ExamLabs

(ISC)^2

CISSP Certified Information Systems Security Professional

Official Study Guide

Exam CISSP

Contents

List of Tables

List of Illustrations

Introduction

The *(ISC)2 CISSP: Certified Information Systems Security Professional Official Study Guide, Eighth Edition,* offers you a solid foundation for the Certified Information Systems Security Professional (CISSP) exam. By purchasing this book, you've shown a willingness to learn and a desire to develop the skills you need to achieve this certification. This introduction provides you with a basic overview of this book and the CISSP exam.

This book is designed for readers and students who want to study for the CISSP certification exam. If your goal is to become a certified security professional, then the CISSP certification and this study guide are for you. The purpose of this book is to adequately prepare you to take the CISSP exam.

Before you dive into this book, you need to have accomplished a few tasks on your own. You need to have a general understanding of IT and of security. You should have the necessary five years of full-time paid work experience (or four years if you have a college degree) in two or more of the eight domains covered by the CISSP exam. If you are qualified to take the CISSP exam according to $(ISC)^2$, then you are sufficiently prepared to use this book to study for it. For more information on $(ISC)^2$, see the next section.

$(ISC)^2$ also allows for a one-year reduction of the five-year experience requirement if you have earned one of the approved certifications from the $(ISC)^2$ prerequisite pathway. These include certifications such as CAP, CISM, CISA, CCNA Security, Security+, MCSA, MCSE, and many of the GIAC certifications. For a complete list of qualifying certifications, visit https://www.isc2.org/Certifications/CISSP/Prerequisite-Pathway. Note: You can use only one of the experience reduction measures, either a college degree or a certification, not both.

$(ISC)^2$

The CISSP exam is governed by the International Information Systems Security Certification Consortium (ISC)². (ISC)² is a global not-for-profit organization. It has four primary mission goals:

- Maintain the Common Body of Knowledge (CBK) for the field of information systems security.
- Provide certification for information systems security professionals and practitioners.
- Conduct certification training and administer the certification exams.
- Oversee the ongoing accreditation of qualified certification candidates through continued education.

The (ISC)² is operated by a board of directors elected from the ranks of its certified practitioners.

(ISC)² supports and provides a wide variety of certifications, including CISSP, SSCP, CAP, CSSLP, CCFP, HCISPP, and CCSP. These certifications are designed to verify the knowledge and skills of IT security professionals across all industries. You can obtain more information about (ISC)² and its other certifications from its website at www.isc2.org.

The Certified Information Systems Security Professional (CISSP) credential is for security professionals responsible for designing and maintaining security infrastructure within an organization.

Topical Domains

The CISSP certification covers material from the eight topical domains. These eight domains are as follows:

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security

- Identity and Access Management (IAM)
- Security Assessment and Testing
- Security Operations
- Software Development Security

These eight domains provide a vendor-independent overview of a common security framework. This framework is the basis for a discussion on security practices that can be supported in all types of organizations worldwide.

The most recent revision of the topical domains will be reflected in exams starting April 15, 2018. For a complete view of the breadth of topics covered on the CISSP exam from the eight domain groupings, visit the (ISC)² website at www.isc2.org to request a copy of the Candidate Information Bulletin. This document includes a complete exam outline as well as other relevant facts about the certification.

Prequalifications

(ISC)² has defined the qualification requirements you must meet to become a CISSP. First, you must be a practicing security professional with at least five years' full-time paid work experience or with four years' experience and a recent IT or IS degree. Professional experience is defined as security work performed for salary or commission within two or more of the eight CBK domains.

Second, you must agree to adhere to a formal code of ethics. The CISSP Code of Ethics is a set of guidelines the (ISC)² wants all CISSP candidates to follow to maintain professionalism in the field of information systems security. You can find it in the Information section on the (ISC)² website at www.isc2.org.

(ISC)² also offers an entry program known as an Associate of (ISC)². This program allows someone without any or enough experience to qualify as a CISSP to take the CISSP exam anyway and then obtain experience afterward. Associates are granted six years to obtain five years' of security experience. Only after providing proof of such

experience, usually by means of endorsement and a resume, can the individual be awarded CISSP certification.

