A** is incorrect because SAML is an XML-based open standard for exchanging authentication and authorization data between security domains—that is, between an identity provider (a producer of assertions) and a service provider (a consumer of assertions). So authentication data is used with SAML, not security attributes. Also, SOAP encapsulates messages, it does not encrypt them.
 - B** is incorrect because authentication data is used with SAML and the transmission does not take place over a TLS connection by default. The transmission can take place over SSL or TLS, but this was not what was outlined in the question.
 - D** is incorrect because SOAP encapsulates web service requests and data, not HTTP. After SOAP encapsulates web service data, it is then encapsulated with HTTP for transmission purposes.
- 20.** Jill is establishing a companywide sales program that will require different user groups with different privileges to access information on a centralized database. How should the security manager secure the database?
- A.** Increase the database's security controls and provide more granularity.
 - B.** Implement access controls that display each user's permissions each time they access the database.
 - C.** Change the database's classification label to a higher security status.
 - D.** Decrease the security so that all users can access the information as needed.

- A.** The best approach to securing the database in this situation would be to increase the controls and assign very granular permissions. These measures would ensure that users cannot abuse their privileges and that the confidentiality of the information would be maintained. Granularity of permissions gives network administrators and security professionals additional control over the resources they are charged with protecting, and a fine level of detail enables them to give individuals just the precise level of access they need.
 - B** is incorrect because implementing access controls that display each user's permissions each time they access the database is an example of one control. It is not the overall way of dealing with user access to a full database of information. This may be an example of increasing database security controls, but it is only one example, and more would need to be put into place.
 - C** is incorrect because the classification level of the information in the database was previously determined based on its confidentiality, integrity, and availability levels. These levels do not change simply because more users need access to the data. Thus, you would never increase or decrease the classification level of information when more users or groups need to access that information. Increasing the classification level would only mean a smaller subset of users could access the database.
 - D** is incorrect because it puts data at risk. If security is decreased so that all users can access it as needed, then users with lower privileges will be able to access data of higher classification levels. Lower security also makes it easier for intruders to break into the database. As stated in answer C, a classification level is not changed just because the number of users who need to access the data increases or decreases.
- 21.** Bethany is working on a mandatory access control (MAC) system. She has been working on a file that was classified as Secret. She can no longer access this file because it has been reclassified as Top Secret. She deduces that the project she was working on has just increased in confidentiality and she now knows more about this project than her clearance and need-to-know allows. Which of the following refers to a concept that attempts to prevent this type of scenario from occurring?
- A.** Covert storage channel
 - B.** Inference attack

C. Noninterference

D. Aggregation

- C.** Multilevel security properties can be expressed in many ways, one being noninterference. This concept is implemented to ensure that any actions that take place at a higher security level do not affect or interfere with actions that take place at a lower level. So if an entity at a higher security level performs an action, it cannot change the state for the entity at the lower level. If a lower-level entity were aware of a certain activity that took place by an entity at a higher level and the state of the system changed for this lower-level entity, the entity might be able to deduce too much information about the activities of the higher state, which in turn is a way of leaking information.
- A** is incorrect because a covert channel allows for the ability to share information between processes that weren't intended to communicate. Noninterference is a model intended to prevent covert channels along with other malicious ways of communicating. The model looks at the shared resources that the different users of a system will use and tries to identify how information can be passed from a process working at a higher security clearance to a process working at a lower security clearance. If two users are working on the same system at the same time, they will most likely have to share some type of resources. So the model is made up of rules to ensure that User A cannot carry out any activities that can allow User B to infer information she does not have the clearance to know.
- B** is incorrect because an inference attack refers to Bethany's ability to infer that the project that she was working on is now Top Secret and has increased in importance and secrecy. The question is asking for the concept that helps to prevent an inference attack. An inference attack occurs when someone has access to some type of information and can infer (or guess) something that she does not have the clearance level or authority to know. For example, let's say that Tom is working on a file that contains information about supplies that are being sent to Russia. He closes out of that file and one hour later attempts to open the same file. During this time, the file's classification has been elevated to Top Secret, so when Tom attempts to access it, he is denied. Tom can infer that some type of Top Secret mission is getting ready to take place with Russia. He does not have clearance to know this; thus, it would be an inference

attack or “leaking information.”

- D** is incorrect because aggregation is the act of combining information from separate sources. The combination of the data forms new information, which the subject does not have the necessary rights to access. The combined information can have a sensitivity that is greater than that of the individual parts. Aggregation happens when a user does not have the clearance or permission to access specific information but does have the permission to access components of this information. She can then figure out the rest and obtain restricted information.

22. A number of attacks can be performed against smart cards. Side-channel is a class of attacks that doesn't try to compromise a flaw or weakness. Which of the following is NOT a side-channel attack?
- A.** Differential power analysis
 - B.** Microprobing analysis
 - C.** Timing analysis
 - D.** Electromagnetic analysis
- B.** A noninvasive attack is one in which the attacker watches how something works and how it reacts in different situations instead of trying to “invade” it with more intrusive measures. Examples of side-channel attacks are fault generation, differential power analysis, electromagnetic analysis, timing, and software attacks. These types of attacks are used to uncover sensitive information about how a component works without trying to compromise any type of flaw or weakness. A more intrusive smart card attack is microprobing. Microprobing uses needles and ultrasonic vibration to remove the outer protective material on the card's circuits. Once this is complete, data can be accessed and manipulated by directly tapping into the card's ROM chips.
 - A** is incorrect because differential power analysis (DPA) is a noninvasive attack. DPA involves examining the power emissions released during processing. By statistically analyzing data from multiple cryptographic operations, for example, an attacker can determine the intermediate values within cryptographic computations. This can be done without any knowledge of how the target device is designed. Thus, an attacker can extract cryptographic keys or other sensitive information from the card.
 - C** is incorrect because a timing analysis is a noninvasive attack. It

involves calculating the time a specific function takes to complete its task. Timing analysis attacks are based on measuring how much time various computations take to perform. For example, by observing how long it takes a smart card to transfer key information, it is sometimes possible to determine how long the key is in this instance.

- D** is incorrect because electromagnetic analysis is a noninvasive attack that involves examining the frequencies emitted. All electric currents emit electromagnetic emanations. In smart cards, the power consumption—and, therefore, the electromagnetic emanation field—varies as data is processed. An electromagnetic analysis attempts to make correlations between the data and the electromagnetic emanations in an effort to uncover cryptographic keys or other sensitive information on the smart card.
- 23.** Emily is listening to network traffic and capturing passwords as they are sent to the authentication server. She plans to use the passwords as part of a future attack. What type of attack is this?
 - A.** Brute-force attack
 - B.** Dictionary attack
 - C.** Social engineering attack
 - D.** Replay attack
- D.** A replay attack occurs when an intruder obtains and stores information and later uses it to gain unauthorized access. In this case, Emily is using a technique called electronic monitoring (sniffing) to obtain passwords being sent over the wire to an authentication server. She can later use the passwords to gain access to network resources. Even if the passwords are encrypted, the retransmission of valid credentials can be sufficient to obtain access.
- A** is incorrect because a brute-force attack is performed with tools that cycle through many possible character, number, and symbol combinations to uncover a password. One way to prevent a successful brute-force attack is to restrict the number of login attempts that can be performed on a system. An administrator can set operating parameters that allow a certain number of failed logon attempts to be accepted before a user is locked out; this is a type of clipping level.
- B** is incorrect because a dictionary attack involves the automated

comparison of the user's password to files of thousands of words until a match is found. Dictionary attacks are successful because users tend to choose passwords that are short, are single words, or are predictable variations of dictionary words.

- C** is incorrect because in a social engineering attack the attacker falsely convinces an individual that she has the necessary authorization to access specific resources. Social engineering is carried out against people directly and is not considered a technical attack necessarily. The best defense against social engineering is user education. Password requirements, protection, and generation should be addressed in security awareness programs so that users understand why they should protect their passwords and how passwords can be stolen.
- 24.** Which of the following is the best way to reduce brute-force attacks that allow intruders to uncover users' passwords?
 - A.** Increase the clipping level.
 - B.** Lock out an account for a certain amount of time after the clipping level is reached.
 - C.** After a threshold of failed login attempts is met, the administrator must physically lock out the account.
 - D.** Choose a weaker algorithm that encrypts the password file.
- B.** A brute-force attack is an attack that continually tries different inputs to achieve a predefined goal, which can then be used to obtain credentials for unauthorized access. A brute-force attack to uncover passwords means that the intruder is attempting all possible sequences of characters to uncover the correct password. If the account would be disabled (or locked out) after this type of attack attempt took place, this would prove to be a good countermeasure.
- A** is incorrect because clipping levels should be implemented to establish a baseline of user activity and acceptable errors. An entity attempting to log in to an account should be locked out once the clipping level is met. A higher clipping level gives an attacker more attempts between alerts or lockout. Decreasing the clipping level would be a good countermeasure.
- C** is incorrect because it is not practical to have an administrator physically lock out accounts. This type of activity can easily be taken care of through automated software mechanisms. Accounts should be automatically locked out for a certain amount of time

after a threshold of failed login attempts has been met.

- D** is incorrect because using a weaker algorithm that encrypts passwords and/or password files would increase the likelihood of success of a brute-force attack.

25. Phishing and pharming are similar. Which of the following correctly describes the difference between phishing and pharming?

- A.** Personal information is collected from victims through legitimate-looking websites in phishing attacks, while personal information is collected from victims via e-mail in pharming attacks.
- B.** Phishing attacks point e-mail recipients to a form where victims input personal information, while pharming attacks use pop-up forms at legitimate websites to collect personal information from victims.
- C.** Victims are pointed to a fake website with a domain name that looks similar to a legitimate site's domain name in a phishing attack, while victims are directed to a fake website as a result of a legitimate domain name being incorrectly translated by the DNS server in a pharming attack.
- D.** Phishing is a technical attack, while pharming is a type of social engineering.
- C.** In both phishing and pharming, attackers can create websites that look very similar to legitimate sites in an effort to collect personal information from victims. In a phishing attack, attackers can provide URLs with domain names that look very similar to the legitimate site's address. For example, www.amazon.com might become www.amzaon.com. Or use a specially placed @ symbol. For example, www.msn.com@notmsn.com would actually take the victim to the website notmsn.com and provide the username of www.msn.com to this website. The username www.msn.com would not be a valid username for notmsn.com, so the victim would just be shown the home page of notmsn.com. Now, notmsn.com is a nefarious site created to look and feel just like www.msn.com. The victim feels he is at the legitimate site and logs in with his credentials. In a pharming attack, the victim is given a legitimate domain name, but that domain name is redirected to the attacker's website as a result of DNS poisoning. When the DNS server is poisoned to carry out a pharming attack, the records have been changed so that instead of sending the correct IP address for www.logicalsecurity.com, it sends the IP address of a legitimate-

looking, but fake, website created by the attacker.

- A** is incorrect because a pharming attack does not commonly involve the collection of information via e-mail. In fact, the benefit of a pharming attack to the attacker is that it can affect a large amount of victims without the need to send out e-mails. Like a phishing attack, a pharming attack involves a seemingly legitimate, yet fake, website. Victims are directed to the fake website because the hostname is incorrectly resolved as a result of DNS poisoning.
- B** is incorrect because both descriptions are true of phishing attacks. Pharming attacks do not use pop-up forms. However, some phishing attacks use pop-up forms when a victim is at a legitimate website. So if you were at your bank's actual website and a pop-up window appeared asking you for some sensitive information, this probably wouldn't worry you, since you were communicating with your actual bank's website. You may believe the window came from your bank's web server, so you fill it out as instructed. Unfortunately, this pop-up window could be from another source entirely, and your data could be placed right in the attacker's hands, not your bank's.
- D** is incorrect because both attacks are technical ways of carrying out social engineering. Phishing is a type of social engineering with the goal of obtaining personal information, credentials, credit card numbers, or financial data. The attackers lure, or fish, for sensitive data through various different methods, such as e-mail and pop-up forms. Pharming involves DNS poisoning. The attacker modifies the records in a DNS server so that it resolves a hostname into an incorrect IP address. The victim's system sends a request to a poisoned DNS server, which points the victim to a different website. This different website looks and feels just like the requested website, so the user enters his username and password and may even be presented with web pages that look legitimate.

- 26.** There are several types of intrusion detection systems (IDSs). What type of IDS builds a profile of an environment's normal activities and assigns an anomaly score to packets based on the profile?
- A.** State-based
 - B.** Statistical anomaly-based
 - C.** Misuse-detection system
 - D.** Protocol signature-based

- B.** A statistical anomaly-based IDS is a behavioral-based system. Behavioral-based IDS products do not use predefined signatures, but rather are put in a learning mode to build a profile of an environment's "normal" activities. This profile is built by continually sampling the environment's activities. The longer the IDS is put in a learning mode, in most instances, the more accurate a profile it will build and the better protection it will provide. After this profile is built, all future traffic and activities are compared to it. With the use of complex statistical algorithms, the IDS looks for anomalies in the network traffic or user activity. Each packet is given an anomaly score, which indicates its degree of irregularity. If the score is higher than the established threshold of "normal" behavior, then the preconfigured action will take place.
- A** is incorrect because a state-based IDS has rules that outline which state transition sequences should sound an alarm. The initial state is the state prior to the execution of an attack, and the compromised state is the state after successful penetration. The activity that takes place between the initial and compromised state is what the state-based IDS looks for, and it sends an alert if any of the state-transition sequences match its preconfigured rules.
- C** is incorrect because a misuse-detection system is simply another name for a signature-based IDS, which compares network or system activity to signatures or models of how attacks are carried out. Any action that is not recognized as an attack is considered acceptable. Signature-based IDSs are the most popular IDS products today, and their effectiveness depends upon regularly updating the software with new signatures, as with antivirus software. This type of IDS is weak against new types of attacks because it can only recognize those that have been previously identified and have had signatures written for them.
- D** is incorrect because a protocol signature-based IDS is not a formal IDS. This is a distracter answer.
- 27.** A rule-based IDS takes a different approach than a signature-based or anomaly-based system. Which of the following is characteristic of a rule-based IDS?
- A.** Uses IF/THEN programming within expert systems
 - B.** Identifies protocols used outside of their common bounds
 - C.** Compares patterns to several activities at once

D. Can detect new attacks

- A.** Rule-based intrusion detection is commonly associated with the use of an expert system. An expert system is made up of a knowledge base, an inference engine, and rule-based programming. Knowledge is represented as rules, and the data to be analyzed is referred to as facts. The knowledge of the system is written in rule-based programming (IF situation THEN action). These rules are applied to the facts, the data that comes in from a sensor, or a system that is being monitored. For example, an IDS pulls data from a system's audit log and stores it temporarily in its fact database. Then, the preconfigured rules are applied to this data to indicate whether anything suspicious is taking place. In our scenario, the rule states "*IF a root user creates File1 AND creates File2 SUCH THAT they are in the same directory THEN there is a call to Administrative Tool TRIGGER send alert.*" This rule has been defined such that if a root user creates two files in the same directory and then makes a call to a specific administrative tool, an alert should be sent.
- B** is incorrect because a protocol anomaly-based IDS identifies protocols used outside of their common bounds. The IDS has specific knowledge of each protocol that it will monitor. A protocol anomaly pertains to the format and behavior of a protocol. If a protocol is formatted differently or is demonstrating abnormal behavior, then the IDS triggers an alarm.
- C** is incorrect because a stateful matching IDS compares patterns to several activities at once. It is a type of signature-based IDS, meaning that it does pattern matching, similar to antivirus software. State is a snapshot of an operating system's values in volatile, semipermanent, and permanent memory locations. In a state-based IDS, the initial state is the state prior to the execution of an attack, and the compromised state is the state after successful penetration. The IDS has rules that outline which state transition sequences should sound an alarm.
- D** is incorrect because a rule-based IDS cannot detect new attacks. An anomaly-based IDS can detect new attacks because it doesn't rely on predetermined rules or signatures, which are only available after security researchers have had time to study an attack. Instead, an anomaly-based IDS learns the "normal" activities of an environment and triggers an alarm when it detects activity that differs from the norm. The three types of anomaly-based IDS are

statistical, protocol, and traffic. They are also called behavior or heuristic based.

- 28.** Tom works at a large retail company that recently deployed radio-frequency identification (RFID) to better manage its inventory processes. Employees use scanners to gather product-related information instead of manually looking up product data. Tom has found out that malicious customers have carried out attacks on the RFID technology to reduce the amount they pay on store items. Which of the following is the most likely reason for the existence of this type of vulnerability?
- A. The company's security team does not understand how to secure this type of technology.
 - B. The cost of integrating security within RFID is cost prohibitive.
 - C. The technology has low processing capabilities and encryption is very processor intensive.
 - D. RFID is a new and emerging technology, and the industry does not currently have ways to secure it.
- C. A common security issue with RFID is that the data can be captured as it moves from the tag to the reader and modified. While encryption can be integrated as a countermeasure, it is not common because RFID is a technology that has low processing capabilities and encryption is very processor intensive.
- A is incorrect because it is not necessarily the best answer here. The company in the question may understand RFID and its common security issues, but security usually has to be integrated within the RFID technology. This means the vendor of the RFID product would have to integrate security into the product, and the available security solutions are commonly limited because RFID tags and readers do not usually have the necessary processing power to carry out the necessary cryptographic functions.
- B is incorrect because the cost of integrating security into RFID products may or may not be a factor. It usually comes down to the limitation of the technology itself, not necessarily the costs involved.
- D is incorrect because it is not the best answer here. RFID has been around for many years, and many in the industry understand how it works and its security issues. Integrating security into a technology with so many limitations demands real needs and motivation. In

most situations the data that is being transferred through RFID is not overly sensitive, so there has not been a true perceived need to integrate security into it. As RFID evolves it will most likely be better equipped to handle security countermeasures, but the industry has not fully gotten to this place yet.

29. Tanya is the security administrator for a large distributed retail company. The company's network has many different network devices and software appliances that generate logs and audit data. Tanya and her staff have become overwhelmed with trying to review all of the log files when attempting to identify if anything suspicious is taking place within the network. Which of the following is the best solution for this company to implement?
- A. Security information and event management
 - B. Event correlation tools
 - C. Intrusion detection systems
 - D. Security event correlation management tools
- A. Today, many organizations are implementing security event management (SEM) systems, also called security information and event management (SIEM) systems. These products gather logs from various devices (servers, firewalls, routers, etc.) and attempt to correlate the log data and provide analysis capabilities. Companies also have different types of solutions on a network (IDS, IPS, antimalware, proxies, etc.) collecting logs in various proprietary formats, which require centralization, standardization, and normalization. Log formats are different per product type and vendor; thus, SIEM puts them into a standardized format for useful reporting.
- B is incorrect because answer A provides a more accurate portrayal of the needed solution. SEM and SIEM tools zero in on malicious events and provide a centralized management capability. The logs are commonly aggregated onto one system, and the SIEM software “translates” the logs into a standardized format. The standardization allows for the log data to be analyzed and reports generated.
- C is incorrect because an intrusion detection system is a product that identifies malicious activities and carries out notification activities. While these types of products may aggregate logs for analysis, they do not have the capability of standardizing log formats from different product types.

D is incorrect because it is not the best answer here. An argument can be made that security event correlation management tools is what the correct answer “Security information and event management” is carrying out, but on the exam you will be required to pick the *best* answer. Security information and event management (SIEM) is the actual term the industry uses for products that provide this type of functionality.

- 30.** The Logistics Agency of a country’s department of defense is responsible for ensuring that all necessary materials get to the proper locations to support the department’s day-to-day activities. The data that this agency maintains must be protected according to the three main security principles of security controls. For this agency’s responsibilities, which security principle has the highest priority?

- A.** Confidentiality
- B.** Integrity
- C.** Availability
- D.** Privacy

A. The three main security principles for any and all security controls are availability, integrity, and confidentiality (AIC). Clearly each of these is a concern for this organization’s mission. However, the confidentiality as to the disposition and location of these materials is of the highest priority. If an adversary were to gain access to knowledge of something as mundane as where large volumes of toilet paper were being shipped, they could infer troop movements in advance of a military offensive action.

B is incorrect because, although an operation could be severely impacted if an adversary were able to compromise the logistical deployment of materials for a military unit by violating the integrity of the data about it, this presupposes a violation of its confidentiality first.

C is incorrect because, although the availability of military logistics systems is clearly an extremely high priority for a fully functional deployment, in this context the confidentiality of which systems and data are key for any given operation is of even higher priority.

D is incorrect because, although privacy is an increasingly important consideration, it is not considered one of the three main security principles, as it is really a specific aspect of confidentiality.

- 31.** Claudia is the CISO for a global financial institution, overseeing the security of hundreds of millions of bank accounts. Which of the three main security principles should she consider most important when prioritizing the controls her enterprise should deploy?
- A.** Confidentiality
 - B.** Integrity
 - C.** Availability
 - D.** Authenticity
- B.** The three main security principles for any and all security controls are availability, integrity, and confidentiality (AIC). Clearly each of these is a concern for Claudia's organization's security. However, among these, the integrity of the account data is foremost. Integrity is the assurance that the bank account data has not been altered in an unauthorized way. A compromise of this principle could essentially mean that the account holders' money has been stolen—that the bank has been robbed.
- A** is incorrect because, although Claudia must be concerned with the confidentiality of her account holders' data, most likely to comply with banking and privacy regulations in multiple countries, the threat of an account being modified by an attacker is far greater.
- C** is incorrect because, although certainly Claudia's bank must be concerned with the availability of both data and systems to support 24/7 transactions, the threat of the unauthorized modification of the 1's and 0's the accounts contain (money!) is of greatest concern to a bank.
- D** is incorrect because the authenticity of entities attempting to perform transactions is also a concern, but only in so much as the transactions never result in unauthorized modifications to the account details. This is an integrity issue first and foremost.
- 32.** Which of the following is an example of a credential management system, also known as an identity management (IdM) system?
- A.** A historic log of the activities performed by users once they have presented their credentials to a central authorizing system
 - B.** A database of the credentials that have been registered to each individual in an enterprise, in order to correlate users with usernames and locales
 - C.** A security information and event management (SIEM) system that

contains the logs for various credentialing systems in the enterprise, for correlation of activities by ID

- D. A Kerberos Key Distribution Center (KDC) that contains the symmetric keys of all the entities and systems in a Kerberos realm, which can be centrally administered to ensure that it is up-to-date with respect to additions and deletions of keys
- D. Kerberos is a common solution to credential and identity management, facilitating all the needs of such a system, including the creation of accounts across systems, the assignment of account details and privileges, and the decommissioning of accounts when they are no longer required. It is the core technology behind Microsoft's Active Directory, which is the most common IdM solution in an enterprise environment.
- A is incorrect because, although it is important to be able to review the historical activities of individual users whose credentials have been provisioned by a central authorizing system, this is just one feature of a robust IdM system.
- B is incorrect because, although the data store of account information is a central feature of a credential management system, the ability to manage this data on a day-to-day basis is the salient feature.
- C is incorrect because, although a SIEM can be useful in tracking the activities of credentialed users across multiple systems in a large environment, its use is dependent upon a centralized credential management system such as Kerberos or Active Directory.

33. Which of the following attributes is used to biometrically authenticate a user's identity?

- A. Something you know
B. Something you have
C. Something you are
D. Someplace you are
- C. Each of "something you know," "something you have," and "something you are" are classic factors of authentication used to validate a user's claim of identity. Biometric authentication seeks to authenticate a user based on some unique physical attribute of the user, such as a fingerprint, the granularly pixilated color pattern of the iris of the eye, or the digitized pattern of a voice. This is innate

to the user, and so comprises “something you are.”

- A** is incorrect because something a user knows, such as a password, passphrase, or PIN number, is something that can easily be shared among users, and so is not an innate attribute to one user only.
- B** is incorrect because, likewise, something a user physically possesses, such as a token, card, or physical key, can be easily transferred or stolen. As such it is not necessarily unique to a user.
- D** is incorrect because “someplace you are” certainly isn’t innate to the user. It is a newer authentication factor that could be, for example, a geolocation provided by a GPS system or the physicality of a login on console (which places the user in a data center, perhaps). It can be used in multifactor authentication but isn’t particularly useful on its own.

34. Within biometric authentication, what is a Type II error rate?

- A.** The rate of errors where the system falsely accepts the authentication of an individual who is not who they purport to be
 - B.** The rate of errors where the system falsely rejects the authentication of an individual who is who they purport to be
 - C.** The rate of errors that the system produces where false rejections and false acceptances are equal
 - D.** The rate of errors where the system fails to either accept or reject the authentication of an individual regardless of their validity
- A.** The false acceptance rate (FAR) is the rate of Type II errors within a biometric system and represents the rate at which a system accepts impostors who should have been declined access. These are the most critical errors a biometric system should be tuned to minimize.
 - B** is incorrect because it describes the false rejection rate (FRR), which is the rate of Type I errors within a biometric system and represents the rate at which a system rejects authentic users who should have been granted access. Type I errors are the less critical errors, as they don’t result in an authentication bypass, but they are an annoyance to the user, who must try again to authenticate successfully.
 - C** is incorrect because it describes the crossover error rate (CER), which is the point in the sensitivity tuning of a biometric system in which the FAR and FRR are equal. The CER is used as a metric of

performance for any given biometric system, such that the lower the CER, the more accurate the system can be configured to be.

- D** is incorrect because the rate at which a system fails to perform altogether, either via FAR or FRR, is not a metric used for performance evaluation of a biometric system, but likely represents a systemic failure.
- 35.** Which of the following criteria is the most important consideration for the selection and deployment of a biometric authentication system?
- A.** False acceptance rate (FAR) or Type II error rate
 - B.** False rejection rate (FRR) or Type I error rate
 - C.** Crossover error rate (CER) or equal error rate (EER)
 - D.** Processing speed
- D.** Processing speed is the length of time it takes a biometric system to actually authenticate a user upon the presentation of the body part. Regardless of how well a system can be tuned with respect to FAR, FRR, or CER, unless the system can process a sufficient throughput of individuals in actual deployment, it will become a costly bottleneck. Much as different systems have different thresholds for accuracy, they have differing thresholds for throughput, based on the body part being used for authentication.
- A, B, and C** are incorrect because, although all of these measures are critical in consideration of which type of system to deploy, the most critical consideration in the real world is whether or not the system can meet the needs of the users being authenticated and the business mission the system has been deployed to support.
- 36.** Though “something you know,” in the form of passwords, is the most common authentication factor still used today, it is considered one of the weakest. This is because passwords are easy for users to share, and relatively easy for adversaries to steal or guess. Which of the following measures is the best way to counter attacks on this form of authentication?
- A.** Store all passwords in encrypted form only, so that recovering them requires a special key to decrypt them for authentication.
 - B.** Employ a password policy to ensure that passwords are chosen in such a way that they are neither easy for an attacker to guess nor easy for an attacker to brute force.
 - C.** Require that all passwords be composed of a combination of unique

characters, regardless of length.

- D. Ensure that accounts are locked out after a minimum number of incorrect guesses within a short amount of time.
- B.** Employing a comprehensive password policy is the best method for ensuring that the passwords selected by users are as strong as possible against all forms of attack. This includes making them less easy to guess, by prohibiting the use of strings that are associated with knowable attributes of the user, such as names, birth dates, etc. Passwords should include some amount of complexity beyond simple dictionary words as well, which typically requires the use of some special characters to make them less likely to be brute forceable. Most importantly, they should be required to be as long as is practical given the system implementing them. Password aging and periodic strength audits are also best practices.
- A** is incorrect because, although storing passwords in encrypted form only is absolutely required, the encryption used should not be reversible with any key. One-way hashing of passwords satisfies this requirement. Even so, encryption is but one aspect of a salient password policy.
- C** is incorrect because, as provided in the correct answer explanation, password complexity is a necessary but not sufficient requirement. Enforcing a password length requirement beyond 15 characters at a bare minimum is part of an effective password policy.
- D** is incorrect because account lockout after a small threshold of password guessing activity is also a necessary but insufficient aspect of an effective password policy.

37. Which of the following is the correct sequence in the Kerberos authentication process with respect to passwords, Key Distribution Centers (KDCs), ticket granting servers (TGSs), ticket granting tickets (TGTs), services, and service tickets?
- A. The user provides a username/password to the workstation, the workstation obtains a TGT from the TGS, then subsequently obtains a service ticket from the KDC, which it presents to the service.
- B. The workstation obtains a TGT from the KDC, which the user then validates with a password. The TGT is then exchanged for a service ticket from the TGS, which is presented to the service.

- C. The user provides a username/password to the workstation, the workstation obtains a TGT from the KDC, then subsequently obtains a service ticket from the TGS, which it presents to the service.
 - D. The user obtains a service ticket from the service. The user then validates this ticket with a username/password provided to the TGS, which results in a TGT that is further validated by the KDC in a final step.
- C. The user must first authenticate to the workstation with a username and password. These credentials are then forwarded by the workstation to the authentication service (AS) on the KDC, which then returns a TGT encrypted with the TGS's secret key. Later, when a service is required, the TGT is presented back to the TGS that can authenticate it, and which then returns a service ticket encrypted with the service's secret key. When the service ticket is presented to the service, mutual authentication can occur: the service knows the user must be authentic, because the user couldn't have a valid service ticket without having authenticated to the KDC and TGS, and the user knows the service is authentic, because it can decrypt the service ticket.
- A is incorrect because authentication with the KDC precedes interaction with the TGS.
- B is incorrect because the user must first authenticate with the workstation, so that it has the credentials to authenticate with the KDC.
- D is incorrect because this sequence is nonsensical and completely out of order.
- 38.** In practical use, which of the following best describes a “session”?
- A. Any data exchange between two discrete endpoints, over any arbitrary duration
 - B. Any authenticated exchange between two parties that is used to carry on a conversation, with a discrete beginning, period of activity, and termination
 - C. Any discrete period of time that a user is logged into a workstation
 - D. The volume of data exchanged between two systems during a discrete period of time
- B. In most practical uses of the word, a “session” implies some

initial form of authentication between two parties, be it between a user and a workstation or between two systems on a network. Subsequent to the authentication phase at the session's initiation, the two parties carry on an exchange of data interactively, and then terminate the exchange when the session is no longer required, most commonly through mutual agreement. A session therefore has a discrete beginning, period of interactive activity, and a discrete termination.

- A** is incorrect because this definition, although loosely accurate, misses the most common components of mutual initiation/authentication and termination. Though the duration may be arbitrary in length, it is commonly discretely limited.
 - C** is incorrect because a user logging into a workstation can certainly be considered a session by this definition, but it is a special case. Sessions can transpire between systems and services equally.
 - D** is incorrect because, although data will be exchanged during any session, the volume of it is not what defines a session, but rather the conversational nature of the exchange.
- 39.** The use of “resource servers” and “authorization servers” to enable a “client” web service (such as LinkedIn) to access a “resource owner” (such as Google) for federated authorization is a hallmark of what open standard?
- A.** OpenID
 - B.** SAML
 - C.** SSO
 - D.** OAuth
- D.** OAuth is an open standard for website-to-website authorization (not authentication). It is used to allow an account that a user is authenticated to on one site to access resources on another third-party site.
 - A** is incorrect because OpenID is an open standard not for authorization but for authentication by a third-party site that maintains the actual credentials for that user. It involves a “relying party” and an OpenID “provider.”
 - B** is incorrect because the Security Assertion Markup Language (SAML) is an XML-based standard for conveying authentication in a federated identity management system, commonly from business

to business.

- C** is incorrect because single sign-on (SSO), although also an authentication mechanism, is not an open standard and is typically managed and used within a single enterprise for heterogeneous system access.

40. Which of the following is NOT true of OpenID Connect (OIDC)?

- A.** It is mainly used as an open standards-based single sign-on (SSO) mechanism between disparate platforms within an enterprise environment.
- B.** It is layered on the OAuth protocol to allow both authentication and authorization in a transparent way for client resource requests.
- C.** It supports three flows: authorization code flow, implicit flow, and hybrid flow.
- D.** It involves browser redirections from the OpenID provider back to the relying party using authorization codes.
- A.** OAuth, OpenID, and OIDC are all open protocols and standards for use in authentication and authorization across, rather than within, enterprises to facilitate federated identity management (IdM).
- B** is incorrect because it is a true statement that OIDC is layered on OAuth 2.0, extending it to be able to provide authorization for third-party services, transparently to the user, in addition to authentication.
- C** is incorrect because it is a true statement that OIDC supports the three flows. Authorization code flow provides an authorization code to the relying party, which is then used to directly request an ID token from the identity provider (IdP). Implicit flow provides the relying party with the ID token directly, which is passed through the user's browser. Hybrid flow uses a combination of the two.
- D** is incorrect because it is a true statement that OIDC involves browser redirections from the OpenID provider back to the relying party using authorization codes (in hybrid flows, as described in option C, previously).

41. Which of the following attributes are added beyond traditional access control mechanisms (RBAC, MAC, and DAC) in order to implement ABAC?

- A.** Subjects

B. Objects

C. Actions

D. Context

- D.** Traditional methods such as role-based access control (RBAC), mandatory access control (MAC), and discretionary access control (DAC) each rely on categories of subjects and objects, and assign actions that can be performed based on combinations of the two. Attribute-based access control (ABAC) includes contexts, such as the time of day, the state or phase of a project, and other contextual events, in order to provide further granularity to which objects can be accessed by which subjects, when, and how.
- A** is incorrect because subjects (which users and systems) and their clearance levels are employed by all access control systems.
- B** is incorrect because objects (files, folders, processes, and other resources) and their classification or sensitivity labels are employed by all access control systems.
- C** is incorrect because actions that can be performed (read, write, execute, etc.) are also employed by all access control systems.

Security Assessment and Testing

This domain includes questions from the following topics:

- Internal, external, and third-party audits
 - Vulnerability testing
 - Penetration testing
 - Log reviews
 - Synthetic transactions
 - Code review and testing
 - Misuse case testing
 - Interface testing
 - Account management
 - Backup data verification
 - Disaster recovery and business continuity
 - Security training and security awareness
 - Key performance and risk indicators
 - Analyzing and reporting
 - Management review and approval
-
-

While it is the least represented domain in (ISC)²'s official documentation, security assessment and testing is one of the fastest-growing areas of activity in the information security realm. A great amount of attention has been given to this requirement by both regulatory auditors and the Payment Card Industry (PCI), resulting in a commercial service that is in high demand by enterprises seeking to remain compliant. Furthermore, the increase in media exposure garnered by high-profile breaches such as those suffered by both public and private enterprises has made senior-level management much more sensitive to such events.

It is increasingly understood that adequate protection of sensitive data cannot be provided without nearly continuous monitoring and testing of the systems deployed to do so. An untested system is a system of unknown

off: secu

Q

QUESTIONS

- 1.** How is interface testing different from misuse case testing?

 - A.** Interface testing is intended to determine correct function, whereas misuse case testing is intended to determine error conditions.
 - B.** Interface testing is intended to determine usability, whereas misuse case testing is intended to determine when misuse has occurred.
 - C.** Interface testing and misuse case testing are essentially the same.
 - D.** Interface testing is intended to determine correct function, whereas misuse case testing is intended to determine if an error condition could be problematic.
- 2.** What are the key stages of account management?

 - A.** Provisioning or adding accounts, modifying accounts, and suspending accounts
 - B.** Adding accounts, deleting accounts, and deleting users' data
 - C.** Verifying account passwords, validating account usage, and deleting accounts
 - D.** Provisioning accounts, modifying accounts, auditing the use of accounts, and suspending accounts
- 3.** What is a code review?

 - A.** Making sure coders work in parallel to watch each others' work while they are coding
 - B.** Making sure coders' work has been reviewed by other coders after they are done
 - C.** Making sure that the appropriate Q/A harnesses have been applied prior to check in
 - D.** Making sure that appropriate Q/A harnesses exist
- 4.** Which of the following statements is true with respect to security audits, vulnerability assessments, and penetration tests?

 - A.** Third-party security audits are only necessary when regulations require them.
 - B.** Vulnerability assessments and penetration tests are essentially the same.

- C. Vulnerability assessments help to prioritize weaknesses that need to be addressed.
 - D. Internal assessments have very little value.
5. Which of the following is the most important reason to log events remotely?
- A. To prevent against log tampering
 - B. To have several copies of the logs of every event
 - C. To make it easier to back up the logs on a single write-once media
 - D. To facilitate log review and analysis
6. How can a backup strategy be made most effective?
- A. By ensuring that all user data is backed up
 - B. By testing restoration procedures
 - C. By backing up database management systems (DBMSs) via their proprietary methods
 - D. By reviewing backup logs to ensure they are complete
7. What is a synthetic transaction?
- A. A bogus user transaction that must be disallowed
 - B. A scripted process used to emulate user behavior
 - C. User behavior intended to falsify records
 - D. A scripted process by an attacker used to violate policy
8. Why are security metrics so important as performance and/or risk indicators?
- A. They enable management to understand the performance of a security program.
 - B. They can be used to document deviations from standards.
 - C. They can help auditors determine whether incidents have been properly resolved.
 - D. They can be used to determine the cost of a countermeasure.
9. When providing a security report to management, which of the following is the most important component?
- A. A list of threats, vulnerabilities, and the probabilities that they will occur

- B. A comprehensive list of the probabilities and impacts of adverse events anticipated
 - C. An executive summary that is comprehensive but does not exceed two pages
 - D. An executive summary that is as long as is necessary to be technically comprehensive and that includes the lists referenced in options A and B
- 10. What is the difference between security training and a security awareness program, and which is most important?
 - A. A security awareness program addresses all employees regardless of role, whereas security training is role specific. The awareness program is most important.
 - B. A security awareness program focuses on specific roles, whereas security training addresses the needs of all employees. Both are equally important.
 - C. A security awareness program focuses on specific roles, whereas security training addresses the needs of all employees. Training is most important.
 - D. A security awareness program addresses all employees regardless of role, whereas security training is role specific. Both are equally important.
- 11. Which of the following describes a parallel test during disaster recovery testing?
 - A. It is performed to ensure that some systems will run at the alternate site.
 - B. All departments receive a copy of the disaster recovery plan to review it for completeness.
 - C. Representatives from each department come together and go through the test collectively.
 - D. Normal operations are shut down.
- 12. Which of the following describes a structured walk-through test during disaster recovery testing?
 - A. It is performed to ensure that critical systems will run at the alternate site.
 - B. All departments receive a copy of the recovery plan to review it for

completeness.

- C. Representatives from each department come together and go through the test collectively.
 - D. Normal operations are shut down.
13. John and his team are conducting a penetration test of a client's network. The team will conduct its testing armed only with knowledge it acquired from the Web. The network staff is aware that the testing will take place, but the penetration testing team will only work with publicly available data and some information from the client. What is the degree of the team's knowledge, and what type of test is the team carrying out?
- A. Full knowledge; blind test
 - B. Partial knowledge; blind test
 - C. Partial knowledge; double-blind test
 - D. Zero knowledge; targeted test
14. Fred is a new security officer who wants to implement a control for detecting and preventing users who attempt to exceed their authority by misusing the access rights that have been assigned to them. Which of the following best fits this need?
- A. Management review
 - B. Two-factor identification and authentication
 - C. Capturing this data in audit logs
 - D. Implementation of a strong security policy
15. What is the difference between a test and an assessment?
- A. An assessment is a comparison between the properties of a system and some predetermined standardized configuration. A test is a series of related assessments.
 - B. A test is a comparison between the properties of a system and some predetermined standardized configuration. An assessment is a series of related tests.
 - C. An assessment is a systematic test to determine a system's satisfaction of some external standard authored by a third party.
 - D. A test is a systematic assessment to determine a system's satisfaction of some external standard authored by a third party.

