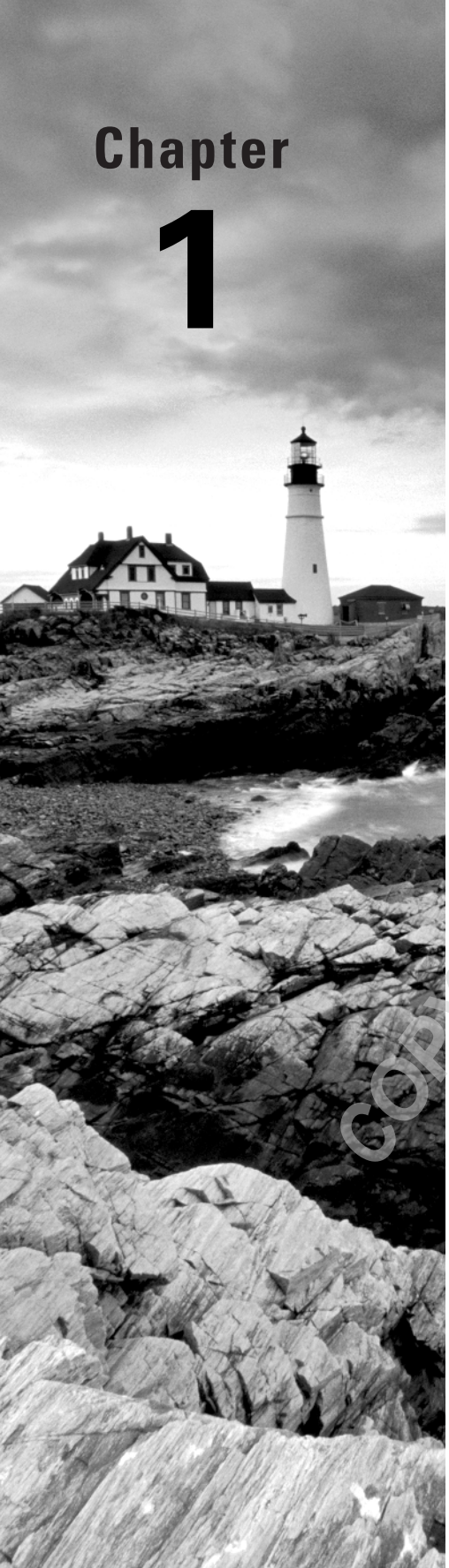


Chapter

1

Information Security: The Systems Security Certified Practitioner Certification

As a candidate for the Systems Security Certified Practitioner certification from (ISC)^2, you should be familiar with the (ISC)^2 organization and the examination requirements, registration procedures, endorsement requirements, and continuing education and annual fee requirements. In addition to introducing you to the requirements, this chapter will help you prepare for the examination. You will learn about various successful study techniques used by other candidates as well as how to register for the exam.

It is important for you to relax and do your best work. By knowing what to expect during your time at the examination center and by being prepared, you will be at ease and will be able to concentrate on the examination subject.

About the (ISC)^2 Organization

The International Information Systems Security Certification Consortium (ISC)^2 is a not-for-profit organization formed in 1989 to offer standardized vendor-neutral certification programs for the computer security industry. The first certification offered by the organization was the Certified Information Systems Security Professional (CISSP) certification. It was based upon a Common Body of Knowledge (CBK). The original CBK was intended to be all-encompassing, taking into consideration every aspect of information security from technical networking, information security models, and theory to physical security, such as fire extinguishers, perimeter lighting, and fences. The Systems Security Certified Practitioner (SSCP) credential was launched in 2001. It was intended as a foundational security credential requiring slightly less in-depth knowledge and a much more limited job experience criteria.

A key element central to the foundation of (ISC)^2 is a Code of Ethics. Every member of the (ISC)^2 organization, including candidates sitting for any of the certification examinations, must agree to and sign the Code of Ethics. It warrants that the members of the (ISC)^2 organization adhere to the highest standards of conduct in the performance of their security duties.

