EXAM CRAM

CISSP

Practice Questions

Third Edition

CD FEATURES 1,001 PRACTICE QUESTIONS

PEARSON IT
CERTIFICATION

MICHAEL GREGG

EXAM CRAM

CISSP Practice Questions

Third Edition

Michael Gregg

CISSP Practice Questions Exam Cram, Third Edition

ISBN-13: 978-0-7897-4959-8
ISBN-10: 0-7897-4959-9

Library of Congress Cataloging-in-Publication data is on file.

Printed in the United States of America

First Printing: September 2012

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the CD or programs accompanying it.

Bulk Sales

Pearson IT Certification offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact

U.S. Corporate and Government Sales
1-800-382-3419
corpsales@pearsontechgroup.com

For sales outside of the U.S., please contact

International Sales
international@pearsoned.com

Associate Publisher
Dave Dusthimer

Acquisitions Editor
Betsy Brown

Senior Development Editor
Christopher Cleveland

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Sheri Cain

Technical Editors
Shawn Merdinger
Patrick Ramseier

Publishing Coordinator
Vanessa Evans

Multimedia Developer
Timothy Warner

Interior Designer
Gary Adair

Cover Designer
Alan Clements

Compositor
TnT Design, Inc.

Contents at a Glance

Table of Contents

About the Author

As the founder and president of Superior Solutions, Inc., a Houston-based IT security consulting and auditing firm, **Michael Gregg** has more than 20 years of experience in information security and risk management. He holds two associate's degrees, a bachelor's degree, and a master's degree. Some of the certifications he holds include CISA, CISSP, MCSE, CTT+, A+, N+, Security+, CASP, CCNA, GSEC, CEH, CHFI, CEI, CISA, CISM, CGEIT, and SSCP.

In addition to his experience performing security audits and assessments, Michael has authored or coauthored more than 15 books, including *Certified Ethical Hacker Exam Prep* (Que), *CISSP Exam Cram 2* (Que), and *Security Administrator Street Smarts* (Sybex). He is a site expert for TechTarget.com websites, such as SearchNetworking.com. He also serves on their editorial advisory board. His articles have been published on IT websites, and he has been quoted on Fox News and *The New York Times*. He has created more than 15 security-related courses and training classes for various companies and universities. Although audits and assessments are where he spends the bulk of his time, teaching and contributing to the written body of IT security knowledge are how Michael believes he can give something back to the community that has given him so much.

He is a board member for Habitat For Humanity and, when not working, Michael enjoys traveling and restoring muscle cars.

Dedication

I dedicate this book to those who have been my mentors along the way, because without them, this book would not have been possible.

Acknowledgments

I want like to thank everyone who helped make this project a reality, including Betsy Brown, Chris Cleveland, Shawn Merdinger, Patrick Ramseier, and the entire crew at Pearson.

About the Technical Reviewers

Shawn Merdinger is a security researcher and analyst at the University of Florida Academic Health Center. He has worked with Cisco Systems, 3Com/TippingPoint, and as an independent consultant. His current research focuses on medical device security, and he is the founder of the MedSec group on LinkedIn. Shawn regularly presents original research at security/hacker conferences such as DEFCON, Ph-Neutral, ShmooCon, CONfidence, NoConName, O'Reilly, CSI, IT Underground, CarolinaCon, and SecurityOpus.

Patrick Ramseier is a technical editor and author and manages a team of security and unified access consultants. He has held several management and technical positions in different security companies over the past 18 years and currently works on the Borderless Network Security and Unified Access team for Cisco in the Bay Area, where he leads a senior consulting team covering the entire western United States. Patrick has provided many technical edits/reviews for several major publishing companies, including Pearson Education, McGraw Hill, Wiley, and Sybex. He has a BA in Business Administration and MIS and holds CCNA, CISSP, and CISCP certifications.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Mail: Dave Dusthimer
Associate Publisher
Pearson IT Certification
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at www.pearsonitcertification.com/register for convenient access to any updates, downloads, or errata that might be available for this book.

Introduction

Welcome to the *CISSP Practice Questions Exam Cram*! This book provides you with practice questions, complete with answers and explanations, that help you learn, drill, and review for the CISSP certification exam.

Who This Book Is For

If you have studied the CISSP exam's content, and you believe that you are ready to put your knowledge to the test but you're not sure you want to take the actual exam yet, this book is for you! Maybe you have answered other practice questions or unsuccessfully taken the real exam, reviewed, and wanted to do more practice questions before retaking the exam. If so, this book is for you, too!

Be aware that *the CISSP exam is difficult and challenging*; therefore, this book shouldn't be your only vehicle for CISSP study. Because of the breadth and depth of knowledge needed to successfully pass the CISSP exam, be sure to use plenty of study material and use this book as a drill, review, and practice vehicle. It is recommended that you use this book with the *CISSP Exam Cram*, Third Edition, by Michael Gregg.

What You Will Find in This Book

This book is all about practice questions. It is divided into the ten domains that you find on the CISSP exam. Each chapter represents a domain, and each chapter has three elements:

- **Practice Questions:** This section includes numerous questions that help you learn, drill, and review.
- **Quick-Check Answer Key:** After you finish answering the questions, you can quickly grade your exam from this section. Only the correct answers are given here. No explanations are offered yet.
- **Answers and Explanations:** This section gives the correct answers and detailed explanations about the content posed in that question. Use this information to learn why an answer is correct and reinforce the content in your mind for exam day.

Hints for Using This Book

Because this book is a paper practice product, you might want to complete its exams on separate pieces of paper so that you can reuse the exams without having previous answers in your way. Also, a rule of thumb across all practice-question products is to make sure that you score into the high 90-percent range in all topics before attempting the actual exam. The higher you score on practice-question products, the better your chances of passing the real exam. Of course, we can't guarantee that you will receive a passing score on the real exam, but we can offer you plenty of opportunities to practice and assess your knowledge levels before you take the exam.

Pearson IT Certification Practice Test Engine and Questions on the CD

This book's accompanying CD includes the Pearson IT Certification Practice Test engine—software that displays and grades a set of exam-realistic multiple-choice questions. Using the Pearson IT Certification Practice Test engine, you can either study by going through the questions in Study Mode or take a simulated exam that mimics real exam conditions.

The installation process requires two major steps: installing the software and activating the exam. The CD has a recent copy of the Pearson IT Certification Practice Test engine. The practice exam—the database of exam questions—is not on the CD.

NOTE

The cardboard CD case in the back of this book includes the CD and a piece of paper. The paper lists the activation code for the practice exam associated with this book. *Do not lose the activation code.* On the opposite side of the paper from the activation code is a unique, one-time-use coupon code for the purchase of the Premium Edition eBook and Practice Test.

Install the Software from the CD

The Pearson IT Certification Practice Test is a Windows-only desktop application. You can run it on a Mac using a Windows virtual machine, but it was built specifically for the PC platform. The minimum system requirements are as follows:

- Windows XP (SP3), Windows Vista (SP2), or Windows 7
- Microsoft .NET Framework 4.0 client
- Microsoft SQL Server Compact 4.0
- Pentium class 1GHz processor (or equivalent)
- 512 MB RAM
- 650 MB disc space plus 50 MB for each downloaded practice exam

The software-installation process is routine compared with other software-installation processes. If you have already installed the Pearson IT Certification Practice Test software from another Pearson product, there is no need for you to reinstall the software. Simply launch the software on your desktop and proceed to activate the practice exam from this book by using the activation code that's included in the CD sleeve.

The following steps outline the installation process:

1. Insert the CD into your PC.
2. The software that automatically runs is the Pearson software to access and use all CD-based features, including the exam engine and the CD-only appendixes. From the main menu, click the **Install the Exam Engine** option.
3. Respond to Windows prompts, like you would with any typical software-installation process.

The installation process gives you the option to activate your exam with the activation code supplied on the paper in the CD sleeve. This process requires you to establish a Pearson website login. You need this login to activate the exam, so please register when prompted. If you already have a Pearson website login, there is no need to register again; just use your existing login.

Activate and Download the Practice Exam

After the exam engine is installed, you should then activate the exam associated with this book (if you did not do so during the installation process), as follows:

1. Start the Pearson IT Certification Practice Test software from the Windows **Start** menu or from your desktop shortcut icon.
2. To activate and download the exam associated with this book, from the **My Products** or **Tools** tab, select the **Activate** button.

3. At the next screen, enter the activation key from the paper inside the cardboard CD holder. Once entered, click the **Activate** button.
4. The activation process downloads the practice exam. Click **Next**, and then click **Finish**.