- 16.** Which of the following statements is most true with regard to internal security audits versus external, second-party audits?
- A.** Internal audits aren't as valid as external, second-party audits, because the insiders conducting them have an unrealistic advantage over real attackers due to their knowledge of the systems being inspected.
 - B.** Due to insider knowledge, internal audits require less technical skill to perform and so are more cost effective than external, second-party audits.
 - C.** Internal audits provide no logistical advantage over external, second-party audits, because in either case, management must schedule around disparate teams and routine program activities.
 - D.** The advantage in knowledge that an inside team has in conducting an internal audit is illusory, as advanced adversaries often approach or exceed the level of knowledge the inside team possesses.
- 17.** Which of the following is the most critical best practice when conducting an internal security audit?
- A.** Take advantage of the logistical flexibility that an internal audit can offer. Ad hoc scheduling makes internal audits much easier to execute than external ones.
 - B.** Compensate for the "insider knowledge" advantage of your internal audit team by sharing with them the least amount of information possible, especially with respect to policies, procedures, and configurations.
 - C.** Make sure to keep the audit report's audience in mind at all times during the process. The audit report needs to have an impact on not only managers but also operations staff.
 - D.** Rely on the defensive team to document what was done successfully against them, including when and how. That way the auditing team doesn't have to get bogged down with documenting all the things that were tried but ultimately didn't work.
- 18.** With respect to external audits, what is the difference between a second-party audit and a third-party audit?
- A.** A second-party audit is typically tied to the terms of a contract between business entities, while a third-party audit is usually used to determine if an entity is compliant with applicable government regulations.

- B. A third-party audit is typically tied to the terms of a contract between business entities, while a second-party audit is usually used to determine if an entity is compliant with applicable government regulations.
- C. A third-party audit is performed without the assistance of the entity's internal teams, whereas a second-party audit makes extensive use of them.
- D. There is no real distinction. Both terms can be used interchangeably.
19. Which of the following statements is true of audits conducted by external parties?
- A. They are inherently adversarial in nature, as the entity under inspection must seek to limit the extent of adverse findings, while the external party must seek to maximize them.
- B. Participation by the internal teams within the entity under inspection must be kept to a bare minimum, so as not to skew the objectivity of the external teams' findings.
- C. The terms of any contractual obligations relevant to the controls being audited must be kept confidential and not divulged to the external party conducting the inspection, so as not to skew the objectivity of the external teams' methodology or framework.
- D. The activities of the internal and external teams must be collaborative in nature, so as to maximize the auditor's ability to accurately assess the controls under inspection.
20. Which of the following is an advantage of having an audit performed by an external, third party?
- A. Third-party audits are cheaper to conduct than internal ones, as they tend to be less extensive.
- B. Third-party audit teams are likely to have a breadth of experience beyond what internal teams may possess, due to having inspected a wider array of systems, controls, and enterprises.
- C. Third-party audit teams are likely to better understand the systems and controls they are inspecting than the internal teams responsible for architecting, deploying, and maintaining them.
- D. Due to their experience having audited a broad array of enterprises, a third-party assessor is likely to better and more objectively understand the internal dynamics and politics of the target

organization.

- 21.** Which of the following is NOT an important practice when facilitating a third-party audit?
- A. Ensure that the internal teams responsible for the systems and controls under audit are keenly aware of the requirements, methodology, and framework for the assessment.
 - B. Conduct an internal audit ahead of time, using the same framework and methodology that the third party will use, so that there are no surprises.
 - C. Keep the details of the progress and findings of the third-party assessment tightly confidential, disclosing the results to management only once they have been finalized, so as to avoid unnecessary alarm or managerial interference.
 - D. Be prepared to facilitate the third party's inspection of internal systems, but also to maintain control of them at all times in case the auditors' activities threaten to cause inadvertent disruption or other adverse effects.
- 22.** Why is "test coverage" an important consideration during an audit?
- A. The percentage of systems or controls to be tested should not exceed the threshold beyond which further testing yields no additional results or useful information, in order to limit unnecessary expense.
 - B. The coverage of any given test should always include all possible systems and controls within scope of the audit. Nothing should be excluded unnecessarily.
 - C. Tests should cover not only the systems in scope, but also the adjoining or ancillary systems whose configurations may possibly affect the systems within scope.
 - D. The systems to be covered within any given test should not be decided by the enterprise being tested, but rather designated only by a third-party assessor.
- 23.** Which of the following statements is true with respect to vulnerability tests versus penetration tests?
- A. They are essentially the same. In most cases both terms may be used interchangeably.
 - B. The goals between the two differ slightly, but are similar enough

- that they should be handled in effectively the same way.
- C. Many of the same tools and techniques are commonly employed regardless of which of the two tests is being conducted.
 - D. Though the goals, tools, and techniques are distinctly different between the two, either approach can be an acceptable replacement for the other.
- 24.** Which of the following types of tests involves discursive explorations of existing response procedures, based on a likely adverse scenario, designed to determine if desired outcomes will result?
- A. Structured walk-through test
 - B. Tabletop exercise
 - C. Simulation test
 - D. Checklist test
- 25.** Camellia has just concluded a security audit of some critical services within her environment and the state of the controls deployed to protect them. She has the results of a battery of technical tests and must now organize them into a written report to her chain of management. In analyzing these results, what must her immediate goal be?
- A. Forwarding these results to upper management in as much technical detail as possible, as quickly as possible, so that upper management can sort out what to do about them
 - B. Crafting a high-level summary of the results for upper management so that they can decide the relative importance of the results to the business mission
 - C. Exploring countermeasures for every one of the negative findings in order to ascertain the least costly approach to fixing all the problems
 - D. Seeking to understand what the results mean, the relative importance of each result, and what, if anything, can and should be done about each
- 26.** As a security analyst writing a technical report about the findings of a technical security assessment, what should your primary goal be?
- A. Detailing as much of the raw data that went into the report as possible so that operations staff has absolutely everything they need to understand the issues that need to be remediated

- B.** Providing step-by-step remediation advice for each of the most critical findings so that corrections can be deployed as easily and rapidly as possible
 - C.** Distilling the findings of the assessment into an executive summary, accessible to all levels of management
 - D.** Constructing a cogent and compelling narrative that will persuade the intended audience to enact the measures necessary to reduce critical risks to the business mission, based on an honest and factual analysis
- 27.** Why is a “Methodology” section as critical to a technical security assessment report as the findings themselves?
 - A.** It isn’t. The findings and suggested mitigations are far more important.
 - B.** It helps management understand the value of the expensive tools that have been purchased to conduct the assessment, and the expense of the effort it took to use them to produce the results.
 - C.** It describes how the tests can be repeated by others to validate the results as required, and to further validate that mitigations, once deployed, have been effective.
 - D.** It provides the audience with the context of how, where, and why the inspection was conducted.
- 28.** Which of the following types of vulnerabilities CANNOT be discovered in the course of a routine vulnerability assessment?
 - A.** Zero-day vulnerability
 - B.** Kernel flaw
 - C.** Buffer overflow
 - D.** File and directory permissions

QUICK ANSWER KEY

- 1.** D
- 2.** D
- 3.** B
- 4.** C
- 5.** A

- 6.** B
- 7.** B
- 8.** A
- 9.** C
- 10.** D
- 11.** A
- 12.** C
- 13.** B
- 14.** A
- 15.** B
- 16.** D
- 17.** C
- 18.** A
- 19.** D
- 20.** B
- 21.** C
- 22.** A
- 23.** C
- 24.** B
- 25.** D
- 26.** D
- 27.** C
- 28.** A

ANSWERS A

- 1.** How is interface testing different from misuse case testing?
 - A.** Interface testing is intended to determine correct function, whereas misuse case testing is intended to determine error conditions.
 - B.** Interface testing is intended to determine usability, whereas misuse case testing is intended to determine when misuse has occurred.
 - C.** Interface testing and misuse case testing are essentially the same.

D. Interface testing is intended to determine correct function, whereas misuse case testing is intended to determine if an error condition could be problematic.

- D.** All apps must undergo interface testing to be properly functional and usable. But they should also undergo misuse case testing in order to determine whether an intentional misuse of them could result in an error that subverts the confidentiality, integrity, and availability of the data the app provides access to.
- A** is incorrect because error conditions are likely to arise, but not necessarily as a result of misuse conditions.
- B** is incorrect because, while detection of events of misuse is important, testing for the results of intentional misuses is more important.
- C** is incorrect because of the distinct differences discussed for answers A and B.

2. What are the key stages of account management?

- A.** Provisioning or adding accounts, modifying accounts, and suspending accounts
 - B.** Adding accounts, deleting accounts, and deleting users' data
 - C.** Verifying account passwords, validating account usage, and deleting accounts
 - D.** Provisioning accounts, modifying accounts, auditing the use of accounts, and suspending accounts
- D.** All stages in the life cycle of authenticated access should be accounted for. Access should not be granted without appropriate direction, nor should access be allowed or denied without expected permissions. And the suspension of access should be auditable as well.
 - A** is incorrect because the auditing of the use of accounts is not included.
 - B** is incorrect because the deletion of users' data may conflict with data retention requirements.
 - C** is incorrect because it is simply a stage of authentication and doesn't relate to account management.

3. What is a code review?

- A.** Making sure coders work in parallel to watch each others' work while they are coding
 - B.** Making sure coders' work has been reviewed by other coders after they are done
 - C.** Making sure that the appropriate Q/A harnesses have been applied prior to check in
 - D.** Making sure that appropriate Q/A harnesses exist
- B.** A static code review requires that at least one other set of eyes inspects the code before it is deployed in order to search for flaws that may have not been obvious to the author but may be apparent to another engineer. In science we call it peer review.
- A** is incorrect because, while parallel or team coding is a good practice to provide peer review, it is not considered a static review.
- C** is incorrect, though a good practice.
- D** is incorrect, but is likewise a best practice.
- 4.** Which of the following statements is true with respect to security audits, vulnerability assessments, and penetration tests?
- A.** Third-party security audits are only necessary when regulations require them.
 - B.** Vulnerability assessments and penetration tests are essentially the same.
 - C.** Vulnerability assessments help to prioritize weaknesses that need to be addressed.
 - D.** Internal assessments have very little value.
- C.** The most valuable aspect of vulnerability assessments, whether conducted internally or by a third party, is that they help to enumerate all of the potential vulnerabilities that an enterprise has so that remediation can be prioritized.
- A** is incorrect because even though some organizations may not be required to have independent reviews, they will often bring to light weaknesses that might otherwise have been overlooked.
- B** is incorrect because vulnerability assessments seek to enumerate every weakness so that the countermeasures for them can be appropriately prioritized. Penetration tests seek to examine the likelihood that a real-world attacker could exploit any given

weakness to achieve a goal.

- D** is incorrect because internal audits of an enterprise security posture are not usually sufficient, but can be very beneficial if conducted in concert with third-party reviews.

5. Which of the following is the most important reason to log events remotely?

- A.** To prevent against log tampering
 - B.** To have several copies of the logs of every event
 - C.** To make it easier to back up the logs on a single write-once media
 - D.** To facilitate log review and analysis
- A.** Event logs are usually one of the first things that an intruder will seek to modify in order to cover their tracks. If events are being logged only locally, a compromise means that those logs can no longer be considered valid for investigative purposes.
 - B** is incorrect because even though redundancy of event logs can be useful, the primary reason to log events remotely is to ensure that a copy exists that hasn't been subject to tampering, making it a valid tool in the investigation of the compromise.
 - C** is incorrect because backing up logs to immutable media is important for many reasons, but the best one is that events recorded remotely cannot easily be altered by an intruder.
 - D** is incorrect in this context, even while true. Log aggregation can certainly facilitate reviews of events, and aid in intrusion detection and analysis. However, answer A is still the most important reason because all intrusion analysis relies on unaltered evidence.

6. How can a backup strategy be made most effective?

- A.** By ensuring that all user data is backed up
 - B.** By testing restoration procedures
 - C.** By backing up database management systems (DBMSs) via their proprietary methods
 - D.** By reviewing backup logs to ensure they are complete
- B.** Unless the ability to restore from backups successfully is tested routinely, no other activities around data retention have value.
 - A** is incorrect because although making copies of user data is

important, unless the copies can be assured to be restorable, copying is futile.

- C** is incorrect because although it is a good idea to use a DBMS's native means for ensuring transactional copies are available, those copies are not to be trusted unless restoration is tested.
- D** is incorrect because although monitoring backup logs for completion is a good operational practice, it is no replacement for periodic testing of the backups themselves and the ability to truly recover from data loss.

7. What is a synthetic transaction?

- A.** A bogus user transaction that must be disallowed
 - B.** A scripted process used to emulate user behavior
 - C.** User behavior intended to falsify records
 - D.** A scripted process by an attacker used to violate policy
- B.** Testing applications commonly involves the need to emulate usual user behaviors. However, in a test environment, the typical load of user activity is unavailable. Consequently, scripts of common user transactions can be constructed to facilitate various forms of tests.
 - A** is incorrect because synthetic transactions are neither bogus nor user driven. Improper user behavior can be systematically tested through synthetic transactions, but the behavior is generated by a script.
 - C** is incorrect because live attacks are not synthetic. Attempts to bypass integrity controls can be part of a scripted set of tests, but they do not involve actual users.
 - D** is incorrect because a scripted process by an attacker is not a synthetic transaction, for the reasons stated in the previous explanations. Emulating scripted attack traffic may be the goal of synthetic transactions, but the actual live attack is out of the context of lab testing.

8. Why are security metrics so important as performance and/or risk indicators?

- A.** They enable management to understand the performance of a security program.
- B.** They can be used to document deviations from standards.

- C. They can help auditors determine whether incidents have been properly resolved.
 - D. They can be used to determine the cost of a countermeasure.
- A. The greatest value of security metrics is to establish the key performance indicators (KPIs) and key risk indicators (KRIs) that must be used by senior management to evaluate the effectiveness of an information security management system (ISMS). The best way to determine whether such a program is actually improving the security posture of an enterprise and reducing overall risk is through longitudinal tracking of quantified data.
- B is correct, but it is not the best answer. Incidents of discovered deviations from standards can be quantified and provide the basis for KPIs and KRIs, but they are useless unless they are tracked consistently and are acted upon by management in concert with other indicators.
- C is incorrect because the necessary requirement for auditors to determine proper resolution of security incidents is an adequate tracking system capable of recording the process of response and mitigation.
- D is incorrect because although the total cost of ownership (TCO) of any countermeasure should optimally be thoroughly quantified, those costs are not usually related to security metrics. Rather, those costs are usually measured in terms of capital expenditures (CAPEX) and operational expenditures (OPEX).
9. When providing a security report to management, which of the following is the most important component?
- A. A list of threats, vulnerabilities, and the probabilities that they will occur
 - B. A comprehensive list of the probabilities and impacts of adverse events anticipated
 - C. An executive summary that is comprehensive but does not exceed two pages
 - D. An executive summary that is as long as is necessary to be technically comprehensive and that includes the lists referenced in options A and B
- C. No matter how technically comprehensive a report to management must be, the executive summary should never exceed

two pages. IT security professionals must understand that the risks posed to an enterprise by data compromise are only one of many concerns that senior management must try to understand and prioritize. C-level executives have to be concerned with a lot of risks, and highly technical threats with which they are not familiar may be difficult for them to sort out appropriately. That means that it is the primary job of the IT security professional to summarize the risks in a way that makes sense to management, and as briefly as possible.

- A** is incorrect because it is not the most important component when reporting to management. While such a list is essential to a comprehensive security report, providing it to management will be unlikely to result in effective action without a well-crafted executive summary.
 - B** is incorrect because it is not the most important component when reporting to management. Again, while such a list is critical in any technical report, the executive summary is crucial to achieving action on the goal of risk reduction.
 - D** is incorrect because it describes what might be the most common and critical failure when reporting to management. The audience of the executive summary is unlikely to read past a page or (at most) two of technical details, which is reasonable given the need to balance their attention among so many competing concerns. For a topic with which they are particularly unfamiliar, their tolerance for obscure information will be low.
- 10.** What is the difference between security training and a security awareness program, and which is most important?
- A.** A security awareness program addresses all employees regardless of role, whereas security training is role specific. The awareness program is most important.
 - B.** A security awareness program focuses on specific roles, whereas security training addresses the needs of all employees. Both are equally important.
 - C.** A security awareness program focuses on specific roles, whereas security training addresses the needs of all employees. Training is most important.
 - D.** A security awareness program addresses all employees regardless of role, whereas security training is role specific. Both are equally

important.

- D.** The main difference between a security awareness program and security training is the focus on employee role. All employees have a role in maintaining enterprise security, so awareness of the threats and their responsibilities to be mindful of them is the goal of an awareness program. Conversely, some employee roles require skill-specific training in security because it is an inherent part of their job. This requires specific security training. Regardless of the difference between the two, both are absolutely equally required for an enterprise to be secure.
 - A** is incorrect because of the second sentence. A security awareness program is essential, but equally so is security training for specific critical employee roles.
 - B** is incorrect because it transposes the focus of a security awareness program and the focus of role-specific security training.
 - C** is incorrect for the same reason as answer B and further emphasizes one over the other.
- 11.** Which of the following describes a parallel test during disaster recovery testing?
- A.** It is performed to ensure that some systems will run at the alternate site.
 - B.** All departments receive a copy of the disaster recovery plan to review it for completeness.
 - C.** Representatives from each department come together and go through the test collectively.
 - D.** Normal operations are shut down.
- A.** In a parallel test, some systems are run at the alternate site and results are compared with how processing takes place at the primary site. This is to ensure the systems work at the alternate site and productivity is not affected. This also extends the previous test and allows the team to walk through the steps of setting up and configuring systems at the offsite facility.
 - B** is incorrect because this option describes a checklist test.
 - C** is incorrect because this option describes a structured walk-through test.
 - D** is incorrect because this option describes a full-interruption test.

- 12.** Which of the following describes a structured walk-through test during disaster recovery testing?
- A. It is performed to ensure that critical systems will run at the alternate site.
 - B. All departments receive a copy of the recovery plan to review it for completeness.
 - C. Representatives from each department come together and go through the test collectively.
 - D. Normal operations are shut down.
- C. During a structured walk-through test, functional representatives meet and review the plan to ensure its accuracy and that it correctly and accurately reflects the company's recovery strategy by walking through it step-by-step.
- A is incorrect because this option describes a parallel test.
- B is incorrect because this option describes a checklist test.
- D is incorrect because this option describes a full-interruption test.
- 13.** John and his team are conducting a penetration test of a client's network. The team will conduct its testing armed only with knowledge it acquired from the Web. The network staff is aware that the testing will take place, but the penetration testing team will only work with publicly available data and some information from the client. What is the degree of the team's knowledge, and what type of test is the team carrying out?
- A. Full knowledge; blind test
 - B. Partial knowledge; blind test
 - C. Partial knowledge; double-blind test
 - D. Zero knowledge; targeted test
- B. The penetration testing team can have varying degrees of knowledge about the penetration target before the tests are actually carried out. These degrees of knowledge are zero knowledge, partial knowledge, and full knowledge. John and his team have partial knowledge; the team has some information about the target. Tests may also be blind, double-blind, or targeted. John's team is carrying out a blind test, meaning that the network staff knows that the test will take place.

- A** is incorrect because John and his team do not have full knowledge of the target. Full knowledge means that the team has intimate knowledge of the target and fully understands the network, its software, and configurations. John's team has gathered information from the Web and partial information from the client. This is partial knowledge. The rest of the answer is correct; the team is conducting a blind test.
- C** is incorrect because John and his team are not conducting a double-blind test. A double-blind test, also called a stealth assessment, is when the assessor carries out a blind test without the security staff's knowledge. This enables the test to evaluate the network's security level and the staff's responses, log monitoring, and escalation processes and is a more realistic demonstration of the likely success or failure of an attack.
- D** is incorrect because John and his team do not have zero knowledge, nor are they conducting a targeted test. Zero knowledge means that the team does not have any knowledge of the target and must start from ground zero. John's team is starting the project with knowledge it acquired about the target online and with information provided by the client. Targeted tests commonly involve external consultants and internal staff carrying out focused tests on specific areas of interest. For example, before a new application is rolled out, the team might test it for vulnerabilities before installing it into production. John's team is not focusing its testing efforts on any one specific area.

- 14.** Fred is a new security officer who wants to implement a control for detecting and preventing users who attempt to exceed their authority by misusing the access rights that have been assigned to them. Which of the following best fits this need?
- A.** Management review
 - B.** Two-factor identification and authentication
 - C.** Capturing this data in audit logs
 - D.** Implementation of a strong security policy
- A.** The goal of this question is for you to realize that management and supervisor involvement is critical to ensure that these types of things do not take place or are properly detected and acted upon if they do take place. If the users know that management will take action if they misbehave, this can be considered preventive in

nature. The activities will only be known of after they take place, which means that the security office has to carry out some type of detective activity so that he can then inform management.

- B** is incorrect because identification and authentication is preventive, not detective.
- C** is incorrect because audit logs are detective but not preventive. However, in order to be detective, the audit logs must be reviewed by a security administrator. While some of the strongest security protections come from preventive controls, detective controls such as reviewing audit logs are also required.
- D** is incorrect because a security policy is preventive, not detective. A security policy is developed and implemented to inform users of what is expected of them and the potential ramifications if they do not follow the constructs of the policy.

15. What is the difference between a test and an assessment?

- A.** An assessment is a comparison between the properties of a system and some predetermined standardized configuration. A test is a series of related assessments.
 - B.** A test is a comparison between the properties of a system and some predetermined standardized configuration. An assessment is a series of related tests.
 - C.** An assessment is a systematic test to determine a system's satisfaction of some external standard authored by a third party.
 - D.** A test is a systematic assessment to determine a system's satisfaction of some external standard authored by a third party.
- B.** A test is an examination of the properties or behaviors of a particular system compared to a baseline established by the enterprise to satisfy the approved security posture for the system or device. An assessment is a series of such tests across a deployment of related devices or systems, performed to determine the general security posture of an entire functional area.
 - A** is incorrect, in that it is backward with respect to tests and assessments.
 - C** is incorrect because when discussing the satisfaction of third-party standards, we are generally referring to an audit, which is an effort of much larger scope than tests and assessments, and subsumes and includes them both.

D is incorrect, as per the explanation of option C.

- 16.** Which of the following statements is most true with regard to internal security audits versus external, second-party audits?
- A. Internal audits aren't as valid as external, second-party audits, because the insiders conducting them have an unrealistic advantage over real attackers due to their knowledge of the systems being inspected.
 - B. Due to insider knowledge, internal audits require less technical skill to perform and so are more cost effective than external, second-party audits.
 - C. Internal audits provide no logistical advantage over external, second-party audits, because in either case, management must schedule around disparate teams and routine program activities.
 - D. The advantage in knowledge that an inside team has in conducting an internal audit is illusory, as advanced adversaries often approach or exceed the level of knowledge the inside team possesses.
- D.** A dedicated and persistent adversary will likely gain a level of knowledge of their target that rivals or exceeds that of the internal audit team, both in breadth and accuracy. Further, their reconnaissance will likely be much more targeted than an internal team will leverage, and will be better aware of their own goals than the defender imagines.
- A** is incorrect, per the reasons discussed for the correct answer.
- B** is incorrect because regardless of the level of advance knowledge of the systems to be inspected, the level of skill required to thoroughly audit them remains the same. Unfortunately, most enterprises don't have the level of internal skills necessary to emulate the level of skill the adversary is likely to be able to leverage.
- C** is incorrect because audits performed purely internally bring all components and teams within the scope of enterprise management, and so make facilitating an agile and flexible schedule much simpler than scheduling the availability and logistics of external teams.
- 17.** Which of the following is the most critical best practice when conducting an internal security audit?
- A. Take advantage of the logistical flexibility that an internal audit can

offer. Ad hoc scheduling makes internal audits much easier to execute than external ones.

- B.** Compensate for the “insider knowledge” advantage of your internal audit team by sharing with them the least amount of information possible, especially with respect to policies, procedures, and configurations.
 - C.** Make sure to keep the audit report’s audience in mind at all times during the process. The audit report needs to have an impact on not only managers but also operations staff.
 - D.** Rely on the defensive team to document what was done successfully against them, including when and how. That way the auditing team doesn’t have to get bogged down with documenting all the things that were tried but ultimately didn’t work.
- C.** The most important practice when conducting internal audits is to ensure both that the results are actionable by operations staff and that their importance is well understood by the management team that is responsible for actions being taken. Otherwise, such audit activities present negative value, introducing liability for the organization by demonstrating institutional knowledge of weaknesses which then go unaddressed.
- A** is incorrect because internal teams need just as much lead time for preparation and proper scheduling of resources as an external team does; otherwise, such efforts will likely be very poorly executed, and opportunities to gain critical insights will be lost.
- B** is incorrect because it is based on the fallacy that a true external adversary will not gain the level of operational knowledge that an insider may have. To gain the greatest benefit of any audit, the audit team should be armed with the greatest possible amount of intelligence about the current state of technical capabilities of the enterprise.
- D** is incorrect because in many, if not most, cases the defensive team will not have any understanding as to what weaknesses were uncovered unless accurately documented by the audit team. Likewise, great value can be gained through the documentation of the absence of weaknesses where testing can demonstrate the proper functioning of controls.
- 18.** With respect to external audits, what is the difference between a second-party audit and a third-party audit?

- A.** A second-party audit is typically tied to the terms of a contract between business entities, while a third-party audit is usually used to determine if an entity is compliant with applicable government regulations.
- B.** A third-party audit is typically tied to the terms of a contract between business entities, while a second-party audit is usually used to determine if an entity is compliant with applicable government regulations.
- C.** A third-party audit is performed without the assistance of the entity's internal teams, whereas a second-party audit makes extensive use of them.
- D.** There is no real distinction. Both terms can be used interchangeably.
- A.** Second-party audits are typically performed by external parties, in order to give business partners the assurance that the entity being audited is living up to the terms of contractual agreements between the two with respect to due care and due diligence in the handling of the business partner's assets. Third-party audits are commonly performed as part of an entity's requirements to satisfy regulatory compliance with respect to systems processing information deemed to be in the public interest.
- B** is incorrect because it is the reverse of what is true, per the discussion of the correct answer.
- C** is incorrect because whether performed to assess adherence to contractual obligations or compliance with governmental regulations, all external audits must be facilitated by internal teams to the greatest extent possible. Without the assistance of internal operations for access and context, an external audit cannot produce useful results.
- D** is incorrect because, although the external parties conducting each type of audit may not differ and might follow the same methodology or framework, the goals of each type are quite distinctly different, as would be the audience for the results, per the discussion of the correct answer.
- 19.** Which of the following statements is true of audits conducted by external parties?
- A.** They are inherently adversarial in nature, as the entity under inspection must seek to limit the extent of adverse findings, while

the external party must seek to maximize them.

- B.** Participation by the internal teams within the entity under inspection must be kept to a bare minimum, so as not to skew the objectivity of the external teams' findings.
 - C.** The terms of any contractual obligations relevant to the controls being audited must be kept confidential and not divulged to the external party conducting the inspection, so as not to skew the objectivity of the external teams' methodology or framework.
 - D.** The activities of the internal and external teams must be collaborative in nature, so as to maximize the auditor's ability to accurately assess the controls under inspection.
- D.** Without a high degree of collaboration and cooperation between the teams on both sides, any such audit will be far less likely to come to an accurate assessment of the state of the security controls being inspected. An adversarial approach will greatly decrease the overall value of the effort, while simultaneously increasing the cost of performing it. One of the main goals of any external audit is to engender trust, which invariably requires honest and active cooperation among all participants.
- A** is incorrect, though a common misconception. As described for the correct answer, a major goal of such an effort is the fostering of mutual trust, and this is highly unlikely to be achieved via an adversarial regime. Furthermore, neither party benefits from inaccurate findings, whether positive or negative, and this is more likely to be the outcome of teams actively working in opposition to one another.
- B** is incorrect, though also a common misconception. An objective assessment is certainly the goal, and one of the main reasons an external party is brought in to conduct the audit in the first place, but without the active participation and assistance of the enterprise under inspection, accurate results simply cannot be achieved, and inaccurate findings benefit no one.
- C** is incorrect because without a keen understanding of the context and purpose of the audit, the external assessor has no hope of being able to properly focus their efforts and to keep their activities within the proper scope.
- 20.** Which of the following is an advantage of having an audit performed by an external, third party?

- A.** Third-party audits are cheaper to conduct than internal ones, as they tend to be less extensive.
 - B.** Third-party audit teams are likely to have a breadth of experience beyond what internal teams may possess, due to having inspected a wider array of systems, controls, and enterprises.
 - C.** Third-party audit teams are likely to better understand the systems and controls they are inspecting than the internal teams responsible for architecting, deploying, and maintaining them.
 - D.** Due to their experience having audited a broad array of enterprises, a third-party assessor is likely to better and more objectively understand the internal dynamics and politics of the target organization.
- B.** One of the great strengths of an external auditor is expected to be the experience of assessing a broader array of systems and controls than are deployed and maintained within any single enterprise. This should bring with it a better understanding of the broader context within which these controls operate, as well as some perspective as to issues the target enterprise is not aware of or hasn't fully considered.
- A** is incorrect not only because it is quite uncommon for an external audit to be less expensive overall than a purely internal assessment, but also because the scope of an external audit may be wider or narrower than an audit conducted internally, depending on the goals of the effort. If done properly, internal teams will be nearly as engaged in the external effort as with an internal one, so there is no cost savings there.
- C** is incorrect because, although the external assessor should bring experience with a broader array of systems and controls, their knowledge and understanding of how any given enterprise has deployed, configured, and maintains their own systems and controls will reasonably be dwarfed by the team responsible for them.
- D** is incorrect because, although an external assessor typically brings a level of objectivity that may be hard to come by from a purely internal and perhaps insulated perspective, and has probably experienced all manner of internal dynamics and politics, this doesn't necessarily equate to a keener understanding of the specifics of any given enterprise environment with which they have limited familiarity.

- 21.** Which of the following is NOT an important practice when facilitating a third-party audit?
- A. Ensure that the internal teams responsible for the systems and controls under audit are keenly aware of the requirements, methodology, and framework for the assessment.
 - B. Conduct an internal audit ahead of time, using the same framework and methodology that the third party will use, so that there are no surprises.
 - C. Keep the details of the progress and findings of the third-party assessment tightly confidential, disclosing the results to management only once they have been finalized, so as to avoid unnecessary alarm or managerial interference.
 - D. Be prepared to facilitate the third party's inspection of internal systems, but also to maintain control of them at all times in case the auditors' activities threaten to cause inadvertent disruption or other adverse effects.
- C. While it is certainly the case that preliminary findings may be inaccurate, and hence cause some amount of unnecessary alarm if viewed without proper context, management must be kept apprised of the auditors' activities and discoveries at all times. Management still bears the responsibility of operating the business, which includes responding to adverse conditions, even as the audit effort is ongoing.
- A is incorrect, as it is quite important that the enterprise be adequately prepared to facilitate the third-party assessors fully, within the scope of the audit. Doing so will help keep cost and disruption to a minimum, and maximize the accuracy and value of the effort.
- B is incorrect because performing an internal audit ahead of the third-party one, using the same techniques, framework, and scope, can give the enterprise the opportunity to address the most significant gaps in advance, or to at least set management's expectations as to what the results are likely to be. Surprise findings by an external party are inevitably more disruptive to the business mission. Furthermore, if an external assessor can be made aware that a problem is already known and is in the process of being addressed, the issue may be deemed less critical, and the remedial efforts may be reflected in the final report even if they are not yet completed. This can be a much more positive finding.

D is incorrect because any technical assessment poses risks of disruption and breaches of confidentiality, nondisclosure agreements notwithstanding, so the enterprise absolutely must maintain a position of control over the systems and controls under inspection. This is why a collaborative approach is so critical. A common misconception is that when a third-party assessor is brought in, the target enterprise must cede all control over the environment under inspection. Nothing can or should be further from the truth.

22. Why is “test coverage” an important consideration during an audit?

- A.** The percentage of systems or controls to be tested should not exceed the threshold beyond which further testing yields no additional results or useful information, in order to limit unnecessary expense.
 - B.** The coverage of any given test should always include all possible systems and controls within scope of the audit. Nothing should be excluded unnecessarily.
 - C.** Tests should cover not only the systems in scope, but also the adjoining or ancillary systems whose configurations may possibly affect the systems within scope.
 - D.** The systems to be covered within any given test should not be decided by the enterprise being tested, but rather designated only by a third-party assessor.
- A.** When testing a set of controls across a fleet of systems, if it can be determined that they are uniformly configured and deployed, it may make little sense to inspect each of them individually, and certainly will increase the cost of the assessment. As with any activity within a business environment, costs and benefits must be considered with a goal of achieving the best balance between them.
- B** is incorrect because it ignores the increasing cost of the activity without consideration of the benefit to be gained, as discussed for the correct answer.
- C** is incorrect because the scope of any assessment should be determined ahead of time and limited as strictly as possible to avoid undue cost and disruption while still satisfying the primary goals. Some systems and controls must remain out of scope out of pure necessity.
- D** is incorrect because the scope of an assessment, with respect to

the goals and therefore the systems and controls to be inspected, should be the result of a collaborative effort between the target enterprise and the assessor, so that maximum benefit can be gained at the minimum level of cost and potential disruption.

- 23.** Which of the following statements is true with respect to vulnerability tests versus penetration tests?
- A. They are essentially the same. In most cases both terms may be used interchangeably.
 - B. The goals between the two differ slightly, but are similar enough that they should be handled in effectively the same way.
 - C. Many of the same tools and techniques are commonly employed regardless of which of the two tests is being conducted.
 - D. Though the goals, tools, and techniques are distinctly different between the two, either approach can be an acceptable replacement for the other.
- C. Though vulnerability assessments and penetration testing are very different activities with distinctly different goals, many of the same tools and techniques will necessarily be employed regardless of which type of test is being conducted.
- A and B are incorrect because, as described for the correct answer, vulnerability assessments and penetration testing are very different activities with very different goals. A vulnerability assessment is designed to enumerate all knowable weaknesses within a set of systems within scope of the test. A penetration test is designed to actually exercise, or exploit, vulnerabilities to demonstrate what an attacker could successfully do with them. As a result, these activities must be managed in very different ways.
- D is incorrect precisely because the goals, tools, and techniques are distinctly different; regardless of some overlap in tools and techniques, the approaches are simply not interchangeable.
- 24.** Which of the following types of tests involves discursive explorations of existing response procedures, based on a likely adverse scenario, designed to determine if desired outcomes will result?
- A. Structured walk-through test
 - B. Tabletop exercise
 - C. Simulation test

D. Checklist test

- B.** The goal of tabletop exercises (TTXs) is to examine existing controls and response procedures to the manifestation of a likely threat, to ensure that everyone who would be involved knows their role and that the resulting outcome across multiple contingencies would be what is desired. Branches in activities are typically explored to some degree, based on cascading dependencies, as well as sequels to the scenario under discussion.
 - A** is incorrect because, though a somewhat similar exercise to a TTX, the goal of a structured walk-through is to ensure that the objectives of step-by-step disaster recovery plans can be met and that all testing, maintenance, and training requirements are in place.
 - C** is incorrect because a simulation test involves much more activity than mere discussion or review. A simulation test seeks to actually exercise the response capacity, by practicing the steps in its execution. This form of test commonly includes all available materials, procedures, and personnel, and proceeds just up to the point of an actual relocation of processing to an alternate facility.
 - D** is incorrect because in checklist testing, copies of the disaster recovery or business continuity procedures are distributed to all stakeholders for review, in order to ensure that no necessary materials or steps are omitted.
25. Camellia has just concluded a security audit of some critical services within her environment and the state of the controls deployed to protect them. She has the results of a battery of technical tests and must now organize them into a written report to her chain of management. In analyzing these results, what must her immediate goal be?
- A.** Forwarding these results to upper management in as much technical detail as possible, as quickly as possible, so that upper management can sort out what to do about them
 - B.** Crafting a high-level summary of the results for upper management so that they can decide the relative importance of the results to the business mission
 - C.** Exploring countermeasures for every one of the negative findings in order to ascertain the least costly approach to fixing all the problems
 - D.** Seeking to understand what the results mean, the relative importance of each result, and what, if anything, can and should be

done about each

- D.** Before Camellia can craft a cogent and actionable report for both management and all the other stakeholders involved, she must first seek to make sense of them herself. After all, she is the subject matter expert in this scenario, and the business must rely on her expertise to understand what the results mean and the relative importance of each of her discoveries within the context of the business's technical operations. While it is management's ultimate responsibility to mitigate critical weaknesses, it is up to her to guide their decisions as to how best to do so.
 - A** is incorrect because upper management will unlikely be able to make sense of the raw technical details delivered in the results of her tests, and much less likely to be able to formulate a way to mitigate them. Not only will a report of this nature likely be ignored, it will almost certainly result in future such efforts being curtailed as a cost without obvious benefit.
 - B** is incorrect because, although crafting such an executive summary is certainly an important component of the final report, the relative importance of the issues discovered should not be left to management to infer. Rather, a detailed contextual analysis must precede it, so that management has the best information as to what should be prioritized, and why.
 - C** is incorrect because, although Camellia must certainly assist management by evaluating available mitigations, this should only be done following a detailed analysis as to the relative importance of each result.
- 26.** As a security analyst writing a technical report about the findings of a technical security assessment, what should your primary goal be?
- A.** Detailing as much of the raw data that went into the report as possible so that operations staff has absolutely everything they need to understand the issues that need to be remediated
 - B.** Providing step-by-step remediation advice for each of the most critical findings so that corrections can be deployed as easily and rapidly as possible
 - C.** Distilling the findings of the assessment into an executive summary, accessible to all levels of management
 - D.** Constructing a cogent and compelling narrative that will persuade the intended audience to enact the measures necessary to reduce

critical risks to the business mission, based on an honest and factual analysis

- D.** No amount of raw details, step-by-step remediation instructions, or easily digestible high-level overview presented following a security assessment will matter if the resulting report is not delivered in a compelling and convincing manner. Beyond what is important and what must be done about it, why it is important must be the key takeaway.
 - A** is incorrect because, though an important component, it is a secondary goal. Such details should be included as an appendix that is easily searchable and understandable by the technical staff that will be tasked with ensuring that proper and comprehensive mitigations are put in place. However, these details will be of no use if management is not convinced of the need to leverage them.
 - B** is incorrect because, though an important component, it is also a secondary goal. To the extent that operations staff can be easily guided through streamlined remediations, the cost of mitigations can be reduced. But again, even with such reduced impact, unless management is convinced of the necessity, this guidance will not be employed.
 - C** is incorrect because the executive summary is dependent on completion of the primary goal of constructing a cogent and compelling narrative. The executive summary conveys the most compelling aspects of the story.
- 27.** Why is a “Methodology” section as critical to a technical security assessment report as the findings themselves?
- A.** It isn’t. The findings and suggested mitigations are far more important.
 - B.** It helps management understand the value of the expensive tools that have been purchased to conduct the assessment, and the expense of the effort it took to use them to produce the results.
 - C.** It describes how the tests can be repeated by others to validate the results as required, and to further validate that mitigations, once deployed, have been effective.
 - D.** It provides the audience with the context of how, where, and why the inspection was conducted.
 - C.** For any given finding to be deemed truly valid, the method for

testing it must also be deemed both valid and repeatable by other analysts seeking to understand the nature and scope of the weakness exposed.