Today, (ISC)^2 is a global entity spanning more than 150 countries worldwide with membership totaling in excess of 100,000 members. The organization has been referred to as the “largest IT security organization in the world.”

(ISC)² History

As the stand-alone PC era evolved into an era of networking during the early 1980s, it became evident that there was a need for network security standardization. Security professionals required the ability to describe their problems and solutions with common terminology. Concepts, tools, and techniques had to be shared between individuals on a worldwide basis to solve common problems and take advantage of shared opportunities. Although during this time various vendors coined terms and definitions specific to their products or sector of the industry, a desire arose for a vendor-neutral body of knowledge and a methodology for granting credentials for individuals who exhibited the knowledge and competence required of the IT security industry.

(ISC)² was founded during the summer of 1989 as a nonprofit organization to address the needs of IT security industry. The organization immediately began organizing a collection of topics relevant to the IT security industry. These topics were structured into a framework of concepts and terminology, with contributions from IT professionals around the world. The framework of ideas, terms, and concepts now known as the Common Body of Knowledge (CBK) allowed individuals from security practitioners to those in academia to discuss, create, and improve the IT security industry as it has evolved through the years.

Organizational Structure and Programs

(ISC)² has evolved into a multifaceted organization offering numerous certifications and credential programs. The organization also offers an outreach program where members can use (ISC)² tools and information to educate themselves and others and to increase the awareness of cyber crime in their local communities. Every year, tens of thousands attend an annual (ISC)² Security Congress, which features seminars and exhibits. Central to the organization is the continuous education of its members. During the year, numerous seminars, webinars, and other training sessions are available for (ISC)² members.

Certifications Offered

The award of a CISSP certification is a global recognition that an individual has proven knowledge in the security information field and has attained a high level of information understanding and professional competence. The CISSP certification has met all of the requirements of the ISO/IEC 17024 standard.

CISSP – Certified Information Systems Security Professional The CISSP certification is recognized around the world as a standard of achievement that recognizes an individual's knowledge in the field of information security. These individuals generally serve in IT management and information assurance and may be employed as managers who assure the security of a business environment.

SSCP – Systems Security Certified Practitioner The SSCP certification is ideal for individuals with at least one year of experience. These individuals may be employed as security practitioners in a network operations center, security operations center, or data center. The SSCP certification is the perfect starting point for somebody beginning an IT security career.

Additional certifications (ISC)^2 offers several additional certifications in the area of healthcare, computer forensics, and system authorization professional and a variety of CISSP certifications. Additional information is available on the (ISC)^2 website.

Worldwide Recognition

(ISC)^2 has principal offices in the United States and additional offices in London, Hong Kong, and Tokyo. Major corporations around the world seek out and employ individuals with (ISC)^2 certifications.

With over 93,000 certified IT professionals located in over 135 countries worldwide, the (ISC)^2 organization has set the standard around the world as the leader in IT security certifications.

Industrial and Government Standards

The SSCP certification has been accredited by the American National Standards Institute (ANSI). The certification is in compliance with the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 17024 standard.

DoD Directive 8570.1 and DoD Directive 8140

In the aftermath of the September 11, 2001, terrorist attacks and with cybersecurity threats surfacing virtually every day around the world, the United States Department of Defense (DoD) has determined that information security and assurance is of paramount importance to the national security of United States. To provide a basis for enterprise-wide standardization to train, certify, and manage the DoD Information Assurance (IA) workforce, The department issued DoD Directive (DoDD) 8570.1.

DoDD 8570.1, enacted in 2004 and rolled out in 2005, is always evolving. Since 2005, major advancements in technology and cybersecurity have occurred, leading to the newest DoDD, 8140. DoDD 8140 was launched in the first quarter of 2015, retiring 8570.1 in full. DoDD 8140 is based on the National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) standard. DoDD 8140 will update DoDD 8570.1, adding additional categories and further defining job roles for better training.