After the activation process is complete, the **My Products** tab should list your new exam. If you do not see the exam, make sure you have selected the **My Products** tab on the menu. At this point, the software and practice exam are ready to use. Simply select the exam and click the **Open Exam** button.

To update a particular exam that you have already activated and downloaded, simply select the **Tools** tab and select the **Update Products** button. Updating your exams ensures that you have the latest changes and updates to the exam data.

If you want to check for updates to the Pearson IT Certification Practice Test exam engine software, simply select the **Tools** tab and select the **Update Application** button. This ensures that you are running the latest version of the software engine.

Activating Other Exams

The exam software-installation process, and the registration process, has to happen only once. Then, for each new exam, only a few steps are required. For example, if you buy another new Pearson IT Certification Cert Guide or Cisco Press Official Cert Guide, extract the activation code from the CD sleeve in the back of that book—you don't even need the CD at this point. From there, all you have to do is start the exam engine (if it's not still up and running) and perform Steps 2 through 4 from the previous list.

Need Further Study?

If you have a difficult time correctly answering these questions, you probably need further review. Read the sister product to this book, *CISSP Exam Cram*, Third Edition (by Pearson), for further review.

8

CHAPTER EIGHT

Software Development Security

The Software Development Security domain is concerned with the security controls used by applications during their design, development, and use. Individuals studying this domain should understand the security and controls of application security, which includes the systems development process, application controls, and knowledge-based systems. Test candidates should also understand the concepts used to ensure data and application integrity. The following list gives you some specific areas of knowledge to be familiar with for the CISSP exam:

- SDLC (software development life cycle)
- Change (life cycle) management
- Database security
- Artificial Intelligence systems
- Mobile code
- Malware, viruses, and worms

Quick Check

Practice Questions

1. Which of the following is *not* a valid database management system model?

   Quick Answer: **259**
   Detailed Answer: **260**

   ❍ **A.** The hierarchical database management system
   ❍ **B.** The structured database management system
   ❍ **C.** The network database management system
   ❍ **D.** The relational database management system

2. During which stage of the software development life cycle should security be implemented?

   Quick Answer: **259**
   Detailed Answer: **260**

   ❍ **A.** Development
   ❍ **B.** Project initiation
   ❍ **C.** Deployment
   ❍ **D.** Installation

3. In which software development life cycle phase do the programmers and developers become deeply involved and do the majority of the work?

   Quick Answer: **259**
   Detailed Answer: **260**

   ❍ **A.** System Design Specifications
   ❍ **B.** Software Development
   ❍ **C.** Operation and Maintenance
   ❍ **D.** Functional Design Analysis and Planning

4. In the software development life cycle, what is used to maintain changes to development or production?

   Quick Answer: **259**
   Detailed Answer: **260**

   ❍ **A.** Certification
   ❍ **B.** Audit control team
   ❍ **C.** Manufacturing review board
   ❍ **D.** Change control

5. What is the most-used type of database management system?

   Quick Answer: **259**
   Detailed Answer: **260**

   ❍ **A.** The hierarchical database management system
   ❍ **B.** The structured database management system
   ❍ **C.** The network database management system
   ❍ **D.** The relational database management system

6. Place the software development life cycle phases in the proper order.

   Quick Answer: **259**
   Detailed Answer: **260**

   ❍ **A.** Initiation, software development, functional design analysis, operation, installation, disposal

Quick Check

❍ **B.** Initiation, software development, functional design analysis, installation, operation, disposal

❍ **C.** Initiation, functional design analysis, software development, installation, operation, disposal

❍ **D.** Initiation, functional design analysis, software development, operation, installation, disposal

7. Which of the following statements about Java applets is correct?

Quick Answer: **259**
Detailed Answer: **260**

❍ **A.** They are downloaded from a server.

❍ **B.** They are not restricted in computer memory.

❍ **C.** They are run from the browser.

❍ **D.** They are executed by your system.

8. Which of the following is a valid system development methodology?

Quick Answer: **259**
Detailed Answer: **260**

❍ **A.** The spring model

❍ **B.** The spiral model

❍ **C.** The production model

❍ **D.** The Gantt model

9. Which of the following best describes the Waterfall model?

Quick Answer: **259**
Detailed Answer: **260**

❍ **A.** The Waterfall model states that development is built one stage at a time, at which point the results flow to the next stage.

❍ **B.** The Waterfall model states that development should progress in a parallel fashion, with a strong change control process being used to validate the process.

❍ **C.** The Waterfall model states that the development process proceeds in a series of discrete steps, each completed before proceeding to the next.

❍ **D.** The Waterfall model states that all the various phases of software development should proceed at the same time.

10. Your friend is trying to learn more about databases and their structure. She wants to know what a tuple is.

Quick Answer: **259**
Detailed Answer: **260**

❍ **A.** A description of the structure of the database

❍ **B.** A “row” in a relational database that might be viewed as being similar to a “record” in a flat file

❍ **C.** An ordered set of values within a row in the database table

❍ **D.** Something that uniquely identifies each row in a table

Quick Check

11. Which of the software development life cycle phases is the point at which new systems need to be configured and steps need to be taken to make sure that security features are being used in the intended way?

    ❍ **A.** System Design Specifications

    ❍ **B.** Operation and Maintenance

    ❍ **C.** Functional Design Analysis and Planning

    ❍ **D.** Installation and Implementation

Quick Answer: **259**
Detailed Answer: **260**

12. Your CISSP study group has asked you to research information about databases. Specifically, they want you to describe what metadata is. What is your response?

    ❍ **A.** Metadata is data that describes data.

    ❍ **B.** Metadata is the data used in knowledge-based systems.

    ❍ **C.** Metadata is used for fraud detection.

    ❍ **D.** Metadata is the data used for metadictionaries.

Quick Answer: **259**
Detailed Answer: **261**

13. Jamie, your assistant, is taking some classes on database controls and security features. She wants to know what aggregation is. How will you answer her?

    ❍ **A.** It is the process of combining data into large groups that can be used for data mining.

    ❍ **B.** It is the process of combining security privileges to gain access to objects that would normally be beyond your level of rights.

    ❍ **C.** It is the process of combining items of low sensitivity to produce an item of high sensitivity.

    ❍ **D.** It is the process of combining several databases to view a virtual table.

Quick Answer: **259**
Detailed Answer: **261**

14. What term describes users' ability to infer or deduce information about data at sensitivity levels for which they do not have access privileges or rights?

    ❍ **A.** Views

    ❍ **B.** Inference

    ❍ **C.** Channeled view

    ❍ **D.** Presumption

Quick Answer: **259**
Detailed Answer: **261**

15. Which of the following best describes a database schema?

    ❍ **A.** The structure of the database

    ❍ **B.** The capability of different versions of the same information to exist at different classification levels within the database

Quick Answer: **259**
Detailed Answer: **261**

Quick Check

❍ **C.** An ordered set of values within a row in the database table

❍ **D.** Something that uniquely identifies each row in a table

16. Which type of malware is considered self-replicating?

Quick Answer: **259**
Detailed Answer: **261**

❍ **A.** Boot sector

❍ **B.** Meme virus

❍ **C.** Script virus

❍ **D.** Worm

17. Ashwin is building your company's new data warehouse. In a meeting, he said, "Data in the data warehouse needs to be normalized." What does this mean?

Quick Answer: **259**
Detailed Answer: **261**

❍ **A.** Data is divided by a common value.

❍ **B.** Data is restricted to a range of values.

❍ **C.** Data is averaged.

❍ **D.** Redundant data is removed.

18. Which of the following best describes the term "data dictionary"?

Quick Answer: **259**
Detailed Answer: **261**

❍ **A.** A dictionary for programmers

❍ **B.** A database of databases

❍ **C.** A virtual table of the rows and tables from two or more combined databases

❍ **D.** A dictionary used within a database

19. Which of the following best describes data mining?

Quick Answer: **259**
Detailed Answer: **261**

❍ **A.** The use of data to analyze trends and support strategic decisions

❍ **B.** The use of data to determine how the information was collected and formatted

❍ **C.** The process of querying databases for metadata

❍ **D.** The process of adjusting the granularity of a database search

20. Jerry has top-secret access to a database and can see that the USS *Yorktown* has left for Iraq. Ted has only public access to the same database. He can see that the ship has left port. However, the record shows that it is bound for Spain. What is this called?

Quick Answer: **259**
Detailed Answer: **261**

❍ **A.** Polyinstantiation

❍ **B.** Tuple

❍ **C.** Schema

❍ **D.** Knowledgebase system

Quick Check

21. Which of the software development life cycle phases is the point at which a project plan is developed, test schedules are assigned, and expectations of the product are outlined?