Overview of the CISSP Exam

The CISSP exam focuses on security from a 30,000-foot view; it deals more with theory and concept than implementation and procedure. It is very broad but not very deep. To successfully complete this exam, you'll need to be familiar with every domain but not necessarily be a master of each domain.

As of December 18, 2017, the CISSP exam is in an adaptive format. (ISC)² calls the new version CISSP-CAT (Computerized Adaptive Testing). For complete details of this new version of exam presentation, please see https://www.isc2.org/certifications/CISSP/CISSP-CAT.

The CISSP-CAT exam will be a minimum of 100 questions and a maximum of 150. Not all items you are presented with count toward your score or passing status. These unscored items are called *pretest questions* by (ISC)², while the scored items are called *operational items*. The questions are not labeled on the exam as to whether they are scored or unscored. Test candidates will receive 25 unscored items on their exam, regardless of whether they achieve a passing rank at question 100 or see all of the 150 questions.

The CISSP-CAT grants a maximum of three hours to take the exam. If you run out of time before achieving a passing rank, you will automatically fail.

The CISSP-CAT does not allow you to return to a previous question to change your answer. Your answer selection is final once you leave a question.

The CISSP-CAT does not have a published or set score to achieve. Instead, you must demonstrate the ability to answer above the (ISC)² bar for passing, called the *passing standard* (which is not disclosed), within the last 75 operational items (i.e., questions).

If the computer determines that you have a less than 5 percent chance

of achieving a passing standard and you have seen 75 operational items, your test will automatically end with a failure. You are not guaranteed to see any more questions than are necessary for the computer grading system to determine with 95 percent confidence your ability to achieve a passing standard or to fail to meet the passing standard.

If you do not pass the CISSP exam on your first attempt, you are allowed to retake the CISSP exam under the following conditions:

- You can take the CISSP exam a maximum of 3 times per 12-month period.
- You must wait 30 days after your first attempt before trying a second time.
- You must wait an additional 90 days after your second attempt before trying a third time.
- You must wait an additional 180 days after your third attempt before trying again or as long as needed to reach 12 months from the date of your first attempt.

You will need to pay full price for each additional exam attempt.

It is not possible to take the previous paper-based or CBT (computer based testing) flat 250 question version of the exam. CISSP is now available only in the CBT CISSP-CAT format.

The refreshed CISSP exam will be available in English, French, German, Brazilian Portuguese, Spanish, Japanese, Simplified Chinese and Korean.

Effective December 18, 2017, the Certified Information Systems Security Professional (CISSP) exam (English version only) will be available exclusively via CAT through (ISC)2-authorized Pearson VUE test centers in authorized markets. CISSP exams administered in languages other than English and all other (ISC)2 certification exams will continue to be available as fixed-form, linear examinations.

CISSP Exam Question Types

Most of the questions on the CISSP exam are four-option, multiple-choice questions with a single correct answer. Some are straightforward, such as asking you to select a definition. Some are a bit more involved, asking you to select the appropriate concept or best practice. And some questions present you with a scenario or situation and ask you to select the best response. Here's an example:

1. What is the most important goal and top priority of a security solution?
   A. Preventing disclosure
   B. Maintaining integrity
   C. Maintaining human safety
   D. Sustaining availability

You must select the one correct or best answer and mark it. In some cases, the correct answer will be very obvious to you. In other cases, several answers may seem correct. In these instances, you must choose the best answer for the question asked. Watch for general, specific, universal, superset, and subset answer selections. In other cases, none of the answers will seem correct. In these instances, you'll need to select the least incorrect answer.

.By the way, the correct answer for this sample question is C. Maintaining human safety is always your first priority.

In addition to the standard multiple-choice question format, (ISC)² has added a few advanced question formats, which it calls *advanced innovative questions*. These include drag-and-drop questions and hotspot questions. These types of questions require you to place topics or concepts in order of operations, in priority preference, or in relation to proper positioning for the needed solution. Specifically, the drag-and-drop questions require the test taker to move labels or icons to mark items on an image. The hotspot questions require the test taker to pinpoint a location on an image with a cross-hair marker. These

question concepts are easy to work with and understand, but be careful about your accuracy of dropping or marking.

Advice on Taking the Exam

The CISSP exam consists of two key elements. First, you need to know the material from the eight domains. Second, you must have good test-taking skills. You have a maximum of 3 hours to achieve a passing standard with the potential to see up to 150 questions. Thus, you will have on average just over a minute for each question. Thus, it is important to work quickly, without rushing but also without wasting time.