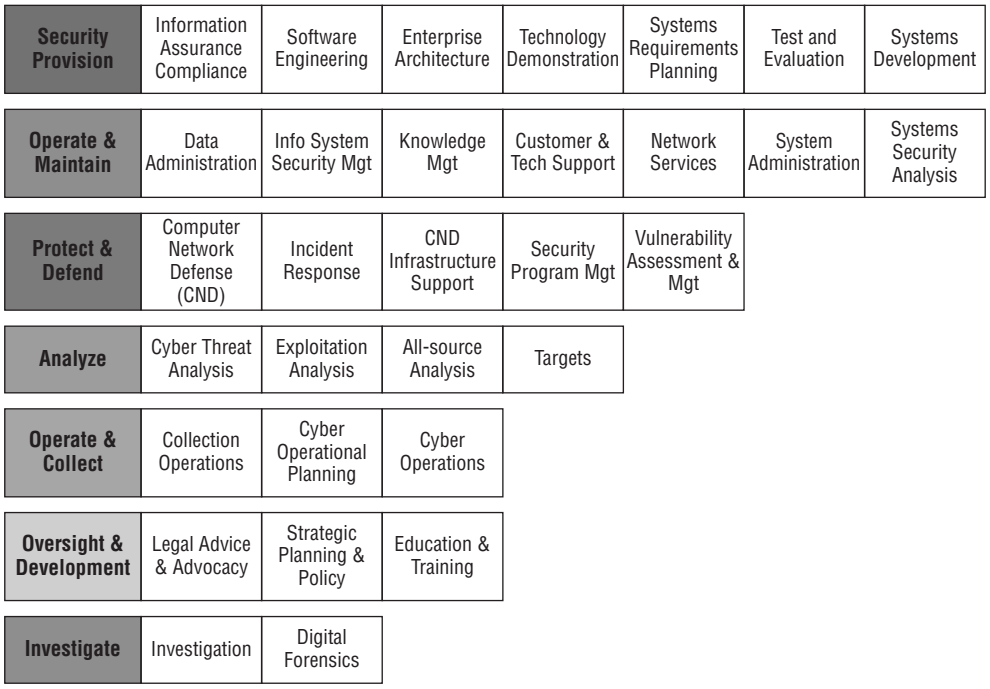
The 8140 directive stipulates a much broader scope than the original 8570.1 document by stating that a person that comes in contact with DoD information must abide by 8140 framework standards. The 8140 document does not concentrate on specific job roles as in the 8570.1 but instead lists categories of job tasks that may be performed by any individual throughout the defense industry.

The 8140 directive consists of several main categories that are further broken down into tasks or special areas. Job skills, training, and focus areas are better defined using this category system. There are seven main categories that have tasks or special areas of their own. The main categories are as follows (see Figure 1.1):

- Security Provision
- Operate and Maintain
- Protect and Defend
- Analyze
- Operate and Collect
- Oversight and Development
- Investigate

The SSCP certified individual may be employed at many of these job types but most specifically in the Protect and Defend job category. The jobs and skill requirements in this category center on securing and defending against cyber-related attacks. Computer Network Defense, Computer Network Defense Infrastructure Support, Incident Response, Security Program Management, and Vulnerability Assessment and Management are the special areas in this category.

FIGURE 1.1 The DODD 8140 chart



Exams, Testing, and Certification

Why certify? Certification represents a mark of achievement and indicates that the individual has attained the required knowledge through personal study, classroom work, or laboratory applications and has passed a requisite examination of sufficient difficulty to thoroughly assess depth of knowledge. To many, the certification represents a milestone in an individual's career. It illustrates diligence, hard work, and a strong desire for self-improvement.

The importance of a certification is a reflection of the esteem and recognition of the institution or organization granting the certification. Hiring officials must recognize the certification as a representation of diligence and hard work on behalf of the individual and also a clear testament to the overall knowledge and skill set as evaluated by an examination. The concept of certifications eliminates the requirement of the hiring official having to "test" the job candidate or having to evaluate their depth of knowledge by some manner.

Certification Qualification: The SSCP Common Body of Knowledge

$(ISC)^2$ has developed, in association with industry experts, a Common Body of Knowledge (CBK) that the certified SSCP individual must know to adequately perform the typical duties required by the job position for which they were hired. In this body of information are seven general categories referred to as *domains*.