Quick Answer: **259**
Detailed Answer: **261**

- ❍ **A.** Software Development
- ❍ **B.** Functional Design Analysis and Planning
- ❍ **C.** Project Initiation
- ❍ **D.** System Design Specifications

22. Data checks and validity checks are examples of what type of application controls?

Quick Answer: **259**
Detailed Answer: **261**

- ❍ **A.** Preventive
- ❍ **B.** Constructive
- ❍ **C.** Detective
- ❍ **D.** Corrective

23. Which of the following is *not* a valid form of application control?

Quick Answer: **259**
Detailed Answer: **261**

- ❍ **A.** Preventive
- ❍ **B.** Constructive
- ❍ **C.** Detective
- ❍ **D.** Corrective

24. What document guarantees the quality of a service to a subscriber by a network service provider, setting standards on response times, available bandwidth, and system up times?

Quick Answer: **259**
Detailed Answer: **261**

- ❍ **A.** Service-level agreement
- ❍ **B.** Service agreement
- ❍ **C.** Business continuity agreement
- ❍ **D.** Business provider agreement

25. Which of the following is *not* one of the three main components of a SQL database?

Quick Answer: **259**
Detailed Answer: **261**

- ❍ **A.** Views
- ❍ **B.** Schemas
- ❍ **C.** Tables
- ❍ **D.** Object-oriented interfaces

26. Cyclic redundancy checks, structured walk-throughs, and hash totals are examples of what type of application controls?

Quick Answer: **259**
Detailed Answer: **261**

- ❍ **A.** Detective
- ❍ **B.** Preventive
- ❍ **C.** Error checking
- ❍ **D.** Parity

Quick Check

27. Christine has been alerted by her IDS that a web server on her network was attacked. While examining a trace of the ICMP traffic, she noticed that the attacker's packets were addressed to the network broadcast address and were spoofed to be from her web server. What type of attack has she been subjected to?

Quick Answer: **259**
Detailed Answer: **262**

❍ **A.** Smurf
❍ **B.** LAND
❍ **C.** Fraggle
❍ **D.** SYN flood

28. Which of the following best describes the OS protection mechanism that mediates all access that subjects have to objects to ensure that the subjects have the necessary rights to access the objects?

Quick Answer: **259**
Detailed Answer: **262**

❍ **A.** Accountability control
❍ **B.** Reference monitor
❍ **C.** Security kernel
❍ **D.** Security perimeter

29. Which of the following describes mobile code?

Quick Answer: **259**
Detailed Answer: **262**

❍ **A.** Code that can be used on a handheld device
❍ **B.** Code that can be used on several different platforms, such as Windows, Mac, and Linux
❍ **C.** Code that can be executed within a network browser
❍ **D.** A script that can be executed within an Office document

30. Black Hat Bob has just attacked Widget, Inc.'s network. Although the attack he perpetrated did not give him access to the company's network, it did prevent legitimate users from gaining access to network resources. What type of attack did he launch?

Quick Answer: **259**
Detailed Answer: **262**

❍ **A.** Spoofing
❍ **B.** TOC/TOU
❍ **C.** ICMP redirect
❍ **D.** DoS

31. Java-enabled web browsers allow Java code to be embedded in a web page, downloaded across the Net, and run on a local computer. This makes the security of the local computer a big concern. With this in mind, how does the Java runtime system ensure secure execution of the Java code?

Quick Answer: **259**
Detailed Answer: **262**

❍ **A.** Digital certificates
❍ **B.** Sandbox
❍ **C.** Applet boundaries
❍ **D.** Defense-in-depth

Quick Check

32. Chandra wants to learn more about the Software Capability Maturity Model. Help her put the five levels of this model in the proper order, from 1 to 5.

Quick Answer: **259**
Detailed Answer: **262**

❍ **A.** Initiating, defined, repeatable, optimizing, managed

❍ **B.** Initiating, defined, repeatable, managed, optimizing

❍ **C.** Initiating, repeatable, defined, managed, optimizing

❍ **D.** Initiating, repeatable, defined, optimizing, managed

33. Which of the following Software CMM levels is the step at which project management processes and practices are institutionalized and locked into place by policies, procedures, and guidelines?

Quick Answer: **259**
Detailed Answer: **262**

❍ **A.** Defined

❍ **B.** Repeatable

❍ **C.** Initiating

❍ **D.** Managed

34. Which of the following technologies establishes a trust relationship between the client and the server by using digital certificates to guarantee that the server is trusted?

Quick Answer: **259**
Detailed Answer: **262**

❍ **A.** ActiveX

❍ **B.** Java

❍ **C.** Proxy

❍ **D.** Agent

35. What is the process of cataloging all versions of a component configuration called?

Quick Answer: **259**
Detailed Answer: **262**

❍ **A.** The configuration library

❍ **B.** The component library

❍ **C.** The catalog database

❍ **D.** The software component library

36. Which of the following best describes a covert storage channel?

Quick Answer: **259**
Detailed Answer: **262**

❍ **A.** It is a communication channel that violates normal communication channels.

❍ **B.** It is a storage process that writes to storage in an unauthorized manner that typically is undetectable and written through an unsecure channel.

❍ **C.** It is a communication path that allows two processes to access the same storage and allows the contents to be read through a separate, less-secure channel.

❍ **D.** It is a storage process that requires the application of a root kit.

Quick Check

37. Which of the following is *not* one of the three ways in which inference can be achieved?

Quick Answer: **259**
Detailed Answer: **262**

❍ **A.** Preventive

❍ **B.** Deductive

❍ **C.** Abductive

❍ **D.** Statistical

38. Raj has been studying database security features. He reads that two control policies are used to protect relational databases. He remembers that one is MAC, but he has forgotten the second one. Which one is it?

Quick Answer: **259**
Detailed Answer: **263**

❍ **A.** PAC

❍ **B.** DAC

❍ **C.** SAC

❍ **D.** RBAC

39. Boyd just downloaded a game from a peer-to-peer network. Although the game seemed to install OK, his computer now is acting strangely. The mouse cursor moves by itself, URLs are opening on their own, and his web camera keeps turning itself on. What has happened?

Quick Answer: **259**
Detailed Answer: **263**

❍ **A.** A logic bomb was installed.

❍ **B.** A RAT (Remote-Access Trojan) was installed.

❍ **C.** A DDoS client was installed.

❍ **D.** An email virus was installed.

40. What is the goal of CRM?

Quick Answer: **259**
Detailed Answer: **263**

❍ **A.** To learn the behavior and buying habits of your customers

❍ **B.** To search for recurrences in data that can aid in making predictions about future events

❍ **C.** To uncover events that are interconnected

❍ **D.** To hunt for instances of events that are followed up by other events after a certain period

41. What technology is based on the methods by which the human brain is believed to work?

Quick Answer: **259**
Detailed Answer: **263**

❍ **A.** Neutron networks

❍ **B.** Fuzzy logic

❍ **C.** Neuron networks

❍ **D.** Neural technology

Quick Check

42. Now that your organization is preparing to retire its mainframe systems, you are asked to look at a distributed system as the replacement. What five requirements should a distributed system meet?

Quick Answer: **259**
Detailed Answer: **263**

- ❍ **A.** Interoperability, scalability, transparency, extensibility, control
- ❍ **B.** Interoperability, portability, transparency, extensibility, security
- ❍ **C.** Interoperability, portability, transparency, extensibility, control
- ❍ **D.** Interoperability, scalability, transparency, extensibility, security

43. George receives an email that did not come from the individual listed in the email. What is the process of changing email message names to look as though they came from someone else?

Quick Answer: **259**
Detailed Answer: **263**

- ❍ **A.** Spoofing
- ❍ **B.** Masquerading
- ❍ **C.** Relaying
- ❍ **D.** Redirecting

44. Raj is still studying database design and security. Can you tell him what cardinality means?

Quick Answer: **259**
Detailed Answer: **263**

- ❍ **A.** The number of rows in a relation
- ❍ **B.** The number of fields in a relation
- ❍ **C.** The number of attributes in a field
- ❍ **D.** The number of attributes in a relation

45. Wes asks you to help him prepare a practice test for your CISSP study group. Can you tell him which of the following relationships is incorrect?

Quick Answer: **259**
Detailed Answer: **263**

- ❍ **A.** Relation = table
- ❍ **B.** Record = attribute
- ❍ **C.** Tuple = row
- ❍ **D.** Attribute = column

46. Joey has been reading about databases and application security. He has asked you to define perturbation for him. Which of the following offers the best answer?

