CHAPTER

Becoming a CISSP

This chapter presents the following

- The definition of a CISSP
- Reasons to become a CISSP
- What the CISSP exam entails
- The Common Body of Knowledge and what it contains
- The history of $(ISC)^2$ and the CISSP exam
- Recertification requirements
- An assessment test to gauge your current knowledge of security

This book is intended not only to provide you with the necessary information to help you gain a CISSP certification, but also to welcome you into the exciting and challenging world of security.

The Certified Information Systems Security Professional (CISSP) exam covers ten different subjects, more commonly referred to as domains. The subject matter of each domain can easily be seen as its own area of study, and in many cases individuals work exclusively in these fields as experts. For many of these subjects, extensive resources can be consulted and referenced to become an expert in that area. Because of this, a common misconception is that the only way to succeed at the CISSP exam is to immerse yourself in a massive stack of texts and study materials. Fortunately, an easier approach exists. By using this fourth edition of the *CISSP All-in-One Exam Guide*, you can successfully complete and pass the CISSP exam and achieve your CISSP certification. The goal of this book is to combine into a single resource all the information you need to pass the CISSP exam. This book should also serve as a useful reference tool long after you've achieved your CISSP certification.

Why Become a CISSP?

As our world changes, the need for improvements in security and technology continues to grow. Security was once a hot issue only in the field of technology, but now it is becoming more and more a part of our everyday lives. Security is a concern of every organization, government agency, corporation, and military unit. Ten years ago *computer and information security* was an obscure field that only concerned a few people. Because the risks were essentially low, few were interested in security expertise. Ethical hacking

and vulnerability assessments required great talent and knowledge and thus were not a common practice.

Things have changed, however, and today corporations and other organizations are desperate to recruit talented and experienced security professionals to help protect the resources they depend on to run their businesses and to remain competitive. With a CISSP certification, you will be seen as a security professional of proven ability who has successfully met a predefined standard of knowledge and experience that is well understood and respected throughout the industry. By keeping this certification current, you will demonstrate your dedication to staying abreast of security developments.

Reasons for attaining a CISSP certification:

- To meet the growing demand and to thrive in an ever-expanding field
- To broaden your current knowledge of security concepts and practices
- To bring security expertise to your current occupation
- To become more marketable in a competitive workforce
- To show a dedication to the security discipline
- To increase your salary and be eligible for more employment opportunities

The CISSP certification helps companies identify which individuals have the ability, knowledge, and experience necessary to implement solid security practices, perform risk analysis, identify necessary countermeasures, and help the organization as a whole protect its facility, network, systems, and information. The CISSP certification also shows potential employers you have achieved a level of proficiency and expertise in skill sets and knowledge required by the security industry. The increasing importance placed on security in corporate success will only continue in the future, leading to even greater demands for highly skilled security professionals. CISSP certification shows that a respected third-party organization has recognized an individual's technical and theoretical knowledge and expertise, and distinguishes that individual from those who lack this level of knowledge.

Understanding and implementing security practices is an essential part of being a good network administrator, programmer, or engineer. Job descriptions that do not specifically target security professionals still often require that a potential candidate have a good understanding of security concepts as well as how to implement them. Due to staff size and budget restraints, many organizations can't afford separate network and security staffs. But this doesn't mean they don't believe security is vital to their organization. Thus, they often try to combine knowledge of technology and security into a single role. With a CISSP designation, you can put yourself head and shoulders above other individuals in this regard.

The CISSP Exam

To meet the certification requirements of a CISSP, you must have one of the following:

- Five years professional experience in two (or more) of the domains within the Common Body of Knowledge (CBK).