- A** is incorrect because no reputable assessor would claim to have found a flaw requiring remediation without providing the details as to how the flaw was discovered and illustrating the degree of certainty with which it should be considered to be true.
 - B** is incorrect because, though it might be a welcome side effect of the methodological discussion, it is not why a “Methodology” section is critical to a technical security assessment report.
 - D** is incorrect, though only partially so. The “Methodology” section should certainly contain this information, but with the goal of demonstrating the validity of the findings and providing the means to repeat the tests with the same results.
- 28.** Which of the following types of vulnerabilities CANNOT be discovered in the course of a routine vulnerability assessment?
- A.** Zero-day vulnerability
 - B.** Kernel flaw
 - C.** Buffer overflow
 - D.** File and directory permissions
- A.** A zero-day vulnerability is one that has been discovered by a potential adversary but has not yet been publicly disclosed, and as such is being kept in “escrow.” By this very definition, it is a type of flaw that cannot be tested for by any technical means as part of a routine test, but rather must be discovered independently.
 - B** is incorrect because kernel flaws, to the extent that they have been publicly disclosed, can be discovered in the course of a routine vulnerability assessment. Kernel flaws are vulnerabilities that exist within the core of the operating system itself, and may manifest themselves as native system calls that can be abused through the improper handling of network or disk I/O, or other such low-level operations. If successfully exploited, they can potentially provide the attacker with complete control over the system.
 - C** is incorrect because buffer overflows are perhaps the most commonly known and commonly exploited vulnerabilities and thus can be discovered in the course of a routine vulnerability assessment. Buffer overflows can provide the successful attacker

with control over the process containing the coding flaw. The most serious of these can provide remote code execution (RCE) access to a system.

- D** is incorrect because the improper configuration of local file and directory permissions (which can allow an attacker to access resources in ways that should not be permitted, often resulting in a local privilege escalation) can generally be inspected for via automated assessment tools.

Security Operations

This domain includes questions from the following topics:

- Operations department responsibilities
- Administrative management responsibilities
- Physical security
- Secure resource provisioning
- Network and resource availability
- Preventive and detective measures
- Incident management
- Investigations
- Disaster recovery
- Liability
- Personnel safety concerns

Security operations consists of the routine tasks involved with maintaining a network and its systems after they are developed and implemented. It includes ensuring that entities have the proper access privileges, that oversight is implemented, that network and systems run correctly and securely, and that applications are running in a secure and protected manner. It is also a very important topic, because as networks and computing environments continually evolve, individuals responsible for security operations must respond accordingly.

Q QUESTIONS

1. Which of the following is not a common component of configuration management change control steps?
 - A. Tested and presented
 - B. Service level agreement approval
 - C. Report change to management
 - D. Approval of the change
2. A change management process should include a number of procedures.

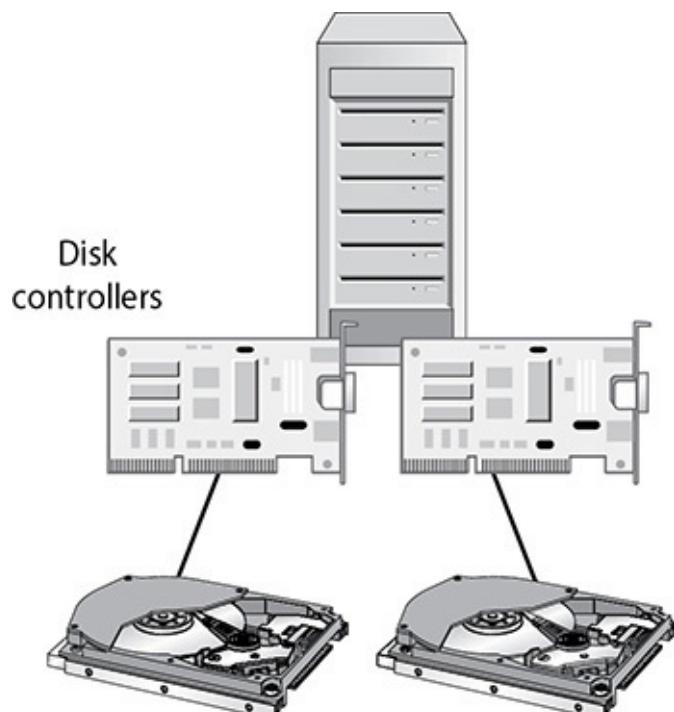
Which of the following incorrectly describes a characteristic or component of a change control policy?

- A. Changes that are unanimously approved by the change control committee must be tested to uncover any unforeseen results.
 - B. Changes approved by the change control committee should be entered into a change log.
 - C. A schedule that outlines the projected phases of the change should be developed.
 - D. An individual or group should be responsible for approving proposed changes.
3. Device backup and other availability solutions are chosen to balance the value of having information available against the cost of keeping that information available. Which of the following best describes fault-tolerant technologies?
- A. They are among the most expensive solutions and are usually only for the most mission-critical information.
 - B. They help service providers identify appropriate availability services for a specific customer.
 - C. They are required to maintain integrity, regardless of the other technologies in place.
 - D. They allow a failed component to be replaced while the system continues to run.
4. Which of the following refers to the expected amount of time it will take to get a device fixed and back into production after its failure?
- A. SLA
 - B. MTTR
 - C. Hot-swap
 - D. MTBF
5. Which of the following correctly describes direct access and sequential access storage devices?
- A. Any point on a direct access storage device may be promptly reached, whereas every point in between the current position and the desired position of a sequential access storage device must be traversed in order to reach the desired position.

- B. RAID is an example of a direct access storage device, while RAID is an example of a sequential access storage device.
 - C. MAID is a direct access storage device, while RAID is an example of a sequential access storage device.
 - D. As an example of sequential access storage, tape drives are faster than direct access storage devices.
- 6. Various levels of RAID dictate the type of activity that will take place within the RAID system. Which level is associated with byte-level parity?
 - A. RAID level 0
 - B. RAID level 3
 - C. RAID level 5
 - D. RAID level 10
- 7. RAID systems use a number of techniques to provide redundancy and performance. Which of the following activities divides and writes data over several drives?
 - A. Parity
 - B. Mirroring
 - C. Striping
 - D. Hot-swapping
- 8. What is the difference between hierarchical storage management and storage area network technologies?
 - A. HSM uses optical or tape jukeboxes, and SAN is a standard of how to develop and implement this technology.
 - B. HSM and SAN are one and the same. The difference is in the implementation.
 - C. HSM uses optical or tape jukeboxes, and SAN is a network of connected storage.
 - D. SAN uses optical or tape jukeboxes, and HSM is a network of connected storage systems.
- 9. There are often scenarios where the IT staff must react to emergencies and quickly apply fixes or change configurations. When dealing with such emergencies, which of the following is the best approach to making changes?

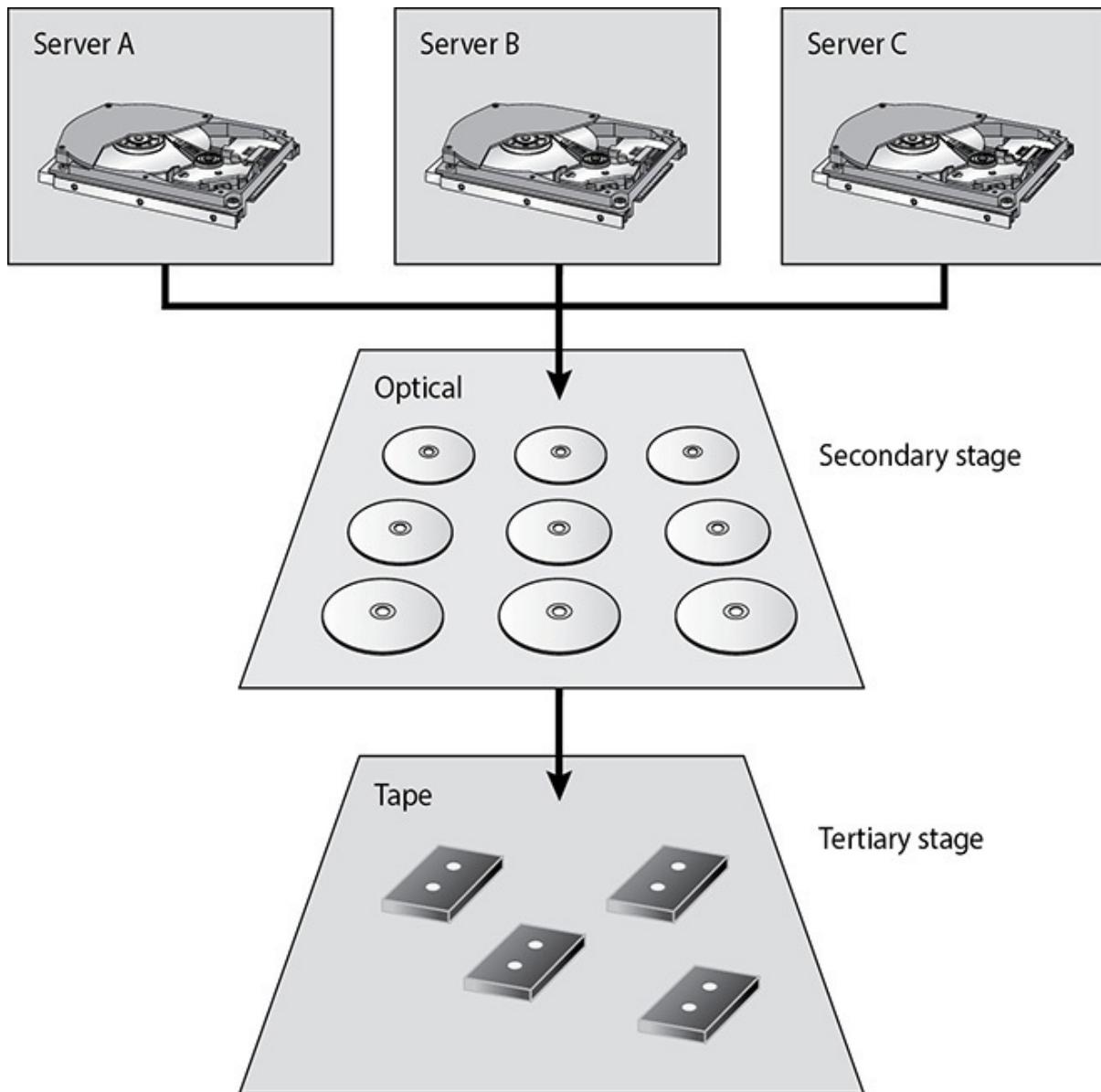
- A.** Review the changes within 48 hours of making them.
 - B.** Review and document the emergency changes after the incident is over.
 - C.** Activity should not take place in this manner.
 - D.** Formally submit the change to a change control committee and follow the complete change control process.
- 10.** Countries around the world are focusing on cyber warfare and how it can affect their utility and power grid infrastructures. Securing water, power, oil, gas, transportation, and manufacturing systems is an increasing priority for governments. These critical infrastructures are made up of different types of industrial control systems (ICS) that provide this type of functionality. Which of the following answers is not considered a common ICS?
- A.** Central control systems
 - B.** Programmable logic controllers
 - C.** Supervisory control and data acquisition
 - D.** Distributed control systems
- 11.** John is responsible for providing a weekly report to his manager outlining the week's security incidents and mitigation steps. What steps should he take if a report has no information?
- A.** Send his manager an e-mail telling her so.
 - B.** Deliver last week's report and make sure it's clearly dated.
 - C.** Deliver a report that states "No output."
 - D.** Don't do anything.
- 12.** Brian, a security administrator, is responding to a virus infection. The antivirus application reports that a file has been infected with a dangerous virus and disinfecting it could damage the file. What course of action should Brian take?
- A.** Replace the file with the file saved from the day before.
 - B.** Disinfect the file and contact the vendor.
 - C.** Restore an uninfected version of the patched file from backup media.
 - D.** Back up the data and disinfect the file.

- 13.** Guidelines should be followed to allow secure remote administration. Which of the following is not one of those guidelines?
- A.** A small number of administrators should be allowed to carry out remote functionality.
 - B.** Critical systems should be administered locally instead of remotely.
 - C.** Strong authentication should be in place.
 - D.** Telnet should be used to send commands and data.
- 14.** In a redundant array of inexpensive disks (RAID) system, data and parity information are striped over several different disks. What is parity information?
- A.** Information used to create new data
 - B.** Information used to erase data
 - C.** Information used to rebuild data
 - D.** Information used to build data
- 15.** Mirroring of drives is when data is written to two drives at once for redundancy purposes. What similar type of technology is shown in the graphic that follows?



- A.** Direct access storage
- B.** Disk duplexing
- C.** Striping

- D. Massive array of inactive disks
16. There are several different types of important architectures within backup technologies. Which architecture does the graphic that follows represent?



- A. Clustering
B. Grid computing
C. Backup tier security
D. Hierarchical storage management
17. _____ provides for availability and scalability. It groups physically different systems and combines them logically, which helps to provide immunity to faults and improves performance.

- A.** Disc duping
 - B.** Clustering
 - C.** RAID
 - D.** Virtualization
- 18.** Bob is a new security administrator at a financial institution. The organization has experienced some suspicious activity on one of the critical servers that contain customer data. When reviewing how the systems are administered, he uncovers some concerning issues pertaining to remote administration. Which of the following should not be put into place to reduce these concerns?
- i.** Commands and data should not be sent in cleartext.
 - ii.** SSH should be used, not Telnet.
 - iii.** Truly critical systems should be administered locally instead of remotely.
 - iv.** Only a small number of administrators should be able to carry out remote functionality.
 - v.** Strong authentication should be in place for any administration activities.
- A.** i, ii
 - B.** None of them
 - C.** ii, iv
 - D.** All of them
- 19.** A suspected crime has been reported within your organization. Which of the following steps should the incident response team take first?
- A.** Establish a procedure for responding to the incident.
 - B.** Call in forensic experts.
 - C.** Determine that a crime has been committed.
 - D.** Notify senior management.
- 20.** Which of the following is a correct statement regarding digital forensics?
- A.** It is the study of computer technology.
 - B.** It is a set of hardware-specific processes that must be followed in order for evidence to be admissible in a court of law.

- C. It encompasses network and code analysis, and may be referred to as electronic data discovery.
 - D. Digital forensic responsibilities should be assigned to a network administrator before an incident occurs.
- 21.** Which of the following dictates that all evidence be labeled with information indicating who secured and validated it?
- A. Chain of custody
 - B. Due care
 - C. Investigation
 - D. Motive, opportunity, and means
- 22.** Which of the following is not true of a forensic investigation?
- A. The crime scene should be modified as necessary.
 - B. A file copy tool may not recover all data areas of the device that are necessary for investigation.
 - C. Contamination of the crime scene may not negate derived evidence, but it should still be documented.
 - D. Only individuals with knowledge of basic crime scene analysis should have access to the crime scene.
- 23.** Stephanie has been put in charge of developing incident response and forensics procedures her company needs to carry out if an incident occurs. She needs to ensure that their procedures map to the international principles for gathering and protecting digital evidence. She also needs to ensure that if and when internal forensics teams are deployed, they have labels, tags, evidence bags, cable ties, imaging software, and other associated tools. Which of the following best describes what Stephanie needs to build for the deployment teams?
- A. Local and remote imaging system
 - B. Forensics field kit
 - C. Chain of custody procedures and tools
 - D. Digital evidence collection software
- 24.** When developing a recovery and continuity program within an organization, different metrics can be used to properly measure potential damages and recovery requirements. These metrics help us quantify our risks and the benefits of controls we can put into place.

Two metrics commonly used in the development of recovery programs are recovery point objective (RPO) and recovery time objective (RTO). Data restoration (RPO) requirements can be different from service restoration (RTO) requirements. Which of the following best defines these two main recovery measurements in this type of scenario?

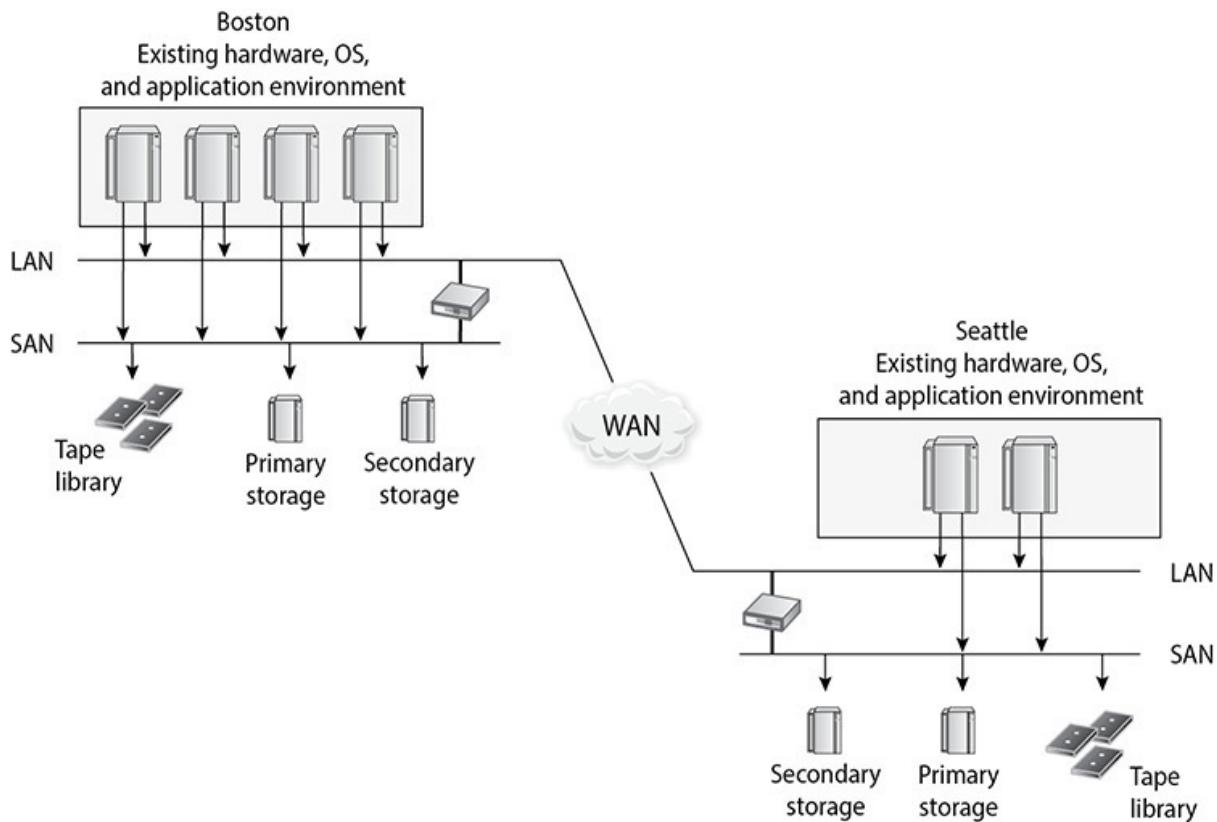
- A. RPO is the acceptable amount of data loss measured in time. RTO is the acceptable time period before a service level must be restored.
 - B. RTO is the earliest time period in which a data set must be restored. RPO is the acceptable amount of downtime in a given period.
 - C. RPO is the acceptable amount of data loss measured in time. RTO is the earliest time period in which data must be restored.
 - D. RPO is the acceptable amount of downtime measured. RTO is the earliest time period in which a service level must be restored.
- 25.** An approach to alternate offsite facilities is to establish a reciprocal agreement. Which of the following describes the pros and cons of a reciprocal agreement?
- A. It is fully configured and ready to operate within a few hours, but is the most expensive of the offsite choices.
 - B. It is an inexpensive option, but it takes the most time and effort to get up and running after a disaster.
 - C. It is a good alternative for companies that depend upon proprietary software, but annual testing is not usually available.
 - D. It is the cheapest of the offsite choices, but mixing operations could introduce many security issues.
- 26.** The operations team is responsible for defining which data gets backed up and how often. Which type of backup process backs up files that have been modified since the last time all data was backed up?
- A. Incremental process
 - B. Full backup
 - C. Partial backup
 - D. Differential process
- 27.** After a disaster occurs, a damage assessment needs to take place. Which of the following steps occurs last in a damage assessment?
- A. Determine the cause of the disaster.

- B. Identify the resources that must be replaced immediately.
 - C. Declare a disaster.
 - D. Determine how long it will take to bring critical functions back online.
- 28. Of the following plans, which establishes senior management and a headquarters after a disaster?
 - A. Continuity of operations plan
 - B. Cyber-incident response plan
 - C. Occupant emergency plan
 - D. IT contingency plan
- 29. Gizmos and Gadgets has restored its original facility after a disaster. What should be moved in first?
 - A. Management
 - B. Most critical systems
 - C. Most critical functions
 - D. Least critical functions
- 30. Several teams should be involved in carrying out the business continuity plan. Which team is responsible for starting the recovery of the original site?
 - A. Damage assessment team
 - B. BCP team
 - C. Salvage team
 - D. Restoration team
- 31. ACME, Inc., paid a software vendor to develop specialized software, and that vendor has gone out of business. ACME, Inc., does not have access to the code and therefore cannot keep it updated. What mechanism should the company have implemented to prevent this from happening?
 - A. Reciprocal agreement
 - B. Software escrow
 - C. Electronic vaulting
 - D. Business interruption insurance

32. Which of the following incorrectly describes the concept of executive succession planning?

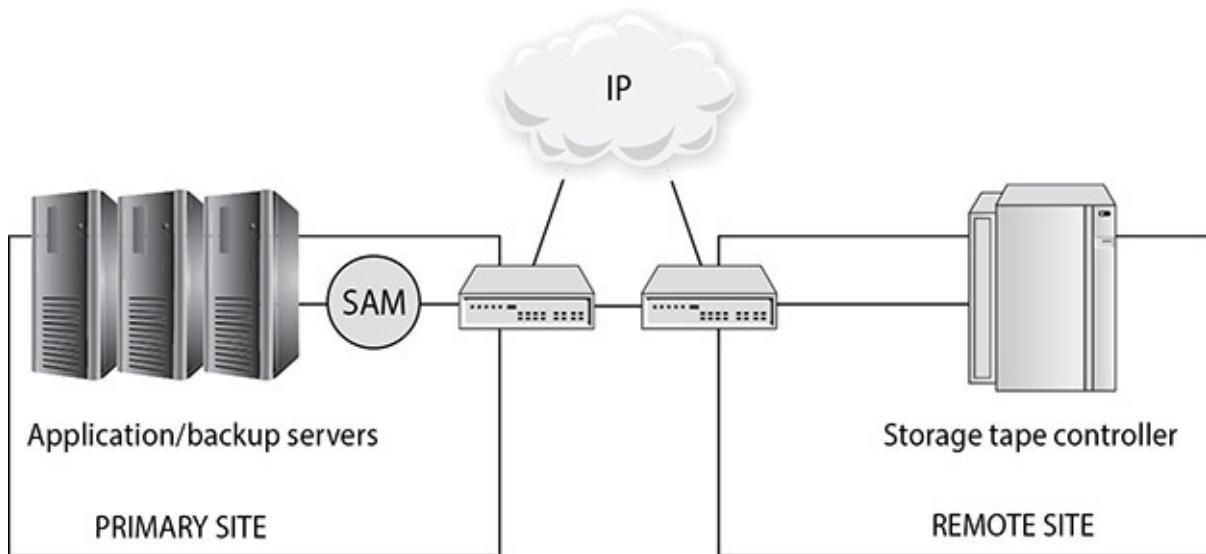
- A.** Predetermined steps protect the company if a senior executive leaves.
- B.** Two or more senior staff cannot be exposed to a particular risk at the same time.
- C.** It documents the assignment of deputy roles.
- D.** It covers assigning a skeleton crew to resume operations after a disaster.

33. What type of infrastructural setup is illustrated in the graphic that follows?

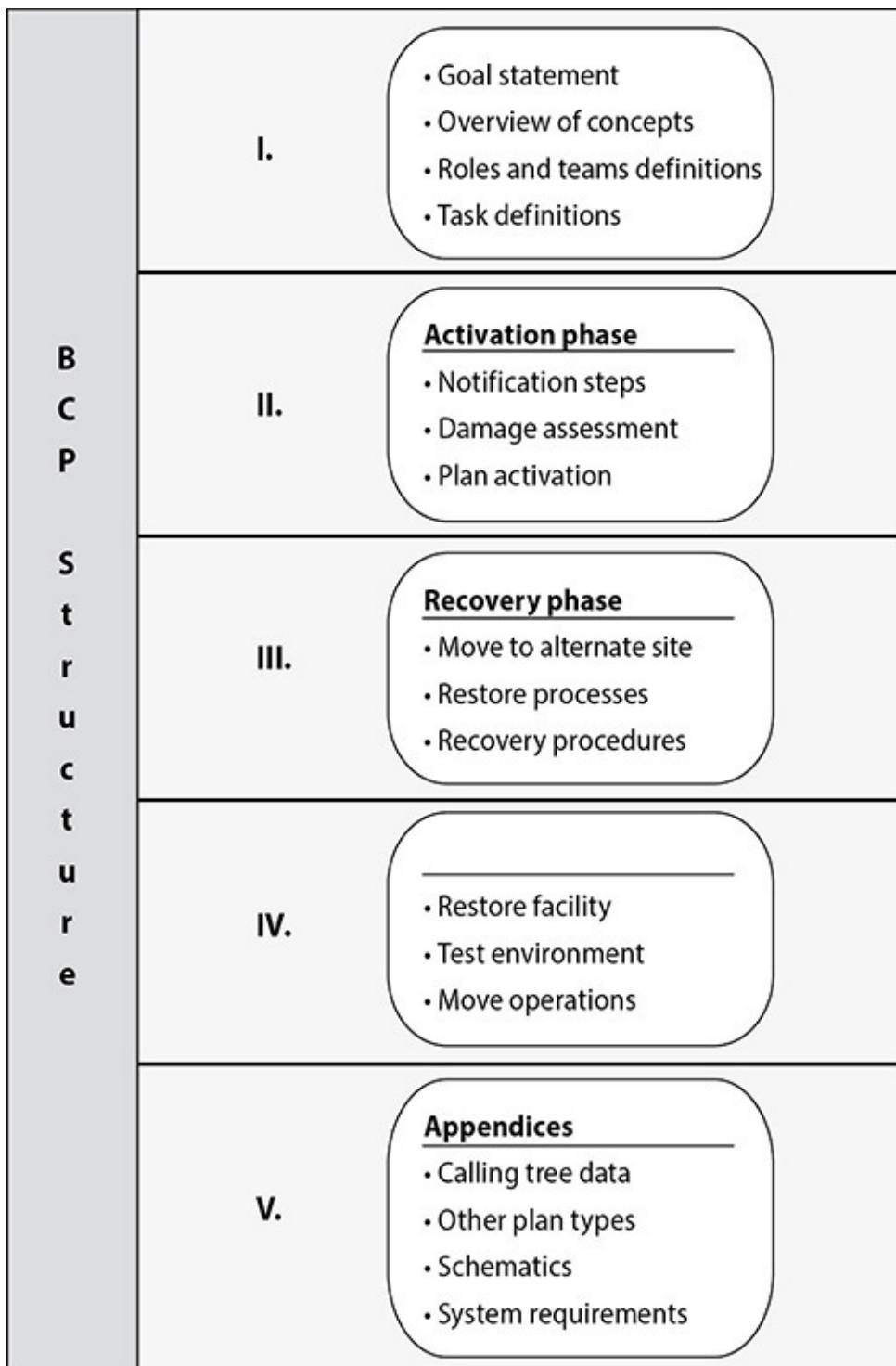


- C.** Hot site
- B.** Warm site
- C.** Cold site
- D.** Reciprocal agreement

34. There are several types of redundant technologies that can be put into place. What type of technology is shown in the graphic that follows?



- A. Tape vaulting
 - B. Remote journaling
 - C. Electronic vaulting
 - D. Redundant site
35. Here is a graphic of a business continuity policy. Which component is missing from this graphic?



- A. Damage assessment phase
 - B. Reconstitution phase
 - C. Business resumption phase
 - D. Continuity of operations plan
36. The recovery time objective (RTO) and maximum tolerable downtime (MTD) metrics have similar roles, but their values are very different.

Which of the following best describes the difference between RTO and MTD metrics?

- A. The RTO is a time period that represents the inability to recover, and the MTD represents an allowable amount of downtime.
 - B. The RTO is an allowable amount of downtime, and the MTD represents a time period after which severe and perhaps irreparable damage is likely.
 - C. The RTO is a metric used in disruptions, and the MTD is a metric used in disasters.
 - D. The RTO is a metric pertaining to loss of access to data, and the MTD is a metric pertaining to loss of access to hardware and processing capabilities.
- 37.** High availability (HA) is a combination of technologies and processes that work together to ensure that specific critical functions are always up and running at the necessary level. To provide this level of high availability, a company has to have a long list of technologies and processes that provide redundancy, fault tolerance, and failover capabilities. Which of the following best describes these characteristics?
- A. Redundancy is the duplication of noncritical components or functions of a system with the intention of decreasing reliability of the system. Fault tolerance is the capability of a technology to discontinue to operate as expected even if something unexpected takes place. If a technology has a failover capability, this means that if there is a failure that cannot be handled through normal means, then processing is “switched over” to a working system.
 - B. Redundancy is the duplication of critical components or functions of a system with the intention of increasing reliability of the system. Fault tolerance is the capability of a technology to discontinue to operate as expected even if something unexpected takes place. If a technology has a failover capability, this means that if there is a failure that cannot be handled through normal means, then processing is “switched over” to a working system.
 - C. Redundancy is the duplication of critical components or functions of a system with the intention of increasing reliability of the system. Fault tolerance is the capability of a technology to continue to operate as expected even if something unexpected takes place. If a technology has a failover capability, this means that if there is a

failure that cannot be handled through normal means, then processing is “switched over” to a nonworking system.

- D. Redundancy is the duplication of critical components or functions of a system with the intention of increasing reliability of the system. Fault tolerance is the capability of a technology to continue to operate as expected even if something unexpected takes place. If a technology has a failover capability, this means that if there is a failure that cannot be handled through normal means, then processing is “switched over” to a working system.

The following scenario applies to questions 38 and 39.

Jeff is leading the business continuity group in his company. They have completed a business impact analysis and have determined that if the company’s credit card processing functionality was unavailable for 48 hours the company would most likely experience such a large financial hit that it would have to go out of business. The team has calculated that this functionality needs to be up and running within 28 hours after experiencing a disaster for the company to stay in business. The team has also determined that the restoration steps must be able to restore data that is 60 minutes old or less.

38. In this scenario, which of the following is the work recovery time value?
- A. 48 hours
 - B. 28 hours
 - C. 20 hours
 - D. 1 hour
39. In this scenario, what would the 60-minute time period be referred to as?
- A. Recovery time period
 - B. Maximum tolerable downtime
 - C. Recovery point objective
 - D. Recovery point time period
40. For evidence to be legally admissible, it must be relevant, complete, sufficient, and reliably obtained. Which characteristic refers to the evidence having a reasonable and sensible relationship to the findings?
- A. Complete

- B.** Reliable
- C.** Relevant
- D.** Sufficient

- 41.** Alex works for a chemical distributor that assigns employees tasks that separate their duties and routinely rotates job assignments. Which of the following best describes the differences between these countermeasures?
- A.** They are the same thing with different titles.
 - B.** They are administrative controls that enforce access control and protect the company's resources.
 - C.** Separation of duties ensures that one person cannot perform a high-risk task alone, and job rotation can uncover fraud because more than one person knows the tasks of a position.
 - D.** Job rotation ensures that one person cannot perform a high-risk task alone, and separation of duties can uncover fraud because more than one person knows the tasks of a position.
- 42.** Maria has been tasked with reviewing and ultimately augmenting her organization's physical security. Of the following controls and approaches, which should be her highest priority to ensure are properly implemented?
- A.** Physical facility access controls, such as mechanical and device locks, on all necessary ingress points
 - B.** Personnel access controls, such as badges, biometric systems, etc.
 - C.** External boundary controls, including perimeter intrusion detection and assessment system (PIDAS) fencing, security guards, etc.
 - D.** Layered facility access controls, with multiple internal and external ingress and egress controls
- 43.** Which of the following statements is true with respect to preventing and/or detecting security disasters?
- A.** Information security continuous monitoring (ISCM), defined by NIST Special Publication 800-137 as maintaining an ongoing awareness of your current security posture, vulnerabilities, and threats, is the best way to facilitate sound risk management decisions.
 - B.** Whitelisting allowed executables or, barring that, blacklisting

known bad ones is the only effective means of preventing malware from compromising systems and causing a serious security breach.

- C. A rigorous regime of vulnerability and patch management can effectively eliminate the risk of known malware compromising critical corporate systems.
 - D. By aggregating and correlating asset data and the security events concerning them, the deployment of a security information and event management (SIEM) system is the best way to ensure that attacks can be properly dealt with before they result in disaster.
- 44.** Miranda has been directed to investigate a possible violation of her organization's acceptable use policy (AUP) by a coworker suspected of running cryptocurrency mining software on his desktop system. Which of the following is NOT a very likely scenario that could arise during her investigation?
- A. During the course of her investigation, Miranda discovered that her coworker was also downloading and storing pornographic images, many of which appeared to involve minors. What began as an administrative investigation became a criminal one.
 - B. Miranda was able to find evidence that appeared to corroborate the intentional use of illicit software to mine cryptocurrency using corporate resources (mainly CPU and power). As a result, Miranda's coworker was charged with a criminal violation of the Computer Fraud and Abuse Act (CFAA).
 - C. As a result of Miranda's investigation, her coworker was terminated for violating the AUP. However, he hired an attorney and sued the company for wrongful dismissal based on knowledge that other employees were also running cryptocurrency mining software but went unpunished. Her administrative case became a civil one.
 - D. Compelling evidence was found of a significant AUP violation, resulting in termination. However, during the subsequent wrongful dismissal suit (as described in option C), it was discovered that Miranda had not anticipated a court case, and so had not properly obtained or preserved the evidence. Consequently, the judge found summarily for the plaintiff, who got his job back along with compensatory damages.

QUICK ANSWER KEY

1. B

2. A

3. A

4. B

5. A

6. B

7. C

8. C

9. B

10. A

11. C

12. C

13. D

14. C

15. B

16. D

17. B

18. B

19. C

20. C

21. A

22. A

23. B

24. A

25. D

26. D

27. C

28. A

29. D

30. C

31. B

32. D

33. A

34. A

35. B

36. B

37. D

38. C

39. C

40. C

41. C

42. D

43. A

44. B

ANSWERS A

- 1.** Which of the following is not a common component of configuration management change control steps?

 - A.** Tested and presented
 - B.** Service level agreement approval
 - C.** Report change to management
 - D.** Approval of the change
- B.** A well-structured change management process should be established to aid staff members through many different types of changes to the environment. This process should be laid out in the change control policy. Although the types of changes vary, a standard list of procedures can help keep the process under control and ensure it is carried out in a predictable manner. A change control policy should include procedures for requesting a change to take place, approving the change, documentation of the change, testing and presentation, implementation, and reporting the change to management. Configuration management change control processes do not commonly have an effect on service level agreement approvals.

- A** is incorrect because testing and presentation should be included in a standard change control policy. All changes must be fully tested to uncover any unforeseen results. Depending on the severity of the change and the company's organization, the change and implementation may need to be presented to a change control committee. This helps show different sides to the purpose and outcome of the change and the possible ramifications.
 - C** is incorrect because a procedure for reporting a change to management should be included in a standard change control policy. After a change is implemented, a full report summarizing the change should be submitted to management. This report can be submitted on a periodic basis to keep management up to date and ensure continual support.
 - D** is incorrect because a procedure for obtaining approval for the change should be included in a standard change control policy. The individual requesting the change must justify the reasons and clearly show the benefits and possible pitfalls of the change. Sometimes the requester is asked to conduct more research and provide more information before the change is approved.
- 2.** A change management process should include a number of procedures. Which of the following incorrectly describes a characteristic or component of a change control policy?
- A.** Changes that are unanimously approved by the change control committee must be tested to uncover any unforeseen results.
 - B.** Changes approved by the change control committee should be entered into a change log.
 - C.** A schedule that outlines the projected phases of the change should be developed.
 - D.** An individual or group should be responsible for approving proposed changes.
- A.** A well-structured change management process should be put into place to aid staff members through many different types of changes to the environment. This process should be laid out in the change control policy. Although the types of changes vary, a standard list of procedures can help keep the process under control and ensure it is carried out in a predictable manner. All changes approved by the change control committee (not just those unanimously approved) must be fully tested to uncover any unforeseen results. Depending

on the severity of the change and the company's organization, the change and implementation may need to be presented to a change control committee. This helps show different sides to the purpose and outcome of the change and the possible ramifications.

- B** is incorrect because it is true that changes approved by the change control committee should be entered into a change log. The log should be updated as the process continues toward completion. It is important to track and document all changes that are approved and implemented.
 - C** is incorrect because once a change is fully tested and approved, a schedule should be developed that outlines the projected phases of the change being implemented and the necessary milestones. These steps should be fully documented, and progress should be monitored.
 - D** is incorrect because requests should be presented to an individual or group that is responsible for approving changes and overseeing the activities of changes that take place within an environment.
3. Device backup and other availability solutions are chosen to balance the value of having information available against the cost of keeping that information available. Which of the following best describes fault-tolerant technologies?
- A. They are among the most expensive solutions and are usually only for the most mission-critical information.
 - B. They help service providers identify appropriate availability services for a specific customer.
 - C. They are required to maintain integrity, regardless of the other technologies in place.
 - D. They allow a failed component to be replaced while the system continues to run.
- A. Fault-tolerant technologies keep information available not only against individual storage device faults, but even against whole system failures. Fault tolerance is among the most expensive possible solutions for availability and is commonly justified only for the most mission-critical information. All technology will eventually experience a failure of some form. A company that would suffer irreparable harm from any unplanned downtime can justify paying the high cost for fault-tolerant systems.