Quick Answer: **259**
Detailed Answer: **263**

- ❍ **A.** It is used to protect against polyinstantiation.
- ❍ **B.** It is a tool used to prevent aggregation.
- ❍ **C.** It is a tool used to aid in data mining.
- ❍ **D.** It is a tool used to fight inference attacks.

Quick Check

47. SubSeven and NetBus typically are placed in which of the following categories?

Quick Answer: **259**
Detailed Answer: **263**

❍ **A.** Virus

❍ **B.** Trapdoor

❍ **C.** Backdoor

❍ **D.** Malware

48. Jennifer's network has been hit by the following attack pattern: The attacker made many connection attempts to FTP. Each time, the handshake was not completed, and the source addresses were spoofed. The result was that legitimate users could not FTP to that computer. Which type of attack does this attack pattern match?

Quick Answer: **259**
Detailed Answer: **263**

❍ **A.** ACK attack

❍ **B.** Teardrop

❍ **C.** Fraggle

❍ **D.** SYN flood

49. What is the point in the software development life cycle phase at which information may need to be archived or discarded and a team may be assembled to examine ways to improve subsequent iterations of this or other products?

Quick Answer: **259**
Detailed Answer: **263**

❍ **A.** Revision and Replacement

❍ **B.** Functional Design Analysis and Planning

❍ **C.** Disposal and Postmortem Review

❍ **D.** System Design Specifications

50. Which type of virus can spread by multiple methods?

Quick Answer: **259**
Detailed Answer: **264**

❍ **A.** Multipartite

❍ **B.** Polymorphic

❍ **C.** Double partite

❍ **D.** Prolific

51. Polyinstantiation is a solution used by which of the following to remedy multiparty update conflicts?

Quick Answer: **259**
Detailed Answer: **264**

❍ **A.** Database locking

❍ **B.** SODA

❍ **C.** GREP

❍ **D.** Belief-based model

Quick Check

52. The following security labels exist on a network operating in a multilevel security mode:

Quick Answer: **259**
Detailed Answer: **264**

Label	Jack	John	File A	File B	File C	File D
Sensitivity	Top-Secret	Secret	Secret	Secret	Top-Secret	Top-Secret
Categories	North	East	East	East	East	North
	South	West		West		West
	East					
	West					

Jack edits file B and file C simultaneously and then saves both. Which files can John now access?

❍ **A.** Files A, B, C, and D

❍ **B.** Files A, B, and C

❍ **C.** Files A and B

❍ **D.** File A

53. Which generation of code development is most likely to focus on constraints?

Quick Answer: **259**
Detailed Answer: **264**

❍ **A.** Generation 5

❍ **B.** Generation 4

❍ **C.** Generation 3

❍ **D.** Generation 2

54. The network administrator has been analyzing network reports and is convinced that the network has been the victim of a SYN flooding DoS attack. What evidence might have been discovered that would support this conclusion?

Quick Answer: **259**
Detailed Answer: **264**

❍ **A.** Customers reporting that their connection requests were rerouted to a malicious web server

❍ **B.** The web server crashing with each request

❍ **C.** Excessive traffic on the front-end load-balancing servers

❍ **D.** IDS logs of incoming malformed packets

55. Which language, when used for development of your company's front-end application, results in a program that is least likely to have vulnerable code?

Quick Answer: **259**
Detailed Answer: **264**

❍ **A.** Machine code

❍ **B.** Assembler code

❍ **C.** C code

❍ **D.** SQL code

Quick Check

56. In your corporation, it is critical that the metadata surrounding business data be revealed to only the proper authorities, even though all employees require access to the business data. Access to the metadata is being controlled through the use of views so that only the appropriate authorities have deeper access. What is this technique called?

Quick Answer: **259**
Detailed Answer: **264**

- ❍ **A.** Encapsulation
- ❍ **B.** Polymorphism
- ❍ **C.** Instantiation
- ❍ **D.** Abstraction

57. To prevent covert channels via race conditions, it is critical that software modules be able to execute independently of each other. What is this called?

Quick Answer: **259**
Detailed Answer: **264**

- ❍ **A.** Low coupling and low cohesion
- ❍ **B.** Low coupling and high cohesion
- ❍ **C.** High coupling and low cohesion
- ❍ **D.** High coupling and high cohesion

58. Expert systems use forward and reverse chaining that is based on what?

Quick Answer: **259**
Detailed Answer: **264**

- ❍ **A.** The inference engine
- ❍ **B.** Certainty factors
- ❍ **C.** The rulebase
- ❍ **D.** Neural structures

59. What is the most common problem related to audit logs?

Quick Answer: **259**
Detailed Answer: **264**

- ❍ **A.** Audit logs can be examined only by auditors.
- ❍ **B.** Audit logs use parsing tools that distort the true record of events.
- ❍ **C.** Audit logs are not backed up.
- ❍ **D.** Audit logs are collected but not analyzed.

60. When you're dealing with mobile code and wireless devices, many security issues can arise. For example, when you're working with wireless devices that are using Wireless Application Protocol (WAP), which of the following is the primary security concern?

Quick Answer: **259**
Detailed Answer: **265**

- ❍ **A.** WAP is not a secure protocol.
- ❍ **B.** The web server that the wireless device is communicating with via SSL may have vulnerabilities.
- ❍ **C.** The wireless device may have vulnerabilities in its OS.
- ❍ **D.** The WAP gateway can be targeted by attackers.

Quick Check

61. Which generation(s) of code is/are most likely to focus on the logic of the algorithms?

❍ **A.** Generation 5

❍ **B.** Generations 2, 3, and 4

❍ **C.** Generations 1 and 2

❍ **D.** Generations 1 and 5

Quick Answer: **259**
Detailed Answer: **265**

62. Which type of database combines related records and fields into a logical tree structure?

❍ **A.** Relational

❍ **B.** Hierarchical

❍ **C.** Object-oriented

❍ **D.** Network

Quick Answer: **259**
Detailed Answer: **265**

63. What type of database is unique because it can have multiple records that can be either parent or child?

❍ **A.** Relational

❍ **B.** Hierarchical

❍ **C.** Object-oriented

❍ **D.** Network

Quick Answer: **259**
Detailed Answer: **265**

64. Your colleague wants to know when the best point within the software development life cycle (SDLC) is to create a list of potential security issues. What do you tell her?

❍ **A.** Feasibility

❍ **B.** Development

❍ **C.** Design

❍ **D.** Requirements

Quick Answer: **259**
Detailed Answer: **265**

65. Which of the following are correct?

I. The object linking and embedding database (OLE DB) is a replacement for open database connectivity (ODBC).

II. ActiveX Data Objects (ADO) is an API that allows applications to access back-end database systems.

III. Java Database Connectivity is a markup standard that is self-defining and provides a lot of flexibility in how data within the database is presented.

IV. The data definition language (DDL) defines the structure and schema of the database.

Quick Answer: **259**
Detailed Answer: **265**

Quick Check

❍ **A.** I and IV

❍ **B.** II, III, and IV

❍ **C.** I, II, III, and IV

❍ **D.** I, II, and IV

66. How can referential integrity best be defined?

Quick Answer: **259**
Detailed Answer: **265**

❍ **A.** Structural and semantic rules are enforced.

❍ **B.** Semantic rules are enforced.

❍ **C.** Structural rules are enforced.

❍ **D.** All foreign keys reference existing primary keys.

67. Lenny is trying to determine how much money a new employee makes. His job in HR allows him to see total payroll by department but not by person. The individual he is curious about just started a month ago, so Lenny simply compares that department's previous month's total salary to the current month's total salary. What has Lenny just done?

Quick Answer: **259**
Detailed Answer: **265**

❍ **A.** Enumeration

❍ **B.** An inference attack

❍ **C.** Polyinstantiation

❍ **D.** Online transaction processing (OLTP)

68. While browsing the company directory, you notice that your address is incorrect. To rectify the situation, you decide to modify the database that holds this information. Although the change seems to work, you notice later that the information has reverted to the previous, incorrect information. What do you believe is the source of the problem?

Quick Answer: **259**
Detailed Answer: **265**

❍ **A.** The user does not have modification rights.

❍ **B.** The schema does not allow changes from the user's machine.

❍ **C.** Someone in personnel has put a lock on the cell.

❍ **D.** Replication integrity is inaccurate due to mismatched times.

69. Knowledge discovery is also known as what?

Quick Answer: **259**
Detailed Answer: **266**

❍ **A.** Data warehousing

❍ **B.** Metadata

❍ **C.** Data mining

❍ **D.** Atomicity

Quick Check

70. Which of the following statements are true?

Quick Answer: **259**
Detailed Answer: **266**

I. Data definition language (DDL) allows users to make requests of the database.

II. Data manipulation language (DML) maintains the commands that enable a user to view, manipulate, and use the database.