- Four years experience in two (or more) of the ten domains, and a four-year college degree or master's degree in information security from a National Center of Excellence.
- At least three years experience in two (or more) of the ten domains and a four-year college degree or master's degree in information security from a National Center of Excellence, plus a professional certification from the following list (candidates are permitted a waiver of one year of experience for any credential on the approved credentials list):
  - CERT Certified Computer Security Incident Handler (CSIH)
  - Certified Business Continuity Planner (CBCP)
  - Certified Computer Crime Investigator (Advanced) (CCCI)
  - Certified Computer Crime Prosecutor
  - Certified Computer Examiner (CCE)
  - Certified Fraud Examiner (CFE)
  - Certified Information Systems Auditor (CISA)
  - Certified Information Security Manager (CISM)
  - Certified Internal Auditor (CIA)
  - Certified Protection Professional (CPP)
  - Certified Wireless Security Professional (CWSP)
  - CompTIA Security+
  - Computer Forensic Computer Examiner (CFCE)
  - GIAC Security Essentials Certification (GSEC)
  - GIAC Certified Firewall Analyst (GCFW)
  - GIAC Certified Intrusion Analyst (GCIA)
  - GIAC Certified Incident Handler (GCIH)
  - GIAC Certified Windows Security Administrator (GCWN)
  - GIAC Certified UNIX Security Administrator (GCUX)
  - GIAC Certified Forensic Analyst (GCFA)
  - GIAC Information Security Officer (GISO)
  - GIAC IT Security Audit Essentials (GSAE)
  - GIAC Security Expert (GSE)
  - GIAC Certified ISO-17799 Specialist (G7799)
  - GIAC Security Leadership Certification (GSLC)
  - GIAC Systems and Network Auditor (GSNA)
  - GIAC Certified Security Consultant (GCSC)
  - Microsoft Certified Systems Administrator (MCSA)
  - Microsoft Certified Systems Engineer (MCSE)
  - Master Business Continuity Planner (MBCP)
  - System Security Certified Practitioner (SSCP)

Consult www.isc2.org for a complete list and description of requirements for your CISSP certification.

Because the CISSP exam covers the ten domains making up the CISSP CBK, it is often described as being "an inch deep and a mile wide," a reference to the fact that many questions on the exam are not very detailed in nature and do not require you to be an expert in every subject. However, the questions do require you be familiar with many different security subjects.

The CISSP exam is comprised of 250 multiple-choice questions, and you have six hours to complete it. The questions are pulled from a much larger question bank to ensure the exam is as unique as possible for each entrant. In addition, the test bank constantly changes and evolves to more accurately reflect the real world of security. The exam questions are continually rotated and replaced in the bank as necessary. Each question has four answer choices, only one of which is correct. Only 225 questions are graded, while 25 are used for research purposes. The 25 research questions are integrated into the exam, so you won't know which go towards your final grade. To pass the exam, you need a minimum raw score of 700 points out of 1,000. Questions are weighted based on their difficulty; not all questions are worth the same number of points. The exam is not product- or vendor-oriented, meaning no questions will be specific to certain products or vendors (for instance, Windows 2000, Unix, or Cisco). Instead, you will be tested on the security models and methodologies used by these types of systems.

$(ISC)^2$ has also added scenario-based questions to the CISSP exam. These questions present a short scenario to the test taker rather than asking the test taker to identify terms and/or concepts. A scenario-based question would be worded something like "John returned from lunch and found that the company's IDS indicated that a critical server has had continuous ICMP traffic sent to it for over 45 minutes, which is taking up 85% of the server's CPU resource. What does John need to do at this point?"

The goal of the scenario-based questions is to ensure that test takers not only know and understand the concepts within the CBK, but also can apply this knowledge to real-life situations. This is more practical because in the real world, you won't be challenged by having someone come up to you and ask, "What is the definition of collusion?" You need to know how to detect and prevent collusion from taking place, in addition to knowing the definition of the term.

NOTE Hundreds of scenario-based questions have been added to the CD-ROM in the back of this book to help you prepare for this exam.

The International Information Systems Security Certification Consortium $(ISC)^2$ process for earning credentials will change as of October 2007. In order to obtain this credential, candidates for any of the $(ISC)^2$ credential will be required to obtain an endorsement of their candidature exclusively from an $(ISC)^2$ certified professional in good standing. The professional endorsing the candidate can hold any $(ISC)^2$ certification, such as the CISSP, SSCP, or CAP. This sponsor will vouch for your years of experience.