It is not clear from (ISC)²'s description of the CISSP-CAT format whether guessing is a good strategy in every case, but it does seem to be a better strategy than skipping questions. We recommend you attempt to eliminate as many answer selections as possible before making a guess, and consider skipping the question instead of randomly guessing only if you are unable to eliminate any answer options. Make educated guesses from a reduced set of options to increase your chance of getting a question correct.

Also note that (ISC)² does not disclose if there is partial credit given for multiple-part questions if you get only some of the elements correct. So, pay attention to questions with check boxes instead of radio buttons, and be sure to select as many items as necessary to properly address the question.

You will be provided a dry-erase board and a marker to jot down thoughts and make notes. But nothing written on that board will be used to alter your score. And that board must be returned to the test administrator prior to departing the test facility.

To maximize your test-taking activities, here are some general guidelines:

- Read each question, then read the answer options, and then reread the question.
- Eliminate wrong answers before selecting the correct one.

- Watch for double negatives.
- Be sure you understand what the question is asking.

Manage your time. You can take breaks during your test, but this might consume some of your test time. You might consider bringing a drink and snacks, but your food and drink will be stored for you away from the testing area, and that break time will count against your test time limit. Be sure to bring any medications or other essential items, but leave all things electronic at home or in your car. You should avoid wearing anything on your wrists, including watches, fitness trackers, and jewelry. You are not allowed to bring any form of noise-canceling headsets or ear buds, although you can use foam earplugs. We also recommend wearing comfortable clothes and taking a light jacket with you (some testing locations are a bit chilly).

If English is not your first language, you can register for one of several other language versions of the exam. Or, if you choose to use the English version of the exam, a translation dictionary is allowed. (Be sure to contact your test facility to organize and arrange this beforehand.) You must be able to prove that you need such a dictionary; this is usually accomplished with your birth certificate or your passport.

Study and Exam Preparation Tips

We recommend planning for a month or so of nightly intensive study for the CISSP exam. Here are some suggestions to maximize your learning time; you can modify them as necessary based on your own learning habits:

- Take one or two evenings to read each chapter in this book and

work through its review material.

- Answer all the review questions and take the practice exams provided in the book and in the test engine. Complete the written labs from each chapter, and use the review questions for each chapter to help guide you to topics for which more study or time spent working through key concepts and strategies might be beneficial.
- Review the (ISC)²'s Exam Outline: www.isc2.org.
- Use the flashcards included with the study tools to reinforce your understanding of concepts.

Completing the Certification Process

Once you have been informed that you successfully passed the CISSP certification, there is one final step before you are actually awarded the CISSP certification. That final step is known as *endorsement*. Basically, this involves getting someone who is a CISSP, or other (ISC)² certification holder, in good standing and familiar with your work history to submit an endorsement form on your behalf. The endorsement form is accessible through the email notifying you of your achievement in passing the exam. The endorser must review your résumé, ensure that you have sufficient experience in the eight CISSP

domains, and then submit the signed form to (ISC)² digitally or via fax or post mail. You must have submitted the endorsement files to (ISC)² within 90 days after receiving the confirmation-of-passing email. Once (ISC)² receives your endorsement form, the certification process will be completed and you will be sent a welcome packet via USPS.

Post-CISSP Concentrations

(ISC)² has three concentrations offered only to CISSP certificate holders. The (ISC)² has taken the concepts introduced on the CISSP exam and focused on specific areas, namely, architecture, management, and engineering. These three concentrations are as follows:

Information Systems Security Architecture Professional (ISSAP) Aimed at those who specialize in information security architecture. Key domains covered here include access control systems and methodology; cryptography; physical security integration; requirements analysis and security standards, guidelines, and criteria; technology-related aspects of business continuity planning and disaster recovery planning; and telecommunications and network security. This is a credential for those who design security systems or infrastructure or for those who audit and analyze such structures.

Information Systems Security Management Professional (ISSMP) Aimed at those who focus on management of information security policies, practices, principles, and procedures. Key domains covered here include enterprise security management practices; enterprise-wide system development security; law, investigations, forensics, and ethics; oversight for operations security compliance; and understanding business continuity planning, disaster recovery planning, and continuity of operations planning. This is a credential for professionals who are responsible for security infrastructures, particularly where mandated compliance comes into the picture.