III. Query language (QL) defines the structure and schema of the database. The structure could mean the table size, key placement, views, and data element relationship.

IV. The report generator creates printouts of data in a user-defined manner.

❍ **A.** I and II

❍ **B.** II and IV

❍ **C.** II, III, and IV

❍ **D.** I, II, III, and IV

71. Jim's new job at the headquarters of a major grocery store has him examining buyer trends. He uses the database to find a relationship between beer and diapers. He discovers that men over 20 are the primary buyers of these two items together after 10 p.m. What best describes Jim's actions?

Quick Answer: **259**
Detailed Answer: **266**

❍ **A.** Data warehousing

❍ **B.** Metadata

❍ **C.** Data mining

❍ **D.** Atomicity

72. Your application developer has created a new module for a customer-tracking system. This module will result in greater productivity. The application has been examined and tested by a second person in the development group. A summary of the test shows no problems. Based on the results, which of the following is not a recommended best practice?

Quick Answer: **259**
Detailed Answer: **266**

❍ **A.** The new code should be passed to quality assurance personnel so that they can certify the application.

❍ **B.** The application should be placed into operations and implemented.

❍ **C.** An accrediting official should wait for the results of certification.

❍ **D.** All changes must be logged in the change management database (CMDB).

Quick Check

73. Which of the following describes verification and validation?

Quick Answer: **259**
Detailed Answer: **266**

- ○ **A.** Verification verifies that the product meets specifications. Validation is the completion of the certification and accreditation process.
- ○ **B.** Verification measures how well the program or application solves a real-world problem. Validation verifies that the product meets specifications.
- ○ **C.** Verification verifies that the product meets specifications. Validation measures how well the program or application solves a real-world problem.
- ○ **D.** Verification verifies that the program or application meets certification requirements. Validation verifies that the product received accreditation.

74. You are assigned to modify an application to address a specific problem with the current release of the program. When the change is complete, you notice that other modules that should not have been affected appear to be nonfunctional. What do you believe is the cause?

Quick Answer: **259**
Detailed Answer: **266**

- ○ **A.** The module has low cohesion.
- ○ **B.** The module has high cohesion.
- ○ **C.** The module is tightly coupled.
- ○ **D.** The module is loosely coupled.

75. Jake has become concerned that a citizen programmer in the group has developed code for others in the department. What should be your primary concern?

Quick Answer: **259**
Detailed Answer: **266**

- ○ **A.** That the programs are tested by others in the department
- ○ **B.** That the programs have not been certified and verified
- ○ **C.** That a copy of the code is held in a library
- ○ **D.** That the code is adequately commented

76. Which of the following statements is most correct?

Quick Answer: **259**
Detailed Answer: **266**

- ○ **A.** Relational database parents can have only one child.
- ○ **B.** A relational database is designed so that a child can have only one parent.
- ○ **C.** A hierarchical database is designed so that a parent can have only one child.
- ○ **D.** A hierarchical database is designed so that a child can have only one parent.

Quick Check

77. What level of the capability maturity model features quantitative process improvement?

Quick Answer: **259**
Detailed Answer: **266**

❍ **A.** Managed

❍ **B.** Defined

❍ **C.** Repeatable

❍ **D.** Optimized

78. Your company has just signed a software escrow agreement. Which of the following best describes this document?

Quick Answer: **259**
Detailed Answer: **266**

❍ **A.** An offsite backup

❍ **B.** A form of maintenance agreement

❍ **C.** A form of insurance

❍ **D.** A clustered software service

79. With regard to database operations, canceling a set of changes and restoring the database to its prior state is called what?

Quick Answer: **259**
Detailed Answer: **267**

❍ **A.** Savepoint

❍ **B.** Commit

❍ **C.** Rollback

❍ **D.** Audit point

80. The capability maturity model features five maturity levels that begin with initial. What is the proper order of the remaining four levels?

Quick Answer: **259**
Detailed Answer: **267**

❍ **A.** Repeatable, defined, managed, optimized

❍ **B.** Managed, repeatable, defined, optimized

❍ **C.** Repeatable, managed, defined, optimized

❍ **D.** Defined, optimized, repeatable, managed

81. Data that describes other data is called what?

Quick Answer: **259**
Detailed Answer: **267**

❍ **A.** Metadata

❍ **B.** Nonatomic data

❍ **C.** Data structure

❍ **D.** Transaction processing

82. In which database model do you perceive the database as a set of tables that are composed of rows and columns?

Quick Answer: **259**
Detailed Answer: **267**

❍ **A.** Hierarchical

❍ **B.** Network

❍ **C.** Relational

❍ **D.** Object

Quick Check

83. With a relational database management system, you can constrain what a particular application or user sees by using what?

Quick Answer: **259**
Detailed Answer: **267**

- ❍ **A.** Schema
- ❍ **B.** Device media control language (DMCL)
- ❍ **C.** Data mine
- ❍ **D.** Database view

84. Security controls must be considered at which phases of the software life cycle?

Quick Answer: **259**
Detailed Answer: **267**

- ❍ **A.** Design analysis, software development, installation, and implementation
- ❍ **B.** Project initiation, software development, and operation maintenance
- ❍ **C.** Design specifications
- ❍ **D.** All of the above

85. The change control process is structured so that various steps must be completed to verify that no undocumented, unapproved, or untested changes are implemented. Which of the following is the final step?

Quick Answer: **259**
Detailed Answer: **267**

- ❍ **A.** Configure the hardware properly.
- ❍ **B.** Update documentation and manuals.
- ❍ **C.** Inform users of the change.
- ❍ **D.** Report the change to management.

86. You are asked to develop an advanced program that will interact with users. You are asked to look at knowledge-based systems. As such, expert systems use what type of information to make a decision?

Quick Answer: **259**
Detailed Answer: **267**

- ❍ **A.** `if...then` statements
- ❍ **B.** Weighted computations
- ❍ **C.** A process similar to that used by the human brain (reasoning)
- ❍ **D.** Weighted computations based on previous results

87. Which of the following is considered a middleware technology?

Quick Answer: **259**
Detailed Answer: **267**

- ❍ **A.** Atomicity
- ❍ **B.** OLE
- ❍ **C.** CORBA
- ❍ **D.** Object-oriented programming

Quick Check

88. The CMMI contains how many process areas?

Quick Answer: **259**
Detailed Answer: **267**

- ❍ **A.** 4
- ❍ **B.** 5
- ❍ **C.** 20
- ❍ **D.** 22

89. At which level of the CMM are processes likely to be variable (inconsistent) and depend heavily on institutional knowledge?

Quick Answer: **259**
Detailed Answer: **268**

- ❍ **A.** Level 1
- ❍ **B.** Level 2
- ❍ **C.** Level 3
- ❍ **D.** Level 4

90. When dealing with expert systems, which of the following are valid methods for reasoning when using inference rules?

Quick Answer: **259**
Detailed Answer: **268**

I. Forward chaining

II. Knowledge transparency

III. Backward chaining

IV. Knowledge representation

- ❍ **A.** II
- ❍ **B.** I and III
- ❍ **C.** I and IV
- ❍ **D.** I, II, III, and IV

91. Which of the following is a project-development method that uses pairs of programmers who work off of detailed specifications?

Quick Answer: **259**
Detailed Answer: **268**

- ❍ **A.** Waterfall
- ❍ **B.** Spiral
- ❍ **C.** Extreme
- ❍ **D.** RAD

92. Jake is using a commercial program that is free to use without pay with only limited functionality. This is most correctly called what?

Quick Answer: **259**
Detailed Answer: **268**

- ❍ **A.** Commercial software
- ❍ **B.** Freeware
- ❍ **C.** Shareware
- ❍ **D.** Crippleware

Quick Check

93. Which of the following can best be described as byte-code?

❍ **A.** Java

❍ **B.** Assembly

❍ **C.** C language

❍ **D.** Fortran

Quick Answer: **259**
Detailed Answer: **268**

94. Which of the following is an example of open vendor-neutral middleware?

❍ **A.** OOA

❍ **B.** COM

❍ **C.** CORBA

❍ **D.** OOD

Quick Answer: **259**
Detailed Answer: **268**

95. Which of the following allows objects written with different OOP languages to communicate?

❍ **A.** OOA

❍ **B.** COM

❍ **C.** OOD

❍ **D.** CORBA

Quick Answer: **259**
Detailed Answer: **268**

Practice Questions (True or False)

96. SQL is an example of a 4GL language.

❍ True

❍ False

Quick Answer: **259**
Detailed Answer: **268**

97. 5GL languages are designed to categorize assembly languages.