The SSCP CBK consists of the following seven domains:

Access Controls Access controls include mechanisms that are based upon policies, procedures, and user identification that control or determine what a user or subject may access and what permissions they have to read, write, or modify any information on a system.

- Administrative, technical, and physical access controls
- Methods of authentication
- Administration of access controls
- Trust architectures, Domains, and zones
- Managing identity using automation
- Aspects of cloud computing

Security Operations and Administration Understanding the concepts of availability, integrity, and confidentiality and how policies, standards, procedures, and guidelines are used to support the AIC Triad.

- Administering security throughout the enterprise
- Managing change, change control mechanisms, change control board
- Baseline security, establishing security criteria

- Culture of security, enterprise security training
- Data and information communication infrastructure
- Host, node and endpoint device security
- Information management policies
- Establishing security practices throughout the enterprise

Monitoring and Analysis Designing and implementing system monitoring controls used to identify events including a process to escalate events into incidents. Utilizing processes and monitoring technology to collect and analyze data from numerous sources.

- Continuous network monitoring
- Analysis of monitoring of real-time and historical event information

Risk, Response, and Recovery The procedures used to perform a risk analysis and the calculations used to determine asset value and cost consequences if the asset is lost. Determine the methods by which risk may be mitigated and addressed. Plan for the ability to maintain essential operations and determine a plan for recovery back to normal operations after an adverse event.

- Risk assessment, risk mitigation
- Risk calculations
- Incident response concepts and activities
- Creating business continuity plans (BCP)
- Creating disaster recovery plans (DRP)

Cryptography The protection of information using techniques that ensure its integrity, confidentiality, authenticity, and non-repudiation, and the recovery of encrypted information in its original form.

The use of encryption methods to protect valuable information from access, ensure data integrity, authenticity, and create non-repudiation and proof of message origin.

- Cryptographic terms and concepts
- Symmetric and asymmetric cryptography
- Non-repudiation, digital signatures and proof or origin
- Certificates

Networks and Communications The design and implementation of network devices, protocols, and telecommunication services to transport information on both public and private networks.

- Network Design and implementation
- Telecommunication methods
- Remote network access

- Network hardware devices
- Utilizing wireless and cellular network technologies

Malicious Code and Activity The implementation of controls and countermeasures to detect and prevent malicious code from attacking either the network or the hosts on the network.

- Detecting malicious code
- Countermeasures against malicious code
- Detecting malicious activity
- Coountermeasures against malicious activity

Additional Sources of Information

The complete candidate information bulletin (CIB) is available on the (ISC)² website. The CIB provides the basic information about the domains covered in the examination. The CIB outline is only a summary of the topics covered on the examination. It is not specifically a study or review guide. The CIB is subject to change, and it is suggested that the candidate refer back to the (ISC)² website from time to time to ensure that the most up-to-date examination information is being studied.

The candidate must also demonstrate at least one year of paid cumulative employment experience in an IT security position. *Cumulative* means that over your working career you spent some time performing the duties within one or more of the seven domains. When listing your experience, combine all of your experiences from any "work" endeavor to obtain a combined amount of experience time. If in doubt, you are invited to call (ISC)² and speak with the representatives about meeting your work experience requirements. You will find that they are extremely friendly and helpful.

If you lack the required work experience, you may still take the examination and become an Associate of (ISC)² until you have gained the required work experience time on the job.

The endorsement form requires the endorser to complete a number of questions specifically about your employment background and experience. This person then signs the form. If a local endorser is not available, (ISC)² may serve as your endorser.

After Passing the Exam

Once you take and pass the exam, you must complete an application and have the application endorsed before you will be awarded the SSCP credential. You may also download the

SSCP Applicant Endorsement Assistance Form from the (ISC)^2 website for endorsement information. The endorsement form may be completed and signed by an (ISC)^2 certified professional who is an active member. During the completion of the endorsement form, the certified professional will attest to your professional experience. If you do not have access to an (ISC)^2 certified professional, you may send all materials to (ISC)^2, which can act as an endorser for you.