After passing the exam, you will be asked to supply documentation, supported by a sponsor, proving that you indeed have this type of experience. The sponsor must sign a document vouching for the security experience you are submitting. So, make sure you have this sponsor lined up prior to registering for the exam and providing payment. You don't want to pay for and pass the exam, only to find you can't find a sponsor for the final step needed to achieve your certification.

The reason behind the sponsorship requirement is to insure that those who achieve the certification have real-world experience to offer companies. Book knowledge is extremely important for understanding theory, concepts, standards, and regulations, but it can never replace hands-on experience. Proving you have practical experience supports the relevance of the certification.

Afterward, a small sample group of individuals selected at random will be audited after passing the exam. The audit consists mainly of individuals from (ISC)^2 calling on the candidates' stated sponsors and contacts to verify that the test taker's related experience is true.

What makes this exam challenging is that most candidates, although they work in the security field, are not necessarily familiar with all ten CBK domains. If a security professional is considered an expert in vulnerability testing or application security, for example, she may not be familiar with physical security, cryptography, or security practices. Thus, studying for this exam will broaden your knowledge of the security field.

The exam questions address the ten CBK security domains, which are described in Table 1-1.

(ISC)^2 attempts to keep up with changes in technology and methodologies brought to the security field by adding a large number of new questions to the test question bank each year. These questions are based on current technologies, practices, approaches, and standards. For example, the CISSP exam given in 1998 did not have questions pertaining to wireless security, but present and future exams will.

Other examples of material not on past exams include security governance, instant messaging, phishing, botnets, VoIP, and spam. Though these subjects weren't issues in the past, they are now—and in the case of botnets, VoIP, and spam, they will be in the future.

The test is based on internationally accepted information security standards and practices. If you look at the (ISC)^2 web site for test dates and locations, you may find, for example, that the same test is offered this Tuesday in California and next Wednesday in Saudi Arabia.

If you do not pass the exam, you have the option of retaking it as soon as you like. (ISC)^2 used to subject individuals to a waiting period before they could retake the exam, but this rule has been removed. (ISC)^2 keeps track of which exam version you were given on your first attempt and ensures you receive a different version for any retakes. (ISC)^2 also provides a report to a CISSP candidate who did not pass the exam, detailing the areas where the candidate was weakest. Though you could retake the exam soon afterward, it's wise to devote additional time to these weak areas to improve your score on the retest.

Domain	Description
Access Control	This domain examines mechanisms and methods used to enable administrators and managers to control what subjects can access, the extent of their capabilities after authorization and authentication, and the auditing and monitoring of these activities. Some of the topics covered include: • Access control security models • Identification and authentication technologies and techniques • Access control administration • Single sign-on technologies • Attack methods
Telecommunications and Network Security	This domain examines internal, external, public, and private communication systems; networking structures; devices; protocols; and remote access and administration. Some of the topics covered include: • OSI model and layers • Local area network (LAN), metropolitan area network (MAN), and wide area network (WAN) technologies • Internet, intranet, and extranet issues • Virtual private networks (VPNs), firewalls, routers, bridges, and repeaters • Network topologies and cabling • Attack methods
Information Security and Risk Management	This domain examines the identification of company assets, the proper way to determine the necessary level of protection required, and what type of budget to develop for security implementations, with the goal of reducing threats and monetary loss. Some of the topics covered include: • Data classification • Policies, procedures, standards, and guidelines • Risk assessment and management • Personnel security, training, and awareness
Application Security	This domain examines the security components within operating systems and applications and how to best develop and measure their effectiveness. It looks at software life cycles, change control, and application security. Some of the topics covered include: • Data warehousing and data mining • Various development practices and their risks • Software components and vulnerabilities • Malicious code
Cryptography	This domain examines methods and techniques for disguising data for protection purposes. This involves cryptography techniques, approaches, and technologies. Some of the topics covered include: • Symmetric versus asymmetric algorithms and uses • Public key infrastructure (PKI) and hashing functions • Encryption protocols and implementation • Attack methods