Information Systems Security Engineering Professional (ISSEP) Aimed at those who focus on the design and engineering of secure hardware and software information systems, components, or applications. Key domains covered include certification and

accreditation, systems security engineering, technical management, and U.S. government information assurance rules and regulations. Most ISSEPs work for the U.S. government or for a government contractor that manages government security clearances.

For more details about these concentration exams and certifications, please see the (ISC)² website at www.isc2.org.

Notes on This Book's Organization

This book is designed to cover each of the eight CISSP Common Body of Knowledge domains in sufficient depth to provide you with a clear understanding of the material. The main body of this book comprises 21 chapters. The domain/chapter breakdown is as follows:

Chapters 1, 2, 3, and 4: Security and Risk Management

Chapter 5: Asset Security

Chapters 6, 7, 8, 9, and 10: Security Architecture and Engineering

Chapters 11 and 12: Communication and Network Security

Chapters 13 and 14: Identity and Access Management (IAM)

Chapters 15: Security Assessment and Testing

Chapters 16, 17, 18, and 19: Security Operations

Chapters 20 and 21: Software Development Security

Each chapter includes elements to help you focus your studies and test your knowledge, detailed in the following sections. Note: please see the table of contents and chapter introductions for a detailed list of domain topics covered in each chapter.

The Elements of This Study Guide

You'll see many recurring elements as you read through this study guide. Here are descriptions of some of those elements:

Exam Essentials The Exam Essentials highlight topics that could appear on the exam in some form. While we obviously do not know exactly what will be included in a particular exam, this section

reinforces significant concepts that are key to understanding the Common Body of Knowledge (CBK) area and the test specs for the CISSP exam.

Chapter Review Questions Each chapter includes practice questions that have been designed to measure your knowledge of key ideas that were discussed in the chapter. After you finish each chapter, answer the questions; if some of your answers are incorrect, it's an indication that you need to spend some more time studying the corresponding topics. The answers to the practice questions can be found at the end of each chapter.

Written Labs Each chapter includes written labs that synthesize various concepts and topics that appear in the chapter. These raise questions that are designed to help you put together various pieces you've encountered individually in the chapter and assemble them to propose or describe potential security strategies or solutions.

Real-World Scenarios As you work through each chapter, you'll find descriptions of typical and plausible workplace situations where an understanding of the security strategies and approaches relevant to the chapter content could play a role in fixing problems or in fending off potential difficulties. This gives readers a chance to see how specific security policies, guidelines, or practices should or may be applied to the workplace.

Summaries The summary is a brief review of the chapter to sum up what was covered.

Assessment Test

1. Which of the following types of access control seeks to discover evidence of unwanted, unauthorized, or illicit behavior or activity?
   A. Preventive
   B. Deterrent
   C. Detective
   D. Corrective
2. Define and detail the aspects of password selection that distinguish good password choices from ultimately poor password choices.
   A. Difficult to guess or unpredictable
   B. Meet minimum length requirements
   C. Meet specific complexity requirements
   D. All of the above
3. Which of the following is most likely to detect DoS attacks?
   A. Host-based IDS
   B. Network-based IDS
   C. Vulnerability scanner
   D. Penetration testing
4. Which of the following is considered a denial-of-service attack?
   A. Pretending to be a technical manager over the phone and asking a receptionist to change their password
   B. While surfing the Web, sending to a web server a malformed URL that causes the system to consume 100 percent of the CPU
   C. Intercepting network traffic by copying the packets as they pass through a specific subnet
   D. Sending message packets to a recipient who did not request them

simply to be annoying

5. At which layer of the OSI model does a router operate?
   A. Network layer
   B. Layer 1
   C. Transport layer
   D. Layer 5
6. Which type of firewall automatically adjusts its filtering rules based on the content of the traffic of existing sessions?
   A. Static packet filtering
   B. Application-level gateway
   C. Circuit level gateway
   D. Dynamic packet filtering
7. A VPN can be established over which of the following?
   A. Wireless LAN connection
   B. Remote access dial-up connection
   C. WAN link
   D. All of the above
8. What type of malware uses social engineering to trick a victim into installing it?
   A. Viruses
   B. Worms
   C. Trojan horse
   D. Logic bomb
9. The CIA Triad comprises what elements?
   A. Contiguousness, interoperable, arranged
   B. Authentication, authorization, accountability
   C. Capable, available, integral