- B** is incorrect because service level agreements (SLAs) help service providers, whether they are an internal IT operation or an outsourcer, decide what type of availability technology and service is appropriate. From this determination, the price of a service or the budget of the IT operation can be set. The process of developing an SLA with a business is also beneficial to the business. While some businesses have performed this type of introspection on their own, many have not, and being forced to go through the exercise as part of budgeting for their internal IT operations or external sourcing helps the business understand the real value of its information.
 - C** is incorrect because fault-tolerant technologies do not necessarily have anything to do with data or system integrity.
 - D** is incorrect because “hot-swappable” hardware does not require shutting down the system and may or may not be considered a fault-tolerant technology. Hot-swapping allows the administrator to replace the failed component while the system continues to run and information remains available; usually degraded performance results, but unplanned downtime is avoided.
4. Which of the following refers to the expected amount of time it will take to get a device fixed and back into production after its failure?
- A. SLA
 - B. MTTR
 - C. Hot-swap
 - D. MTBF
- B.** Mean time to repair (MTTR) is the expected amount of time it will take to get a device fixed and back into production after its failure. For a hard drive in a redundant array, the MTTR is the amount of time between the actual failure and the time when, after noticing the failure, someone has replaced the failed drive and the redundant array has completed rewriting the information on the new drive. This is likely to be measured in hours. For a nonredundant hard drive in a desktop PC, the MTTR is the amount of time between when the drive goes down and the point at which the replaced hard drive has been reloaded with the operating system, software, and any backed-up data belonging to the user. This is likely to be measured in days. For an unplanned reboot, the MTTR is the amount of time between the failure of the system and the point in time when it has rebooted its operating system, checked the

state of its disks, restarted its applications, allowed its applications to check the consistency of their data, and once again begun processing transactions.

- A** is incorrect because a service level agreement (SLA) addresses the degree of availability that will be provided to a customer, whether that customer be an internal department within the same organization or an external customer. The MTTR is the expected amount of time it will take to get a device fixed and back into production. The MTTR may pertain to fixing a component or the device or replacing the device.
 - C** is incorrect because hot-swapping refers to the replacement of a failed component while the system continues to run and information remains available. Usually degraded performance results, but unplanned downtime is avoided. Hot-swapping does not refer to the amount of time needed to get a system back up and running.
 - D** is incorrect because MTBF refers to mean time between failure, which is the estimated lifespan of a piece of equipment. It is calculated by the vendor of the equipment or a third party. The reason for using this value is to know approximately when a particular device will need to be replaced. It is used as a benchmark for reliability by predicting the average time that will pass in the operation of a component or a system until it needs to be replaced.
5. Which of the following correctly describes direct access and sequential access storage devices?
- A.** Any point on a direct access storage device may be promptly reached, whereas every point in between the current position and the desired position of a sequential access storage device must be traversed in order to reach the desired position.
 - B.** RAIT is an example of a direct access storage device, while RAID is an example of a sequential access storage device.
 - C.** MAID is a direct access storage device, while RAID is an example of a sequential access storage device.
 - D.** As an example of sequential access storage, tape drives are faster than direct access storage devices.
- A.** Direct access storage device (DASD) is a general term for magnetic disk storage devices, which historically have been used in mainframe and minicomputer (mid-range computer) environments. A redundant array of independent disks (RAID) is a type of DASD.

The key distinction between DASDs and sequential access storage devices (SASDs) is that any point on a DASD may be promptly reached, whereas every point in between the current position and the desired position of an SASD must be traversed in order to reach the desired position. Tape drives are SASDs. Tape storage is the lowest-cost option for very large amounts of data but is very slow compared to disk storage.

- B** is incorrect because RAID stands for redundant array of independent tapes. RAID uses tape drives, which are SASDs. In RAID, data is striped in parallel to multiple tape drives, with or without a redundant parity drive. This provides the high capacity at low cost typical of tape storage, with higher-than-usual tape data transfer rates and optional data integrity. RAID is a type of DASD. RAID combines several physical disks and aggregates them into logical arrays. When data is saved, the information is written across all drives. A RAID appears as a single drive to applications and other devices.
 - C** is incorrect because both MAID, a massive array of inactive disks, and RAID are examples of DASDs. Any point on these magnetic disk storage devices can be reached without traversing every point between the current and desired positions. This makes DASDs faster than SASDs.
 - D** is incorrect because SASDs are slower than DASDs. Tape drives are an example of SASD technology.
6. Various levels of RAID dictate the type of activity that will take place within the RAID system. Which level is associated with byte-level parity?
- A. RAID level 0
 - B. RAID level 3
 - C. RAID level 5
 - D. RAID level 10
- B.** Redundant array of inexpensive disks (RAID) provides fault tolerance for hard drives and can improve system performance. Redundancy and speed are provided by breaking up the data and writing it across several disks so that different disk heads can work simultaneously to retrieve the requested information. Recovery data is also created—this is called parity—so that if one disk fails, the parity data can be used to reconstruct the corrupted or lost

information. Different activities that provide fault tolerance or performance improvements occur at different levels of a RAID system. RAID level 3 is a scheme employing byte-level striping and a dedicated parity disk. Data is striped over all but the last drive, with parity data held on only the last drive. If a drive fails, it can be reconstructed from the parity drive. The most common RAID levels used today is level 5.

- A** is incorrect because only striping occurs at level 0. Data is striped over several drives. No redundancy or parity is involved. If one volume fails, the entire volume can be unusable. Level 0 is used for performance only.
 - C** is incorrect because RAID 5 employs block-level striping and interleaving parity across all disks. Data is written in disk block units to all drives. Parity is written to all drives also, which ensures there is no single point of failure. RAID level 5 is the most commonly used mode.
 - D** is incorrect because level 10 is associated with striping and mirroring. It is a combination of levels 1 and 0. Data is simultaneously mirrored and striped across several drives and can support multiple drive failures.
7. RAID systems use a number of techniques to provide redundancy and performance. Which of the following activities divides and writes data over several drives?
- A.** Parity
 - B.** Mirroring
 - C.** Striping
 - D.** Hot-swapping
- C.** Redundant array of inexpensive disks (RAID) is a technology used for redundancy and/or performance improvement. It combines several physical disks and aggregates them into logical arrays. When data is saved, the information is written across all drives. A RAID appears as a single drive to applications and other devices. When striping is used, data is written across all drives. This activity divides and writes the data over several drives. Both write and read performance are increased dramatically because more than one head is reading or writing data at the same time.
 - A** is incorrect because parity is used to rebuild lost or corrupted data.

Various levels of RAID dictate the type of activity that will take place within the RAID system. Some levels deal only with performance issues, while other levels deal with performance and fault tolerance. If fault tolerance is one of the services a RAID level provides, parity is involved. If a drive fails, the parity is basically instructions that tell the RAID system how to rebuild the lost data on the new hard drive. Parity is used to rebuild a new drive so that all the information is restored.

- B** is incorrect because mirroring occurs when data is written to two drives at once. If one drive fails, the other drive has the exact same data available. Mirroring provides redundancy. Mirroring occurs at level 1 of RAID systems, and with striping in level 10.
 - D** is incorrect because hot-swappable refers to a type of disk that is in most RAID systems. RAID systems with hot-swapping disks are able to replace drives while the system is running. When a drive is swapped out, or added, the parity data is used to rebuild the data on the new disk that was just added.
- 8.** What is the difference between hierarchical storage management and storage area network technologies?
- A.** HSM uses optical or tape jukeboxes, and SAN is a standard of how to develop and implement this technology.
 - B.** HSM and SAN are one and the same. The difference is in the implementation.
 - C.** HSM uses optical or tape jukeboxes, and SAN is a network of connected storage.
 - D.** SAN uses optical or tape jukeboxes, and HSM is a network of connected storage systems.
- C.** Hierarchical storage management (HSM) provides continuous online backup functionality. It combines hard disk technology with the cheaper and slower optical or tape jukeboxes. The HSM system dynamically manages the storage and recovery of files, which are copied to storage media devices that vary in speed and cost. The faster media hold the data that is accessed more often, and the seldom-used files are stored on the slower devices, or near-line devices. The storage media could include optical disks, magnetic disks, and tapes. This functionality happens in the background without the knowledge of the user or any need for user intervention. A storage area network (SAN), on the other hand, consists of

numerous storage devices linked together by a high-speed private network and storage-specific switches. When a user makes a request for a file, he does not need to know which server or tape drive to go to—the SAN software finds it and provides it to the user.

- A** is incorrect because SAN is not a standard for how to develop and implement HSM. A SAN is a network of connected storage devices. SANs provide redundancy, fault tolerance, reliability, and backups, and they allow the users and administrators to interact with the SAN as one virtual entity. Because the network that carries the data in the SAN is separate from a company's regular data network, all of this performance, reliability, and flexibility comes without impact to the data networking capabilities of the systems on the network.
 - B** is incorrect because HSM and SAN are not the same. HSM uses conventional hard disk backup processes combined with optical/tape jukeboxes. A SAN uses a networked system of storage devices integrated into an established network.
 - D** is incorrect because the statement is backward. HSM uses optical or tape jukeboxes, and SAN is a network of connected storage systems. HSM was created to save money and time. It provides an economical and efficient way of storing data by combining higher-speed, higher-cost storage media for frequently accessed data with lower-speed, lower-cost media for infrequently accessed data. SANs, on the other hand, are for companies that have to keep track of terabytes of data and have the funds for this type of technology. They are not commonly used in large or midsized companies.
- 9.** There are often scenarios where the IT staff must react to emergencies and quickly apply fixes or change configurations. When dealing with such emergencies, which of the following is the best approach to making changes?
- A.** Review the changes within 48 hours of making them.
 - B.** Review and document the emergency changes after the incident is over.
 - C.** Activity should not take place in this manner.
 - D.** Formally submit the change to a change control committee and follow the complete change control process.
- B.** After the incident or emergency is over, the staff should review the changes to ensure that they are correct and do not open security

holes or affect interoperability. The changes need to be properly documented and the system owner needs to be informed of changes.

- A** is incorrect because it is not the best answer. The changes should be reviewed after the incident is over, but not necessarily within 48 hours. Many times the changes should be reviewed hours after they are implemented—not days.
- C** is incorrect because, while it would be nice if emergencies didn't happen, they are unavoidable. At one point or another, for example, an IT administrator will have to roll out a patch or change configurations to protect systems against a high-profile vulnerability.
- D** is incorrect because if an emergency is taking place, then there is no time to go through the process of submitting a change to the change control committee and following the complete change control process. These steps usually apply to large changes that take place to a network or environment. These types of changes are typically expensive and can have lasting effects on a company.

- 10.** Countries around the world are focusing on cyber warfare and how it can affect their utility and power grid infrastructures. Securing water, power, oil, gas, transportation, and manufacturing systems is an increasing priority for governments. These critical infrastructures are made up of different types of industrial control systems (ICS) that provide this type of functionality. Which of the following answers is not considered a common ICS?

- A.** Central control systems
 - B.** Programmable logic controllers
 - C.** Supervisory control and data acquisition
 - D.** Distributed control systems
- A.** The most common types of industrial control systems (ICS) are distributed control systems (DCSs), programmable logical controllers (PLCs), and supervisory control and data acquisition (SCADA) systems. While these systems provide a type of central control functionality, this is not considered a common type of ICS because these systems are distributed in nature. DCSs are used to control product systems for industries such as water, electrical, and oil refineries. The DCS uses a centralized supervisory control loop to connect controllers that are distributed throughout a geographic location. The supervisor controllers on this centralized loop request

status data from field controllers and feed this information back to a central interface for monitoring. The status data captured from sensors can be used in failover situations. The DCS can provide redundancy protection through a modular approach. This reduces the impact of a single fault, meaning that if one portion of the system went down, the whole system would not be down.

- B** is incorrect because programmable logic controllers (PLCs) are common industrial control systems (ICS) and are used to connect sensors throughout the utility network and convert this sensor signal data into digital data that can be processed by monitoring and managing software. PLCs were originally created to carry out simplistic logic functions within basic hardware, but have evolved into powerful controllers used in both SCADA and DCS systems. In SCADA systems, the PLCs are most commonly used to communicate with remote field devices, and in DCS systems, they are used as local controllers in a supervisory control scheme. The PLC provides an application programming interface to allow for communication to an engineering control software application.
- C** is incorrect because supervisory control and data acquisition (SCADA) refers to a computerized system that is used to gather and process data and apply operational controls to the components that make up a utility-based environment. It is a common type of ICS. The SCADA control center allows for centralized monitoring and control for field sites (e.g., power grids, water systems). The field sites have remote station control devices (field devices), which provide data to the central control center. Based upon the data that is sent from the field device, an automated process or an operator can send out commands to control the remote devices to fix problems or change configurations for operational needs. This is a challenging environment to work within because the hardware and software are usually proprietary to the specific industry; are privately owned and operated; and communication can take place over telecommunication links, satellites, and microwave-based systems.
- D** is incorrect because the distributed control system (DCS) is a common type of ICS. In a DCS, the control elements are not centralized. The control elements are distributed throughout the system and are managed by one or more computers. SCADA systems, DCSs, and PLCs are used in industrial sectors such as water, oil and gas, electric, transportation, etc. These systems are

considered “critical infrastructure” and are highly interconnected and dependent systems. In the past, these critical infrastructure environments did not use the same type of technology and protocols as the Internet, and thus were isolated and very hard to attack. Over time, these proprietary environments have been turned into IP-based environments using networking devices and connected IP-based workstations. This shift allows for better centralized controlling and management, but opens them up to the same type of cyber attacks that the computer industry has always been vulnerable to.

- 11.** John is responsible for providing a weekly report to his manager outlining the week’s security incidents and mitigation steps. What steps should he take if a report has no information?

 - A.** Send his manager an e-mail telling her so.
 - B.** Deliver last week’s report and make sure it’s clearly dated.
 - C.** Deliver a report that states “No output.”
 - D.** Don’t do anything.

C. If a report has no information (nothing to report), it should state, “No output.” This ensures that the manager is aware that there is no information to report and that John isn’t just slacking in his responsibilities.

A is incorrect because John should still deliver his manager a report. It should say, “No output.” Even though an e-mail achieves the objective of communicating that there’s nothing to report, a report should still be delivered for consistency.

B is incorrect because delivering last week’s report does not provide documentation or communicate to John’s manager that there is nothing to report this week. He should give his manager a report that reads, “No output.”

D is incorrect because if John doesn’t do anything when there is nothing to report, his manager must track John down and ask him for the report. For all she knows, John is slacking on his job duties. By providing a report that reads, “No output,” John is communicating this information to his manager in an efficient manner that she has come to expect.
- 12.** Brian, a security administrator, is responding to a virus infection. The antivirus application reports that a file has been infected with a dangerous virus and disinfecting it could damage the file. What course

of action should Brian take?

- A. Replace the file with the file saved from the day before.
 - B. Disinfect the file and contact the vendor.
 - C. Restore an uninfected version of the patched file from backup media.
 - D. Back up the data and disinfect the file.
- C. The best course of action is to install an uninfected version of a patched file from backup media. Attempts to disinfect the file could corrupt it, and it is important to restore a file that is known to be “clean.”
- A is incorrect because the previous day’s file could also be infected. It is best to replace the file entirely with a freshly installed and patched version.
- B is incorrect because disinfecting the file could cause damage, as stated in the question. In addition, the vendor of the application will not necessarily be useful in this situation. It is easier to restore a clean version of the file and move on with production.
- D is incorrect because backing up the file will also back up the virus, and as the question stated, disinfecting the file will cause damage and potential data loss.

13. Guidelines should be followed to allow secure remote administration. Which of the following is not one of those guidelines?

- A. A small number of administrators should be allowed to carry out remote functionality.
 - B. Critical systems should be administered locally instead of remotely.
 - C. Strong authentication should be in place.
 - D. Telnet should be used to send commands and data.
- D. Telnet should not be allowed for remote administration because it sends all data, including administrator credentials, in cleartext. This type of communication should go over more secure protocols, as in SSH.
- A is incorrect because it is true that only a small number of administrators should be able to carry out remote functionality. This helps minimize the risk posed to the network.
- B is incorrect because it is true that critical systems should be

administered locally instead of remotely. It is safer to send administrative commands over the internal, private network than it is to do so over a public network.

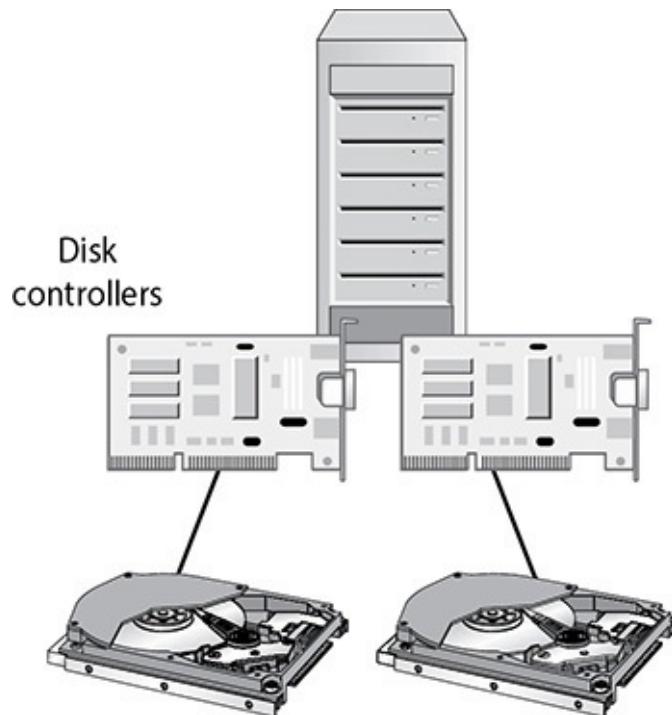
- C** is incorrect because it is true that strong authentication should be in place for any administration activities. Anything less than strong authentication, such as a password, would be easy for an attacker to crack and thereby gain administrative access.

14. In a redundant array of inexpensive disks (RAID) system, data and parity information are striped over several different disks. What is parity information?

- A.** Information used to create new data
 - B.** Information used to erase data
 - C.** Information used to rebuild data
 - D.** Information used to build data
- C.** Redundant array of inexpensive disks (RAID) provides fault tolerance for hard drives and the data they hold and can improve system performance. Redundancy and speed are provided by breaking up the data and writing it across several disks so that different disk heads can work simultaneously to retrieve the requested information. Control data is also spread across each disk —this is called parity—so that if one disk fails, the other disks can work together and restore its data. If fault tolerance is one of the services a RAID level provides, parity is involved.
 - A** is incorrect because parity information is not used to create new data but is used as instructions on how to re-create data that has been lost or corrupted. If a drive fails, the parity is basically instructions that tell the RAID system how to rebuild the lost data on the new hard drive. Parity is used to rebuild a new drive so that all the information is restored.
 - B** is incorrect because parity information is not used to erase data, but is used as instructions on how to re-create data that has been lost or corrupted.
 - D** is incorrect because parity information is not used to build data, but is used as instructions on how to re-create data that has been lost or corrupted.

15. Mirroring of drives is when data is written to two drives at once for redundancy purposes. What similar type of technology is shown in the

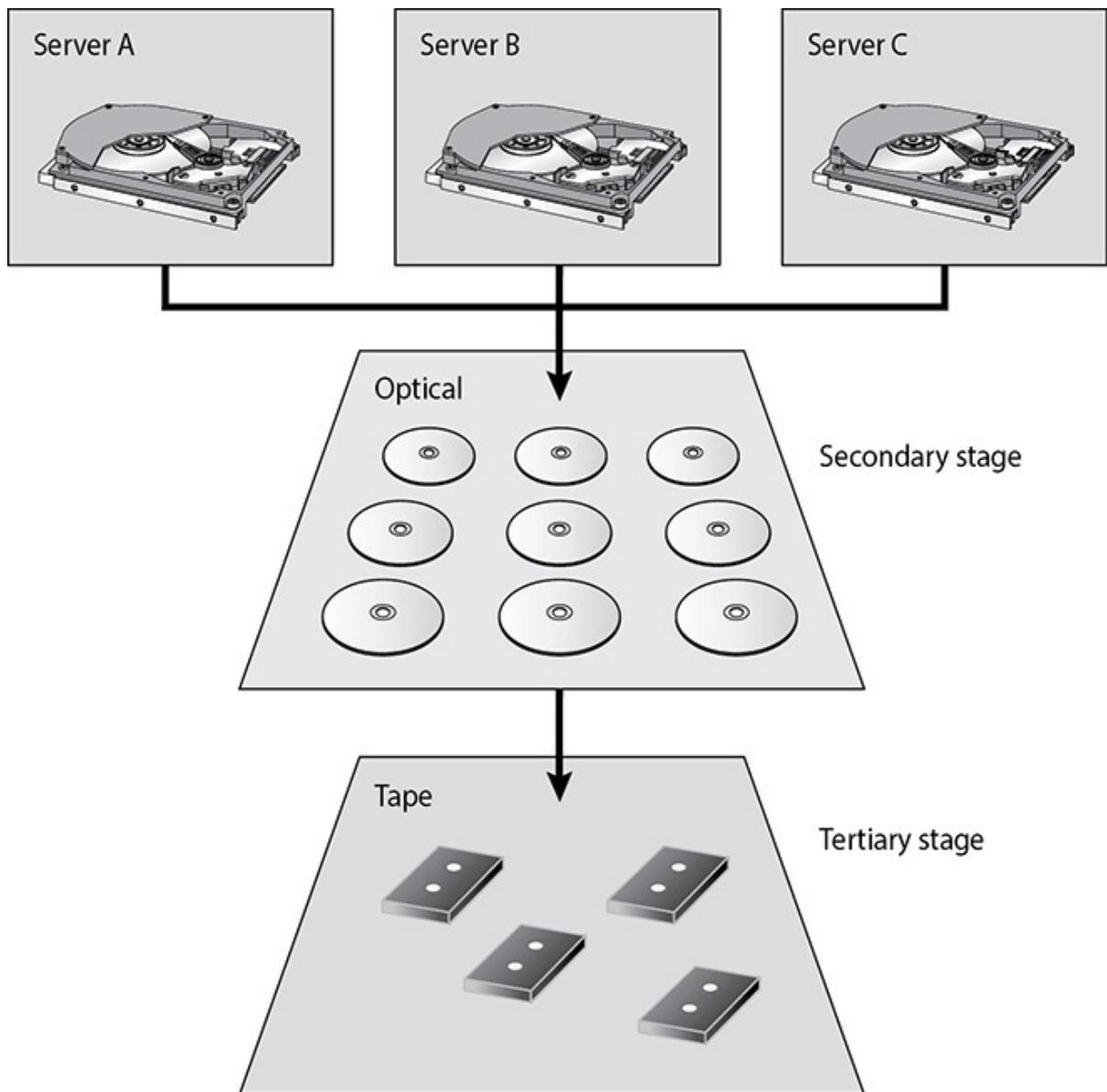
graphic that follows?



- A. Direct access storage
 - B. Disk duplexing
 - C. Striping
 - D. Massive array of inactive disks
- B. Information that is required to always be available should be mirrored or duplexed. In both mirroring (also known as RAID 1) and duplexing, every data write operation occurs simultaneously or nearly simultaneously in more than one physical place. The distinction between mirroring and duplexing is that with mirroring the two (or more) physical places where the data is written may be attached to the same controller, leaving the storage still subject to the single point of failure of the controller itself; in duplexing, two or more controllers are used.
- A is incorrect because direct access storage is a general term for magnetic disk storage devices, which historically have been used in mainframe and minicomputer (mid-range computer) environments. A redundant array of independent disks (RAID) is a type of direct access storage device (DASD).
- C is incorrect because when data is written across all drives, the technique of striping is used. This activity divides and writes the data over several drives. The write performance is not affected, but

the read performance is increased dramatically because more than one head is retrieving data at the same time. Parity information is used to rebuild lost or corrupted data. Striping just means data and potentially parity information is written across multiple disks.

- D** is incorrect because in a massive array of inactive disks (MAID), rack-mounted disk arrays have all inactive disks powered down, with only the disk controller alive. When an application asks for data, the controller powers up the appropriate disk drive(s), transfers the data, and then powers the drive(s) down again. By powering down infrequently accessed drives, energy consumption is significantly reduced, and the service life of the disk drives may be increased.
- 16.** There are several different types of important architectures within backup technologies. Which architecture does the graphic that follows represent?



- A. Clustering
 - B. Grid computing
 - C. Backup tier security
 - D. Hierarchical storage management
- D. Hierarchical storage management (HSM) provides continuous online backup functionality. It combines hard disk technology with the cheaper and slower optical or tape jukeboxes. The HSM system dynamically manages the storage and recovery of files, which are copied to storage media devices that vary in speed and cost. The faster media hold the data that is accessed more often, and the seldom-used files are stored on the slower devices, or near-line devices.

- A** is incorrect because clustering is a fault-tolerant server technology that is similar to redundant servers, except each server takes part in processing services that are requested. A server cluster is a group of servers that are viewed logically as one server to users and can be managed as a single logical system. Clustering provides for availability and scalability. It groups physically different systems and combines them logically, which provides immunity to faults and improves performance.
- B** is incorrect because grid computing is a load-balanced parallel means of massive computation, similar to clusters, but implemented with loosely coupled systems that may join and leave the grid randomly. Most computers have extra CPU processing power that is not being used many times throughout the day. Just like the power grid provides electricity to entities on an as-needed basis, computers can volunteer to allow their extra processing power to be available to different groups for different projects. The first project to use grid computing was SETI (Search for Extraterrestrial Intelligence), where people allowed their systems to participate in scanning the universe looking for aliens who are trying to talk to us.
- C** is incorrect because backup tier security is not a formal technology and is a distracter answer.

17. _____ provides for availability and scalability. It groups physically different systems and combines them logically, which helps to provide immunity to faults and improves performance.
- A.** Disc duping
 - B.** Clustering
 - C.** RAID
 - D.** Virtualization
- B.** Clustering is a fault-tolerant server technology that is similar to redundant servers, except each server takes part in processing services that are requested. A server cluster is a group of servers that are viewed logically as one server to users and can be managed as a single logical system. Clustering provides for availability and scalability. It groups physically different systems and combines them logically, which helps to provide immunity to faults and improves performance. Clusters work as an intelligent unit to balance traffic, and users who access the cluster do not know they may be accessing different systems at different times. To the users,

all servers within the cluster are seen as one unit.

- A** is incorrect because this is a distracter answer. There is not an official technology with this name.
- C** is incorrect because redundant array of inexpensive disks (RAID) provides fault tolerance for hard drives and can improve system performance. Redundancy and speed are provided by breaking up the data and writing them across several disks so different disk heads can work simultaneously to retrieve the requested information. RAID does not address scalability and performance.
- D** is incorrect because virtualization is the creation of a virtual version of something, such as a hardware platform, operating system, storage device, or network resource. Hardware virtualization or platform virtualization refers to the creation of a virtual machine that acts like a real system with an operating system. Software executed on these virtual machines is separated from the underlying hardware resources by an abstraction layer.

- 18.** Bob is a new security administrator at a financial institution. The organization has experienced some suspicious activity on one of the critical servers that contain customer data. When reviewing how the systems are administered, he uncovers some concerning issues pertaining to remote administration. Which of the following should not be put into place to reduce these concerns?

- i. Commands and data should not be sent in cleartext.
- ii. SSH should be used, not Telnet.
- iii. Truly critical systems should be administered locally instead of remotely.
- iv. Only a small number of administrators should be able to carry out remote functionality.
- v. Strong authentication should be in place for any administration activities.

- A.** i, ii
- B.** None of them
- C.** ii, iv
- D.** All of them

- B.** All of these countermeasures should be put into place for proper remote administration activities.

- A** is incorrect because sensitive commands and data should not be sent in cleartext (that is, they should be encrypted) to critical systems. For example, SSH should be used, not Telnet. SSH is a network protocol for secure data communication. It allows for remote shell services and command execution and other secure network services between two networked systems. It was designed as a replacement for Telnet and other insecure remote shell protocols such as the Berkeley rsh and rexec protocols, which send information, notably passwords, in plaintext, rendering them susceptible to interception and disclosure.
 - C** is incorrect because sensitive commands and data should not be sent in cleartext (that is, they should be encrypted). For example, SSH should be used, not Telnet. Truly critical systems should be administered locally instead of remotely. Only a small number of administrators should be able to carry out this remote functionality.
 - D** is incorrect because all of these countermeasures should be put into place for proper remote administration activities.
- 19.** A suspected crime has been reported within your organization. Which of the following steps should the incident response team take first?
- A.** Establish a procedure for responding to the incident.
 - B.** Call in forensic experts.
 - C.** Determine that a crime has been committed.
 - D.** Notify senior management.
- C.** When a suspected crime is reported, the incident response team should follow a set of predetermined steps to ensure uniformity in their approach and make sure no steps are skipped. First, the incident response team should investigate the report and determine that an actual crime has been committed. If the team determines that a crime has been carried out, senior management should be informed immediately. At this point, the company must decide if it wants to conduct its own forensic investigation or call in external experts.
 - A** is incorrect because a procedure for responding to an incident should be established before an incident takes place. Incident handling is commonly a recovery plan that responds to malicious technical threats. While the primary goal of incident handling is to contain and mitigate any damage caused by an incident and to prevent any further damage, other objectives include detecting a

problem, determining its cause, resolving the problem, and documenting the entire process.

- B** is incorrect because calling in a forensics team does not occur until the incident response team has investigated the report and verified that a crime has occurred. Then the company can decide if it wants to conduct its own forensic investigation or call in external experts. If experts are going to be called in, the system that was attacked should be left alone in order to try and preserve as much evidence of the attack as possible.
 - D** is incorrect because the incident response team must first determine that a crime has indeed been carried out before it can notify senior management. There is no need to alarm senior management if the report is false.
- 20.** Which of the following is a correct statement regarding digital forensics?
- A.** It is the study of computer technology.
 - B.** It is a set of hardware-specific processes that must be followed in order for evidence to be admissible in a court of law.
 - C.** It encompasses network and code analysis, and may be referred to as electronic data discovery.
 - D.** Digital forensic responsibilities should be assigned to a network administrator before an incident occurs.
 - C.** Forensics is a science and an art that requires specialized techniques for the recovery, authentication, and analysis of electronic data that could have been affected by a criminal act. It is the coming together of computer science, information technology, and engineering with the legal system. When discussing digital forensics with others, you might hear the terms computer forensics, network forensics, electronic data discovery, cyberforensics, and forensic computing. (ISC)² uses *digital forensics* as a synonym for all of these other terms, so that's what you will most likely see on the CISSP exam. Digital forensics encompasses all domains in which evidence is in a digital or electronic form, either in storage or on the wire.
 - A** is incorrect because digital forensics involves more than just the study of information technology. It encompasses the study of information technology but stretches into evidence gathering/protecting and working within specific legal systems.

- B** is incorrect because digital forensics does not refer to hardware or software. It is a set of specific processes relating to reconstruction of computer usage, examination of residual data, authentication of data by technical analysis or explanation of technical features of data, and computer usage that must be followed in order for evidence to be admissible in a court of law.
 - D** is incorrect because digital forensics should be conducted by people with the proper training and skill set, which could or could not be the network administrator. Digital evidence can be fragile and must be worked with appropriately. If someone reboots the attacked system or inspects various files, it could corrupt viable evidence, change timestamps on key files, and erase footprints the criminal may have left.
- 21.** Which of the following dictates that all evidence be labeled with information indicating who secured and validated it?
- A.** Chain of custody
 - B.** Due care
 - C.** Investigation
 - D.** Motive, opportunity, and means
- A.** A crucial piece in the digital forensics process is keeping a proper chain of custody of the evidence. Because evidence from these types of crimes can be very volatile and easily dismissed from court due to improper handling, it is important to follow very strict and organized procedures when collecting and tagging evidence in every single case. Furthermore, the chain of custody should follow evidence through its entire life cycle, beginning with identification and ending with its destruction, permanent archiving, or return to owner. When copies of data need to be made, this process must meet certain standards to ensure quality and reliability. Specialized software for this purpose can be used. The copies must be able to be independently verified and must be tamperproof. Each piece of evidence should be marked in some way with the date, time, initials of the collector, and a case number if one has been assigned. The piece of evidence should then be sealed in a container, which should be marked with the same information. The container should be sealed with evidence tape, and if possible, the writing should be on the tape so that a broken seal can be detected.
 - B** is incorrect because due care means to carry out activities that a

reasonable person would be expected to carry out in the same situation. In short, due care means that a company practiced common sense and prudent management and acted responsibly. If a company does not practice due care in its efforts to protect itself from computer crime, it can be found negligent and legally liable for damages. A chain of custody, on the other hand, is a history that shows how evidence was collected, analyzed, transported, and preserved in order to be presented in court. Because electronic evidence can be easily modified, a clearly defined chain of custody demonstrates that the evidence is trustworthy.

- ☒ **C** is incorrect because investigation involves the proper collection of relevant data during the incident response process and includes analysis, interpretation, reaction, and recovery. The goals of this stage are to reduce the impact of the incident, identify the cause of the incident, resume operations as soon as possible, and apply what was learned to prevent the incident from recurring. It is also at this stage where it is determined whether a forensic investigation will take place. The chain of custody dictates how this material should be properly collected and protected during its life cycle of being evidence.
- ☒ **D** is incorrect because motive, opportunity, and means (MOM) is a strategy used to understand why a crime was carried out and by whom. This is the same strategy used to determine the suspects in a traditional, noncomputer crime. Motive is the “who” and “why” of a crime. Understanding the motive for a crime is an important piece in figuring out who would engage in such an activity. For example, many hackers attack big-name sites because when the sites go down, it is splashed all over the news. However, once these activities are no longer so highly publicized, the individuals will eventually stop initiating these types of attacks because their motive will have been diminished. Opportunity is the “where” and “when” of a crime. Opportunities usually arise when certain vulnerabilities or weaknesses are present. If a company does not have a firewall, hackers and attackers have all types of opportunities within that network. Once a crime fighter finds out why a person would want to commit a crime (motive), she will look at what could allow the criminal to be successful (opportunity). Means pertains to the capabilities a criminal would need to be successful. Suppose a crime fighter was asked to investigate a complex embezzlement that took place within a financial institution. If the suspects were three people who knew how to use a mouse, a keyboard, and a word

processing application, but only one of them was a programmer and system analyst, the crime fighter would realize that this person may have the means to commit this crime much more successfully than the other two individuals.

- 22.** Which of the following is not true of a forensic investigation?
- A. The crime scene should be modified as necessary.
 - B. A file copy tool may not recover all data areas of the device that are necessary for investigation.
 - C. Contamination of the crime scene may not negate derived evidence, but it should still be documented.
 - D. Only individuals with knowledge of basic crime scene analysis should have access to the crime scene.
- A.** The principles of criminalistics are included in the forensic investigation process. They are identification of the crime scene, protection of the environment against contamination and loss of evidence, identification of evidence and potential sources of evidence, and collection of evidence. In regard to minimizing the degree of contamination, it is important to understand that it is impossible not to change a crime scene—be it physical or digital. The key is to minimize changes and document what you did and why, and how the crime scene was affected.
- B** is incorrect because it is true that a file copy tool may not recover all data areas of the device necessary for investigation. During the examination and analysis process of a forensic investigation, it is critical that the investigator works from an image that contains all of the data from the original disk. It must be a bit-level copy, sector by sector, to capture deleted files, slack spaces, and unallocated clusters. These types of images can be created through the use of specialized tools such as FTK Imager, EnCase, or the dd Unix utility.
- C** is incorrect because it is true that if a crime scene becomes contaminated, that should be documented. While it may not negate the derived evidence, it will make investigating the crime and providing useful evidence for court more challenging. Whether the crime scene is physical or digital, it is important to control who comes in contact with the evidence of the crime to ensure its integrity.
- D** is incorrect because the statement is true. Only authorized

individuals should be allowed to access the crime scene, and these individuals should have knowledge of basic crime scene analysis. Other measures to protect the crime scene include documenting who is at the crime scene and the last individuals to interact with the system. In court, the integrity of the evidence may be in question if there were too many people milling around the crime scene.

23. Stephanie has been put in charge of developing incident response and forensics procedures her company needs to carry out if an incident occurs. She needs to ensure that their procedures map to the international principles for gathering and protecting digital evidence. She also needs to ensure that if and when internal forensics teams are deployed, they have labels, tags, evidence bags, cable ties, imaging software, and other associated tools. Which of the following best describes what Stephanie needs to build for the deployment teams?
- A. Local and remote imaging system
 - B. Forensics field kit
 - C. Chain of custody procedures and tools
 - D. Digital evidence collection software
- B.** When forensics teams are deployed to investigate a potential crime, they should be properly equipped with all of the tools and supplies needed. The following are some of the common items in the forensics field kits:
- Documentation tools: tags, labels, and timelined forms
 - Disassembly and removal tools: antistatic bands, pliers, tweezers, screwdrivers, wire cutters, and so on
 - Package and transport supplies: antistatic bags, evidence bags and tape, cable ties, and others
- A** is incorrect because imaging software and tools only make up some of the tools that a forensics team needs. These types of tools do not include the items identified in the question, which are labels, tags, evidence bags, cable ties, imaging software, and other associated tools. These items should be organized and be in a field kit.
- C** is incorrect because chain of custody procedures and tools only make up some of the components that a forensics team needs. These types of tools do not include the items identified in the question, which are labels, tags, evidence bags, cable ties, imaging software,

and other associated tools. These items should be organized and be in a field kit. A chain of custody is a history that shows how evidence was collected, analyzed, transported, and preserved in order to be presented in court. Because electronic evidence can be easily modified, a clearly defined chain of custody demonstrates that the evidence is trustworthy.

- D** is incorrect because digital evidence collection tools only make up some of the components that a forensics team needs. These types of tools do not include the items identified in the question, which are labels, tags, evidence bags, cable ties, imaging software, and other associated tools. These items should be organized and be in a field kit. There are specialized software suites that allow forensics personnel to properly collect, analyze, and manage digital evidence through its life cycle. They are important, but only one component of an overall forensics kit.
- 24.** When developing a recovery and continuity program within an organization, different metrics can be used to properly measure potential damages and recovery requirements. These metrics help us quantify our risks and the benefits of controls we can put into place. Two metrics commonly used in the development of recovery programs are recovery point objective (RPO) and recovery time objective (RTO). Data restoration (RPO) requirements can be different from service restoration (RTO) requirements. Which of the following best defines these two main recovery measurements in this type of scenario?
- A.** RPO is the acceptable amount of data loss measured in time. RTO is the acceptable time period before a service level must be restored.
 - B.** RTO is the earliest time period in which a data set must be restored. RPO is the acceptable amount of downtime in a given period.
 - C.** RPO is the acceptable amount of data loss measured in time. RTO is the earliest time period in which data must be restored.
 - D.** RPO is the acceptable amount of downtime measured. RTO is the earliest time period in which a service level must be restored.
- A.** The recovery point objective (RPO) is the acceptable amount of data loss measured in time. This value represents the earliest point in time by which data must be recovered. The higher the value of data, the more funds or other resources that can be put into place to ensure a smaller amount of data is lost in the event of a disaster. For example, if the RPO is set to two hours, this means that the

organization has to have backup and restore processes that will only allow for the loss of up to two hours of data. The restore process cannot be something as time consuming as restoring from a backup tape manually, but will need to be an automated restoration process that can restore data more quickly and allow the production environment to be up and running and carrying out business processes. The recovery time objective (RTO) is the acceptable period before a specific service level must be restored in order to avoid unacceptable consequences after a disruption or disaster. While RPO pertains to data, RTO deals with the actual processing capabilities of an environment.