Table 1-1 Security Domains That Make Up the CISSP CBK

Domain	Description
Security Architecture and Design	This domain examines concepts, principles, and standards for designing and implementing secure applications, operating systems, and systems. This covers international security measurement standards and their meaning for different types of platforms. Some of the topics covered include: • Operating states, kernel functions, and memory mapping • Enterprise architecture • Security models, architectures, and evaluations • Evaluation criteria: Trusted Computer Security Evaluation Criteria (TCSEC), Information Technology Security Evaluation Criteria (ITSEC), and Common Criteria • Common flaws in applications and systems • Certification and accreditation
Operations Security	This domain examines controls over personnel, hardware, systems, and auditing and monitoring techniques. It also covers possible abuse channels and how to recognize and address them. Some of the topics covered include: • Administrative responsibilities pertaining to personnel and job functions • Maintenance concepts of antivirus, training, auditing, and resource protection activities • Preventive, detective, corrective, and recovery controls • Standards, compliance, and due care concepts • Security and fault tolerance technologies
Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)	This domain examines the preservation of business activities when faced with disruptions or disasters. It involves the identification of real risks, proper risk assessment, and countermeasure implementation. Some of the topics covered include: • Business resource identification and value assignment • Business impact analysis and prediction of possible losses • Unit priorities and crisis management • Plan development, implementation, and maintenance
Legal Regulations, Compliance, and Investigation	This domain examines computer crimes, laws, and regulations. It includes techniques for investigating a crime, gathering evidence, and handling procedures. It also covers how to develop and implement an incident-handling program. Some of the topics covered include: • Types of laws, regulations, and crimes • Licensing and software piracy • Export and import laws and issues • Evidence types and admissibility into court • Incident handling
Physical (Environmental) Security	This domain examines threats, risks, and countermeasures to protect facilities, hardware, data, media, and personnel. This involves facility selection, authorized entry methods, and environmental and safety procedures. Some of the topics covered include: • Restricted areas, authorization methods, and controls • Motion detectors, sensors, and alarms • Intrusion detection • Fire detection, prevention, and suppression • Fencing, security guards, and security badge types

Table 1-1 Security Domains That Make Up the CISSP CBK *(continued)*

CISSP: A Brief History

Historically, the field of computer and information security has not been a structured and disciplined profession; rather, the field has lacked many well-defined professional objectives and thus has often been misperceived.

In the mid-1980s, members of the computer security profession recognized they needed a certification program that would give their profession structure and provide ways for computer security professionals to demonstrate competence and present evidence of their qualifications. Establishing such a program would help the credibility of the computer and information security profession as a whole and the individuals who make up the profession.

In November 1988, the Special Interest Group for Computer Security (SIG-CS) of the Data Processing Management Association (DPMA) brought together several organizations interested in forming a security certification program. They included the Information Systems Security Association (ISSA), the Canadian Information Processing Society (CIPS), the Computer Security Institute (CSI), Idaho State University, and several U.S. and Canadian government agencies. As a voluntary joint effort, these organizations developed the necessary components to offer a full-fledged security certification for interested professionals. (ISC)^2 was formed in mid-1989 as a nonprofit corporation to develop a security certification program for information systems security practitioners. The certification was designed to measure professional competence and help companies in their selection of security professionals and personnel. (ISC)^2 was established in North America, but quickly gained international acceptance and now offers testing capabilities all over the world.

Because security is such a broad and diversified field in the technology and business world, the original consortium decided on an information systems security CBK composed of ten domains that pertain to every part of computer, network, business, and information security. In addition, because technology continues to rapidly evolve, staying up-to-date on security trends, technology, and business developments is required to maintain the CISSP certification. The group also developed a Code of Ethics, test specifications, a draft study guide, and the exam itself.