❍ True

❍ False

Quick Answer: **259**
Detailed Answer: **268**

98. The prototyping model is based on the concept that software development is evolutionary.

❍ True

❍ False

Quick Answer: **259**
Detailed Answer: **268**

99. Reengineering attempts to update software by reusing as many of the components as possible instead of designing an entirely new system. Reverse engineering is a technique that can be used to decrease development time by compiling existing code.

❍ True

❍ False

Quick Answer: **259**
Detailed Answer: **268**

Quick Check

100. Programmers should strive to develop modules that have high cohesion and low coupling.

❍ True

❍ False

Quick Answer: **259**
Detailed Answer: **268**

101. Entity relationship diagrams (ERDs) can be used to help define a data dictionary.

❍ True

❍ False

Quick Answer: **259**
Detailed Answer: **268**

102. Web-based application development (WBAD) is an application development technology that is used with technologies such as Extensible Markup Language (XML).

❍ True

❍ False

Quick Answer: **259**
Detailed Answer: **268**

103. Today, prototyping is rarely used because it costs development time and money.

❍ True

❍ False

Quick Answer: **259**
Detailed Answer: **269**

104. Zeroization is as effective as purging.

❍ True

❍ False

Quick Answer: **259**
Detailed Answer: **269**

Practice Questions (Mix and Match)

105. Match each virus term with its definition.

A. Stealth: _____

B. Meme: _____

C. Macro: _____

D. EICAR: _____

E. Encrypted virus: _____

1. Used by attacks such as “I love you” and Melissa

2. Can modify functionality, so detection is very difficult

3. Similar to a polymorphic virus but can change how the virus is stored on the disk

4. Used to verify the functionality of antivirus software

5. Somewhat like a chain letter or pyramid scheme

Quick Answer: **259**
Detailed Answer: **269**

Quick Check Answer Key

1. B
2. B
3. B
4. D
5. D
6. C
7. B
8. B
9. C
10. C
11. B
12. A
13. C
14. B
15. A
16. D
17. D
18. B
19. A
20. A
21. B
22. A
23. B
24. A
25. D
26. A
27. A
28. B
29. C
30. D
31. B
32. C
33. B
34. A
35. A
36. C
37. A
38. B
39. B
40. A
41. D
42. B
43. B
44. A
45. B
46. D
47. C
48. D
49. C
50. A
51. B
52. C
53. A
54. C
55. D
56. B
57. B
58. A
59. D
60. D
61. B
62. B
63. D
64. D
65. D
66. D
67. B
68. D
69. C
70. B
71. C
72. B
73. C
74. A
75. B
76. D
77. B
78. C
79. C
80. A
81. A
82. C
83. D
84. D
85. D
86. A
87. C
88. D
89. A
90. B
91. C
92. D
93. A
94. C
95. B
96. True
97. False
98. False
99. False
100. True
101. True
102. True
103. False
104. False
105. **A.** 2
B. 5
C. 1
D. 4
E. 3

Answers and Explanations

1. **Answer: B.** The structured database management system model is not a valid type. Four common database types are the hierarchical database management system, the object-oriented database management system, the network database management system, and the relational database management system.

2. **Answer: B.** Security should be implemented at the initiation of a project. When security is added during the project initiation phase, substantial amounts of money can be saved. Because the first phase is the project initiation phase, all other answers are incorrect.

3. **Answer: B.** Software Development is the point in the SDLC at which programmers and developers become deeply involved and provide the majority of the work.

4. **Answer: D.** Change control is used to maintain changes to development or production. Without it, control would become very difficult, because there would be no way to track changes that might affect the product's functionality or security.

5. **Answer: D.** The relational database management system is the most used type. It is structured such that the columns represent the variables and the rows contain the specific instance of data.

6. **Answer: C.** The complete list of software development life cycle phases is as follows:

   Project Initiation

   Functional Design Analysis and Planning

   System Design Specifications

   Software Development

   Installation and Implementation

   Operation and Maintenance

   Disposal

7. **Answer: B.** Java is downloaded from the server, executed by the browser, and run on your system. Java has limits placed on what it can do by means of a sandbox and was originally designed with restrictions on what could be done while loaded in memory. Originally their activities were restricted in memory and could not access certain parts of memory or access files or initiate network connections.

8. **Answer: B.** The spiral model is the only valid software development methodology listed. It was developed in 1988 at TRW.

9. **Answer: C.** The Waterfall model states that the development process proceeds in a series of discrete steps, each completed before proceeding to the next.

10. **Answer: C.** A tuple is an ordered set of values within a row in the database table.

11. **Answer: B.** The Operation and Maintenance phase of the SDLC is the point at which new systems need to be configured and steps need to be taken to make sure that no new vulnerabilities or security compromises take place. It is also at this step that if major changes are made to the system, network, or environment, the certification and accreditation process may need to be repeated.

12. **Answer: A.** Metadata is data about data that is used in data-mining and data-warehouse operations. Metadata is not used in knowledge-based systems, for fraud detection, or for data dictionaries.

13. **Answer: C.** Aggregation is the process of combining items of low sensitivity to produce an item of high sensitivity. It has the potential to be a rather large security risk.

14. **Answer: B.** Inference occurs when users can put together pieces of information at one security level to determine a fact that should be protected at a higher security level.

15. **Answer: A.** The schema is the structure of the database.

16. **Answer: D.** The greatest danger of worms is their capability to self-replicate. Left unchecked, this process can grow in volume to an astronomical amount. For example, a worm could send copies of itself to everyone listed in your email address book, and those recipients' computers would then do the same.

17. **Answer: D.** Normalization is the process of removing redundant data. It speeds the analysis process. Normalization is not the process of dividing by a common value, restricting to a range of values, or averaging the data.

18. **Answer: B.** A data dictionary contains a list of all database files. It also contains the number of records in each file and each field name and type.

19. **Answer: A.** Data mining is used to analyze trends and support strategic decisions. It enables complicated business processes to be understood and analyzed. This is achieved through the discovery of patterns in the data relating to the past behavior of business processes or subjects. These patterns can be used to improve the performance of a process by exploiting favorable patterns.

20. **Answer: A.** Polyinstantiation allows different versions of the same information to exist at different classification levels within a database. This permits a security model that can have multiple views of the same information, depending on your clearance level.

21. **Answer: B.** The Functional Design Analysis and Planning stage of the SDLC is the point at which a project plan is developed, test schedules are assigned, and expectations of the product are outlined.

22. **Answer: A.** Application controls are used to enforce an organization's security policy and procedures. Preventive application controls include data checks, validity checks, contingency planning, and backups. Answers C and D are incorrect because they are not controls, and answer B is a distracter.

23. **Answer: B.** The three valid types of application controls are preventive, corrective, and detective.

24. **Answer: A.** A service-level agreement is used to set the standards of service you expect to receive. It includes items such as response times, system utilization rates, the number of online users, available bandwidth, and system up times.

25. **Answer: D.** The three main components of SQL databases are schemas, tables, and views. Object-oriented interfaces are part of object-oriented database management systems.

26. **Answer: A.** Cyclic redundancy checks, structured walk-throughs, and hash totals are all examples of detective application controls. Application controls are used to enforce the organization's security policy and procedures. They can be preventive, detective, or corrective.

27. **Answer: A.** A smurf attack targets the network broadcast address and spoofs the source address to be from the computer to be attacked. The result is that the network amplifies the attack and floods the local device with the resulting broadcast traffic.

28. **Answer: B.** The reference monitor is the OS component that enforces access control and verifies that the user has the rights and privileges to access the object in question.

29. **Answer: C.** Mobile code is code that can be executed within a network browser. Applets are examples of mobile code. Mobile code is not used on a handheld device, nor is it a script that is executed in an Office document. And although mobile code may run on several different platforms, answer B is an incomplete answer.

30. **Answer: D.** A DoS (denial of service) attack does not give Black Hat Bob access to the network; it does, however, prevent others from gaining legitimate access. Spoofing is the act of pretending to be someone you are not. ICMP redirects can be used to route information to an alternative location. TOC/TOU attacks deal with the change of information between the time it was initially checked and the time it was used.

31. **Answer: B.** The sandbox is a set of security rules that are put in place to prevent Java from having unlimited access to memory and OS resources. It creates an environment in which there are strict limitations on what the Java code can request or do.

32. **Answer: C.** The Software Capability Maturity Model (CMM) was first developed in 1986 and is composed of the following five maturity levels:

    Initiating

    Repeatable

    Defined

    Managed

    Optimizing

33. **Answer: B.** The Software CMM is composed of five maturity levels. The Repeatable maturity level is the step at which project management processes and practices are institutionalized and locked in place by procedures, protocols, and guidelines.