- B** is incorrect because the RTO is the earliest time period in which a service level must be restored; thus, it does not explicitly deal with recovering a data set. And the RPO is the acceptable amount of data loss measured in time, not downtime in general. The definitions in this answer are backward. The RPO provides the recovery team with a requirement or goal to work toward when establishing data recovery processes. RPO values for less critical data will be higher; thus, the recovery processes can include slower and cheaper recovery solutions. If an RPO value is high, then the data is more critical in nature and the team must implement solutions that recover this type of data more quickly. RTO values also give the recovery team requirements to work with so that they know the type of recovery solutions that must be deployed. If a production environment has to be up and running within one hour after a disruption, the team must deploy redundancy into the environment so that the systems can respond quickly.
- C** is incorrect because the RTO metric pertains to how quickly services must come back online and not how quickly data must be restored. The RTO provides the recovery team with an objective, which is a goal to achieve as it pertains to getting systems and network capabilities up and running after they went down. This metric tells the team how long the organization can endure being offline and still stay in business. A small business that does not depend upon time-sensitive transactions may be able to be offline for one to two days without negatively affecting the survivability of the company. If a company like [Amazon.com](#) was offline for two days, the financial and reputation hit that it would have to endure may not put the company out of business, but this potential loss is too much to risk, thus expensive recovery solutions are necessary. If you understand how much you can potentially lose, you will make

better decisions about what to put into place to make sure that any potential loss is endurable and not devastating.

- D** is incorrect because the RPO measurement pertains to data recovery and not service downtime. RPO is the maximum tolerable time period during which data may be unavailable, which is not the same as a measurement of how much data may be lost. For example, if a company's main database gets corrupted and the company can absorb the impact of not having the data on this database restored for 48 hours, then the recovery team can implement tape backups that are stored and retrieved from an offsite location. The restoration timeline of this data has to take into account how long it will take for someone to go get the tape from the offsite location, bring it to the production environment, carry out the restore process, and test the newly recovered data. All of those steps have to happen successfully within the RPO window of 48 hours.
- 25.** An approach to alternate offsite facilities is to establish a reciprocal agreement. Which of the following describes the pros and cons of a reciprocal agreement?
- A.** It is fully configured and ready to operate within a few hours, but is the most expensive of the offsite choices.
 - B.** It is an inexpensive option, but it takes the most time and effort to get up and running after a disaster.
 - C.** It is a good alternative for companies that depend upon proprietary software, but annual testing is not usually available.
 - D.** It is the cheapest of the offsite choices, but mixing operations could introduce many security issues.
- D.** A reciprocal agreement, also referred to as mutual aid, means that company A agrees to allow company B to use its facilities if company B is hit by a disaster, and vice versa. This is a cheaper way to go than the other offsite choices, but it is not always the best choice. Most environments are maxed out pertaining to the use of facility space, resources, and computing capability. To allow another company to come in and work out of the same shop could prove to be detrimental to both companies. The stress of two companies working in the same environment could cause tremendous levels of tension. If it did work out, it would only provide a short-term solution. Configuration management could be a nightmare, and the mixing of operations could introduce many

security issues. Reciprocal agreements have been known to work well in specific businesses, such as newspaper printing. These businesses require very specific technology and equipment that will not be available through any subscription service. For most other organizations, reciprocal agreements are generally, at best, a secondary option for disaster protection.

- A** is incorrect because a hot site—not a reciprocal agreement—is fully configured and ready to operate within a few hours. A hot site is also the most expensive offsite option. The only missing resources from a hot site are usually the data, which will be retrieved from a backup site, and the people who will be processing the data. The equipment and system software must be compatible with the data being restored from the main site and must not cause any negative interoperability issues. Hot sites are a good choice for a company that needs to ensure a site will be available for it as soon as possible.
 - B** is incorrect because it describes a cold site, an inexpensive offsite option that takes the most time and effort to actually get up and functioning right after a disaster. With cold sites the vendor supplies the basic environment, electrical wiring, air conditioning, plumbing, and flooring, but none of the equipment or additional services. It may take weeks to get the site activated and ready for work.
 - C** is incorrect because it describes a warm site, a good alternative for companies that depend upon proprietary software. A warm site is equipped with some equipment, but not the actual computers. It is a better choice than a reciprocal agreement or hot site for a company that depends upon proprietary and unusual hardware and software, because they will bring their own hardware and software with them to the site after a disaster hits. The disadvantage of using a warm site is that the vendors' contracts do not usually include annual testing, which helps ensure that the company can return to an operating state within hours.
- 26.** The operations team is responsible for defining which data gets backed up and how often. Which type of backup process backs up files that have been modified since the last time all data was backed up?
- A.** Incremental process
 - B.** Full backup
 - C.** Partial backup

D. Differential process

- D.** Backups can be full, differential, or incremental, and are usually used in some type of combination with each other. Most files are not altered every day, so to save time and resources, it is best to devise a backup plan that does not continually back up data that has not been modified. Backup software reviews the archive bit setting when making its determination on what gets backed up and what does not. If a file is modified or created, the file system sets the archive bit to 1, and the backup software knows to back up that file. A differential process backs up the files that have been modified since the last full backup; in other words, the last time all the data was backed up. When the data needs to be restored, the full backup is laid down first, and then the differential backup is put down on top of it.
 - A** is incorrect because an incremental process backs up all the files that have changed since the last full or incremental backup. If a company experienced a disaster and it used the incremental process, it would first need to restore the full backup on its hard drives and lay down every incremental backup that was carried out before the disaster took place. So, if the full backup was done six months ago and the operations department carried out an incremental backup each month, the restoration team would restore the full backup and start with the older incremental backups and restore each one of them until they are all restored.
 - B** is incorrect because with a full backup, all data is backed up and saved to some type of storage media. During a full backup, the archive bit is cleared, which means that it is set to 0. A company can choose to do full backups only, in which case the restoration process is just one step, but the backup and restore processes could take a long time.
 - C** is incorrect because it is not the best answer to this question. While a backup can be a partial backup, it does not necessarily mean that it backs up all the files that have been modified since the last time a backup process was run.
27. After a disaster occurs, a damage assessment needs to take place. Which of the following steps occurs last in a damage assessment?
- A.** Determine the cause of the disaster.
 - B.** Identify the resources that must be replaced immediately.

- C. Declare a disaster.
 - D. Determine how long it will take to bring critical functions back online.
- C.** The final step in a damage assessment is to declare a disaster. After information from the damage assessment is collected and assessed, it will indicate what teams need to be called to action and whether the BCP actually needs to be activated. The BCP coordinator and team must develop activation criteria before a disaster takes place. After the damage assessment, if one or more of the situations outlined in the criteria have taken place, then the team is moved into recovery mode. Different organizations have different criteria, because the business drivers and critical functions will vary from organization to organization. The criteria may consist of danger to human life, danger to state or national security, damage to facility, damage to critical systems, and estimated value of downtime that will be experienced.
- A** is incorrect because determining the cause of the disaster is the first step of the damage assessment. The issue that caused the damage may still be taking place, and the team must figure out how to stop it before a full damage assessment can take place.
- B** is incorrect because identifying the resources that must be replaced immediately is not the last step of a damage assessment. It does occur near the end of the assessment, however. Once the resources are identified, the team must estimate how long it will take to bring critical functions back online, and then declare a disaster, if necessary.
- D** is incorrect because determining how long it will take to bring critical functions back online is the second-to-last step in a damage assessment. If it will take longer than the previously determined maximum tolerable downtime (MTD) values to restore operations, then a disaster should be declared and the BCP should be put into action.
- 28.** Of the following plans, which establishes senior management and a headquarters after a disaster?
- A. Continuity of operations plan
 - B. Cyber-incident response plan
 - C. Occupant emergency plan

D. IT contingency plan

- A.** A continuity of operations (COOP) plan establishes senior management and a headquarters after a disaster. It also outlines roles and authorities, orders of succession, and individual role tasks. Creating a COOP plan begins with assessing how the organization operates to identify mission-critical staff, materials, procedures, and equipment. If one exists, review the business process flowchart. Identify suppliers, partners, contractors, and other businesses the organization interacts with on a daily basis, and create a list of these and other businesses the organization could use in an emergency. It is important for an organization to make plans for what it will do if the building becomes inaccessible.
 - B** is incorrect because a cyber-incident response plan focuses on malware, hackers, intrusions, attacks, and other security issues. It outlines procedures for incident response with the goal of limiting damage, minimizing recovery time, and reducing costs. A cyber-incident response plan should include a description of the different types of incidents, who to call when an incident occurs, and each person's responsibilities, procedures for addressing different types of incidents, and forensic procedures. The plan should be tested, and all participants should be trained on their responsibilities.
 - C** is incorrect because an occupant emergency plan establishes personnel safety and evacuation procedures. The goal of an occupant emergency plan is to reduce the risk to personnel and minimize the disruption to work and operations in the case of an emergency. The plan should include procedures for ensuring the safety of employees with disabilities, including their evacuation from the facility if necessary. All employees should have access to the occupant emergency response plan, and it should be practiced so that everyone knows how to execute it.
 - D** is incorrect because an IT contingency plan establishes procedures for the recovery of systems, networks, and major applications after disruptions. Steps for creating IT contingency plans are addressed in the NIST 800-34 document.
- 29.** Gizmos and Gadgets has restored its original facility after a disaster. What should be moved in first?
- A.** Management
 - B.** Most critical systems

C. Most critical functions

D. Least critical functions

- D.** After the primary site has been repaired, the least critical components are moved in first. This ensures that the primary site is really ready to resume processing. By doing this, you can validate that environmental controls, power, and communication links are working properly. It can also avoid putting the company into another disaster. If the less critical functions survive, then the more critical components of the company can be moved over.
- A** is incorrect because personnel should not be moved into the facility until it is determined that the environment is safe, everything is in good working order, and all necessary equipment and supplies are present. Least critical functions should be moved back first, so if there are issues in network configurations or connectivity, or important steps were not carried out, the critical operations of the company are not negatively affected.
- B** is incorrect because the most critical systems should not be resumed in the new environment until it has been properly tested. You do not want to go through the trouble of moving the most critical systems and operations from a safe and stable site, only to return them to a main site that is untested. When you move less critical departments over first, they act as the canary. If they survive, then move on to critical systems.
- C** is incorrect because the most critical functions should not be moved over before less critical functions, which serve to test the stability and safety of the site. If the site proves to need further preparation, then no harm is done to the critical functions.

30. Several teams should be involved in carrying out the business continuity plan. Which team is responsible for starting the recovery of the original site?

A. Damage assessment team

B. BCP team

C. Salvage team

D. Restoration team

- C.** The BCP coordinator should have an understanding of the needs of the company and the types of teams that need to be developed and trained. Employees should be assigned to the specific teams

based on their knowledge and skill set. Each team needs to have a designated leader, who will direct the members and their activities. These team leaders will be responsible not only for ensuring that their team's objectives are met, but also for communicating with each other to make sure each team is working in parallel phases. The salvage team is responsible for starting the recovery of the original site. It is also responsible for backing up data from the alternate site and restoring it within the new facility, carefully terminating contingency operations, and securely transporting equipment and personnel to the new facility.

- A** is incorrect because the damage assessment team is responsible for determining the scope and severity of the damage caused. Whether or not a disaster is declared and the BCP is put into action is based on this information collected and assessed by the damage assessment team.
- B** is incorrect because the BCP team is responsible for creating and maintaining the business continuity plan. Therefore, its responsibilities also include identifying regulatory and legal requirements that must be met, identifying all possible vulnerabilities and threats, performing a business impact analysis, and developing procedures and steps in resuming business after a disaster. The BCP team is made up of representatives from a variety of business units and departments, including senior management, the security department, the communications department, and the legal department. This is not the team that starts the physical recovery of the original site.
- D** is incorrect because the restoration team is responsible for getting the alternate site into a working and functioning environment. Both the restoration team and the salvage team must know how to do many tasks, such as install operating systems, configure workstations and servers, string wire and cabling, set up the network and configure networking services, and install equipment and applications. Both teams must also know how to restore data from backup facilities and how to do so in a secure manner that ensures that the systems' and data's confidentiality, integrity, and availability are not compromised.

- 31.** ACME, Inc., paid a software vendor to develop specialized software, and that vendor has gone out of business. ACME, Inc., does not have access to the code and therefore cannot keep it updated. What mechanism should the company have implemented to prevent this from

happening?

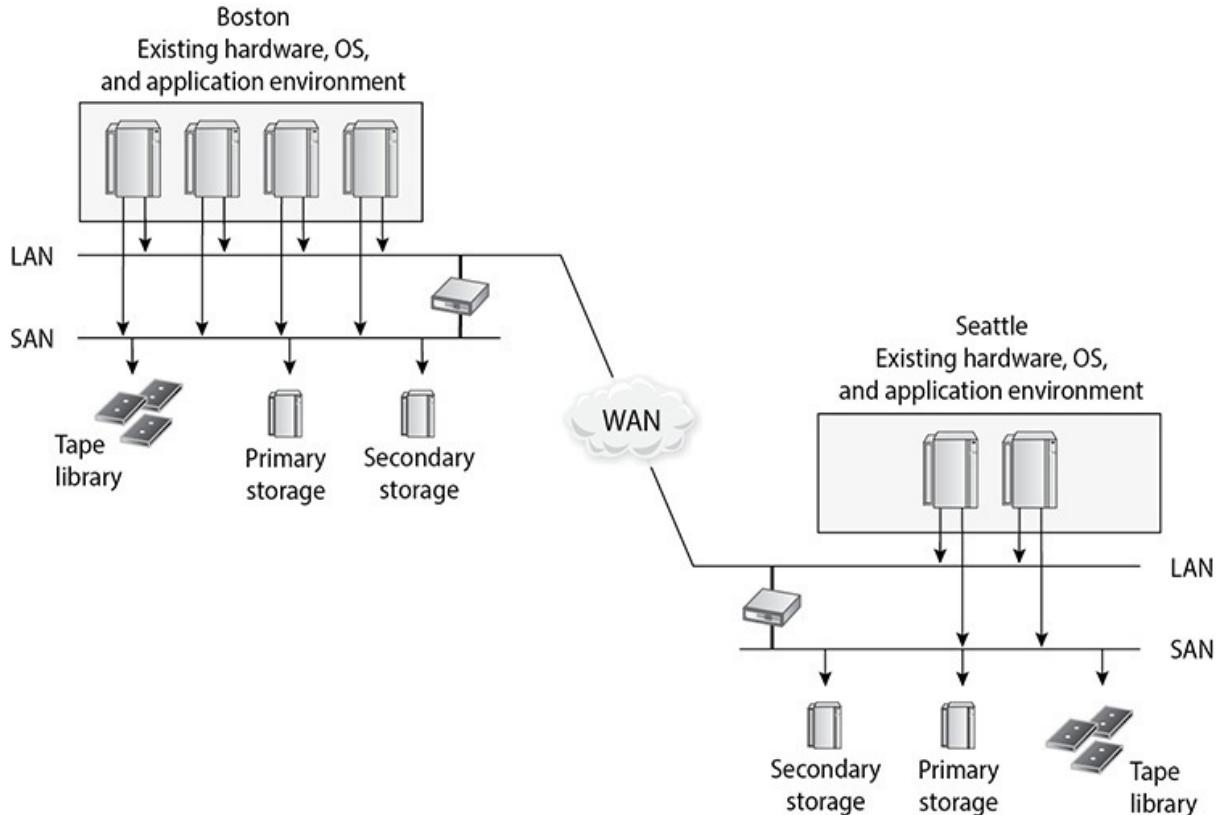
- A.** Reciprocal agreement
 - B.** Software escrow
 - C.** Electronic vaulting
 - D.** Business interruption insurance
- B.** The protection mechanism that ACME, Inc., should have implemented is called software escrow. Software escrow means that a third party holds the source code and backups of the compiled code, manuals, and other supporting materials. A contract between the software vendor, customer, and third party outlines who can do what and when with the source code. This contract usually states that the customer can have access to the source code only if and when the vendor goes out of business, is unable to carry out stated responsibilities, or is in breach of the original contract. If any of these activities takes place, then the customer is protected because it can still gain access to the source code and other materials through the third-party escrow agent.
- A** is incorrect because a reciprocal agreement is an offsite facility option that involves two companies agreeing to share their facility in case a disaster renders one of the facilities unusable. Reciprocal agreements deal with disaster recovery and not software protection when dealing with the developing vendor.
- C** is incorrect because electronic vaulting is a type of electronic backup solution. Electronic vaulting makes copies of files as they are modified and periodically transmits them to an offsite backup site. The transmission does not happen in real time but is carried out in batches. So, a company can choose to have all files that have been changed sent to the backup facility every hour, day, week, or month. The information can be stored in an offsite facility and retrieved from that facility in a short period of time. Electronic vaulting has to do with backing up data so that it is available if there is a disruption or disaster.
- D** is incorrect because a business interruption insurance policy covers specified expenses and lost earnings if a company is out of business for a certain length of time. This insurance is commonly purchased to protect a company in case a disaster takes place and they have to shut down their services for a specific period of time. It does not have anything to do with protection or accessibility of

source code.

32. Which of the following incorrectly describes the concept of executive succession planning?
- A. Predetermined steps protect the company if a senior executive leaves.
 - B. Two or more senior staff cannot be exposed to a particular risk at the same time.
 - C. It documents the assignment of deputy roles.
 - D. It covers assigning a skeleton crew to resume operations after a disaster.
- D.** A skeleton crew consists of the employees who carry out the most critical functions following a disaster. They are put to work first during the recovery process. A skeleton crew is not related to the concept of executive succession planning, which addresses the steps that will be taken to fill a senior executive role should that person retire, leave the company, or die. The objective of a skeleton crew is to maintain critical operations, while the objective of executive succession planning is to protect the company by maintaining leadership roles.
- A** is incorrect because executive succession planning includes predetermined steps that protect the company if someone in a senior executive position retires, leaves the company, or is killed. The loss of a senior executive could tear a hole in the company's fabric, creating a leadership vacuum that must be filled quickly with the right individual. The line-of-succession plan defines who would step in and assume responsibility for this role.
- B** is incorrect because the concept of two or more senior staff not being exposed to a particular risk at the same time is a policy that some larger organizations establish as part of their executive succession planning efforts. The idea is to protect senior personnel and the organization if a disaster were to strike. For example, an organization may decide that the CEO and president cannot travel on the same plane. If the plane went down and both individuals were killed, then the company could be in danger.
- C** is incorrect because executive succession planning can include the assignment of deputy roles. An organization may have a deputy CIO, deputy CFO, and deputy CEO ready to take over the necessary tasks if the CIO, CFO, or CEO becomes unavailable. Executive

succession planning is the decision to have these deputies step into the CIO, CFO, or CEO roles.

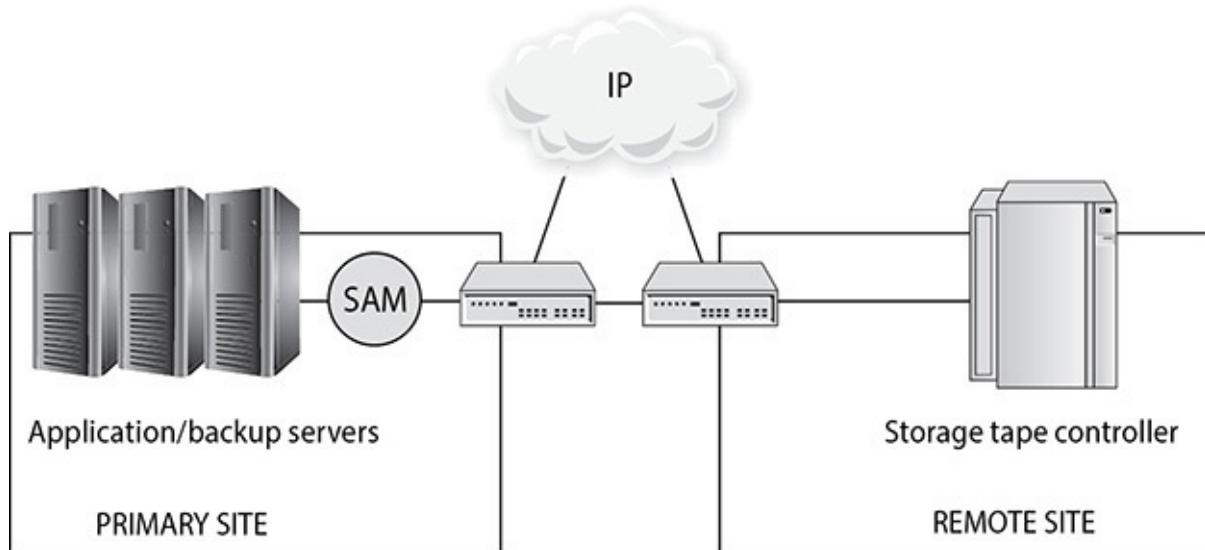
33. What type of infrastructural setup is illustrated in the graphic that follows?



- A. Hot site
 - B. Warm site
 - C. Cold site
 - D. Reciprocal agreement
- A.** A hot site is a facility that is leased or rented and is fully configured and ready to operate within a few hours. The only missing resources from a hot site are usually the data, which will be retrieved from a backup site, and the people who will be processing the data. The equipment and system software must absolutely be compatible with the data being restored from the main site and must not cause any negative interoperability issues. A hot site is a good choice for a company that needs to ensure a site will be available for it as soon as possible.
- B** is incorrect because a warm site is a leased or rented facility that is usually partially configured with some equipment, but not the actual computers. In other words, a warm site is usually a hot site without

the expensive equipment. Staging a facility with duplicate hardware and computers configured for immediate operation is extremely expensive, so a warm site provides an alternate facility with some peripheral devices. This is the most widely used model. It may be a better choice for companies that depend upon proprietary and unusual hardware and software, because they will bring their own hardware and software with them to the site after the disaster hits.

- C** is incorrect because a cold site is a leased or rented facility that supplies the basic environment, electrical wiring, air conditioning, plumbing, and flooring, but none of the equipment or additional services. It may take weeks to get the site activated and ready for work. The cold site could have equipment racks and dark fiber (fiber that does not have the circuit engaged) and maybe even desks, but it would require the receipt of equipment from the client, since it does not provide any. The cold site is the least expensive option but takes the most time and effort to actually get up and functioning right after a disaster.
 - D** is incorrect because a reciprocal agreement is one in which a company promises another company it can move into its facility and share space if it experiences a disaster, and vice versa. Reciprocal agreements are very tricky to implement and are unenforceable. This is a cheaper way to go than the other offsite choices, but it is not always the best choice. Most environments are maxed out pertaining to the use of facility space, resources, and computing capability.
34. There are several types of redundant technologies that can be put into place. What type of technology is shown in the graphic that follows?



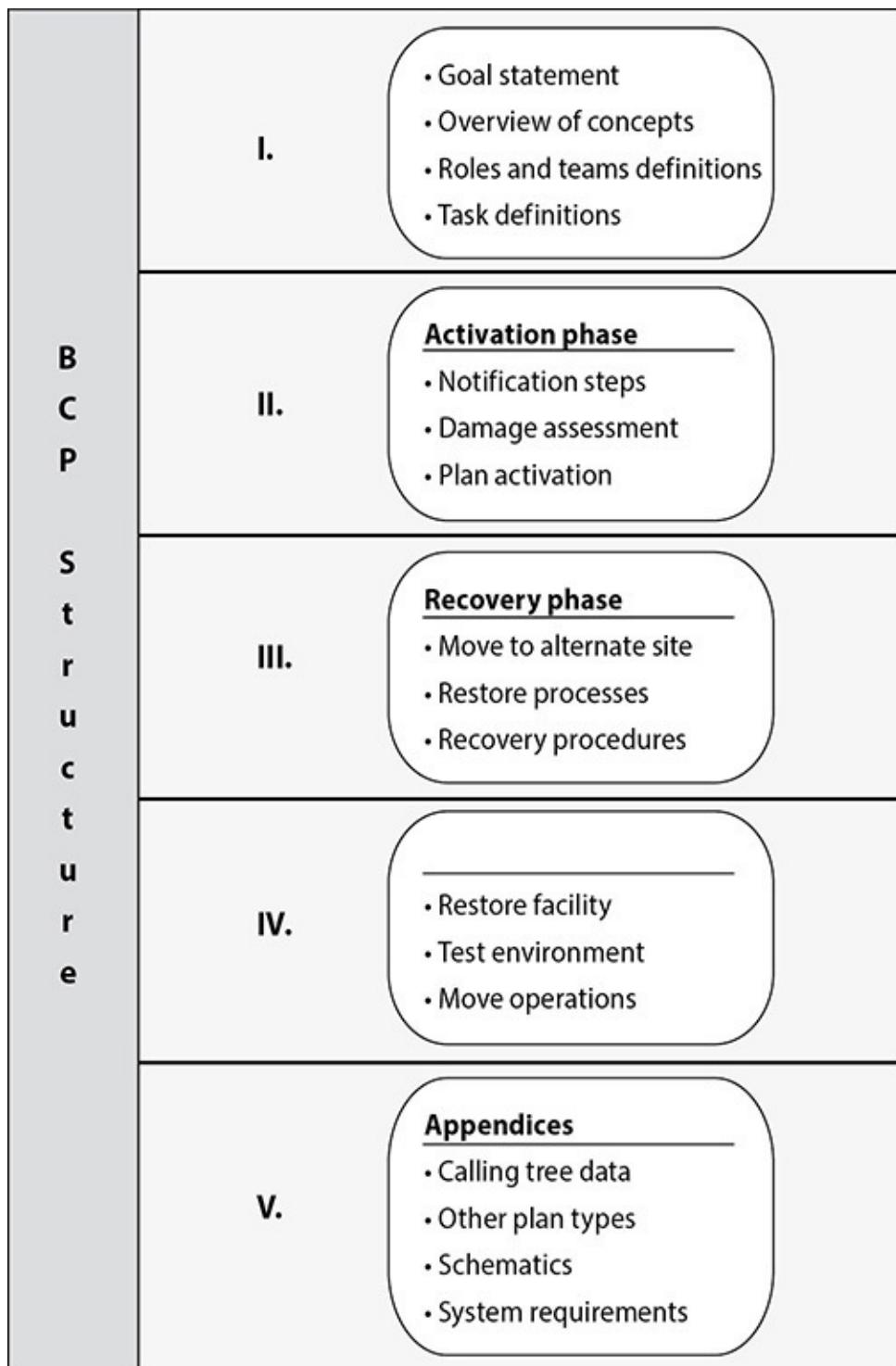
- A.** Tape vaulting
 - B.** Remote journaling
 - C.** Electronic vaulting
 - D.** Redundant site
- A.** Each site should have a full set of the most current and updated information and files, and a commonly used software backup technology is referred to as tape vaulting. Many businesses back up their data to tapes that are then manually transferred to an offsite facility by a courier or an employee. With automatic tape vaulting, the data is sent over a serial line to a backup tape system at the offsite facility. The company that maintains the offsite facility maintains the systems and changes out tapes when necessary. Data can be quickly backed up and retrieved when necessary. This technology reduces the manual steps in the traditional tape backup procedures. Basic vaulting of tape data involves sending backup tapes to an offsite location, but a manual process can be error prone. Electronic tape vaulting transmits data over a network to tape devices located at an alternate data center. Electronic tape vaulting improves recovery speed and reduces errors, and backups can be run more frequently.
- B** is incorrect because remote journaling is a technology used to transmit data to an offsite facility, but this usually only includes moving the journal or transaction logs to the offsite facility, not the actual files. This graphic specifically shows a tape controller, and remote journaling mainly takes place between databases. Remote journaling involves transmitting the journal or transaction log offsite to a backup facility. These logs contain the deltas (changes) that have taken place to the individual files. If and when data is corrupted and needs to be restored, the company can retrieve these logs, which are used to rebuild the lost data. Journaling is efficient for database recovery, where only the reapplication of a series of changes to individual records is required to resynchronize the database.
- C** is incorrect because electronic vaulting most commonly takes place between databases and makes copies of files as they are modified and periodically transmits them to an offsite backup site. The transmission does not happen in real time but is carried out in batches. So, a company can choose to have all files that have been changed sent to the backup facility every hour, day, week, or month.

The information can be stored in an offsite facility and retrieved from that facility in a short period of time. This form of backup takes place in many financial institutions, so when a bank teller accepts a deposit or withdrawal, the change to the customer's account is made locally to that branch's database and to the remote site that maintains the backup copies of all customer records.

- D is incorrect because while the graphic could be illustrating that the tape controller is located at a redundant site, a redundant site is not actually a technology. Some companies choose to have redundant sites, meaning one site is equipped and configured exactly like the primary site, which serves as a redundant environment. These sites are owned by the company and are mirrors of the original production environment. This is one of the most expensive backup facility options, because a full environment must be maintained even though it usually is not used for regular production activities until after a disaster takes place that triggers the relocation of services to the redundant site.
35. Here is a graphic of a business continuity policy. Which component is missing from this graphic?

B
C
P

S
t
r
u
c
t
u
r
e



- A. Damage assessment phase
 - B. Reconstitution phase
 - C. Business resumption phase
 - D. Continuity of operations plan
- B. After a disaster takes place and a company moves out of its facility, it must move back in after the facility is reconstructed.

When it is time for the company to move back into its original site or a new site, the company is ready to enter into the reconstitution phase. A company is not out of an emergency state until it is back in operation at the original primary site or a new site that was constructed to replace the primary site, because the company is always vulnerable while operating in a backup facility. Many logistical issues need to be considered as to when a company must return from the alternate site to the original site. The following lists a few of these issues:

- Ensuring the safety of employees
- Ensuring an adequate environment is provided (power, facility infrastructure, water, HVAC)
- Ensuring that the necessary equipment and supplies are present and in working order
- Ensuring proper communications and connectivity methods are working
- Properly testing the new environment

A is incorrect because a role, or a team, needs to be created to carry out a damage assessment once a disaster has taken place. The assessment procedures should be properly documented and include the following steps:

- Determine the cause of the disaster.
- Determine the potential for further damage.
- Identify the affected business functions and areas.
- Identify the level of functionality for the critical resources.
- Identify the resources that must be replaced immediately.
- Estimate how long it will take to bring critical functions back online.
- If it will take longer than the previously estimated maximum tolerable downtime (MTD) values to restore operations, then a disaster should be declared and the BCP should be put into action.

After this information is collected and assessed, it will indicate which teams need to be called to action and whether the BCP actually needs to be activated. The BCP coordinator and team must develop activation criteria. After the damage assessment, if one or more of the situations outlined in the criteria have taken place, then

the team is moved into recovery mode.

- C** is incorrect because a business resumption plan focuses on how to re-create the necessary business processes that need to be reestablished instead of focusing on only IT components (i.e., it is process oriented instead of procedure oriented). This plan could be mentioned in the BCP policy, but the policy does not outline the specifics of reestablishing business processes.
- D** is incorrect because a continuity of operations (COOP) plan establishes senior management and a headquarters after a disaster. It provides instructions on how to set up a command center so that all activities and communication take place centrally and in a controlled manner. This type of plan also outlines roles and authorities, orders of succession, and individual role tasks that need to be put into place after a disaster takes place. This plan could be mentioned in the BCP policy, but the policy does not outline the specifics of setting up a command center and its components.

36. The recovery time objective (RTO) and maximum tolerable downtime (MTD) metrics have similar roles, but their values are very different. Which of the following best describes the difference between RTO and MTD metrics?

- A.** The RTO is a time period that represents the inability to recover, and the MTD represents an allowable amount of downtime.
- B.** The RTO is an allowable amount of downtime, and the MTD represents a time period after which severe and perhaps irreparable damage is likely.
- C.** The RTO is a metric used in disruptions, and the MTD is a metric used in disasters.
- D.** The RTO is a metric pertaining to loss of access to data, and the MTD is a metric pertaining to loss of access to hardware and processing capabilities.
- B.** The RTO value is smaller than the MTD value, because the MTD value represents the time after which an inability to recover significant operations will mean severe and perhaps irreparable damage to the organization's reputation or bottom line. The RTO assumes that there is a period of acceptable downtime. This means that a company can be out of production for a certain period of time (RTO) and still get back on its feet. But if the company cannot get production up and running within the MTD window, the company is

sinking too fast to properly recover.

- A** is incorrect because the MTD is a time period that represents the inability to recover, and the RTO represents an allowable amount of downtime.
- C** is incorrect because the RTO is the earliest time period and a service level within which a business process must be restored after a disaster to avoid unacceptable consequences associated with a break in business continuity. The RTO value is smaller than the MTD value because the MTD value represents the time after which an inability to recover significant operations will mean severe and perhaps irreparable damage to the organization's reputation or bottom line.
- D** is incorrect because the RTO is the earliest time period and a service level within which a business process must be restored after a disaster to avoid unacceptable consequences associated with a break in business continuity. The RTO value is smaller than the MTD value because the MTD value represents the time after which an inability to recover significant operations will mean severe and perhaps irreparable damage to the organization's reputation or bottom line. RTO is not a metric pertaining to loss of access to data, and the MTD is not a metric pertaining to loss of access to hardware and processing capabilities.

- 37.** High availability (HA) is a combination of technologies and processes that work together to ensure that specific critical functions are always up and running at the necessary level. To provide this level of high availability, a company has to have a long list of technologies and processes that provide redundancy, fault tolerance, and failover capabilities. Which of the following best describes these characteristics?

- A.** Redundancy is the duplication of noncritical components or functions of a system with the intention of decreasing reliability of the system. Fault tolerance is the capability of a technology to discontinue to operate as expected even if something unexpected takes place. If a technology has a failover capability, this means that if there is a failure that cannot be handled through normal means, then processing is “switched over” to a working system.
- B.** Redundancy is the duplication of critical components or functions of a system with the intention of increasing reliability of the system. Fault tolerance is the capability of a technology to

discontinue to operate as expected even if something unexpected takes place. If a technology has a failover capability, this means that if there is a failure that cannot be handled through normal means, then processing is “switched over” to a working system.

- C. Redundancy is the duplication of critical components or functions of a system with the intention of increasing reliability of the system. Fault tolerance is the capability of a technology to continue to operate as expected even if something unexpected takes place. If a technology has a failover capability, this means that if there is a failure that cannot be handled through normal means, then processing is “switched over” to a nonworking system.
 - D. Redundancy is the duplication of critical components or functions of a system with the intention of increasing reliability of the system. Fault tolerance is the capability of a technology to continue to operate as expected even if something unexpected takes place. If a technology has a failover capability, this means that if there is a failure that cannot be handled through normal means, then processing is “switched over” to a working system.
- D.** High availability (HA) is a combination of technologies and processes that work together to ensure that specific critical functions are always up and running. The specific thing can be a database, a network, an application, a power supply, etc. To provide this level of high availability, the company has to have a long list of technologies and processes that provide redundancy, fault tolerance, and failover capabilities. Redundancy, fault tolerance, and failover capabilities increase the reliability of a system or network. High reliability allows for high availability.
- A** is incorrect because redundancy within this type of technology encompasses the duplication of critical components or functions of a system with the intention of *increasing* reliability of the system. Redundancy is commonly built into the network at a routing protocol level. The routing protocols are configured so if one link goes down or gets congested, then traffic is routed over a different network link. Redundant hardware can also be available so if a primary device goes down the backup component can be swapped out and activated.
- B** is incorrect because fault tolerance is the capability of a technology to *continue* to operate as expected even if something unexpected takes place (a fault). If a database experiences an unexpected glitch, it can roll back to a known-good state and

continue functioning as though nothing bad happened. If a packet gets lost or corrupted during a TCP session, the TCP protocol will resend the packet so that system-to-system communication is not affected. If a disk within a RAID system gets corrupted, the system uses its parity data to rebuild the corrupted data so that operations are not affected.

- C** is incorrect because if a technology has a failover capability, this means that if there is a failure that cannot be handled through normal means, then processing is “switched over” to a *working* system.

The following scenario applies to questions 38 and 39.

Jeff is leading the business continuity group in his company. They have completed a business impact analysis and have determined that if the company’s credit card processing functionality was unavailable for 48 hours the company would most likely experience such a large financial hit that it would have to go out of business. The team has calculated that this functionality needs to be up and running within 28 hours after experiencing a disaster for the company to stay in business. The team has also determined that the restoration steps must be able to restore data that is 60 minutes old or less.

- 38.** In this scenario, which of the following is the work recovery time value?
 - A. 48 hours
 - B. 28 hours
 - C. 20 hours
 - D. 1 hour
 - C.** The work recovery time (WRT) is the remainder of the overall MTD value after RTO. RTO usually deals with getting the infrastructure and systems back up and running, and WRT deals with restoring data, testing processes, and then making everything “live” for production purposes.
 - A** is incorrect because in this scenario 48 hours is the MTD value.
 - B** is incorrect because in this scenario 28 hours is the RTO value.
 - D** is incorrect because this value does not represent the WRT.
- 39.** In this scenario, what would the 60-minute time period be referred to as?

- A.** Recovery time period
 - B.** Maximum tolerable downtime
 - C.** Recovery point objective
 - D.** Recovery point time period
- C.** The recovery point objective (RPO) is the acceptable amount of data loss measured in time. This value represents the earliest point in time in which data must be recovered. The higher the business value of data, the more funds or other resources that can be put into place to ensure a smaller amount of data is lost in the event of a disaster.
- A** is incorrect because this is a distracter answer. Recovery time period is not an official term.
- B** is incorrect because the maximum tolerable downtime (MTD) value represents the time after which an inability to recover significant operations will mean severe and perhaps irreparable damage to the organization's reputation or bottom line.
- D** is incorrect because this is a distracter answer. Recovery point time period is not an official term.
- 40.** For evidence to be legally admissible, it must be relevant, complete, sufficient, and reliably obtained. Which characteristic refers to the evidence having a reasonable and sensible relationship to the findings?
- A.** Complete
 - B.** Reliable
 - C.** Relevant
 - D.** Sufficient
- C.** It is important that evidence be admissible, relevant, complete, sufficient, and reliable to the case at hand. These characteristics of evidence provide a foundation for a case and help ensure that the evidence is legally permissible. For evidence to be authentic, or relevant, it must have a reasonable and sensible relationship to the findings. If a judge rules that a person's past traffic tickets cannot be brought up in a murder trial, this means the judge has ruled that the traffic tickets are not relevant to the case at hand. Thus, the prosecuting lawyer cannot even mention them in court. In addition, authentic evidence must be original; that is, it cannot be a copy or a summary of the original.