CAUTION There has been a lot of controversy in the industry about (ISC)^2, a nonprofit organization that maintains the CISSP certification *and* provides training for this certification. Many times the (ISC)^2 Institute has told companies that they cannot have an exam set up for them unless the companies take the (ISC)^2 Institute's training. This is a conflict of interest that has been brought up for years, and civil suits have been threatened. Feel comfortable to take training that best fits your needs, whether it be through the (ISC)^2 Institute or another vendor.

How Do You Become a CISSP?

To become a CISSP, start at www.isc2.org, where you will find an exam registration form you must fill out and send to (ISC)^2. You will be asked to provide your security work history, as well as documents for the necessary educational requirements. Gradu-

ating with a master's degree from one of the listed National Centers of Excellence and having two years of experience will also qualify you. These National Centers of Excellence are listed at www.nsa.gov/ia/academia/CAE.pdf, and the list of colleges and universities is growing. You will also be asked to read the (ISC)² Code of Ethics and sign a form, indicating that you understand these requirements and promise to abide by them. You then provide payment along with the registration form, where you indicate your preference as to the exam location. The numerous testing sites and dates can be found at www.isc2.org.

Although (ISC)² used to count cumulative years of job experience toward the requirements to take the CISSP exam, it has tightened its criteria; test takers must carry out full-time employment in two or more domains. People often think they do not have the necessary experience required to take this exam when they actually do, so it's always a good idea to contact (ISC)² directly to find out if you are indeed qualified before throwing this chance away.

Recertification Requirements

The CISSP certification is valid for three years. To recertify for an additional three years, you can opt to retake the CISSP exam (many other certifications, such as Microsoft and Cisco certifications, require retaking the exam) or you can do what most CISSPs elect to do. They earn continuing professional education (CPE) credits that qualify them for exam-free recertification. Taking this approach for CISSP certification requires that you earn 120 CPE credits over a three-year recertification period. Thus, you can either rest and retake the exam, or gain the 120 CPE credits in the three-year period.

Many types of activities can qualify for CPE credits, and they are broken down into two main sections: activities directly related to information security, and educational activities that either enhance a security professional's skill and knowledge or enhance the knowledge of others through provision of training and education.

The following items can be counted towards CPE credits, helping keep your CISSP certification current:

- Attending a vendor training course or presentation
- Attending a security conference
- Taking a university or college security course related to one of the CBK domains
- Publishing a security article or book
- Providing security training
- Serving on the board of a professional security organization or attending its meetings
- Engaging in self-study
- Reading a security book
- Working as a volunteer, such as proctoring (helping to monitor) a CISSP exam
- Creating and submitting questions for future exams

This is by no means a complete list. Other activities may also count as CPE credits. Therefore, it's best to contact (ISC)² to see which ones are valid.

(ISC)² also offers an Associate CISSP program, which is available to those individuals who have developed a level of competence in a certain security area. They may be capable of passing the CISSP exam, but lack the years of practical work experience required to be fully accredited. In addition, to become an Associate they must also subscribe to the (ISC)² Code of Ethics, as well as keep themselves in good standing with the (ISC)².

So how can you benefit by becoming an Associate of (ISC)²? Well, it's a good way to align yourself in the security community when you have yet to gain enough real-world experience. Employers will know that you recognize the need to prove yourself, and are obviously taking the appropriate steps to set yourself apart from others who are uncertified. It also provides you with the backing and resources of the (ISC)². You may not have a CISSP certification, but you will still be recognized as a member of the CISSP community and will know the secret handshake.

What Does This Book Cover?

This book covers everything you need to know to become an (ISC)²-certified CISSP. It teaches you the hows and whys behind corporations' development and implementation of policies, procedures, guidelines, and standards. It covers network, application, and system vulnerabilities, what exploits them, and how to counter these threats. The book explains physical security, operational security, and why systems implement the security mechanisms they do. It also reviews the U.S. and international security criteria and evaluations performed on systems for assurance ratings, what these criteria mean, and why they are used. This book also explains the legal and liability issues that surround computer systems and the data they hold, including such subjects as computer crimes, forensics, and what should be done to properly prepare computer evidence associated with these topics for court.