D. Availability, confidentiality, integrity

10. Which of the following is not a required component in the support of accountability?

A. Auditing

B. Privacy

C. Authentication

D. Authorization

11. Which of the following is not a defense against collusion?

A. Separation of duties

B. Restricted job responsibilities

C. Group user accounts

D. Job rotation

12. A data custodian is responsible for securing resources after _____ has assigned the resource a security label.

A. Senior management

B. The data owner

C. An auditor

D. Security staff

13. In what phase of the Capability Maturity Model for Software (SW-CMM) are quantitative measures utilized to gain a detailed understanding of the software development process?

A. Repeatable

B. Defined

C. Managed

D. Optimizing

14. Which one of the following is a layer of the ring protection scheme that is not normally implemented in practice?

A. Layer 0

B. Layer 1

C. Layer 3

D. Layer 4

5. What is the last phase of the TCP/IP three-way handshake sequence?

A. SYN packet

B. ACK packet

C. NAK packet

D. SYN/ACK packet

6. Which one of the following vulnerabilities would best be countered by adequate parameter checking?

A. Time of check to time of use

B. Buffer overflow

C. SYN flood

D. Distributed denial of service

7. What is the value of the logical operation shown here?

X: 0 1 1 0 1 0

Y: 0 0 1 1 0 1

_____

X ∨ Y: ?

A. 0 1 1 1 1 1

B. 0 1 1 0 1 0

C. 0 0 1 0 0 0

D. 0 0 1 1 0 1

8. In what type of cipher are the letters of the plain-text message rearranged to form the cipher text?

A. Substitution cipher

B. Block cipher

C. Transposition cipher

D. Onetime pad

9. What is the length of a message digest produced by the MD5 algorithm?

A. 64 bits

B. 128 bits

C. 256 bits

D. 384 bits

10. If Renee receives a digitally signed message from Mike, what key does she use to verify that the message truly came from Mike?

A. Renee's public key

B. Renee's private key

C. Mike's public key

D. Mike's private key

11. Which of the following is not a composition theory related to security models?

A. Cascading

B. Feedback

C. Iterative

D. Hookup

12. The collection of components in the TCB that work together to implement reference monitor functions is called the _____ .

A. Security perimeter

B. Security kernel

C. Access matrix

D. Constrained interface

3. Which of the following statements is true?

A. The less complex a system, the more vulnerabilities it has.

B. The more complex a system, the less assurance it provides.

C. The less complex a system, the less trust it provides.

D. The more complex a system, the less attack surface it generates.

4. Ring 0, from the design architecture security mechanism known as protection rings, can also be referred to as all but which of the following?

A. Privileged mode

B. Supervisory mode

C. System mode

D. User mode

5. Audit trails, logs, CCTV, intrusion detection systems, antivirus software, penetration testing, password crackers, performance monitoring, and cyclic redundancy checks (CRCs) are examples of what?

A. Directive controls

B. Preventive controls

C. Detective controls

D. Corrective controls

6. System architecture, system integrity, covert channel analysis, trusted facility management, and trusted recovery are elements of what security criteria?

A. Quality assurance

B. Operational assurance

C. Lifecycle assurance

D. Quantity assurance

7. Which of the following is a procedure designed to test and perhaps bypass a system's security controls?

   A. Logging usage data

   B. War dialing

   C. Penetration testing

   D. Deploying secured desktop workstations

8. Auditing is a required factor to sustain and enforce what?

   A. Accountability

   B. Confidentiality

   C. Accessibility

   D. Redundancy

9. What is the formula used to compute the ALE?

   A. ALE = AV * EF * ARO

   B. ALE = ARO * EF

   C. ALE = AV * ARO

   D. ALE = EF * ARO

10. What is the first step of the business impact assessment process?

    A. Identification of priorities

    B. Likelihood assessment

    C. Risk identification

    D. Resource prioritization

11. Which of the following represent natural events that can pose a threat or risk to an organization?

    A. Earthquake

    B. Flood

    C. Tornado

    D. All of the above

2. What kind of recovery facility enables an organization to resume operations as quickly as possible, if not immediately, upon failure of the primary facility?