- A** is incorrect because evidence that is complete presents the whole truth. All evidence, even exculpatory evidence, must be handed over. This means that a prosecutor cannot present just part of the evidence that is favorable to his side of the case.
- B** is incorrect because evidence that is reliable must be consistent with the facts. Evidence cannot be reliable if it is based on someone's opinion or copies of an original document because there is too much room for error. Reliable evidence means it is factual and not circumstantial. Examples of unreliable evidence include computer-generated documentation and an investigator's notes because they can be modified without any indication.
- D** is incorrect because evidence that is sufficient, or believable, is persuasive enough to convince a reasonable person of its validity. This means the evidence cannot be subject to personal interpretation. Sufficient evidence also means it cannot be easily doubted.

- 41.** Alex works for a chemical distributor that assigns employees tasks that separate their duties and routinely rotates job assignments. Which of the following best describes the differences between these countermeasures?
- A.** They are the same thing with different titles.
 - B.** They are administrative controls that enforce access control and protect the company's resources.
 - C.** Separation of duties ensures that one person cannot perform a high-risk task alone, and job rotation can uncover fraud because more than one person knows the tasks of a position.
 - D.** Job rotation ensures that one person cannot perform a high-risk task alone, and separation of duties can uncover fraud because more than one person knows the tasks of a position.
- C.** Separation of duties and job rotation are two security controls commonly used within companies to prevent and detect fraud. Separation of duties is put into place to ensure that one entity cannot carry out a task that could be damaging or risky to the company. It requires two or more people to come together to do their individual tasks to accomplish the overall task. Rotation of duties helps ensure that one person does not stay in one position for a long period of time because he may end up having too much control over a segment of the business. Such total control could

result in fraud, data modification, and misuse of resources.

- A** is incorrect because separation of duties and job rotation are two different concepts. They are, however, both put into place to reduce the possibilities of fraud, sabotage, misuse of information, theft, and other security compromises. Separation of duties makes sure that one individual cannot complete a critical task by herself. When a submarine captain needs to launch a nuclear torpedo, the launch usually requires three codes to be entered into the launching mechanism by three different senior crewmembers. This is an example of separation of duties. Job rotation ensures that no single person ends up having too much control over a segment of the business as a result of staying in one position for a long period of time.
 - B** is incorrect because answer C is a more detailed and definitive answer. Answer C describes both of these controls properly and their differences. Both of these controls are administrative in nature and are put into place to control access to company assets, but the CISSP exam requires the best answer out of four.
 - D** is incorrect because the description is backward. Separation of duties, not job rotation, ensures that one person cannot perform a high-risk task alone. Job rotation moves individuals in and out of a specific role to ensure that fraudulent activities are not taking place.
- 42.** Maria has been tasked with reviewing and ultimately augmenting her organization's physical security. Of the following controls and approaches, which should be her highest priority to ensure are properly implemented?
- A.** Physical facility access controls, such as mechanical and device locks, on all necessary ingress points
 - B.** Personnel access controls, such as badges, biometric systems, etc.
 - C.** External boundary controls, including perimeter intrusion detection and assessment system (PIDAS) fencing, security guards, etc.
 - D.** Layered facility access controls, with multiple internal and external ingress and egress controls
- D.** Like any other defensive security discipline, physical security can be effectively implemented only via a defense-in-depth strategy, through layered defenses. It must be based on the assumption that a determined attacker will find a way to bypass any specific control, and therefore compensating controls must be deployed to enable the

defender to detect and correct for any given failure to prevent a breach. The other possible answers each constitute core components of a layered facility protection regime, but cannot be relied upon individually.

- A** is incorrect because regardless of the “grade” or security level provided by any given physical lock, mechanical and device locks can be bypassed by an experienced and knowledgeable adversary. Most commercial warded and tumbler locks can be defeated by amateurs and hobbyists, and even cipher locks that are not well maintained can commonly be brute forced by a savvy attacker. The bottom line is that any unattended physical lock is at best a means of delaying the access of a determined adversary.
 - B** is incorrect because, as with physical, mechanical locks, all personnel access controls can ultimately be defeated. ID badges are trivial to forge, and “smart” badges—particularly near radio frequency varieties—can often be cloned quite readily by a trained attacker. Biometric systems can be spoofed, and so are no panacea.
 - C** is incorrect because, though an important first layer of defense, boundary controls must be deployed with the cognizance that we do intentionally allow individuals to enter through them. To bypass such controls, an attacker need only convince the often human-attended system that they are among the people who should be allowed in. Social engineering is the primary vector for such an attack, and is commonly no less successful in person than it is via e-mail.
- 43.** Which of the following statements is true with respect to preventing and/or detecting security disasters?
- A.** Information security continuous monitoring (ISCM), defined by NIST Special Publication 800-137 as maintaining an ongoing awareness of your current security posture, vulnerabilities, and threats, is the best way to facilitate sound risk management decisions.
 - B.** Whitelisting allowed executables or, barring that, blacklisting known bad ones is the only effective means of preventing malware from compromising systems and causing a serious security breach.
 - C.** A rigorous regime of vulnerability and patch management can effectively eliminate the risk of known malware compromising critical corporate systems.

- D.** By aggregating and correlating asset data and the security events concerning them, the deployment of a security information and event management (SIEM) system is the best way to ensure that attacks can be properly dealt with before they result in disaster.
- A.** Sound risk management is impossible without a thoroughgoing and current understanding of the effectiveness of the deployed controls vis-a-vis the current threats to extant vulnerabilities in the enterprise. Information security continuous monitoring (ISCM) seeks to provide this information on a truly ongoing basis, recognizing that new vulnerabilities are not discovered, nor do new threats to them emerge, on a quarterly basis. Rather, an agile and timely approach is needed to continuously ascertain, via heavy use of metrics and automation, how prepared we actually are, and how we can continuously improve our resilience to expected adversarial tactics, techniques, and procedures (TTPs).
- B** is incorrect because blacklisting known bad things is essentially a futile attempt to “enumerate and avoid all evil,” and although whitelisting is a vastly more effective way to avoid the execution of malware in the corporate environment, bypassing whitelisting systems is a major focus of technical advancement by modern threat actors, and techniques for doing so now constitute commodity attack strategies. Whitelisting alone simply cannot suffice without continuous monitoring for attempts to circumvent such controls.
- C** is incorrect because even the most rigorous infrastructure for vulnerability and patch management rarely has a cycle time shorter than that of exploit development once vulnerabilities become known. Most significant breaches remain the result of the exploitation of vulnerabilities for which patches were available but simply not yet deployed. Vigorous patching is a necessary step, but no more important than proactive monitoring of, and response to, indicators of compromise and post-compromise activities.
- D** is incorrect because a robust SIEM deployment is a necessary but not entirely sufficient component of a defensible infrastructure. By itself, it provides no assurance that significant threat activities are properly understood and effectively responded to. Unfortunately, many organizations simply aggregate their security events with a SIEM, in order to more efficiently ignore them.

- 44.** Miranda has been directed to investigate a possible violation of her organization’s acceptable use policy (AUP) by a coworker suspected of running cryptocurrency mining software on his desktop system. Which

of the following is NOT a very likely scenario that could arise during her investigation?

- A. During the course of her investigation, Miranda discovered that her coworker was also downloading and storing pornographic images, many of which appeared to involve minors. What began as an administrative investigation became a criminal one.
 - B. Miranda was able to find evidence that appeared to corroborate the intentional use of illicit software to mine cryptocurrency using corporate resources (mainly CPU and power). As a result, Miranda's coworker was charged with a criminal violation of the Computer Fraud and Abuse Act (CFAA).
 - C. As a result of Miranda's investigation, her coworker was terminated for violating the AUP. However, he hired an attorney and sued the company for wrongful dismissal based on knowledge that other employees were also running cryptocurrency mining software but went unpunished. Her administrative case became a civil one.
 - D. Compelling evidence was found of a significant AUP violation, resulting in termination. However, during the subsequent wrongful dismissal suit (as described in option C), it was discovered that Miranda had not anticipated a court case, and so had not properly obtained or preserved the evidence. Consequently, the judge found summarily for the plaintiff, who got his job back along with compensatory damages.
- B. Though it could be argued that the employee in question had exceeded his intended, authorized access to a company computer and used it to steal corporate resources (computing and electrical power), the severity of such actions is unlikely to rise to the level of a criminal indictment under the CFAA, particularly as a single instance.
- A is incorrect because, unfortunately, it is a more common scenario than might easily be imagined. A thorough digital forensic examination can easily turn up evidence of criminal activities not previously detected or suspected. This is the main reason that all investigations should be conducted with the necessary professional skill and diligence to conclude them in court if such a situation arises.
- C is incorrect because this scenario is also quite commonplace and is another excellent example as to why all investigations and administrative proceedings should be conducted as though they may

wind up in front of a judge or jury. If, through the discovery process, the plaintiff can demonstrate that others were indeed involved in the same activity, but that he alone was singled out, he is likely to prevail in court. A judge could easily find that because the AUP was not consistently enforced, no AUP exists in practicality.

- D** is incorrect because the scenario is at least somewhat likely. Though the bar in a civil case is merely “a preponderance of evidence,” that evidence must still be legally and reliably obtained, and its integrity properly maintained. Miranda’s evidence may not have been ruled entirely inadmissible in court, but a judge may determine that it should not be afforded sufficient weight for the defense to prevail.

Software Development Security

This domain includes questions from the following topics:

- Common software development issues
 - Software development life cycles
 - Secure software development approaches
 - Development/operations integration (DevOps)
 - Change control and configuration management
 - Security of code repositories
 - Programming language types
 - Database concepts and security issues
 - Malware types and attacks
-

Security is often—mistakenly—an afterthought when it comes to software development. Patches and hot fixes are created after vulnerabilities put assets at risk and are Band-Aid solutions to deeper problems. Adding security after an application or computer system is developed is not only less effective at protecting the product against threats but also more costly. Incorporating security throughout the software development life cycle and integrating security measures within the code itself ensures a functional and protected product. As a CISSP, you must understand application security controls and the vulnerabilities that come in their absence.

Q QUESTIONS

1. A new software development company has been launched to create mobile device apps for different customers. The company has talented software programmers employed, but has not been able to implement standardized development processes that can be improved upon over time. Which of the following would be the best approach for this company to take in order to improve its software development processes?
 - A. Capability Maturity Model Integration
 - B. System development life cycle
 - C. ISO/IEC 27002

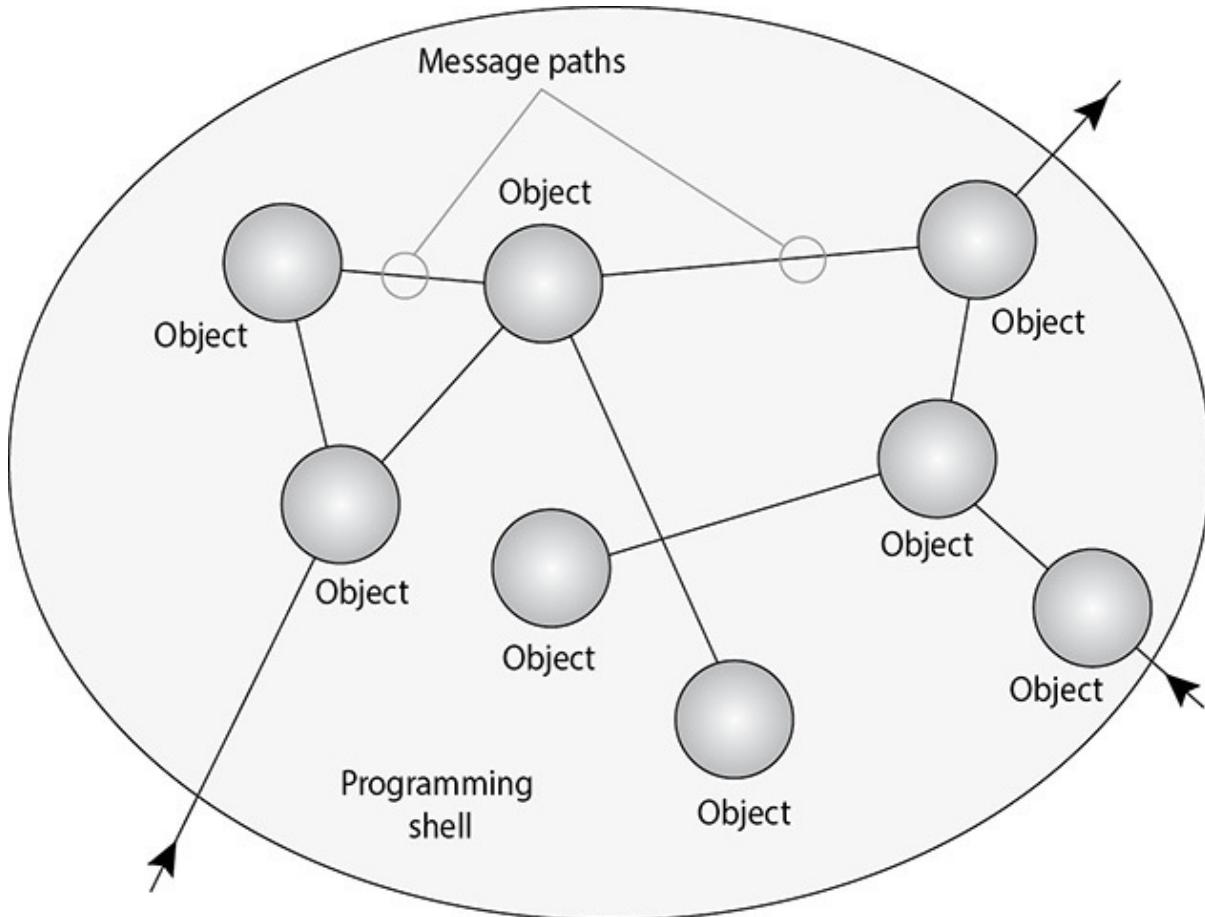
- D. Certification and accreditation processes**
- 2.** Database software should meet the requirements of what is known as the ACID test. Why should database software carry out atomic transactions, which is one requirement of the ACID test, when OLTP is used?
- A.** So that the rules for database integrity can be established
 - B.** So that the database performs transactions as a single unit without interruption
 - C.** To ensure that rollbacks cannot take place
 - D.** To prevent concurrent processes from interacting with each other
- 3.** Lisa has learned that most databases implement concurrency controls. What is concurrency, and why must it be controlled?
- A.** Processes running at different levels, which can negatively affect the integrity of the database if not properly controlled
 - B.** The ability to deduce new information from reviewing accessible data, which can allow an inference attack to take place
 - C.** Processes running simultaneously, which can negatively affect the integrity of the database if not properly controlled
 - D.** Storing data in more than one place within a database, which can negatively affect the integrity of the database if not properly controlled
- 4.** Robert has been asked to increase the overall efficiency of the sales database by implementing a procedure that structures data to minimize duplication and inconsistencies. What procedure is this?
- A.** Polymorphism
 - B.** Normalization
 - C.** Implementation of database views
 - D.** Constructing schema
- 5.** Which of the following correctly best describes an object-oriented database?
- A.** When an application queries for data, it receives both the data and the procedure.
 - B.** It is structured similarly to a mesh network for redundancy and fast data retrieval.

- C. Subjects must have knowledge of the well-defined access path in order to access data.
 - D. The relationships between data entities provide the framework for organizing data.
6. Fred has been told he needs to test a component of the new content management application under development to validate its data structure, logic, and boundary conditions. What type of testing should he carry out?
- A. Acceptance testing
 - B. Regression testing
 - C. Integration testing
 - D. Unit testing
7. Which of the following is the best description of a component-based system development method?
- A. Components periodically revisit previous stages to update and verify design requirements
 - B. Minimizes the use of arbitrary transfer control statements between components
 - C. Uses independent and standardized modules that are assembled into serviceable programs
 - D. Implemented in module-based scenarios requiring rapid adaptations to changing client requirements
8. There are many types of viruses that hackers can use to damage systems. Which of the following is not a correct description of a polymorphic virus?
- A. Intercepts antimalware's call to the operating system for file and system information
 - B. Varies the sequence of its instructions using noise, a mutation engine, or random-number generator
 - C. Can use different encryption schemes requiring different decryption routines
 - D. Produces multiple varied copies of itself
9. Which of the following best describes the role of the Java Virtual Machine in the execution of Java applets?

- A. Converts the source code into bytecode and blocks the sandbox
 - B. Converts the bytecode into machine-level code
 - C. Operates only on specific processors within specific operating systems
 - D. Develops the applets, which run in a user's browser
- 10.** What type of database software integrity service guarantees that tuples are uniquely identified by primary key values?
- A. Concurrent integrity
 - B. Referential integrity
 - C. Entity integrity
 - D. Semantic integrity
- 11.** In computer programming, cohesion and coupling are used to describe modules of code. Which of the following is a favorable combination of cohesion and coupling?
- A. Low cohesion, low coupling
 - B. High cohesion, high coupling
 - C. Low cohesion, high coupling
 - D. High cohesion, low coupling
- 12.** Which of the following statements does not correctly describe SOAP and Remote Procedure Calls?
- A. SOAP was designed to overcome the compatibility and security issues associated with Remote Procedure Calls.
 - B. Both SOAP and Remote Procedure Calls were created to enable application-layer communication.
 - C. SOAP enables the use of Remote Procedure Calls for information exchange between applications over the Internet.
 - D. HTTP was not designed to work with Remote Procedure Calls, but SOAP was designed to work with HTTP.
- 13.** Which of the following is a correct description of the pros and cons associated with third-generation programming languages?
- A. The use of heuristics reduced programming effort, but the amount of manual coding for a specific task is usually more than the preceding generation.

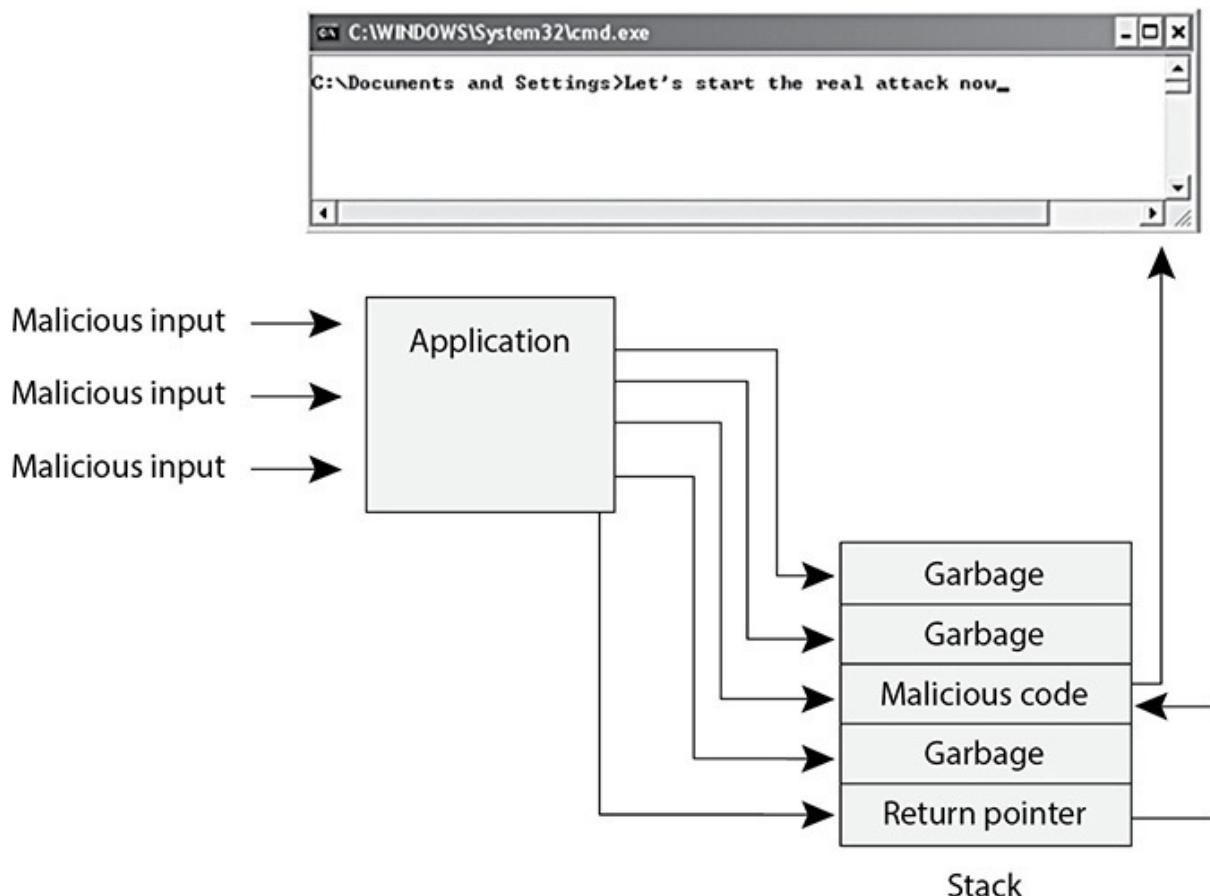
- B. The use of syntax similar to human language reduced development time, but the language is resource intensive.
 - C. The use of binary was extremely time consuming but resulted in fewer errors.
 - D. The use of symbols reduced programming time, but the language required knowledge of machine architecture.
- 14.** It can be very challenging for programmers to know what types of security should be built into the software that they create. The amount of vulnerabilities, threats, and risks involved with software development can seem endless. Which of the following describes the best first step for developers to take to identify the security controls that should be coded into a software project?
- A. Penetration testing
 - B. Regression testing
 - C. Threat modeling
 - D. Attack surface analysis
- 15.** Mary is creating malicious code that will steal a user's cookies by modifying the original client-side Java script. What type of cross-site scripting vulnerability is she exploiting?
- A. Second order
 - B. DOM-based
 - C. Persistent
 - D. Nonpersistent
- 16.** Of the following steps that describe the development of a botnet, which best describes the step that comes first?
- A. Infected server sends attack commands to the botnet.
 - B. Spammer pays a hacker for use of a botnet.
 - C. Controller server instructs infected systems to send spam to mail servers.
 - D. Malicious code is sent out that has bot software as its payload.
- 17.** Which of the following antimalware detection methods is the most recent to the industry and monitors suspicious code as it executes within the operating system?

- A. Behavior blocking
 - B. Fingerprint detection
 - C. Signature-based detection
 - D. Heuristic detection
18. Which of the following describes object-oriented programming deferred commitment?
- A. Autonomous objects, which cooperate through exchanges of messages
 - B. The internal components of an object can be refined without changing other parts of the system
 - C. Object-oriented analysis, design, and modeling maps to business needs and solutions
 - D. Other programs using same objects
19. What object-oriented programming term or concept is illustrated in the graphic that follows?

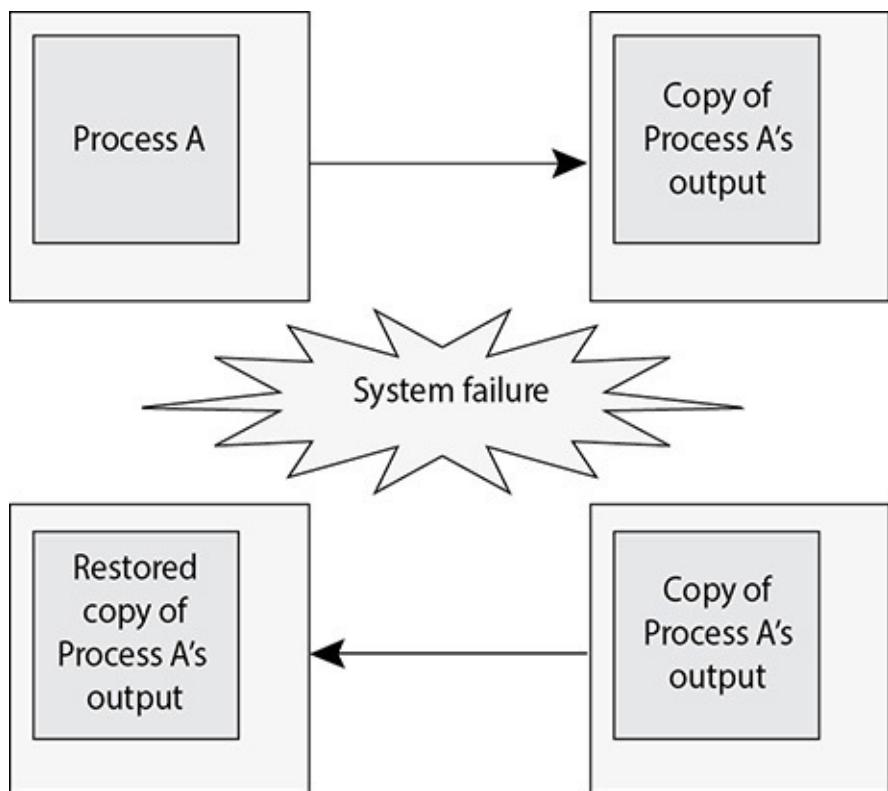


- A. Methods

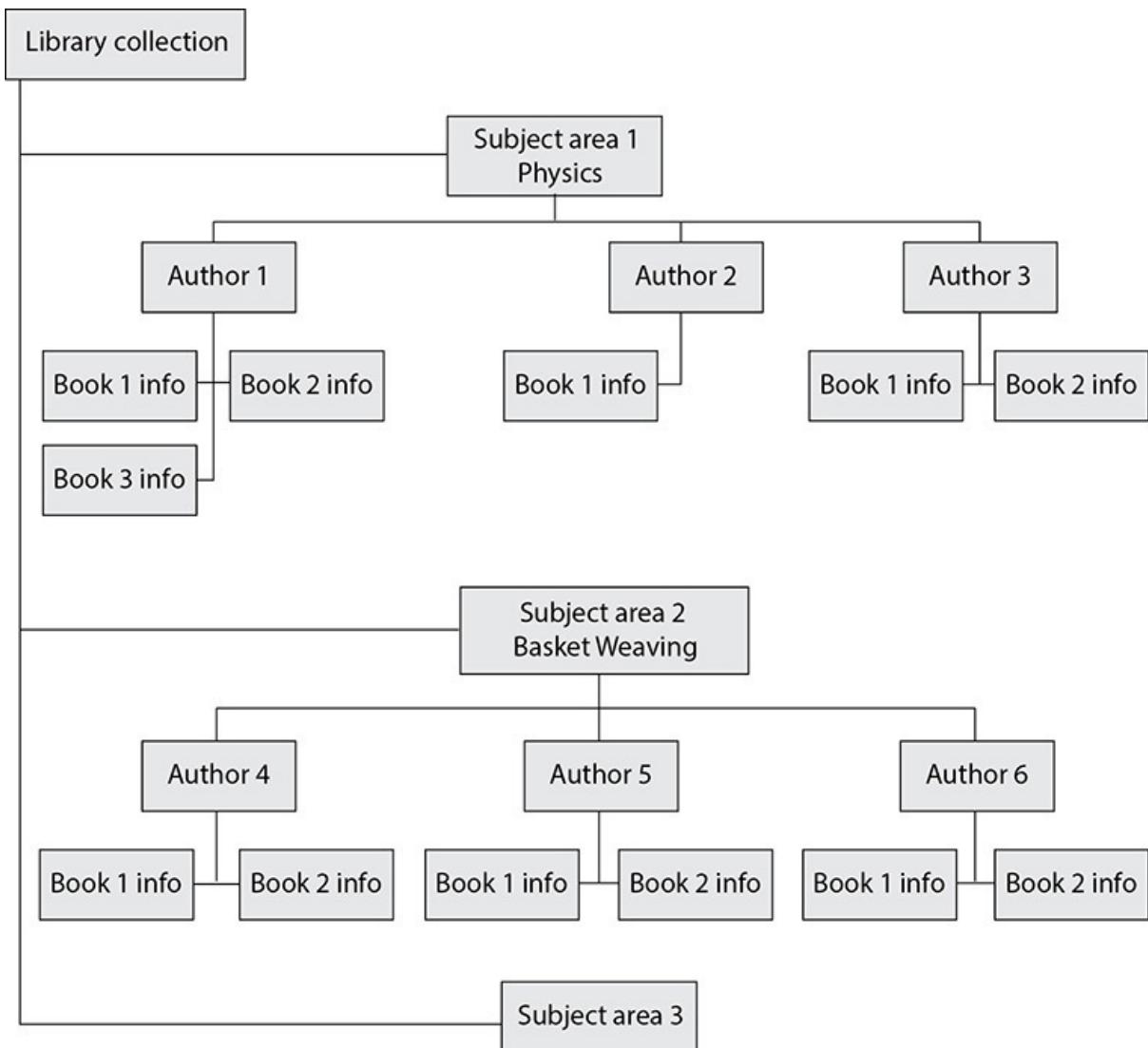
- B. Messages
C. Abstraction
D. Data hiding
20. Protection methods can be integrated into software programs. What type of protection method is illustrated in the graphic that follows?
- | Level | Ship | Cargo | Origin | Destination |
|--------------|----------|---------|----------|-------------|
| Top Secret | Oklahoma | Weapons | Delaware | Ukraine |
| Unclassified | Oklahoma | Food | Delaware | Africa |
- Instantiate and repopulate
-
- A. Polymorphism
B. Polyinstantiation
C. Cohesiveness
D. Object classes
21. There are several types of attacks that programmers need to be aware of. What attack does the graphic that follows illustrate?



- A. Traffic analysis
 - B. Race condition
 - C. Covert storage
 - D. Buffer overflow
- 22.** Databases and applications commonly carry out the function that is illustrated in the graphic that follows. Which of the following best describes the concept that this graphic is showing?



- A. Checkpoint
 - B. Commit
 - C. Two-phase commit
 - D. Data dictionary
23. There are several different types of databases. Which type does the graphic that follows illustrate?



- A.** Relational
- B.** Hierarchical
- C.** Network
- D.** Object-oriented

The following scenario applies to questions 24, 25, and 26.

Trent is the new manager of his company's internal software development department. He has been told by his management that the group needs to be compliant with the international standard that provides guidance to organizations in integrating security into the processes used for managing their applications. His new boss told him that he should join and get familiar with the Open Web Application Security Project (OWASP), and Trent just received an e-mail stating that one of the company's currently deployed applications has a zero-day vulnerability.

- 24.** Which of the following is most likely the standard Trent's company

wants to comply with?

- A. ISO/IEC 27005
- B. ISO/IEC 27001
- C. ISO/IEC 27034
- D. BS 7799

25. Which of the following best describes the consortium Trent's boss wants him to join?

- A. Nonprofit organization that produces open-source software and follows widely agreed-upon best-practice security standards for the World Wide Web
- B. U.S. DHS group that provides best practices, tools, guidelines, rules, principles, and other resources for software developers, architects, and security practitioners to use
- C. Group of experts who create proprietary software tools used to help improve the security of software worldwide
- D. Group of experts and organizations who certify products based on an agreed-upon security criteria

26. Which of the following best describes the type of vulnerability mentioned in this scenario?

- A. Dynamic vulnerability that is polymorphic
- B. Static vulnerability that is exploited by server-side injection parameters
- C. Vulnerability that does not currently have an associated solution
- D. Database vulnerability that directly affects concurrency

27. _____ provides a machine-readable description of the specific operations provided by a specific web service.

_____ provides a method for web services to be registered by service providers and located by service consumers.

- A. Web Services Description Language; Universal Description, Discovery and Integration
- B. Universal Description, Discovery and Integration; Web Services Description Language
- C. Web Services Description Language; Simple Object Access Protocol

- D. Simple Object Access Protocol; Universal Description, Discovery and Integration
- 28.** Sally has found out that software programmers in her company are making changes to software components and uploading them to the main software repository without following version control or documenting their changes. This is causing a lot of confusion and has caused several teams to use the older versions. Which of the following would be the best solution for this situation?

 - A. Software change control management
 - B. Software escrow
 - C. Software configuration management
 - D. Software configuration management escrow
- 29.** The approach of employing an integrated product team (IPT) for software development is designed to achieve which of the following objectives?

 - A. Developing and testing software with fewer security flaws
 - B. Developing and testing software with fewer defective features
 - C. Developing and testing software that will be most profitable
 - D. Developing and testing software best suited to the deployment environment
- 30.** Which are the best reasons why a code versioning system (CVS) is an important part of a development infrastructure?

 - i. It can ensure that code modifications are made according to corporate policies.
 - ii. It will document who made which changes to ensure accountability.
 - iii. It will reduce the cost of the development infrastructure.
 - iv. It can provide control over unauthorized access to proprietary code.
 - A. i, ii, iv
 - B. iii
 - C. iii, iv
 - D. All of the above
- 31.** What is generally the safest, most secure way to acquire software?

 - A. From a reputable vendor of proprietary software, once tested in the

- deployment environment
- B. Downloading very popular open-source software that has been inspected for bugs by a large and active community
- C. Downloading either proprietary or open-source software, but fuzzing it in a lab environment prior to deployment
- D. Downloading open-source software and deploying it only after the code base has been verified by cryptographic checksum

The following scenario applies to questions 32 and 33.

John is a network administrator and has been told by one of his network staff members that two servers on the network have recently had suspicious traffic traveling to them and then from them in a sporadic manner. The traffic has been mainly ICMP, but the patterns were unusual compared to traffic on other servers over the last 30 days. John lists the directories and subdirectories on the systems and finds nothing unusual. He inspects the running processes and again finds nothing suspicious. He sees that the systems' NICs are not in promiscuous mode, so he is assured that sniffers have not been planted.

- 32.** Which of the following describes the most likely situation as described in this scenario?
 - A. Servers are not infected, but the traffic illustrates attack attempts.
 - B. Servers have been infected with rootkits.
 - C. Servers are vulnerable and need to be patched.
 - D. Servers have been infected by spyware.
- 33.** Which of the following best explains why John does not see anything suspicious on the reported systems?
 - A. The systems have not yet been infected.
 - B. He is not running the correct tools. He needs to carry out a penetration test on the two systems.
 - C. Trojaned files have been loaded and executed.
 - D. A back door has been installed and the attacker enters the system sporadically.
- 34.** Cross-site scripting (XSS) is an application security vulnerability usually found in web applications. What type of XSS vulnerability occurs when a victim is tricked into opening a URL programmed with a rogue script to steal sensitive information?

- A. Persistent XSS vulnerability
 - B. Nonpersistent XSS vulnerability
 - C. Second-order vulnerability
 - D. DOM-based vulnerability
- 35. Widgets, Inc.'s software development processes are documented, and the organization is capable of producing its own standard of software processes. Which of the following Capability Maturity Model Integration levels best describes Widgets, Inc.?
 - A. Initial
 - B. Repeatable
 - C. Defined
 - D. Managed
- 36. Which of the following best describes "change management"?
 - A. It is a systematic approach to deliberately regulating the changing nature of projects.
 - B. It is the process of controlling the specific changes that take place during the life cycle of a system.
 - C. It is an enterprise program for instituting programmatic changes in source code repositories.
 - D. It is the process of controlling how changes to firewalls and other network devices are made.
- 37. Which of the following best describes "change control"?
 - A. It is a systematic approach to deliberately regulating the changing nature of projects.
 - B. It is the process of controlling the specific changes that take place during the life cycle of a system.
 - C. It is an enterprise program for instituting programmatic changes in source code repositories.
 - D. It is the process of controlling how changes to firewalls and other network devices are made.
- 38. What are the three major elements crucial to the security of software development environments?
 - A. The software languages, the integrated development environments

- (IDEs), and the compilers
- B. The development platforms, the code repositories, and the software configurations
 - C. The design teams, the development teams, and the testing teams
 - D. The code repositories, the versioning systems, and the deployment processes
39. Which of the following are key elements of secure coding practices?
- A. Using object-oriented languages instead of procedural ones, and heeding compiler warnings
 - B. Ensuring that quality assurance is thorough, and performed by multiple teams
 - C. Parallel programming, agile methodologies, and iterative testing
 - D. Validating inputs, adhering to the least privilege principle, and keeping code as simple as possible

QUICK ANSWER KEY

- 1. A
- 2. B
- 3. C
- 4. B
- 5. A
- 6. D
- 7. C
- 8. A
- 9. B
- 10. C
- 11. D
- 12. C
- 13. B
- 14. C
- 15. B

- 16.** D
17. A
18. B
19. B
20. B
21. D
22. A
23. B
24. C
25. A
26. C
27. A
28. C
29. D
30. A
31. C
32. B
33. C
34. B
35. C
36. A
37. B
38. B
39. D

ANSWERS A

1. A new software development company has been launched to create mobile device apps for different customers. The company has talented software programmers employed, but has not been able to implement standardized development processes that can be improved upon over time. Which of the following would be the best approach for this company to take in order to improve its software development

processes?

- A.** Capability Maturity Model Integration
 - B.** System development life cycle
 - C.** ISO/IEC 27002
 - D.** Certification and accreditation processes
- A.** Capability Maturity Model Integration (CMMI) for development is a comprehensive integrated set of guidelines for developing products and software. It addresses the different phases of a software development life cycle, including concept definition, requirements analysis, design, development, integration, installation, operations, and maintenance and what should happen in each phase. The model describes procedures, principles, and practices that underlie software development process maturity. This model was developed to help software vendors improve their development processes by providing an evolutionary path from an ad hoc “fly by the seat of your pants” approach to a more disciplined and repeatable method that improves software quality, reduces the life cycle of development, provides better project management capabilities, allows for milestones to be created and met in a timely manner, and takes a more proactive approach than the less effective reactive approach.
- B** is incorrect because the system development life cycle (SDLC) addresses how a system should be developed and maintained throughout its life cycle and does not entail process improvement. Each system has its own life cycle, which is made up of the following phases: initiation, acquisition/development, implementation, operation/maintenance, and disposal. A system development life cycle is different from a software development life cycle, even though they are commonly confused. The industry as a whole is starting to differentiate between system and software life-cycle processes because at a certain point of granularity, the manner in which a computer system is dealt with is different from how a piece of software is dealt with. A computer system should be installed properly, tested, patched, scanned continuously for vulnerabilities, monitored, and replaced when needed. A piece of software should be designed, coded, tested, documented, released, and maintained. In either case, the question is asking for a type of process improvement model for software development, which is the focus of Capability Maturity Model Integration and not a system

development life cycle.