While this book is mainly intended to be used as a study guide for the CISSP exam, it is also a handy reference guide for use after your certification.

Tips for Taking the CISSP Exam

The test is 250 questions and you are given up to six hours to take it. The exams are monitored by CISSP proctors. Depending on the facility that hosts the test, you may or may not be allowed to bring in food or drink, so plan ahead and eat a good breakfast full of protein and fructose for brainpower. Proctors who allow food and beverages typically require they be in a closable container and generally do not allow you to place them on the desk or table where you could spill anything on your exam paper. Some proctors let you keep your goodies in a bag next to you on the floor, or at the front or back of the room. Proctors may inspect the contents of any and all articles entering the test room. Restroom breaks are usually limited to allowing only one person to leave at a time, so drinking 15 cups of coffee right before the exam might not be the best idea.

The exam questions are not long, which is good because the test has so many questions, but this also means you get less information about what the questions are really asking for. Make sure to read the question and its answers thoroughly instead of read-

ing a few words and immediately assuming you know what the question is asking. Some of the answer choices may have only subtle differences, so be patient and devote time to reading through the question more than once.

Like most tests, it is best to go through the questions and answer those you know immediately, and then go back to the ones causing you difficulty. The CISSP exam is not computerized, so you will receive a piece of paper with bubbles to fill in, and one of several colored exam booklets containing the questions. I bring this up because if you scribble outside the lines on the answer sheet, the machine that reads your answers may count a correct answer as wrong. So, I suggest you go through each question and mark the right answer in the booklet with the questions. Repeat this process until you have completed your selections. At such time, go through the questions again and fill in the bubbles. This approach leads to less erasing and fewer potential problems with the scoring machine. You are allowed to write and scribble on your question exam booklet any way you choose. You will turn it in at the end of your exam with your answer sheet, but only answers on the answer sheet will be counted, so make sure you transfer all your answers to the answer sheet.

Other certification exams may be taking place simultaneously in the same room, such as exams for certification as an SSCP (Systems Security Certified Professional), ISSAP or ISSMP (Architecture and Management concentrations, respectively), or ISSEP (Engineering concentration), which is the $(ISC)^2$/NSA government certification. These other exams vary in length and duration, so don't feel rushed if you see others leaving the room early; they may be taking a shorter exam.

Another certification offered by $(ISC)^2$ is the Certification and Accreditation Professional (CAP). This was developed by $(ISC)^2$ along with the U.S. Department of State's Office of Information Assurance to create what they consider the gold standard in the field of global information security. This CAP credential is intended to be an objective gauge of the level of knowledge, abilities, and skills personnel will be required to have to participate in the Certification and Accreditation process. This deals directly with those professionals tasked with the creation and assessment of a formalized process to be used in determining risk and establishing security requirements. They will also be tasked with ensuring that information systems possess the security necessary to counter potential risks. This is another certification that, depending upon your field, can not only benefit your career but the organization you work for as well.

When finished, don't immediately turn in your exam. You have six hours, so don't squander it just because you might be tired or anxious. Use the time wisely. Take an extra couple of minutes to make sure you answered every question, and that you did not accidentally fill in two bubbles for the same question.

Unfortunately, exam results take some time to be returned. $(ISC)^2$ states it can take up to six weeks to get your results to you, but on average it takes between four days to two weeks to receive your results through e-mail and/or the mail.

If you passed the exam, the results sent to you will not contain your score—you will only know that you passed. Candidates who do not pass the test are *always* provided with a score, however. Thus, they know exactly which areas to focus more attention on for the next exam. The domains are listed on this notification with a ranking of weakest to strongest. If you do not pass the exam, it's best to remember that many smart and talented security professionals didn't pass on their first try either, chiefly because the test covers such a broad range of topics.

One of the most commonly heard complaints is about the exam itself. The questions are not longwinded, like many Microsoft tests, but at times it is difficult to decipher between two answers that seem to say the same thing. Although (ISC)² has been removing the use of negatives, such as "not," "except for," and so on, they do still appear on the exam. This is slowly being remedied and should become less and less of an issue over time.