   A. Hot site

   B. Warm site

   C. Cold site

   D. All of the above

3. What form of intellectual property is used to protect words, slogans, and logos?

   A. Patent

   B. Copyright

   C. Trademark

   D. Trade secret

4. What type of evidence refers to written documents that are brought into court to prove a fact?

   A. Best evidence

   B. Payroll evidence

   C. Documentary evidence

   D. Testimonial evidence

5. Why are military and intelligence attacks among the most serious computer crimes?

   A. The use of information obtained can have far-reaching detrimental strategic effects on national interests in an enemy's hands.

   B. Military information is stored on secure machines, so a successful attack can be embarrassing.

   C. The long-term political use of classified information can impact a country's leadership.

   D. The military and intelligence agencies have ensured that the laws

protecting their information are the most severe.

5. What type of detected incident allows the most time for an investigation?

   A. Compromise

   B. Denial of service

   C. Malicious code

   D. Scanning

7. If you want to restrict access into or out of a facility, which would you choose?

   A. Gate

   B. Turnstile

   C. Fence

   D. Mantrap

3. What is the point of a secondary verification system?

   A. To verify the identity of a user

   B. To verify the activities of a user

   C. To verify the completeness of a system

   D. To verify the correctness of a system

9. Spamming attacks occur when numerous unsolicited messages are sent to a victim. Because enough data is sent to the victim to prevent legitimate activity, it is also known as what?

   A. Sniffing

   B. Denial of service

   C. Brute-force attack

   D. Buffer overflow attack

0. Which type of intrusion detection system (IDS) can be considered an expert system?

   A. Host-based

B. Network-based

C. Knowledge-based

D. Behavior-based

Answers to Assessment Test

1. C. Detective access controls are used to discover (and document) unwanted or unauthorized activity.
2. D. Strong password choices are difficult to guess, unpredictable, and of specified minimum lengths to ensure that password entries cannot be computationally determined. They may be randomly generated and utilize all the alphabetic, numeric, and punctuation characters; they should never be written down or shared; they should not be stored in publicly accessible or generally readable locations; and they shouldn't be transmitted in the clear.
3. B. Network-based IDSs are usually able to detect the initiation of an attack or the ongoing attempts to perpetrate an attack (including denial of service, or DoS). They are, however, unable to provide information about whether an attack was successful or which specific systems, user accounts, files, or applications were affected. Host-based IDSs have some difficulty with detecting and tracking down DoS attacks. Vulnerability scanners don't detect DoS attacks; they test for possible vulnerabilities. Penetration testing may cause a DoS or test for DoS vulnerabilities, but it is not a detection tool.
4. B. Not all instances of DoS are the result of a malicious attack. Errors in coding OSs, services, and applications have resulted in DoS conditions. Some examples of this include a process failing to release control of the CPU or a service consuming system resources out of proportion to the service requests it is handling. Social engineering and sniffing are typically not considered DoS attacks.
5. A. Network hardware devices, including routers, function at layer 3, the Network layer.
6. D. Dynamic packet-filtering firewalls enable the real-time modification of the filtering rules based on traffic content.
7. D. A VPN link can be established over any other network communication connection. This could be a typical LAN cable

connection, a wireless LAN connection, a remote access dial-up connection, a WAN link, or even an internet connection used by a client for access to the office LAN.

8. C. A Trojan horse is a form of malware that uses social engineering tactics to trick a victim into installing it—the trick is to make the victim believe that the only thing they have downloaded or obtained is the host file, when in fact it has a malicious hidden payload.
9. D. The components of the CIA Triad are confidentiality, availability, and integrity.
10. B. Privacy is not necessary to provide accountability.
11. C. Group user accounts allow for multiple people to log in under a single user account. This allows collusion because it prevents individual accountability.
12. B. The data owner must first assign a security label to a resource before the data custodian can secure the resource appropriately.
13. C. The Managed phase of the SW-CMM involves the use of quantitative development metrics. The Software Engineering Institute (SEI) defines the key process areas for this level as Quantitative Process Management and Software Quality Management.
14. B. Layers 1 and 2 contain device drivers but are not normally implemented in practice. Layer 0 always contains the security kernel. Layer 3 contains user applications. Layer 4 does not exist.
15. B. The SYN packet is first sent from the initiating host to the destination host. The destination host then responds with a SYN/ACK packet. The initiating host sends an ACK packet, and the connection is then established.
16. B. Parameter checking is used to prevent the possibility of buffer overflow attacks.
17. A. The ~ OR symbol represents the OR function, which is true when one or both of the input bits are true.
18. C. Transposition ciphers use an encryption algorithm to rearrange

the letters of the plain-text message to form a cipher text message.