34. **Answer: A.** ActiveX establishes a trust relationship between the client and server by using digital certificates to guarantee that the server is trusted. The shortcoming of ActiveX is that security is really left to the end user. Users are prompted if any problems are found with a certificate. Therefore, even if the certificate is invalid, a user can override good policy by simply accepting the possibly tainted code.

35. **Answer: A.** The configuration library is the process of cataloging all versions of a component configuration.

36. **Answer: C.** A covert storage channel is a communication path that writes to storage by one process and allows the contents to be read through another, less-secure channel. Answer A describes a covert channel. Answers B and D are distracters.

37. **Answer: A.** Inference occurs when a user with low-level access to data can use this access to infer information or knowledge that is not authorized. The three inference channels are deductive, abductive, and statistical.

38. **Answer: B.** Relational databases use one of two control policies to secure information on multilevel systems: MAC (mandatory access control) and DAC (discretionary access control). Answers A and C are distracters. RBAC (role-based access control) is not used in multilevel relational databases.

39. **Answer: B.** It is very likely that the game Boyd installed was bundled with a RAT (Remote-Access Trojan). The executable seems accessible, but after installation is performed, the Trojan program is loaded into the victim's computer. RATs can control programs because backdoors turn on hardware, open CD-ROM drives, and perform other malicious and ill-willed acts.

40. **Answer: A.** CRM (customer relationship management) is used in conjunction with data mining. The goal of CRM is to learn the behaviors of your customers. Businesses believe that by learning more about their customers, they can provide higher-quality customer service, increase revenues, and switch to more efficient sales techniques. Answer B describes forecasting, answer C describes associations, and answer D describes sequences.

41. **Answer: D.** Neural technology simulates the neural behavior of the human brain. The objective is for a computer to be able to learn to differentiate or model without formal analysis and detailed programming. These systems are targeted to be used in risk management, IDS, and forecasting. Fuzzy logic focuses on how humans think and is used in insurance and financial markets, where there is some uncertainty about the data. Answers A and C are distracters.

42. **Answer: B.** Interoperability, portability, transparency, extensibility, and security are the five requirements that all distributed systems should meet.

43. **Answer: B.** Masquerading is the act of changing email messages to look as though they came from someone else. Spoofing typically involves IP addresses. Relaying occurs when email is sent through an uninvolved third party. Redirecting is the process of sending data to a destination to which it may not have been addressed.

44. **Answer: A.** Cardinality is the number of rows in a relation.

45. **Answer: B.** Answers A, C, and D all represent a valid relationship. Answer B does not, because records are synonymous with rows and tuples, not attributes.

46. **Answer: D.** Perturbation is also called noise and is used as a tool to fight inference attacks. It works by infusing phony information into a database. The goal is to frustrate the attacker so that he or she will give up and move on to an easier target.

47. **Answer: C.** Backdoor programs include SubSeven, NetBus, Back Orifice, and Beast. These programs are characterized by their design. They use two separate components: a server, which is deployed to the victim, and a client, which the attacker uses to control the victim's computer.

48. **Answer: D.** A SYN attack is characterized by a series of TCP SYNs. Each SYN uses a small amount of memory. If the attacker sends enough of these spoofed SYN packets, the victim's machine fills up its queue and does not have adequate resources to respond to legitimate computers, denying other systems service from the victim's computer.

49. **Answer: C.** The Disposal and Postmortem Review phase of the SDLC is the point at which information may need to be archived or discarded. A postmortem team may be assembled to examine ways to improve subsequent iterations of this or other products.

50. **Answer: A.** Multipartite viruses can spread by many different methods. Polymorphic viruses can change themselves over time.

51. **Answer: B.** SODA (Secure Object-Oriented Database) allows the use of polyinstantiation as a solution to the multiparty update conflict. This problem is caused when users of various levels of clearance and sensitivity in a secure database system attempt to use the same information.

52. **Answer: C.** The suggestion here is that Jack somehow contaminated File B and caused it to be raised to a higher security level after he saved it. However, in Mandatory Access Control, a label cannot be changed after it is assigned (or it would be discretionary). John has access to files A and B based on his security clearance (sensitivity label) and need to know (categories) both before and after Jack's edit.

53. **Answer: A.** Fifth-generation languages (LISP, Prolog) are most focused on the logic of constraints. Fourth-generation (SQL, ColdFusion), third-generation (COBOL, Java), and second-generation (Assembly, Byte Code) are focused on the logic of algorithms.

54. **Answer: C.** SYN flooding is a resource attack on bandwidth. The attack does not involve malformed packets. The intent of the flood is to use up all the bandwidth so that legitimate incoming requests cannot be processed (not redirected). This flooding could result in excessive traffic on the front-end, load-balancing servers that seek to balance incoming requests between multiple back-end processing servers. Although crashing the server is not the ultimate goal of the attack, there is the possibility that this could occur.

55. **Answer: D.** The higher the level of language you use when programming, the less likely it is that the code will have unintended flaws that can be attacked. Instead of using C, you should use C++, but both of these are third-generation languages (3GL). SQL is a fourth-generation language (4GL).

56. **Answer: B.** Polymorphism is the ability to present data in a different light depending on the needs of the moment. Encapsulation is when an object has knowledge of functions and traits it requires so that other routines can access the object via standard function calls. Instantiation is the creation of an object based on its rule set. Abstraction refers to the suppression of unnecessary details but not the changing of details.

57. **Answer: B.** Low coupling means that the modules transfer data directly to each other without transferring data through a lot of other modules. High cohesion means that modules stand alone well by handling their own requirements and without calling other modules. High coupling and low cohesion are present when modules depend heavily on each other, leading to race conditions in which multiple modules could be vying for the same resource.

58. **Answer: A.** The inference engine creates the forward and reverse chains. Certainty factors reflect a confidence level that permits the chaining to occur. The rulebase describes what is known. Neural structures belong in artificial neural networks, not expert systems.

59. **Answer: D.** One of the most common problems with audit logs is that they are collected but not analyzed. Often, no one is interested in the audit logs until someone reports a problem. Even though it isn't a technical problem, this is an administrative and policy issue, because no analysis takes place. Answers A, B, and C are all important concerns but are not the most common problem.

60. **Answer: D.** The primary vulnerability is the WAP gateway. WAP requires some type of conversion, and this conversion is performed on the gateway. This means that, for a short period of time, the data is in a clear format while being converted from WAP to SSL, TLS, or another encrypted format. This makes the gateway an attractive target. Answers A, B, and C are incorrect because they do not represent the level of risk that the gateway does.

61. **Answer: B.** Fourth-generation (SQL, ColdFusion), third-generation (COBOL, Java), and second-generation (Assembly, Byte Code) are focused on the logic of algorithms. Fifth-generation languages (LISP, Prolog) are most focused on the logic of constraints. First-generation languages are written in machine language.

62. **Answer: B.** A hierarchical database combines related records and fields into a logical tree structure. A relational database uses columns and rows to organize the information. An object-oriented database is considered much more dynamic than earlier designs because it can handle not only data but also audio, images, and other file formats. A network database is unique in that it supports multiple parent or child records.

63. **Answer: D.** A network database is unique in that it supports multiple parent and child records. A relational database uses columns and rows to organize the information. A hierarchical database combines related records and fields into a logical tree structure. An object-oriented database is considered much more dynamic than earlier designs because it can handle not only data but also audio, images, and other file formats.

64. **Answer: D.** One of the primary reasons to use the SDLC is to build in security from the beginning. As such, security issues need to be identified as soon as possible. Although some issues can be worked out during feasibility, options are still open at that point, which makes final decisions impossible. Waiting until later to build in security simply adds to the cost.

65. **Answer: D.** Java Database Connectivity (JDC) is not a markup standard that is self-defining and provides a lot of flexibility in how data within the database is presented. JDC is an API communication mechanism for databases. Although it is true that the object linking and embedding database (OLE DB) is a replacement for open database connectivity (ODBC), ActiveX Data Objects (ADO) is an API that allows applications to access back-end database systems. The data definition language (DDL) defines the structure and schema of the database.

66. **Answer: D.** Referential integrity ensures that all foreign keys reference existing primary keys.

67. **Answer: B.** Inference is the ability to obtain privileged information that normally is unavailable. Enumeration is performed when the attacker gathers information about the network structure. It includes items such as what open shares and applications are available on a network. Polyinstantiation is the use of different information at different security levels. Online transaction processing is a mechanism used in databases to provide fault tolerance.