- C** is incorrect because ISO/IEC 27002 is an international standard created by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) that outlines how to create and maintain an organizational information security management system (ISMS). While ISO/IEC 27002 has a section that deals with information systems acquisition, development, and maintenance, it does not provide a process improvement model for software development. It provides guidance on how to build security into applications, but it does not provide guidance on how to create standardized development procedures for a team of programmers. The focus of ISO/IEC 27002 is how to build a security program within an organization.
 - D** is incorrect because a certification and accreditation (C&A) process deals with testing and evaluating systems against a predefined criteria. This does not have anything to do with software development process improvement. The certification process is the technical testing of a system. Established verification procedures are followed to ensure the effectiveness of the system and its security controls. Accreditation is the formal authorization given by management to allow a system to operate in a specific environment. The accreditation decision is based upon the results of the certification process. C&A procedures are commonly carried out within government and military environments to ensure that systems and software are providing the necessary functionality and security to support critical missions.
- 2.** Database software should meet the requirements of what is known as the ACID test. Why should database software carry out atomic transactions, which is one requirement of the ACID test, when OLTP is used?
- A.** So that the rules for database integrity can be established
 - B.** So that the database performs transactions as a single unit without interruption
 - C.** To ensure that rollbacks cannot take place
 - D.** To prevent concurrent processes from interacting with each other
- B.** Online transaction processing (OLTP) is used when databases are clustered to provide high fault tolerance and performance. It provides mechanisms to watch for and deal with problems when

they occur. For example, if a process stops functioning, the monitor mechanisms within OLTP can detect this and attempt to restart the process. If the process cannot be restarted, then the transaction taking place will be rolled back to ensure no data is corrupted or that only part of a transaction happens. OLTP records transactions as they occur (in real time), which usually updates more than one database in a distributed environment. This type of complexity can introduce many integrity threats, so the database software should implement the characteristics of what's known as the ACID test:

- **Atomicity** Divides transactions into units of work and ensures that all modifications take effect or none takes effect. Either the changes are committed or the database is rolled back.
- **Consistency** A transaction must follow the integrity policy developed for that particular database and ensure all data is consistent in the different databases.
- **Isolation** Transactions execute in isolation until completed, without interacting with other transactions. The results of the modification are not available until the transaction is completed.
- **Durability** Once the transaction is verified as accurate on all systems, it is committed, and the databases cannot be rolled back.

The term “atomic” means that the units of a transaction will occur together or not at all, thereby ensuring that if one operation fails, the others will not be carried out and corrupt the data in the database.

- ☒ **A** is incorrect because OLTP and ACID enforce, but do not establish, the integrity rules that are outlined in the database security policy. Representing the letter C in ACID, consistency relates to the enforcement and enforceability of integrity rules. Database software that demonstrates consistency conducts transactions that follow a specific integrity policy and ensure all data is the same in the different databases.
- ☒ **C** is incorrect because atomicity divides transactions into units of work and ensures that all modifications take effect or none takes effect. Either the changes are committed or the database is rolled back. This means if something does not happen correctly, the database is reverted (rolled back) to its original state. After the transaction happens properly, a rollback cannot take place, which is the durability component of the ACID test. This question is specifically asking about the atomic transaction approach, not durability.

D is incorrect because atomic transactions do not address the isolation of processes that are carrying out database transactions; this is the “isolation” component of the ACID test. It is important that a process that is carrying out a transaction cannot be interrupted or modified by another process. This is to ensure the integrity, accuracy, and confidentiality of the data that is being processed during the transaction.

3. Lisa has learned that most databases implement concurrency controls. What is concurrency, and why must it be controlled?

- A. Processes running at different levels, which can negatively affect the integrity of the database if not properly controlled
- B. The ability to deduce new information from reviewing accessible data, which can allow an inference attack to take place
- C. Processes running simultaneously, which can negatively affect the integrity of the database if not properly controlled
- D. Storing data in more than one place within a database, which can negatively affect the integrity of the database if not properly controlled

C. Databases are commonly used by many different applications simultaneously and many users interacting with them at one time. Concurrency means that different processes (applications and users) are accessing the database at the same time. If this is not controlled properly, the processes can overwrite each other’s data or cause deadlock situations. The negative result of concurrency problems is the reduction of the integrity of the data held within the database. Database integrity is provided by concurrency protection mechanisms. One concurrency control is locking, which prevents users from accessing and modifying data being used by someone else.

- A** is incorrect because concurrency refers to processes running simultaneously, not at different levels. Concurrency issues come up when the database can be accessed at the same time by different users and/or applications. If controls are not in place, two users can access and modify the same data at the same time, which can be detrimental to a dynamic environment.
- B** is incorrect because the ability to deduce new information from reviewing accessible data occurs when a subject at a lower security level indirectly guesses or infers data at a higher level. This can lead

to an inference attack. It is not related to concurrency. Concurrency has to do with integrity, while inference is related to confidentiality.

- D** is incorrect because storing data in more than one place is not a problem with concurrency. Concurrency becomes a problem when two subjects or applications are trying to modify the same data at the same time.
- 4.** Robert has been asked to increase the overall efficiency of the sales database by implementing a procedure that structures data to minimize duplication and inconsistencies. What procedure is this?
 - A.** Polymorphism
 - B.** Normalization
 - C.** Implementation of database views
 - D.** Constructing schema
- B.** Normalization is a process that eliminates redundancy, organizes data efficiently, reduces the potential for anomalies during data operations, and improves data consistency within databases. It is a systematic way of ensuring that a database structure is designed properly to be free of certain undesirable characteristics—insertion, update, and deletion anomalies—that could lead to a loss of data integrity.
- A** is incorrect because polymorphism is when different objects are given the same input and react differently. As a simplistic example of polymorphism, suppose three different objects receive the input “Bob.” Object A would process this input and produce the output “43-year-old white male.” Object B would receive the input “Bob” and produce the output “Husband of Sally.” Object C would produce the output “Member of User group.” Each object received the same input but responded with a different output.
- C** is incorrect because database views are logical access controls and are implemented to permit one group, or a specific user, to see certain information while restricting another group from viewing it altogether. For example, database views can be implemented to allow middle management to see their departments’ profits and expenses without viewing the whole company’s profits. Database views do not minimize duplicate data; rather, they manipulate how data is viewed by specific users/groups.
- D** is incorrect because schema of a database system is its structure

described in a formal language. In a relational database, the schema defines the tables, the fields, relationships, views, indexes, procedures, queues, database links, directories, and so on. The schema describes the database and its structure, but not the data that will live within that database itself. This is similar to a blueprint of a house. The blueprint can state that there will be four rooms, six doors, 12 windows, and so on, without describing the people who will live in the house.

5. Which of the following correctly best describes an object-oriented database?
 - A. When an application queries for data, it receives both the data and the procedure.
 - B. It is structured similarly to a mesh network for redundancy and fast data retrieval.
 - C. Subjects must have knowledge of the well-defined access path in order to access data.
 - D. The relationships between data entities provide the framework for organizing data.
- A. In an object-oriented database, objects are instantiated when needed, and the data and procedure (called method) go with the object when it is requested. This differs from a relational database, in which the application uses its own procedures to obtain and process data when retrieved from the database.
- B is incorrect because a mesh network is a physical topology and has nothing to do with databases. A mesh topology is a network of interconnected routers and switches that provides multiple paths to all the nodes on the network. In a full mesh topology, every node is directly connected to every other node, which provides a great degree of redundancy. In a partial mesh topology, every node is not directly connected. The Internet is an example of a partial mesh topology.
- C is incorrect because subjects accessing a hierarchical database—not an object-oriented database—must have knowledge of the access path in order to access data. In the hierarchical database model, records and fields are related in a logical tree structure. Parents can have one child, many children, or no children. The tree structure contains branches, and each branch has a number of data fields. To access data, the application must know which branch to

start with and which route to take through each layer until the data is reached.

- D** is incorrect because the relationships between data entities provide the framework for organizing data in a relational database. A relational database is composed of two-dimensional tables, and each table contains unique rows, columns, and cells. Each cell contains one data value that represents a specific attribute within a given row. These data entities are linked by relationships, which provide the framework for organizing the data.

6. Fred has been told he needs to test a component of the new content management application under development to validate its data structure, logic, and boundary conditions. What type of testing should he carry out?

- A.** Acceptance testing
- B.** Regression testing
- C.** Integration testing
- D.** Unit testing

- D.** Unit testing involves testing an individual component in a controlled environment to validate data structure, logic, and boundary conditions. After a programmer develops a component, it is tested with several different input values and in many different situations. Unit testing can start early in development and usually continues throughout the development phase. One of the benefits of unit testing is finding problems early in the development cycle, when it is easier and less expensive to make changes to individual units.
- A** is incorrect because acceptance testing is carried out to ensure that the code meets customer requirements. This testing is for part or all of the application, but not commonly one individual component.
- B** is incorrect because regression testing refers to the retesting of a system after a change has taken place to ensure its functionality, performance, and protection. Essentially, regression testing is done to identify bugs that have caused functionality to stop working as intended as a result of program changes. It is not unusual for developers to fix one problem, only to inadvertently create a new problem, or for the new fix to break a fix to an old problem. Regression testing may include checking previously fixed bugs to make sure they have not re-emerged and rerunning previous tests.

- C** is incorrect because integration testing involves verifying that components work together as outlined in design specifications. After unit testing, the individual components or units are combined and tested together to verify that they meet functional, performance, and reliability requirements.
- 7.** Which of the following is the best description of a component-based system development method?
 - A.** Components periodically revisit previous stages to update and verify design requirements
 - B.** Minimizes the use of arbitrary transfer control statements between components
 - C.** Uses independent and standardized modules that are assembled into serviceable programs
 - D.** Implemented in module-based scenarios requiring rapid adaptations to changing client requirements
- C.** Component-based development involves the use of independent and standardized modules. Each standard module consists of a functional algorithm or instruction set and is provided with interfaces to communicate with each other. Component-based development adds reusability and pluggable functionality into programs, and is widely used in modern programming to augment program coherence and substantially reduce software maintenance costs. A common example of these modules is “objects” that are frequently used in object-oriented programming.
- A** is incorrect because the spiral method of system development periodically revisits previous stages to update and verify design requirements. The spiral method builds upon the waterfall method. It uses discrete phases of development with an emphasis on risk analysis, prototypes, and simulations. The spiral method does not specify the development and testing of components.
- B** is incorrect because structured programming development involves the use of logical blocks to achieve system design using procedural programming. A structured program layout minimizes the use of arbitrary transfer control statements like GOTO and emphasizes on single points of entry and exit. This hierarchical approach makes it easier for the program to be understood and modified later on.
- D** is incorrect because extreme programming is a methodology that

is generally implemented in scenarios requiring rapid adaptations to changing client requirements. Extreme programming emphasizes client feedback to evaluate project outcomes and to analyze project domains that may require further attention. The coding principle of extreme programming throws out the traditional long-term planning carried out for code reuse and instead focuses on creating simple code optimized for the contemporary assignment.

8. There are many types of viruses that hackers can use to damage systems. Which of the following is not a correct description of a polymorphic virus?
 - A. Intercepts antimalware's call to the operating system for file and system information
 - B. Varies the sequence of its instructions using noise, a mutation engine, or random-number generator
 - C. Can use different encryption schemes requiring different decryption routines
 - D. Produces multiple varied copies of itself
- A. A tunneling virus—not a polymorphic virus—attempts to install itself under an antimalware program. When the antimalware conducts its health check on critical files, file sizes, modification dates, etc., it makes a request to the operating system to gather this information. If the virus can put itself between the antimalware and the operating system, then when the antimalware sends out a system call for this type of information, the tunneling virus can intercept the call and respond with information that indicates the system is free of virus infections. The polymorphic virus also attempts to fool antimalware scanners, but it does so by producing varied but operational copies of itself. Even if antimalware software finds and disables one or two copies, other copies may still remain active within the system.
- B is incorrect because a polymorphic virus can vary the sequence of its instructions by including noise, or bogus instructions, with other useful instructions. It can also use a mutation engine and a random-number generator to change the sequence of its instructions in the hopes of not being detected. The original functionality stays the same, but the code changes, making it close to impossible to identify all versions of the virus using a fixed signature.
- C is incorrect because a polymorphic virus can use different

encryption schemes requiring different decryption routines. This requires an antimalware scan for several scan strings, one for each possible decryption method, in order to identify all copies of this type of virus. Polymorphic virus writers most commonly hide a virus's payload with encryption and add a decryption method to the code. Once it is encrypted, the code is meaningless. However, a virus that is encrypted is not necessarily a polymorphic virus. To be polymorphic, the virus's encryption and decryption algorithms must mutate with each new version of itself.

- D** is incorrect because a polymorphic virus produces multiple varied copies of itself in an effort to avoid detection by antimalware software. A polymorphic virus has the capability to change its own code, enabling the virus to have hundreds or thousands of variants. These activities can cause the virus scanner to not properly recognize the virus and to leave it to do its damage.
- 9.** Which of the following best describes the role of the Java Virtual Machine in the execution of Java applets?
 - A.** Converts the source code into bytecode and blocks the sandbox
 - B.** Converts the bytecode into machine-level code
 - C.** Operates only on specific processors within specific operating systems
 - D.** Develops the applets, which run in a user's browser
- B.** Java is an object-oriented, platform-independent programming language. It is employed as a full-fledged programming language and is used to write complete programs and short programs, called applets, which run in a user's browser. Java is platform independent because it creates intermediate code, bytecode, which is not processor specific. The Java Virtual Machine (JVM) then converts the bytecode into machine-level code that the processor on the particular system can understand.
- A** is incorrect because the Java Virtual Machine converts the bytecode into machine-level code. It does not convert the source code into bytecode—a Java compiler does that. The JVM also creates a virtual machine within an environment called a sandbox. This virtual machine is an enclosed environment in which the applet carries out its activities. Applets are commonly sent over HTTP within a requested web page, which means the applet executes as soon as it arrives. It can carry out malicious activity on purpose or

accidentally if the developer of the applet did not do his part correctly. So the sandbox strictly limits the applet's access to any system resources. The JVM mediates access to system resources to ensure the applet code behaves and stays within its own sandbox.

- C** is incorrect because Java is an object-oriented, platform-independent programming language. Other languages are compiled to object code for a specific operating system and processor. This is why a particular application may run on Windows but not on macOS. An Intel processor does not necessarily understand machine code compiled for an Alpha processor, and vice versa. Java is platform independent because it creates intermediate code—bytecode—which is not processor specific.
- D** is incorrect because the Java Virtual Machine does not write applets. Java is employed as a full-fledged programming language and is used to write complete programs and short programs, called applets, which run in a user's browser. A programmer creates a Java applet and runs it through a compiler. The Java compiler converts the source code into bytecode. The user then downloads the Java applet. The bytecode is converted into machine-level code by the JVM. Finally, the applet runs when called upon.

10. What type of database software integrity service guarantees that tuples are uniquely identified by primary key values?

- A.** Concurrent integrity
- B.** Referential integrity
- C.** Entity integrity
- D.** Semantic integrity
- C.** Entity integrity guarantees that the tuples are uniquely identified by primary key values. A tuple is a row in a two-dimensional database. A primary key is a value in the corresponding column that makes each row unique. For the sake of entity integrity, every tuple must contain one primary key. If a tuple does not have a primary key, it cannot be referenced by the database.
- A** is incorrect because concurrent integrity is not a database software formal term. This is a distracter answer. There are three main types of integrity services: semantic, referential, and entity. Concurrency refers to a piece of software being accessed by multiple users and/or applications at the same time. If controls are not in place, two users can access and modify the same data simultaneously.

- B** is incorrect because referential integrity refers to all foreign keys referencing existing primary keys. There should be a mechanism in place that ensures that no foreign key contains a reference to a primary key of a nonexistent record or a null value. This type of integrity control ensures that the relationships between the different tables are working and can properly communicate to each other.
 - D** is incorrect because a semantic integrity mechanism ensures that structural and semantic rules of a database are enforced. These rules pertain to data types, logical values, uniqueness constraints, and operations that could adversely affect the structure of the database.
11. In computer programming, cohesion and coupling are used to describe modules of code. Which of the following is a favorable combination of cohesion and coupling?
- A. Low cohesion, low coupling
 - B. High cohesion, high coupling
 - C. Low cohesion, high coupling
 - D. High cohesion, low coupling
- D.** When a module is described as having high cohesion and low coupling, that is a good thing. Cohesion reflects how many different types of tasks a module can carry out. High cohesion means that the module carries out one basic task (such as subtraction of values) or several tasks that are very similar (such as subtraction, addition, multiplication). The higher the cohesion, the easier it is to update or modify and not affect the other modules that interact with it. This also means the module is easier to reuse and maintain because it is more straightforward when compared to a module with low cohesion. Coupling is a measurement that indicates how much interaction one module requires to carry out its tasks. If a module has low or loose coupling, this means the module does not need to communicate with many other modules to carry out its job. These modules are easier to understand and easier to reuse than those that depend upon many other modules to carry out their tasks. It is also easier to make changes to these modules without affecting many modules around them.
 - A** is incorrect because a module with low cohesion is not desirable. A module with low cohesion carries out multiple different tasks and increases the complexity of the module, which makes it harder to maintain and reuse. The higher a module's cohesion, the fewer tasks

it carries out and the easier it is to update or modify that module without affecting others that interact with it.

- B** is incorrect because a module with high coupling is not desirable. High coupling means a module depends upon many other modules to carry out its tasks. This makes it difficult to understand, reuse, and make changes because of the interdependencies with other modules. As an analogy, a company would want its employees to be able to carry out their individual jobs with the least amount of dependencies on other workers. If Joe had to talk with five other people just to get one task done, too much complexity exists, it's too time consuming, and more places are created where errors can take place.
- C** is incorrect because it states the exact opposite of what is desirable. A module that has low cohesion and high coupling is complex in that it carries out multiple different types of tasks and depends upon many other modules to carry them out. These characteristics make the module harder to maintain and reuse, largely because of the greater possibility of affecting other modules that interact with it.

12. Which of the following statements does not correctly describe SOAP and Remote Procedure Calls?

- A.** SOAP was designed to overcome the compatibility and security issues associated with Remote Procedure Calls.
 - B.** Both SOAP and Remote Procedure Calls were created to enable application-layer communication.
 - C.** SOAP enables the use of Remote Procedure Calls for information exchange between applications over the Internet.
 - D.** HTTP was not designed to work with Remote Procedure Calls, but SOAP was designed to work with HTTP.
- C.** The Simple Object Access Protocol (SOAP) was created to use instead of Remote Procedure Calls (RPCs) to allow applications to exchange information over the Internet. SOAP is an XML-based protocol that encodes messages in a web service setup. It allows programs running on different operating systems to communicate over web-based communication methods.
 - A** is incorrect because SOAP was created to overcome the compatibility and security issues that RPCs introduced when trying to enable communication between objects of different applications

over the Internet. SOAP is designed to work across multiple operating system platforms, browsers, and servers.

- B** is incorrect because it is true that both SOAP and RPCs were created to enable application-layer communication. SOAP is an XML-based protocol that encodes messages in a web service setup. So if you have a Windows client and you need to access a Windows server that offers a specific web service, the programs on both systems can communicate using SOAP without running into interoperability issues. This communication most commonly takes place over HTTP, since it is readily available in basically all computers today.
 - D** is incorrect because the statement is correct: HTTP was not designed to specifically work with RPCs, but SOAP was designed to work with HTTP. SOAP actually defines an XML schema or a structure of how communication is going to take place. The SOAP XML schema defines how objects communicate directly. One advantage of SOAP is that the program calls will most likely get through firewalls since HTTP communication is commonly allowed. This helps ensure that the client/server model is not broken by getting denied by a firewall in between the communicating entities.
- 13.** Which of the following is a correct description of the pros and cons associated with third-generation programming languages?
- A.** The use of heuristics reduced programming effort, but the amount of manual coding for a specific task is usually more than the preceding generation.
 - B.** The use of syntax similar to human language reduced development time, but the language is resource intensive.
 - C.** The use of binary was extremely time consuming but resulted in fewer errors.
 - D.** The use of symbols reduced programming time, but the language required knowledge of machine architecture.
- B.** Third-generation programming languages are easier to work with compared to earlier languages because their syntax is similar to human languages. This reduces program development time and allows for simplified and swift debugging. However, these languages can be very resource intensive when compared to the second-generation programming languages.

- A** is incorrect because it attempts to describe the pros and cons of fourth-generation programming. It is true that the use of heuristics in fourth-generation programming languages drastically reduced the programming effort and the possibility of errors in code. However, it is not true that the amount of manual coding was usually more than that required of third-generation languages. On the contrary, the most remarkable aspect of fourth-generation languages is that the amount of manual coding required to perform a specific task may be ten times less than for the same task on a third-generation language.
- C** is incorrect because the statement alludes to the pros and cons of machine language, the first-generation programming language. The first portion of the statement is true: Programming in binary was time consuming. The second half, however, is incorrect. Programming in binary was very prone to errors.
- D** is incorrect because it describes second-generation programming languages. By introducing symbols to represent complicated binary codes, second-generation programming languages reduced programming and debugging times. Unfortunately, these languages required extensive knowledge of machine architecture, and the programs that were written in it were hardware specific.

- 14.** It can be very challenging for programmers to know what types of security should be built into the software that they create. The amount of vulnerabilities, threats, and risks involved with software development can seem endless. Which of the following describes the best first step for developers to take to identify the security controls that should be coded into a software project?
- A.** Penetration testing
 - B.** Regression testing
 - C.** Threat modeling
 - D.** Attack surface analysis
- C.** Threat modeling is a systematic approach used to understand how different threats could be realized and how a successful compromise could take place. A threat model is created to define a set of possible attacks that can take place so the necessary countermeasures can be identified and implemented. Through the use of a threat model, the software team can identify and rate threats. Rating the threats based upon the probability of exploitation

and the associated impact of each exploitation allows the team to focus on the threats that present the greatest risk. When using threat modeling in software development, the process starts at the design phase and should continue in an iterative process through each phase of the software's life cycle. Different software development threat modeling approaches exist, but they have many of the same steps, including identifying assets, trust boundaries, data flows, entry points, privilege code, etc. This approach also includes building attack trees, which represent the goals of each attack and the attack methodologies. The output of all of these steps is then reviewed and security controls selected and coded into the software.

- ☒ **A** is incorrect because penetration testing is basically attacking a system to identify any weaknesses or vulnerabilities. A penetration test can be carried out on the software only after it has been at least partially developed; it is not a tool that can be used at the coding stage. A penetration test is different from building a threat model. A threat model is developed so that vulnerabilities and their associated threats can be identified and removed or mitigated. A threat model outlines all of the possible attack vectors that could be exploited. A penetration test is the act of exploiting vulnerabilities in the real world to fully understand what an attacker can accomplish when exploiting specific vulnerabilities.
- ☒ **B** is incorrect because regression testing is a type of test that is carried out to identify software bugs that exist after changes have taken place. The goal of regression testing is to ensure that changes that have taken place do not introduce new faults. Testers need to figure out if a change to one part of a software program will affect other parts of the software. A software regression is a bug (flaw) that makes a feature stop working after a change (e.g., patch applied, software upgrade) takes place. A software performance regression is a fault that does not cause the feature to stop working, but the performance of the function is degraded. Regression testing is not security focused and is not used with the goals of identifying vulnerabilities.
- ☒ **D** is incorrect because an attack surface analysis is used to map out the parts of a software program that need to be reviewed and tested for vulnerabilities. An attack surface consists of the components that are available to be used by an attacker against the software itself. The attack surface is a sum of the different attack vectors that can be used by an unauthorized user to compromise the system. The

more attack surface that is available to attackers, the more they have to work with and use against the software itself. Securing software commonly includes reducing the attack surface and applying defense-in-depth to the portions of the software that cannot have their surface reduced. There is a recursive relationship between an attack surface analysis and threat modeling. When there are changes to an attack surface, threat modeling should take place to identify the new threats that will need to be dealt with. So an attack surface analysis charts out what areas need to be analyzed, and threat modeling allows the developers to walk through attack scenarios to determine the reality of each identified threat.

15. Mary is creating malicious code that will steal a user's cookies by modifying the original client-side Java script. What type of cross-site scripting vulnerability is she exploiting?
- A. Second order
 - B. DOM-based
 - C. Persistent
 - D. Nonpersistent
- B.** Mary is exploiting a document object model (DOM)-based cross-site scripting (XSS) vulnerability, which is also referred to as local cross-site scripting. DOM is the standard structure layout to represent HTML and XML documents in the browser. In such attacks the document components such as form fields and cookies can be referenced through JavaScript. The attacker uses the DOM environment to modify the original client-side JavaScript. This causes the victim's browser to execute the resulting abusive JavaScript code. The most effective way to prevent these attacks is to disable scripting support in the browser.
- A** is incorrect because a second-order vulnerability, or persistent XSS vulnerability, is targeted at websites that allow users to input data that is stored in a database or other location, such as a forum or message board. Second-order vulnerabilities allow the most dominant type of attacks.
- C** is incorrect because a persistent XSS vulnerability is simply another name for a second-order vulnerability. As previously stated, these vulnerabilities allow users to input data that is stored in a database or other location such as an online forum or message board. These types of platforms are among the most commonly

plagued by XSS vulnerabilities. The best way to overcome these vulnerabilities is through secure programming practices. Each and every user input should be filtered, and only a limited set of known and secure characters should be allowed for user input.

- D** is incorrect because nonpersistent XSS vulnerabilities, also referred to as reflected vulnerabilities, occur when an attacker tricks the victim into opening a URL programmed with a rogue script to steal the victim's sensitive information (such as a cookie). The principle behind this attack lies in exploiting lack of proper input or output validation on dynamic websites.
- 16.** Of the following steps that describe the development of a botnet, which best describes the step that comes first?
 - A. Infected server sends attack commands to the botnet.
 - B. Spammer pays a hacker for use of a botnet.
 - C. Controller server instructs infected systems to send spam to mail servers.
 - D.** Malicious code is sent out that has bot software as its payload.
- D.** The creation of a botnet begins with the hacker sending systems malicious code that has the bot software as its payload. A bot is a piece of dormant code that carries out functionality for its master. Also known as a zombie, the code can be used to forward items sent to it as in spam or attack commands. The zombie code sends a message to the attacker indicating that a specific system has been compromised and can be used by the attacker. When an attacker has a collection of these compromised systems, it is referred to as a botnet.
- A** is incorrect because before a server can act as a controlling server of the botnet, there must be compromised systems to control. These systems are created by sending malicious code to the individual system that has bot software as its payload. Then, once installed, the bot logs in to an Internet Relay Chat (IRC) server that it is coded to contact. This IRC server then is used to control the botnet. (IRC is just one type of communication channel that can be used.)
- B** is incorrect because the development of a botnet begins with the attacker sending out malicious code that has the bot software as its payload. While a spammer could commission an attacker to develop a botnet, that is not the first step in its actual development. In addition to renting out the botnet to spammers, hackers can use the

infected systems to carry out powerful distributed denial-of-service attacks.

- C** is incorrect because the last step in the use of a botnet to send spam is the controller server instructing the infected systems to send out spam messages to mail servers. Spammers use this method so that their messages have a higher likelihood of getting through mail server spam filters since the sending IP addresses are those of the victim's system. Thus, the source IP addresses change constantly. This also helps ensure that the original sender is not located or identified.
- 17.** Which of the following antimalware detection methods is the most recent to the industry and monitors suspicious code as it executes within the operating system?
 - A.** Behavior blocking
 - B.** Fingerprint detection
 - C.** Signature-based detection
 - D.** Heuristic detection
- A.** Of the methods listed, behavior blocking is the most recent evolution in antimalware detection. Behavior blocking allows suspicious code to execute within the operating system and watches its interactions looking for suspicious activities. These activities include writing to startup files or the Run keys in the Registry; opening, deleting, or modifying files; scripting e-mail messages to send executable code; and creating or modifying macros and scripts. If the antimalware program detects some of these potentially malicious activities, it can terminate the software and provide a message to the user. A drawback to behavior blockers is that the malicious code must actually execute in real time. This type of constant monitoring also requires a high level of system resources.
- B** is incorrect because fingerprint detection (also referred to as signature-based detection) does not monitor suspicious code as it is executing. Instead, antimalware software scans incoming data and compares files, e-mail messages, etc., for signatures that match those in the antimalware's database. A signature is a sequence of code that was extracted from the virus itself, or the steps it carries out in its attack. If a match is identified, then the antimalware software takes whatever protective action(s) it is configured to carry

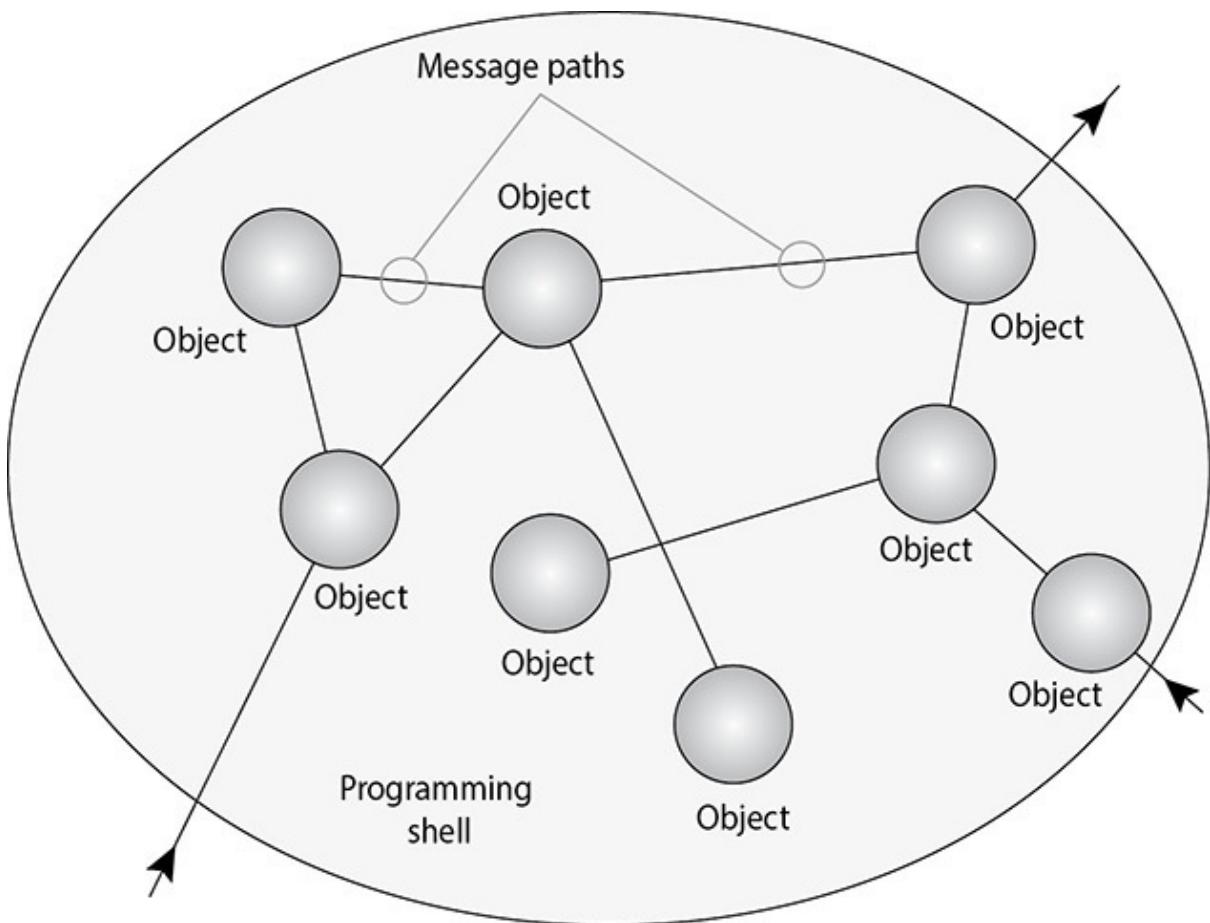
out. It may quarantine the file, attempt to clean the file by removing the virus, provide a warning message dialog box to the user, and/or log the event.

- C** is incorrect because signature-based detection uses signatures (virus code patterns) to identify malicious software or activity patterns before they are executed in the operating system.
Signature-based detection is an effective way to detect malicious software, but there is a delayed response time to new threats. Once a virus is detected, the antimalware vendor must study it, develop and test a new signature, release the signature, and all customers must download it.
- D** is incorrect because heuristic detection analyzes the overall structure of executable code, evaluates the coded instructions and logic functions, and evaluates the likelihood of it being malicious. Antimalware software that uses heuristic detection has a type of “suspiciousness counter,” which is incremented as the program finds more potentially malicious attributes. Once a predefined threshold is met, the code is officially considered dangerous and the antimalware software protects the system.

- 18.** Which of the following describes object-oriented programming deferred commitment?
- A.** Autonomous objects, which cooperate through exchanges of messages
 - B.** The internal components of an object can be refined without changing other parts of the system
 - C.** Object-oriented analysis, design, and modeling maps to business needs and solutions
 - D.** Other programs using same objects
- B.** Deferred commitment means that the internal components of an object can be refined without changing other parts of the system. Non-object-oriented programming applications are written as monolithic entities. This means an application is just one big pile of code. If you need to change something in this pile, you would need to go through the whole program’s logic functions to figure out what your one change is going to break. If you choose to write your program in an object-oriented language, you don’t have one monolithic application, but an application that is made up of smaller components (objects). If you need to make changes or updates to

some functionality in your application, you can just change the code within the class that creates the object carrying out that functionality and not worry about everything else the program actually carries out.

- A** is incorrect because autonomous objects, which cooperate through exchanges of messages, refer to object-oriented programming's modularity. An object is preassembled code that is a self-contained module. Objects need to be able to communicate with each other, and this happens by using messages that are sent to the receiving object's application programming interface. If object A needs to tell object B that a user's checking account must be reduced by \$40, it sends object B a message. The message is made up of the destination, the method that needs to be performed, and the corresponding arguments.
 - C** is incorrect because the description, "Object-oriented analysis, design, and modeling maps to business needs and solutions," refers to naturalness. An object's method should naturally map to business objectives. A method is the functionality or procedure an object can carry out. An object may be constructed to accept data from a user and reformat the request so that a back-end server can understand and process it. Another object may perform a method that extracts data from a database and populates a web page with this information. Or an object may carry out a withdrawal procedure to allow the user of an ATM to extract money from her account. These are business needs.
 - D** is incorrect because reusability refers to different programs being able to use the same objects. Most applications have some type of functionality in common. Instead of developing the same code to carry out the same functionality for ten different applications, using OOP allows you to just create the object once and let it be reused in other applications. This reduces development time and saves money. The objects can be catalogued in a library, which provides an economical way for more than one application to call upon the objects. The library provides an index and pointers to where objects actually live within the system or on another system.
- 19.** What object-oriented programming term or concept is illustrated in the graphic that follows?

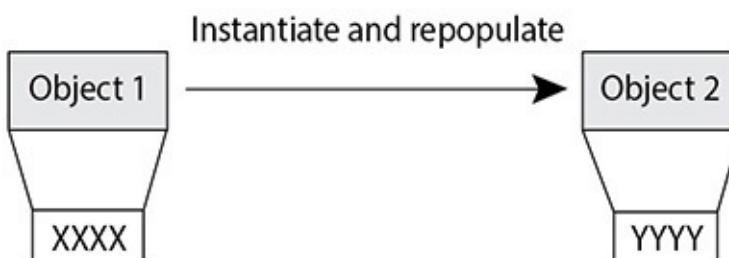


- A. Methods**
 - B. Messages**
 - C. Abstraction**
 - D. Data hiding**
- B.** In object-oriented programming objects need to be able to communicate with each other, and this happens by using messages that are sent to the receiving object's application program interface (API). For example, if object A needs to tell object B that a user's checking account must be reduced by \$40, it sends object B a message. The message is made up of the destination, the method that needs to be performed, and the corresponding arguments. This graphic illustrates object communication through the use of their messaging functionality.
- A** is incorrect because a method is the functionality or procedure an object can carry out, not the way objects communicate with each other. An object, for example, may be constructed to accept data from a user and to reformat the request so that a back-end server can understand and process it. These functions are the methods that

can be carried out by the specific objects—basically what the object can do. Another object may perform a method that extracts data from a database and populates a web page with the necessary information. These are just some examples of the various methods objects may carry out.

- ☒ **C** is incorrect because abstraction is the capability to suppress unnecessary details so the important, inherent properties can be examined and reviewed. Abstraction enables the separation of conceptual aspects of a system. For example, if a software architect needs to understand how data flows through the program, she would want to understand the big pieces of the program and trace the steps the data takes from first being input into the program all the way until it exits the program as output. Abstraction can be provided by OOP, but this is not what is being shown in the graphic.
 - ☒ **D** is incorrect because data hiding refers to the concept that data and operations internal to objects are hidden from other objects. Each object encapsulates its data and processes. Data hiding protects an object's private data from outside access. No object should be allowed to, or have the need to, access another object's internal data or processes. Data hiding is basically keeping what is supposed to be secret, secret.
- 20.** Protection methods can be integrated into software programs. What type of protection method is illustrated in the graphic that follows?