9. B. The MD5 algorithm produces a 128-bit message digest for any input.
0. C. Any recipient can use Mike's public key to verify the authenticity of the digital signature.
1. C. Iterative is not one of the composition theories related to security models. Cascading, feedback, and hookup are the three composition theories.
2. B. The collection of components in the TCB that work together to implement reference monitor functions is called the security kernel.
3. B. The more complex a system, the less assurance it provides. More complexity means more areas for vulnerabilities to exist and more areas that must be secured against threats. More vulnerabilities and more threats mean that the subsequent security provided by the system is less trustworthy.
4. D. Ring 0 has direct access to the most resources; thus user mode is not an appropriate label because user mode requires restrictions to limit access to resources.
5. C. Examples of detective controls are audit trails, logs, CCTV, intrusion detection systems, antivirus software, penetration testing, password crackers, performance monitoring, and CRCs.
6. B. Assurance is the degree of confidence you can place in the satisfaction of security needs of a computer, network, solution, and so on. Operational assurance focuses on the basic features and architecture of a system that lend themselves to supporting security.
7. C. Penetration testing is the attempt to bypass security controls to test overall system security.
8. A. Auditing is a required factor to sustain and enforce accountability.
9. A. The annualized loss expectancy (ALE) is computed as the product of the asset value (AV) times the exposure factor (EF) times

the annualized rate of occurrence (ARO). This is the longer form of the formula ALE = SLE * ARO. The other formulas displayed here do not accurately reflect this calculation.

10. A. Identification of priorities is the first step of the business impact assessment process.

11. D. Natural events that can threaten organizations include earthquakes, floods, hurricanes, tornados, wildfires, and other acts of nature as well. Thus options A, B, and C are correct because they are natural and not man-made.

12. A. Hot sites provide backup facilities maintained in constant working order and fully capable of taking over business operations. Warm sites consist of preconfigured hardware and software to run the business, neither of which possesses the vital business information. Cold sites are simply facilities designed with power and environmental support systems but no configured hardware, software, or services. Disaster recovery services can facilitate and implement any of these sites on behalf of a company.

13. C. Trademarks are used to protect the words, slogans, and logos that represent a company and its products or services.

14. C. Written documents brought into court to prove the facts of a case are referred to as documentary evidence.

15. A. The purpose of a military and intelligence attack is to acquire classified information. The detrimental effect of using such information could be nearly unlimited in the hands of an enemy. Attacks of this type are launched by very sophisticated attackers. It is often very difficult to ascertain what documents were successfully obtained. So when a breach of this type occurs, you sometimes cannot know the full extent of the damage.

16. D. Scanning incidents are generally reconnaissance attacks. The real damage to a system comes in the subsequent attacks, so you may have some time to react if you detect the scanning attack early.

17. B. A turnstile is a form of gate that prevents more than one person from gaining entry at a time and often restricts movement to one direction. It is used to gain entry but not exit, or vice versa.

3. D. Secondary verification mechanisms are set in place to establish a means of verifying the correctness of detection systems and sensors. This often means combining several types of sensors or systems (CCTV, heat and motion sensors, and so on) to provide a more complete picture of detected events.

9. B. A spamming attack (sending massive amounts of unsolicited email) can be used as a type of denial-of-service attack. It doesn't use eavesdropping methods so it isn't sniffing. Brute-force methods attempt to crack passwords. Buffer overflow attacks send strings of data to a system in an attempt to cause it to fail.

0. D. A behavior-based IDS can be labeled an expert system or a pseudo-artificial intelligence system because it can learn and make assumptions about events. In other words, the IDS can act like a human expert by evaluating current events against known events. A knowledge-based IDS uses a database of known attack methods to detect attacks. Both host-based and network-based systems can be either knowledge-based, behavior-based, or a combination of both.