Note that (ISC)² is currently introducing scenario-based questions, which will be long and will expect you to understand concepts in more than one domain to properly answer the question.

Another complaint heard about the test is that some questions seem a bit subjective. For example, whereas it might be easy to answer a technical question that asks for the exact mechanism used in Secure Sockets Layer (SSL) that protects against man-in-the-middle attacks, it's not quite as easy to answer a question that asks whether an eight-foot perimeter fence provides low, medium, or high security. This complaint is mentioned here not to criticize (ISC)² and the test writers, but to instead help you better prepare for the test.

This book covers all the necessary material for the test and contains many questions and self-practice tests. Most of the questions are formatted in such a way as to better prepare you for what you will encounter on the actual test. So make sure to read all the material in the book, and pay close attention to the questions and their formats. Even if you know the subject well, you may still get some answers wrong—it is just part of learning how to actually take tests.

Familiarize yourself with industry standards and expand your technical knowledge and methodology outside the boundaries of what you use today. I cannot stress enough that just because you are the top dog in your particular field, it doesn't mean you are properly prepared for each and every domain the exam covers. Take the assessment test in this chapter to gauge where you stand, and be ready to read a lot of material you have not read before.

How to Use This Book

Much effort has gone into putting all the necessary information into this book. Now it's up to you to study and understand the material and its various concepts. To best benefit from this book, you might want to use the following study method:

1. Study each chapter carefully and make sure you understand each concept presented. Many concepts must be fully understood, and glossing over a couple here and there could be detrimental to you in the end. The CISSP CBK contains over 300 individual topics, so take the time needed to understand them all.
2. Make sure to study and answer all of the questions at the end of the chapter, as well as those on the CD-ROM included with the book. If any questions confuse you, go back and study those sections again. Remember, some of the questions on the actual exam are a bit confusing because they do not seem straightforward. I have attempted to draft several questions in the same manner to prepare you for the exam. So do not ignore the confusing questions, thinking they're not well worded. Instead, pay even closer attention to them because they are there for a reason.

3. If you are not familiar with specific topics, such as firewalls, laws, physical security, or protocol functionality, use other sources of information (books, articles, and so on) to attain a more in-depth understanding of those subjects. Don't just rely on what you think you need to know to pass the CISSP exam.
4. After reading this book, study the questions and answers, and take the practice tests. Then review the $(ISC)^2$ study guide and make sure you are comfortable with each bullet item presented. If you are not comfortable with some items, revisit those chapters.

If you have taken other certification exams—such as Cisco, Novell, or Microsoft—you might be used to having to memorize details and configuration parameters. But remember, the CISSP test is "an inch deep and a mile wide," so make sure you understand the concepts of each subject *before* trying to memorize the small, specific details.

References

- **Logical Security** www.logicalsecurity.com/resources/resources_quiz_select.html
- **$(ISC)^2$** www.isc2.org
- **CISSP.com Web Portal** www.cissps.com
- **CISSP and SSCP Open Study Guides** www.cccure.org

Questions

To get a better feel for your level of expertise and your current level of readiness for the CISSP exam, run through the following questions:

1. What is derived from a passphrase?
   - **A.** A personal password
   - **B.** A virtual password
   - **C.** A user ID
   - **D.** A valid password
2. Which access control method is user-directed?
   - **A.** Nondiscretionary
   - **B.** Mandatory
   - **C.** Identity-based
   - **D.** Discretionary
3. Which item is not part of a Kerberos authentication implementation?
   - **A.** A message authentication code
   - **B.** A ticket-granting ticket
   - **C.** Authentication service
   - **D.** Users, programs, and services