Level	Ship	Cargo	Origin	Destination
Top Secret	Oklahoma	Weapons	Delaware	Ukraine
Unclassified	Oklahoma	Food	Delaware	Africa

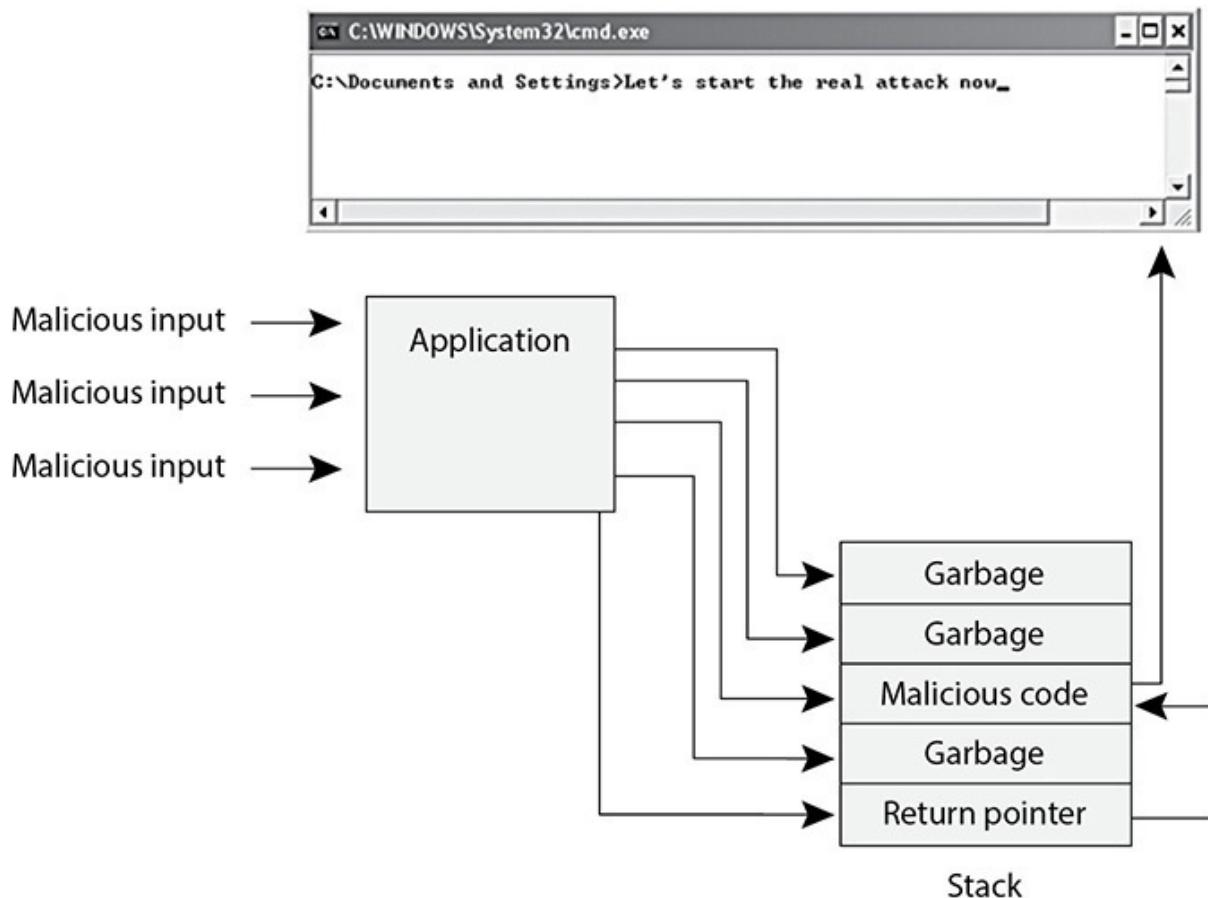


- A.** Polymorphism
- B.** Polyinstantiation
- C.** Cohesiveness
- D.** Object classes

- B.** Polyinstantiation is the simultaneous existence of multiple information objects, which refer to the same real-world concept but differ by their classification level and/or their contents. The multiple instances are commonly distinguished by their security levels.
Polyinstantiation is when more than one copy of an object is made, and the other copy is modified to have different attributes. This can be done for several reasons. A way to use polyinstantiation is for security purposes, to ensure that a lower-level subject could not access an object at a higher level. If a lower-level subject does not have the clearance of Top Secret, then it should not be able to access data at this classification level.
- A** is incorrect because polymorphism is the capability of different objects to respond differently to the same message. This is possible because objects can belong to different classes, meaning they will exhibit different behaviors. Polymorphism can take place in the following example: Object A and Object B are created from the same parent class, but Object B is also under a subclass. Object B would have some different characteristics from Object A because of this inheritance from the parent class and the subclass. When Object A and Object B receive the same input, they would result in different outputs because only one of them inherited characteristics from the subclass. An analogy of polymorphism is if someone gave you and Joe the same message and Joe responded with X and you responded with Y—so the same input and different outputs.
- C** is incorrect because cohesiveness means that one module is carrying out only one task. If a module is highly cohesive, this means that all elements in the module directly deal with the one basic task the module carries out, or a group of similar tasks. A module should have well-defined responsibilities, which means that it has high cohesiveness. If you were a highly cohesive module, you would carry out your one specific task you were built to do—for example, taking out the trash.
- D** is incorrect because an object class is a blueprint or prototype that defines the variables (data) and methods (procedures) common to all objects within it. A class provides a type of empty template of variables that will be populated when the object is instantiated. Objects are members, or instances, of classes. A real-world object, such as a table, is a member (or an instance) of a larger class of objects called “furniture.” The furniture class will have a set of attributes associated with it, and when an object is generated, it

inherits these attributes. The attributes may be color, dimensions, weight, style, and cost. These attributes apply if a chair, table, or loveseat object is generated or instantiated. Because the table is a member of the class furniture, the table inherits all attributes defined for the class.

21. There are several types of attacks that programmers need to be aware of. What attack does the graphic that follows illustrate?

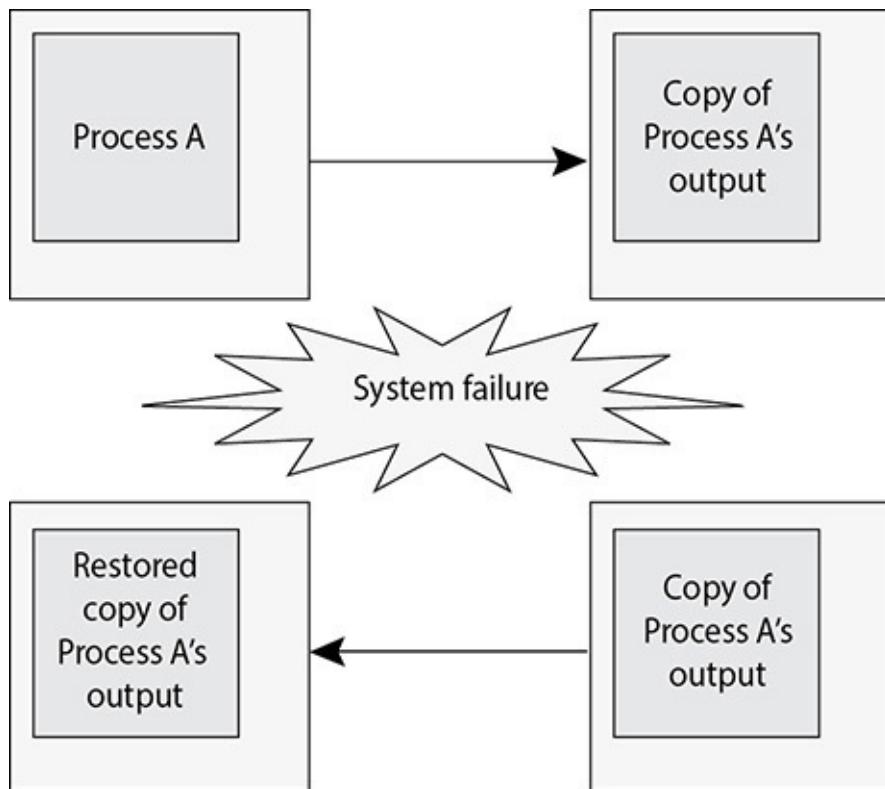


- A. Traffic analysis
 - B. Race condition
 - C. Covert storage
 - D. Buffer overflow
- D. A buffer is an area reserved by an application to store something in it, like some user input. After the application receives the input, an instruction pointer points the application to do something with the input that's been put in the buffer. A buffer overflow occurs when an application erroneously allows an invalid amount of input to be written into the buffer area, overwriting the instruction pointer in the code that told the program what to do with the input. Once

the instruction pointer is overwritten, whatever code has been placed in the buffer can then be executed, all under the security context of the application.

- A** is incorrect because traffic analysis is a method of uncovering information by watching traffic patterns on a network. For example, heavy traffic between the HR department and headquarters could indicate an upcoming layoff. Another example is if there is a lot of traffic between two military units, this may indicate that a military attack is being planned. Traffic padding can be used to counter this kind of attack, in which decoy traffic is sent out over the network to disguise patterns and make it more difficult to uncover them.
- B** is incorrect because it does not depict a race condition attack. When two different processes need to carry out their tasks on a resource, they need to follow the correct sequence. Process one needs to carry out its work before process two accesses the same resource and carries out its tasks. If process two goes before process one, the outcome could be very different. If an attacker could manipulate the processes so that process two did its thing first, she is controlling the outcome of the processing procedure, which is referred to as a race condition attack.
- C** is incorrect because in a covert storage channel, processes are able to communicate through some type of storage space on the system. For example, System A is infected with a Trojan horse that has installed software that will be able to communicate to another process in a nefarious way. System A has a very sensitive file (File 2) that is of great interest to a particular attacker. The software the Trojan horse installed is able to read this file and it needs to send the contents of the file to the attacker, which can only happen one bit at a time. The intrusive software is going to communicate to the attacker by locking a specific file (File 3). When the attacker attempts to access File 3 and finds it has a software lock enabled on it, the attacker interprets this to mean the first bit in the sensitive file is a 1. The second time the attacker attempts to access File 3, it is not locked. The attacker interprets this value to be zero. This continues until all of the data in the sensitive file is sent to the attacker.

- 22.** Databases and applications commonly carry out the function that is illustrated in the graphic that follows. Which of the following best describes the concept that this graphic is showing?



A. Checkpoint

B. Commit

C. Two-phase commit

D. Data dictionary

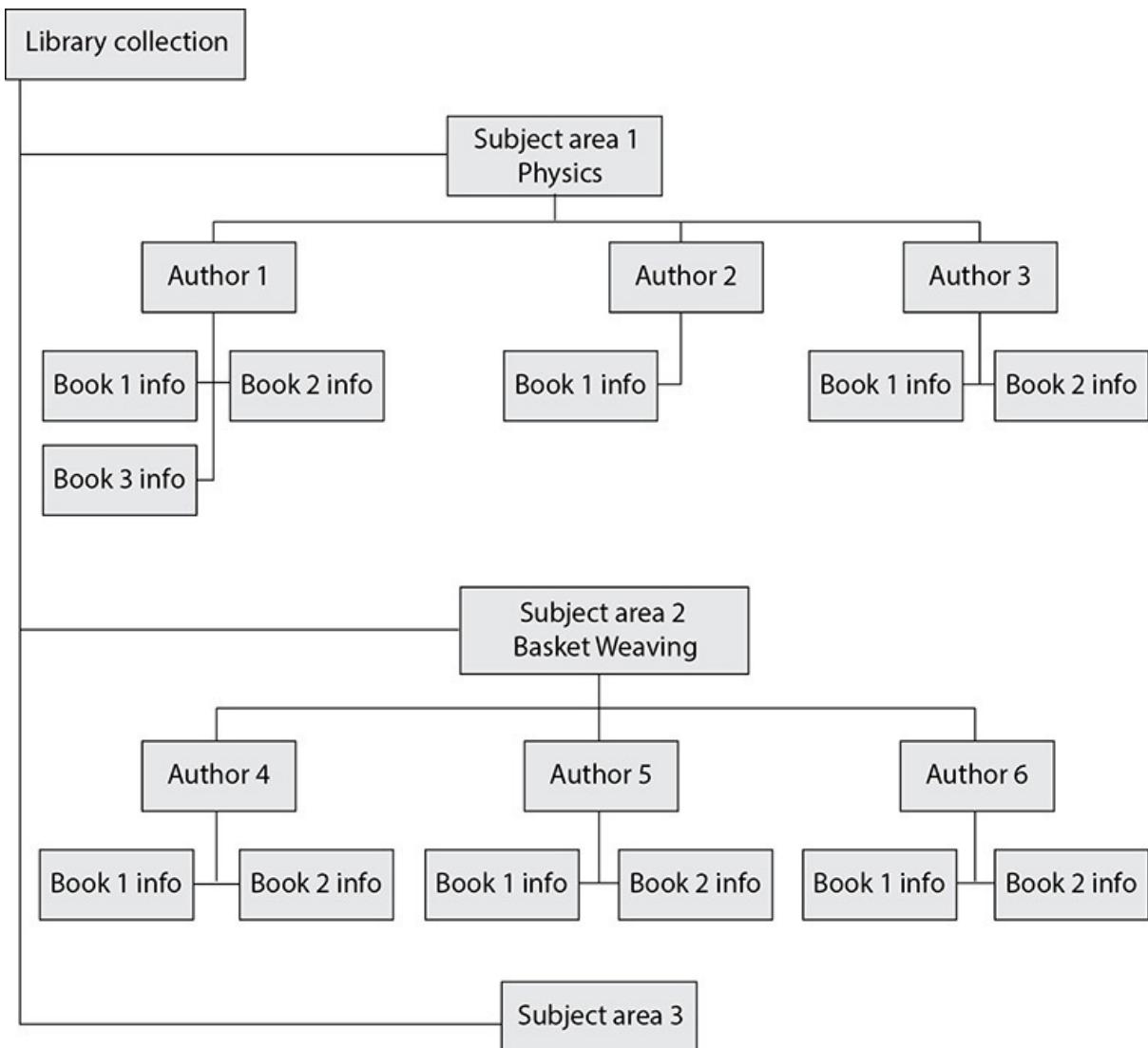
A. A checkpoint is used to recover data if there is a system failure or problem during a transaction. It is used to periodically save the state of the application and the user's information. It is used so that if the application endures a glitch, it has the necessary tools to bring the user back to his working environment without losing any data. You can experience this with a word processor when it asks you if you want to review the recovered version of a file you were working on. The word processor has saved your document as you have worked on it and is able to bring it back in case the system runs into trouble.

B is incorrect because a commit operation completes a transaction and executes all changes just made by the user. As its name indicates, once the commit command is executed, the changes are committed and reflected in the database. These changes can be made to data or schema information. When these changes are committed, they are then available to all other applications and users. If a user attempts to commit a change and it cannot complete correctly, a rollback is performed. This ensures that partial changes

do not take place and that data is not corrupted.

- C** is incorrect because a two-phase commit mechanism is a control that is used in databases to ensure the integrity of the data held within the database. Databases commonly carry out transaction processes, which means the user and the database interact at the same time. The databases need to make sure each database is properly modified, or no modification takes place at all. When a database change is submitted by the user, the different databases initially store these changes temporarily. A transaction monitor will then send out a “precommit” command to each database. If all the right databases respond with an acknowledgment, then the monitor sends out a “commit” command to each database. This ensures that all of the necessary information is stored in all the right places at the right time.
- D** is incorrect because a data dictionary is a central collection of data element definitions, schema objects, and reference keys for a database. The schema objects can contain tables, views, indexes, procedures, functions, and triggers. A data dictionary can also contain the default values for columns, integrity information, the names of users, the privileges and roles for users, and auditing information. It is a tool used to centrally manage parts of a database by controlling data about the data (referred to as metadata) within the database. It provides a cross-reference between groups of data elements and the databases.

- 23.** There are several different types of databases. Which type does the graphic that follows illustrate?



- A.** Relational
- B.** Hierarchical
- C.** Network
- D.** Object-oriented

- B.** A hierarchical database uses a tree-like structure to define relationships between data elements, using a parent/child relationship. The structure and relationship between the data elements are different from those in a relational database. The tree structure contains branches, and each branch has a number of leaves, or data fields. These databases have well-defined, prespecified access paths, but they are not as flexible in creating relationships between data elements as a relational database. Hierarchical databases are useful for mapping one-to-many relationships.

- A** is incorrect because a relational database model uses attributes (columns) and tuples (rows) to contain and organize information. It presents information in the form of tables. A relational database is composed of two-dimensional tables, and each table contains unique rows, columns, and cells (the intersection of a row and a column). Each cell contains only one data value that represents a specific attribute value within a given tuple. These data entities are linked by relationships. The relationships between the data entities provide the framework for organizing data.
- C** is incorrect because a network database model is built upon the hierarchical data model, but instead of being constrained by having to “know” how to go from one branch to another and then from one parent to a child to find a data element, the network database model allows each data element to have multiple parent and child records. This forms a redundant network-like structure instead of a strict tree structure. (The name does not indicate it is on or distributed throughout a network; it just describes the data element relationships.)
- D** is incorrect because an object-oriented database is designed to handle a variety of data (images, audio, documents, video). An object-oriented database management system (ODBMS) is more dynamic in nature than a hierarchical database because objects can be created when needed and the data and procedure (called method) go with the object when it is requested. In a hierarchical database, the application has to use its own procedures to obtain data from the database and then process the data for its needs. The hierarchical database does not actually provide procedures, as object-oriented databases do. The object-oriented database has classes to define the attributes and procedures of its objects.

The following scenario applies to questions 24, 25, and 26.

Trent is the new manager of his company’s internal software development department. He has been told by his management that the group needs to be compliant with the international standard that provides guidance to organizations in integrating security into the processes used for managing their applications. His new boss told him that he should join and get familiar with the Open Web Application Security Project (OWASP), and Trent just received an e-mail stating that one of the company’s currently deployed applications has a zero-day vulnerability.

- 24.** Which of the following is most likely the standard Trent’s company wants to comply with?

- A.** ISO/IEC 27005
 - B.** ISO/IEC 27001
 - C.** ISO/IEC 27034
 - D.** BS 7799
- C.** ISO/IEC 27034 is the international standard that provides guidance to organizations in integrating security to the processes used for managing their applications. It is applicable to in-house developed applications, applications acquired from third parties, and where the development or the operation of the application is outsourced.
- A** is incorrect because ISO/IEC 27005:2011 provides guidelines for information security risk management. It supports ISO/IEC 27001 and is designed to assist in the proper implementation of information security based on a risk management approach.
- B** is incorrect because ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented information security management system within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.
- D** is incorrect because BS 7799 was written by the UK government's Department of Trade and Industry and outlines how an information security management system (ISMS) (aka security program) should be built and maintained. The goal was to provide guidance to organizations on how to design, implement, and maintain policies, processes, and technologies to manage risks to its sensitive information assets.
- 25.** Which of the following best describes the consortium Trent's boss wants him to join?
- A.** Nonprofit organization that produces open-source software and follows widely agreed-upon best-practice security standards for the World Wide Web
 - B.** U.S. DHS group that provides best practices, tools, guidelines, rules, principles, and other resources for software developers, architects, and security practitioners to use
 - C.** Group of experts who create proprietary software tools used to help

improve the security of software worldwide

- D. Group of experts and organizations who certify products based on an agreed-upon security criteria
- A. The Web Application Security Consortium (WASC) is a nonprofit organization made up of an international group of experts, industry practitioners, and organizational representatives who produce open-source and widely agreed-upon best-practice security standards for the World Wide Web.
- B is incorrect because the U.S. Department of Homeland Security (DHS) provides best practices, tools, guidelines, rules, principles, and other resources that software developers, architects, and security practitioners can use to build security into software in every phase of its development. This DHS initiative is called Build Security In (BSI), and it is a collaborative effort that allows many entities across the industry to participate and provide useful material.
- C is incorrect because this is a distracter answer. There is no official organization that provides proprietary tools for the listed purpose.
- D is incorrect because the Web Application Security Consortium does not certify products. Instead it provides guidance and open-source best practices on how to integrate security into software.
26. Which of the following best describes the type of vulnerability mentioned in this scenario?
- A. Dynamic vulnerability that is polymorphic
- B. Static vulnerability that is exploited by server-side injection parameters
- C. Vulnerability that does not currently have an associated solution
- D. Database vulnerability that directly affects concurrency
- C. Zero-day vulnerabilities are vulnerabilities that do not currently have a resolution. If a vulnerability is identified and there is not a pre-established fix (patch, configuration, update), it is considered a zero day. A zero-day attack is an attack that exploits a previously unknown vulnerability in a system, meaning that the attack occurs between the time it is identified and the solution is prepared—that is, on “day zero” of the awareness of the vulnerability. This leaves zero days for the victim to react and apply a patch to the vulnerability.

- A** is incorrect because a zero-day vulnerability can be any type of vulnerability that does not have a current resolution that victims and potential victims can implement. A zero-day vulnerability is not specific in nature, as in a dynamic polymorphic vulnerability; it is just a general category that can include this type of vulnerability and many more. A polymorphic attack just means that it changes itself, with the goal of being undetected.
- B** is incorrect because a zero-day vulnerability can be any type of vulnerability that does not have a current resolution that victims and potential victims can implement. A zero-day vulnerability is not specific in nature, as in server-side injection; it is just a general category that can include this type of vulnerability and many more. Server-side includes (SSI) injection attacks allow the exploitation of a web application by injecting scripts in HTML pages or executing arbitrary codes remotely.
- D** is incorrect because concurrency within databases specifically pertains to correctly executing several transactions simultaneously. If there is a vulnerability that directly affects the successful execution of database transactions, then there is a risk of negatively affecting the integrity of the data held within and processed by database software. This does not have anything to do directly with a zero-day vulnerability.

27. _____ provides a machine-readable description of the specific operations provided by a specific web service.
_____ provides a method for web services to be registered by service providers and located by service consumers.
- A.** Web Services Description Language; Universal Description, Discovery and Integration
 - B.** Universal Description, Discovery and Integration; Web Services Description Language
 - C.** Web Services Description Language; Simple Object Access Protocol
 - D.** Simple Object Access Protocol; Universal Description, Discovery and Integration
- A.** Services within a service-oriented architecture (SOA) are usually provided through web services. A web service allows for web-based communication to happen seamlessly using web-based standards as in Simple Object Access Protocol (SOAP), HTTP, Web Services

Description Language (WSDL), Universal Description, Discovery and Integration (UDDI), and Extensible Markup Language (XML). WSDL provides a machine-readable description of the specific operations provided by the service. UDDI is an XML-based registry that lists available services. UDDI provides a method for services to be registered by service providers and located by service consumers.

- B** is incorrect because the terms are not in the correct order and do not map to the definitions provided within the question. WSDL provides a machine-readable description of the specific operations provided by the service. UDDI is an XML-based registry that lists available services. UDDI provides a method for services to be registered by service providers and located by service consumers.
 - C** is incorrect because Simple Object Access Protocol (SOAP) is an XML-based protocol that encodes messages in a web service environment. SOAP actually defines an XML schema of how communication is going to take place. The SOAP XML schema defines how objects communicate directly. SOAP is not an item identified in this question.
 - D** is incorrect because Simple Object Access Protocol (SOAP) is an XML-based protocol that encodes messages in a web service environment. SOAP actually defines an XML schema of how communication is going to take place. The SOAP XML schema defines how objects communicate directly. This is not what the question is addressing.
28. Sally has found out that software programmers in her company are making changes to software components and uploading them to the main software repository without following version control or documenting their changes. This is causing a lot of confusion and has caused several teams to use the older versions. Which of the following would be the best solution for this situation?
- A. Software change control management
 - B. Software escrow
 - C. Software configuration management
 - D. Software configuration management escrow
- C. When changes take place to a software product during its development life cycle, a configuration management system can be put into place that allows for change control processes to take place

through automation. A product that provides software configuration management (SCM) identifies the attributes of software at various points in time and performs a methodical control of changes for the purpose of maintaining software integrity and traceability throughout the software development life cycle. It defines the need to track changes and provides the ability to verify that the final delivered software has all of the approved changes that are supposed to be included in the release. During a software development project, the centralized code repositories are often kept in systems that can carry out SCM functionality, which manages and tracks revisions made by multiple people against a single master set.

- A** is incorrect because this is not the official term for this type of functionality. Software change control management is only a part of software configuration management. A software configuration management system also provides concurrency management, versioning, and synchronization.
 - B** is incorrect because in a software escrow framework, a third party keeps a copy of the source code, and possibly other materials, which it will release to the customer only if specific circumstances arise, mainly if the vendor who developed the code goes out of business or for some reason is not meeting its obligations and responsibilities. This procedure protects the customer because the customer pays the vendor to develop software code for them, and if the vendor goes out of business, the customer otherwise would no longer have access to the actual code.
 - D** is incorrect because this is a distracter answer. This is not an official term.
- 29.** The approach of employing an integrated product team (IPT) for software development is designed to achieve which of the following objectives?
- A.** Developing and testing software with fewer security flaws
 - B.** Developing and testing software with fewer defective features
 - C.** Developing and testing software that will be most profitable
 - D.** Developing and testing software best suited to the deployment environment
- D.** The IPT approach to the integration between development and operations (DevOps) is specifically designed to ensure that the

development team is building software in an environment that is as close as possible to the deployment environment and understands the deployment environment's operational necessities.

- A** is incorrect because all development and testing methodologies should employ an approach to secure software development life cycle (SDLC), including leveraging tools and techniques such as static code review, revision control, separation of duties, etc., regardless of whether an IPT is part of the infrastructure.
- B** is incorrect because, similar to answer A, all development environments should include the parallel construction of test harnesses and test cases for functional features. These should become automated wherever possible and executed both per module on repository check-in and whenever integration testing is performed.
- C** is incorrect because the return on investment (ROI) on any software project is, of course, paramount, but this answer is a distracter because it is less specific than answer D.

30. Which are the best reasons why a code versioning system (CVS) is an important part of a development infrastructure?

- i. It can ensure that code modifications are made according to corporate policies.
- ii. It will document who made which changes to ensure accountability.
- iii. It will reduce the cost of the development infrastructure.
- iv. It can provide control over unauthorized access to proprietary code.

A. i, ii, iv

B. iii

C. iii, iv

D. All of the above

- A.** When properly configured and deployed, a CVS can help ensure that corporate change control policies and procedures are adhered to and should log all code accesses as a detective control as well. But foremost, a CVS can help ensure that code is only ever accessed by an authorized developer. Such controls present some additional overhead, but tend to be worth the expense.
- B** is incorrect because statement iii is not true; the employment of a CVS adds maintenance overhead to the development environment.

It should ultimately improve the return on investment (ROI) of software development, but it is a front-loaded cost for the infrastructure that must be accounted for.

- C** is incorrect because both control and accountability of code access are important features of a good CVS, but change control is important as well.
- D** is incorrect because since statement iii is false, answer D must also be.

31. What is generally the safest, most secure way to acquire software?

- A.** From a reputable vendor of proprietary software, once tested in the deployment environment
- B.** Downloading very popular open-source software that has been inspected for bugs by a large and active community
- C.** Downloading either proprietary or open-source software, but fuzzing it in a lab environment prior to deployment
- D.** Downloading open-source software and deploying it only after the code base has been verified by cryptographic checksum
- C.** Black-box testing all software in a lab environment is the best way to uncover both feature and security defects prior to deployment into a sensitive environment.
- A** is incorrect because all software vendors, no matter how reputable, have shipped products with both feature and security flaws. Popularity does not equal security. Furthermore, software should be tested in a lab environment before it is introduced into the live deployment environment.
- B** is incorrect because much like the reputation of a popular proprietary vendor, the popularity of an open-source code base does not ensure that it has been adequately white-box tested. As Eric S. Raymond is famous for saying, “given enough eyeballs, all bugs are shallow.” But you have no way of knowing how many eyes have tried, either with open- or closed-source software.
- D** is incorrect because verifying cryptographic checksums is a best practice for sure, but it is not foolproof. If the code base could have been accessed and modified, so could the checksum on the web page that hosts it for distribution.

The following scenario applies to questions 32 and 33.

John is a network administrator and has been told by one of his network staff members that two servers on the network have recently had suspicious traffic traveling to them and then from them in a sporadic manner. The traffic has been mainly ICMP, but the patterns were unusual compared to traffic on other servers over the last 30 days. John lists the directories and subdirectories on the systems and finds nothing unusual. He inspects the running processes and again finds nothing suspicious. He sees that the systems' NICs are not in promiscuous mode, so he is assured that sniffers have not been planted.

- 32.** Which of the following describes the most likely situation as described in this scenario?
- A. Servers are not infected, but the traffic illustrates attack attempts.
 - B. Servers have been infected with rootkits.
 - C. Servers are vulnerable and need to be patched.
 - D. Servers have been infected by spyware.
- B.** Once the level of access is achieved, the attacker can upload a bundle of tools, collectively called a rootkit. A rootkit is software that implements stealth capabilities that are designed to hide the existence of certain processes or programs. Rootkit detection is difficult because a rootkit may be able to subvert the software that is intended to find it.
- A** is incorrect because in the situation laid out in the scenario, the system most likely is infected. The ICMP traffic is probably the commands and status data sent between the attacker and the compromised systems.
- C** is incorrect because it is not the best answer. The servers may be vulnerable and may need to be patched, but that is not what is being asked in the question. Plus, applying a patch will not eradicate an infected system of a rootkit.
- D** is incorrect because it is not the best answer. The scenario best describes a situation where rootkits have been installed. Spyware may be a component of the rootkit, but Trojaned files are most likely installed, which can only happen with rootkits, not spyware.
- 33.** Which of the following best explains why John does not see anything suspicious on the reported systems?
- A. The systems have not yet been infected.
 - B. He is not running the correct tools. He needs to carry out a penetration test on the two systems.

- C. Trojaned files have been loaded and executed.
 - D. A back door has been installed and the attacker enters the system sporadically.
- C. The other tools in the rootkit may vary, but they usually comprise utilities that are used to cover the attacker's tracks. For example, every operating system has basic utilities that a root or administrator user can use to detect the presence of the rootkit, an installed sniffer, and the back door. The hacker replaces these default utilities with new utilities, which share the same name. They are referred to as "Trojaned programs" because they carry out the intended functionality but do some devious activity in the background.
- A is incorrect because it is not the best answer. It is possible that the systems are not infected, but this question asks what is the most likely situation.
- B is incorrect because most rootkits have Trojaned programs that replace these utilities, because the root user could run ps or top and see there is a back-door service running, and thus detect the presence of an attack. Most rootkits also contain sniffers, so the data can be captured and reviewed by the attacker. For a sniffer to work, the system's NIC must be put into promiscuous mode, which just means it can "hear" all the traffic on the network link. The default ipconfig utility allows the root user to employ a specific parameter to see whether or not the NIC is running in promiscuous mode. So, the rootkit also contains a Trojaned ipconfig program, which hides the fact that the NIC is in promiscuous mode.
- D is incorrect because there is most likely more than just installed back doors on these servers. Rootkits include back-door programs to allow attackers to remotely control compromised systems, but rootkits contain many other tools also.
- 34.** Cross-site scripting (XSS) is an application security vulnerability usually found in web applications. What type of XSS vulnerability occurs when a victim is tricked into opening a URL programmed with a rogue script to steal sensitive information?
- A. Persistent XSS vulnerability
 - B. Nonpersistent XSS vulnerability
 - C. Second-order vulnerability

D. DOM-based vulnerability

- B.** XSS attacks enable an attacker to inject their malicious code into vulnerable web pages. When an unsuspecting user visits the infected page, the malicious code executes on the victim's browser and may lead to stolen cookies, hijacked sessions, malware execution, or bypassed access control or aid in exploiting browser vulnerabilities. There are three different XSS vulnerabilities: persistent, nonpersistent, and DOM-based. A *nonpersistent vulnerability* (also called a *reflected vulnerability*) occurs when an attacker tricks the victim into opening a URL programmed with a rogue script to steal the victim's sensitive information, such as a cookie or session ID. The principle behind this attack lies in exploiting the lack of proper input or output validation on dynamic websites. An XSS attack such as this can potentially cause damage on a huge scale. The stolen cookies can lead to compromised web mail systems, flooded blogs, and disclosed bank accounts. Most of the phishing attacks are caused by XSS vulnerabilities.
- A** is incorrect because a persistent vulnerability is targeted at websites that allow users to input data that is stored in a database or similar location, such as a forum or message board. The code for this type of attack can be rendered automatically without the need of luring a user to a third-party website. The best way to overcome the XSS vulnerability is through secure programming practices. Web application developers must ensure that every user input is filtered. Only a limited set of known and secure characters should be allowed for user input.
- C** is incorrect because a second-order vulnerability is another name for a persistent XSS vulnerability, which targets websites that allow users to input data that is stored in a database.
- D** is incorrect because in a DOM-based XSS vulnerability the attacker uses the Document Object Model (DOM) environment to modify the original client-side JavaScript. This causes the victim's browser to execute the resulting abusive JavaScript code. Thus, cross-site attacks can be used to exploit vulnerabilities in the victim's web browser. Once the system is successfully compromised by the attacker, he may further penetrate into other systems on the network or execute scripts that may spread through the internal network. As for the client's side, the most effective way to prevent XSS attacks is to disable scripting language support in the browser. If this is not feasible, then content filtering proxy

servers may be used.

35. Widgets, Inc.'s software development processes are documented, and the organization is capable of producing its own standard of software processes. Which of the following Capability Maturity Model Integration levels best describes Widgets, Inc.?
- A. Initial
 - B. Repeatable
 - C. Defined
 - D. Managed
- C. Capability Maturity Model Integration (CMMI) is a process improvement concept that consists of a collection of techniques used in the process of software development of an organization to design and further enhance software. The CMMI provides a standard for software development process where the level of maturity of the development process can be measured. The CMMI is classified into five levels, which are Initial, Repeatable, Defined, Managed, and Optimizing. The categorization of these levels depends upon the maturity of the software development and its quality assurance. The basis of Defined level (CMMI Level 3) is that the organizations are capable of producing their own standard of software processes. These processes are improved with the passage of time.
- A is incorrect because the processes in the Initial level (CMMI Level 1) are not organized or documented and are hence chaotic. The organizations with CMMI Level 1 are expected to thrive only due to the extraordinary performance of individuals. This makes the environment of the processes more unstable. This level has a very limited scope and is used for unique projects. Success is not likely to be repeated at this level.
- B is incorrect because at the Repeatable level (CMMI Level 2), the processes are documented in a better manner and so the success is repetitive; however, the organization is not yet capable of producing its own standard of software processes. This level ensures that the processes are maintained during the downtime, ensuring that the project is implemented according to the plan.
- D is incorrect because at the Managed level (CMMI Level 4), organizations are able to monitor and control their own processes involved in the software development. It allows management to

point out ways to adjust the processes of a particular project in such a way that there is no considerable loss on its quality or diversion from the main specifications. At the final level, Optimizing (CMMI Level 5), processes are managed for improvement.

- 36.** Which of the following best describes “change management?”
- A.** It is a systematic approach to deliberately regulating the changing nature of projects.
 - B.** It is the process of controlling the specific changes that take place during the life cycle of a system.
 - C.** It is an enterprise program for instituting programmatic changes in source code repositories.
 - D.** It is the process of controlling how changes to firewalls and other network devices are made.
- A.** The key words here are “systematic” and “deliberately.” In any enterprise IT infrastructure, there will be a fairly constant stream of projects that introduce changes from small to potentially immense. Managing them effectively, and in a way that is controlled and sustainable, requires their disciplined regulation. This is especially important when one considers that unmanaged, ad hoc changes of this nature inevitably adversely impact security controls, which are commonly static in deployment and configuration.
- B** is incorrect because this is the definition of “change control,” which is an essential *part* of change management, but which does not comprise its entirety. This is discussed in question 37.
- C** is incorrect because this answer more properly relates to revision control within the context of software development projects. It is an important component of both change control and change management, but is far more limited in scope.
- D** is incorrect because this is also a component of both change control and change management, and relates to configuration management as well. It is also much more limited in scope, however.
- 37.** Which of the following best describes “change control?”
- A.** It is a systematic approach to deliberately regulating the changing nature of projects.
 - B.** It is the process of controlling the specific changes that take place during the life cycle of a system.

- C. It is an enterprise program for instituting programmatic changes in source code repositories.
- D. It is the process of controlling how changes to firewalls and other network devices are made.
- B.** The key words here are “specific changes” and “life cycle.” Change control dictates that changes to a system over the course of its operation and maintenance (O&M) must be approved, documented, and tested according to a rigorous process. This is to ensure that such changes, whether they be mere alterations of configurations or sweeping code revisions, do not adversely impact either the system’s capabilities or the security controls they implement or depend upon.
- A** is incorrect because this is the definition of “change management,” which is discussed in more detail in question 36. Change control is an essential *component* of change management, but is narrower in scope.
- C** is incorrect because this answer more properly relates to revision control within the context of software development projects. It is an important component of both change control and change management, but is far more limited in scope.
- D** is incorrect because this is also a component of both change control and change management, and relates to configuration management as well. It is also much more limited in scope.
- 38.** What are the three major elements crucial to the security of software development environments?
- A. The software languages, the integrated development environments (IDEs), and the compilers
- B. The development platforms, the code repositories, and the software configurations
- C. The design teams, the development teams, and the testing teams
- D. The code repositories, the versioning systems, and the deployment processes
- B.** The security posture of development platforms, code repositories, and software configurations are the three overarching concerns for any software development environment. These determine the security of the entire life cycle of a development program, from how and where software is constructed, to how and where it is

stored, through the state it is in as deployed.

- A** is incorrect because, although the thoughtful selection of these items is crucial to secure development *platforms*, they are only components of this one element of the overall development environment. They do not address secure code storage or the secure configuration of software in deployment.
- C** is incorrect because, although these teams are certainly crucial to implementing security within the software or system's life cycle, and bear a great deal of responsibility for doing so, the infrastructure within which they work (the platforms and repositories) and the configurations of the resulting products are fundamental to their ability to succeed in this goal.
- D** is incorrect because these items are subcomponents of the overall architecture and processes for secure code management and deployment and do not directly address the security of the platforms upon which the code is created and developed.

39. Which of the following are key elements of secure coding practices?

- A.** Using object-oriented languages instead of procedural ones, and heeding compiler warnings
 - B.** Ensuring that quality assurance is thorough, and performed by multiple teams
 - C.** Parallel programming, agile methodologies, and iterative testing
 - D.** Validating inputs, adhering to the least privilege principle, and keeping code as simple as possible
- D.** According to the Carnegie Mellon University's Software Engineering Institute (SEI), the "top 10" secure coding practices (as of May 2018) include these three items, as well as the following seven others:
- Heeding compiler warnings
 - Architecting and designing for security policies
 - Default deny
 - Sanitizing outputs
 - Practicing defense in depth
 - Using effective quality assurance techniques
 - Adopting a secure coding standard

- A** is incorrect because, while heeding compiler warnings is certainly one of the top 10 secure coding practices, the choice of object-oriented languages versus procedural ones is relatively immaterial. While the former do tend to more easily facilitate keeping code more modular, and hence simpler, either of these types of languages can be used properly in practice.
- B** is incorrect because, while achieving thorough quality assurance through the use of effective quality assurance techniques is a top 10 secure coding practice, it doesn't necessarily need to involve multiple teams.
- C** is incorrect because, although these are elements of a software development methodology that have often contribute to the overall success of complex software development projects, they do not directly address the security of any specific coding practices.

About the Online Content

This book comes complete with TotalTester Online customizable practice exam software with more than 1,000 multiple-choice practice exam questions and separate hotspot and drag-and-drop questions.

System Requirements

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

Your Total Seminars Training Hub Account

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

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

Single User License Terms and Conditions

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

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

1. Go to hub.totalsem.com/mheclaim.

2. To register and create a new Training Hub account, enter your e-mail address, name, and password. No further information (such as credit card number) is required to create an account.
3. If you already have a Total Seminars Training Hub account, select “Log in” and enter your e-mail and password.
4. Enter your Product Key: **mpdf-q9v7-zt5x**
5. Click to accept the user license terms.
6. Click “Register and Claim” to create your account. You will be taken to the Training Hub and have access to the content for this book.

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

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

The Content is a copyrighted work of McGraw-Hill Education and McGraw-Hill Education reserves all rights in and to the Content. The Work is © 2019 by McGraw-Hill Education, LLC.

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

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

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

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

TotalTester Online

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

To take a test, follow the instructions provided in the previous section to register and activate your Total Seminars Training Hub account. When you register you will be taken to the Total Seminars Training Hub. From the Training Hub Home page, select **CISSP Practice Exams 5e TotalTester** from the Study drop-down menu at the top of the page, or from the list of Your Topics on the Home page. Select **TotalTester** from the menu on the right side of the screen, and then click the icon to load the tester as instructed on the screen. You can then select the option to customize your quiz and begin testing yourself in Practice Mode or Exam Mode. All exams provide an overall grade and a grade broken down by domain.

Hotspot and Drag-and-Drop Questions

In addition to multiple-choice questions, the CISSP exam includes hotspot and drag-and-drop questions. You can access the practice questions included with this book by navigating to the Resources tab and selecting Hotspot/Drag & Drop Questions. After you have selected the questions, they will appear in your browser.

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

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

Technical Support

For questions regarding the TotalTester software or operation of the Training Hub, visit www.totalsem.com or e-mail support@totalsem.com.

For questions regarding book content, e-mail hep_customer-service@mheducation.com. For customers outside the United States, e-mail international_cs@mheducation.com.