68. **Answer: D.** The most likely cause of the problem is invalid time synchronization. In a distributed environment, this can cause a server to overwrite newer data. If the change took a while to make, answer A cannot be correct. Answer B is incorrect because no change would be possible, even for a short period of time. Answer C is incorrect because it would be impossible for the user to make a change.

69. **Answer: C.** A knowledge discovery database (KDD) is also known as data mining. A data warehouse is used for data storage and can combine data from multiple sources. Metadata is used to discover the unseen relationships between data. Atomicity is used to divide works into units that are processed completely or not at all.

70. **Answer: B.** The correct statements are as follows: The data definition language (DDL) defines the structure and schema of the database. The data manipulation language (DML) contains all the commands that enable a user to manipulate, view, and use the database (view, add, modify, sort, and delete commands). The query language (QL) allows users to make requests of the database. The report generator creates printouts of data in a user-defined manner.

71. **Answer: C.** Jim is data mining—searching for unseen relationships. A data warehouse is used for data storage and can combine data from multiple sources. Metadata is used to discover the unseen relationships between data. Atomicity is used to divide work into units that are processed completely or not at all.

72. **Answer: B.** Before this significant change is made, the module should be technically tested (certification) and administratively approved (accreditation). Answers A, C, and D are all recommended best practices.

73. **Answer: C.** Verification verifies that the product meets specifications. Validation is the measurement of how well the program or application solves a real-world problem.

74. **Answer: A.** Cohesion and coupling are two items that need to be reviewed when creating code or modifying existing code. *Cohesion* is a module's ability to perform only a single precise task. *Coupling* refers to the amount of interaction. Both can have a significant effect on change management. Therefore, the goal is to work toward modules that have high cohesion and loose coupling.

75. **Answer: B.** Citizen (casual) programmers are people who can code but who do so from outside the SDLC process. The concern here is that they are writing programs and allowing others within the department to use them without any type of certification process. These programs have not been shown to work effectively or produce repeatable results. Lack of certification and review is a real problem. Answers A, C, and D are important, but they are not the primary concern.

76. **Answer: D.** A relational database is a two-dimensional table; this allows each table to contain unique rows, columns, and cells. Relational databases have advantages over hierarchical databases. One such advantage is that a number of different relations can be defined, including overcoming the limitation of hierarchical databases that allows a child to have only one parent. Answers A, B, and C are therefore incorrect.

77. **Answer: B.** The capability maturity model features five maturity levels that specify software development process maturity. These levels include initial, repeatable, defined, managed, and optimized. The defined level allows for quantitative process improvement.

78. **Answer: C.** Software escrow is a form of insurance. Suppose company A buys software from company B. Company A is concerned that company B may go broke. A copy of the software source code can be placed in a safe place so that company A can access and modify it in case company B goes bankrupt.

79. **Answer: C.** A commit completes the transaction. A savepoint is designed to allow the system to return to a certain point should an error occur. A rollback is similar, except that it is used when changes need to be canceled. An audit point is used as a control point to verify input, process, or output data.

80. **Answer: A.** The capability maturity model features five maturity levels that specify software development process maturity. These levels are initial, repeatable, defined, managed, and optimized.

81. **Answer: A.** Metadata is data that describes other data. Nonatomic data is a data value that consists of multiple data values. A data structure is a set of data in memory composed of fields. Transaction processing is a mode of computer operation.

82. **Answer: C.** Relational databases are two-dimensional tables; this allows each table to contain unique rows, columns, and cells. Hierarchical, network, and object do not meet these requirements.

83. **Answer: D.** A database view allows the database administrator to control what a specific user at a specific level of access can see. For example, an HR employee may be able to see department payroll totals but not individual employee salaries. A schema is the structure of the database. DMCL is unrelated to databases. Data mining is the process of analyzing metadata.

84. **Answer: D.** Security controls must be considered at all points of the SDLC process. To learn more about the software development life cycle, see NIST 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems."

85. **Answer: D.** The change control process has the following steps: Make a formal request for a change, analyze the request, record the change request, submit the change request for approval, develop the change, and report the results to management.

86. **Answer: A.** Answers B, C, and D not fully define an expert system. An expert system is unique in that it contains a knowledge base of information and mathematical algorithms that use a series of `if...then` statements to infer facts from data.

87. **Answer: C.** Common Object Request Broker Architecture (CORBA) is vendor-independent middleware. Its purpose is to tie together different vendors' products so that they can seamlessly work together over distributed networks. Atomicity deals with the validity of database transactions. Object Linking and Embedding (OLE) is a proprietary system developed by Microsoft that allows applications to transfer and share information. Object-oriented programming is a modular form of programming.

88. **Answer: D.** The Capability Maturity Model (CMM) expired in 2007 and was replaced with the Capability Maturity Model Integration (CMMI) model. It features 22 process areas: causal analysis and resolution, configuration management, decision analysis and resolution, integrated project management, measurement and analysis, organizational innovation and deployment, organizational process definition, organizational process focus, organizational process performance, organizational training, project monitoring and control, project planning, process and product quality assurance, product integration, quantitative project management, requirements management, requirements development, risk management, supplier agreement management, technical solution, validation, and verification.

89. **Answer: A.** At level 1 of the CMM, processes likely to be variable (inconsistent) and depend heavily on institutional knowledge. At level 2, processes are seen as repeatable. At level 3, documented standards are put in place. At level 4, metrics and management standards are in place.

90. **Answer: B.** The two methods of reasoning when using inference rules are forward chaining and backward chaining. Knowledge transparency deals with knowledge representation.

91. **Answer: C.** Extreme programming, which is an off-shoot of agile, uses pairs of programmers who work from detailed specifications. Answer A is not correct because waterfall is a classical method. Answer B is not correct because spiral uses iterations that spiral out every 28 days. Answer D is not correct because RAD uses prototypes.

92. **Answer: D.** Crippleware, or trialware, is software that is partially functioning proprietary software that can be used without payment. Therefore, answers A, B, and C are incorrect.

93. **Answer: A.** Byte code, such as Java, serves as a type of intermediary code that must be converted to machine code before running.

94. **Answer: C.** CORBA is an open vendor-neutral middleware. Answers A, B, and D are incorrect because COM enables objects written in different languages to communicate, and OOA and OOD are software design methodologies.

95. **Answer: B.** COM enables objects written in different languages to communicate. Answers A, C, and D are incorrect because OOA and OOD are software design methodologies, and CORBA is vendor-neutral middleware.

96. **Answer: True.** SQL is a 4GL language. Others include CASE and Statistical Analysis System (SAS).

97. **Answer: False.** 5GL languages are designed to use knowledge-based systems to solve problems and use constraints instead of an algorithm.

98. **Answer: False.** The spiral model is the one that is based on the concept that software development is evolutionary.

99. **Answer: False.** It is true that reengineering attempts to update software by reusing as many of the components as possible instead of designing an entirely new system. However, reverse engineering is a technique that can be used to decrease development time by *decompiling* existing code. Reverse engineering has many legal issues and concerns.

100. **Answer: True.** Cohesion addresses the fact that a module can perform a single task with little input from other modules. Coupling is the measurement of the interconnecting between modules. Low coupling means that a change to one module should not affect another.

101. **Answer: True.** An ERD helps map the requirements and define the relationship between elements. The basic components of an ERD are an entity and a relationship. After a data dictionary is designed, the database schema can be developed.

102. **Answer: True.** WBAD offers standardized integration through the use of application development technologies such as XML. Its components include SOAP, WSDL, and UDDI.

103. **Answer: False.** Prototyping is still used. The advantage is that it can provide real savings in development time and costs.

104. **Answer: False.** Zeroization is the act of writing 0s, or a known pattern of bits, to media to make it difficult to recover the residual data. Purging makes data removal next to impossible. Therefore, purging is the higher level of data removal.

105. The answers are as follows:

- **A.** Stealth: **2.**
- **B.** Meme: **5.**
- **C.** Macro: **1.**
- **D.** EICAR: **4.**
- **E.** Encrypted virus: **3.**

A stealth virus can modify functionality, so detection is very difficult. A meme is not a virus; it works like a chain letter. Its purpose is to forward the message from user to user, propagating the hoax. The "I love you" and Melissa viruses are examples of macro viruses. "I love you" was an active script that could infect via a number of vectors of systems running Microsoft Windows with Windows Scripting Host enabled. Melissa targeted Microsoft Office documents (specifically, Microsoft Word). These viruses target Office documents. The EICAR test is used to verify the functionality of antivirus software. It is basically a signature that all participating vendors recognize. Encrypted viruses are similar to polymorphic viruses but can change how they are stored on the disk. This form of malware can make use of a cryptographic key.