CHAPTER

Becoming a CISSP

This chapter presents the following:

- Description of the CISSP certification
- 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
- 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 subject areas, 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, you can consult and reference extensive resources 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 sixth 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 and help you understand how the domains interact with each other so that you can develop a comprehensive approach to security practices. 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.

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.

Consider the 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. The 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 they still 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

Because the CISSP exam covers the ten domains making up the CISSP Common Body of Knowledge (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 and do not require you to be an expert in every subject. However, the questions do require you to be familiar with many *different* security subjects.

The CISSP exam comprises 250 multiple-choice questions, and you have up to 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 toward 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, Unix, or Cisco). Instead, you will be tested on the security models and methodologies used by these types of systems.

$(ISC)^2$, which stands for International Information Systems Security Certification Consortium, 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. 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 asking you "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.

After passing the exam, you will be asked to supply documentation, supported by a sponsor, proving that you indeed have the type of experience required to obtain this certification. 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 ensure that those who achieve the certification have real-world experience to offer organizations. Book knowledge is extremely important for understanding theory, concepts, standards, and regulations, but it can never replace hands-on experience. Proving your practical experience supports the relevance of the certification.

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' sponsors and contacts to verify the test taker's related experience.

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 forensics. 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.

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 threats • 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, switches, and repeaters • Network topologies and cabling • Attack methods
Information Security Governance 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
Software Development Security	This domain examines secure software development approaches, application security, and software flaws. 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 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 ways that software should be designed securely. It also 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 • 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
Security Operations	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 • Security and fault-tolerance technologies
Business Continuity and Disaster Recovery Planning	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, Investigations, and Compliance	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 • Forensics

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

Domain	Description
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)*

(ISC)² attempts to keep up with changes in technology and methodologies in the security field by adding numerous 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, cross-site scripting attacks, or IPv6.

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.

The test is based on internationally accepted information security standards and practices. If you look at the (ISC)² website 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.

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 that they needed a certification program that would give their profession structure and provide ways for security professionals to demonstrate competence and to present evidence of their qualifications. Establishing such a program would help the credibility of the security profession as a whole and the individuals who comprise it.

In November 1988, the Special Interest Group for Computer Security (SIG-CS) of the Data Processing Management Association (DPMA) brought together several organi-

zations 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 to 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.

How Do You Sign Up for the Exam?

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. You will also be asked to read the (ISC)^2 Code of Ethics and to sign a form indicating that you understand these requirements and promise to abide by them. You then provide payment along with the completed 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.

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 organization's 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.