4. If a company has a high turnover rate, which access control structure is best?
   - **A.** Role-based
   - **B.** Decentralized
   - **C.** Rule-based
   - **D.** Discretionary
5. In discretionary access control, who/what has delegation authority to grant access to data?
   - **A.** A user
   - **B.** A security officer
   - **C.** A security policy
   - **D.** An owner
6. Remote access security using a token one-time password generation is an example of which of the following?
   - **A.** Something you have
   - **B.** Something you know
   - **C.** Something you are
   - **D.** Two-factor authentication
7. What is a crossover error rate (CER)?
   - **A.** A rating used to rank a biometric system
   - **B.** The number of Type I errors
   - **C.** The number of Type II errors
   - **D.** The number reached when Type I errors exceed the number of Type II errors
8. What does a retina scan biometric system do?
   - **A.** Examines the pattern, color, and shading of the area around the cornea
   - **B.** Examines the patterns and records the similarities between an individual's eyes
   - **C.** Examines the pattern of blood vessels at the back of the eye
   - **D.** Examines the geometry of the eyeball
9. If you are using a synchronous token device, what does this mean?
   - **A.** The device synchronizes with the authentication service by using internal time or events.
   - **B.** The device synchronizes with the user's workstation to ensure the credentials it sends to the authentication service are correct.
   - **C.** The device synchronizes with the token to ensure the timestamp is valid and correct.
   - **D.** The device synchronizes by using a challenge-response method with the authentication service.

10. What is a clipping level?

- **A.** The threshold for an activity
- **B.** The size of a control zone
- **C.** Explicit rules of authorization
- **D.** A physical security mechanism

11. Which intrusion detection system would monitor user and network behavior?

- **A.** Statistical
- **B.** Signature-based
- **C.** Static
- **D.** Host-based

12. When should a Class C fire extinguisher be used instead of a Class A?

- **A.** When electrical equipment is on fire
- **B.** When wood and paper are on fire
- **C.** When a combustible liquid is on fire
- **D.** When the fire is in an open area

13. How does Halon suppress fires?

- **A.** It reduces the fire's fuel intake.
- **B.** It reduces the temperature of the area.
- **C.** It disrupts the chemical reactions of a fire.
- **D.** It reduces the oxygen in the area.

14. What is the problem with high humidity in a data processing environment?

- **A.** Corrosion
- **B.** Fault tolerance
- **C.** Static electricity
- **D.** Contaminants

15. What is the definition of a power fault?

- **A.** Prolonged loss of power
- **B.** Momentary low voltage
- **C.** Prolonged high voltage
- **D.** Momentary power outage

16. Who has the primary responsibility of determining the classification level for information?

- **A.** The functional manager
- **B.** Middle management
- **C.** The owner
- **D.** The user

17. Which best describes the purpose of the ALE calculation?
    - **A.** It quantifies the security level of the environment.
    - **B.** It estimates the loss potential from a threat.
    - **C.** It quantifies the cost/benefit result.
    - **D.** It estimates the loss potential from a threat in a one-year time span.
18. How do you calculate residual risk?
    - **A.** Threats × risks × asset value
    - **B.** (Threats × asset value × vulnerability) × risks
    - **C.** SLE × frequency = ALE
    - **D.** (Threats × vulnerability × asset value) × control gap
19. What is the Delphi method?
    - **A.** A way of calculating the cost/benefit ratio for safeguards
    - **B.** A way of allowing individuals to express their opinions anonymously
    - **C.** A way of allowing groups to discuss and collaborate on the best security approaches
    - **D.** A way of performing a quantitative risk analysis
20. What are the necessary components of a smurf attack?
    - **A.** Web server, attacker, and fragment offset
    - **B.** Fragment offset, amplifying network, and victim
    - **C.** Victim, amplifying network, and attacker
    - **D.** DNS server, attacker, and web server
21. In phone phreaking, what is red boxing?
    - **A.** Voltage manipulation
    - **B.** Replaying the noise that coins make when dropping into a pay phone
    - **C.** Using a handheld device attached to a live phone wire to intercept calls
    - **D.** Tone manipulation
22. What do the reference monitor and security kernel do in an operating system?
    - **A.** Intercept and mediate a subject attempting to access objects
    - **B.** Point virtual memory addresses to real memory addresses
    - **C.** House and protect the security kernel
    - **D.** Monitor privileged memory usage by applications

Answers

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