With the endorsement form, you will be asked to send a resume illustrating your total work experience. This type of resume is different from a resume used to gain employment with a firm. (ISC)^2 specifically wants to know the length of time you spent gaining experience in any of the SSCP domains. To provide this information, include the name of the company, your title, and two to three sentences concerning your job. Below the brief job description, clearly state one or more of the SSCP domains for which this employment position offered experience. Indicate the start date and end date in whole months. For instance, list a date as May 2014 to November 2014, seven months. Remember that (ISC)^2 requires "cumulative" experience. This may be represented by different periods within the same company, time spent on several different projects, or time employed in a number of different companies.

Although you may have passed the SSCP certification exam, you may not use the SSCP credential or logo until you specifically receive notification with a congratulatory email from (ISC)^2. It is important when communicating with (ISC)^2 or anyone else to not use the SSCP logo or the letters behind your name until you have been authorized to do so. Should you include SSCP on the previously mentioned resume, it would be returned to you with removal instructions.

It is important that you do not use the SSCP logo or designation letters on any communications prior to receiving your authorization email from (ISC)^2. Specifically, do not include a reference to SSCP on your endorsement form or the qualification resume you send to (ISC)^2.

Certification Maintenance

The (ISC)^2 certification is valid for three years. Recertification or continued certification requires that the credentials be kept in good standing. Each certified member is required to submit continuing professional education (CPE) credits (referred to as CPEs) annually over the three-year period. A total of 60 CPE credits are required during the three-year period with a minimum of 10 CPE credits to be posted annually. More information on qualifying CPE credits is available on the (ISC)^2 SSCP website. If you are ever in doubt about whether a CPE qualifies, you can call and talk to the friendly folks at (ISC)^2.

The concept of requiring continuing professional education is an effort to keep the skill levels of various professionals such as lawyers, doctors, nurses, and IT professionals current and up-to-date with the latest concepts and knowledge in the industry. Individuals may take classes, conduct security courses, write articles or books, attend seminars or

workshops, or attend security conventions. All of these activities afford learning experiences to the individual.

As part of certification maintenance, an annual maintenance fee (AMF) of $65 is due each year.

Do not let your certification expire. If it does, you will be required to retake the examination.

Types of IT Certifications?

There are three general types of IT certifications.

Vendor-Neutral Certification To earn a vendor-neutral certification, you pass an examination covering general industry concepts, theories, and applications. *Vendor-neutral* means that information specific to a particular vendor's product is not part of the examination. Vendor-neutral certifications are available for PC technicians and network technicians and cover the subject areas of general IT security and other topics such as cloud computing, database management, Information Technology Infrastructure Library (ITIL®) processes, and IT support.

Vendor Certification Vendor certifications are available from a variety of hardware and software product manufacturers. They represent the attainment of certain level of expertise with the vendor's products. Due to the frequency of vendor product changes, many vendor certifications must be renewed on an annual basis by retaking an examination.

Professional Association Certification Professional associations offer certifications and credentials to individuals who have validated their competency, work experience level, and knowledge of the job. To become a member and earn a credential, candidates must accomplish various steps, such as complete a rigorous training regime, pass an extensive examination, validate work experience or training experience history, and accomplish routine knowledge maintenance through annual CPE requirements.

Professional association certifications usually have a body of knowledge (BOK) established by the professional association. This body of knowledge is usually quite extensive, encompassing a broad range of topics with which the candidate must be familiar. Professional associations also require members to remain in good standing by paying annual maintenance fees or dues and abide by various rules, bylaws, or codes of conduct.

Typical professional associations include those for IT professionals, accountants, lawyers, medical professionals, project managers, engineers, and many other business, industrial, and service professions. Becoming a member of a professional association is by design a difficult task reserved for those who truly deserve the credential.

Generally, all types of certification organizations award their certification on an all-or-nothing basis. The candidate either passes or fails the examination. There is no such thing as "kind of" a CPA in the accounting profession.

Technical or Managerial

A wide variety of talents are required in the IT security industry. It is not unusual for entry-level positions to be of a technical nature, where individuals learn a wide variety of skills as associates, hardware technicians, help desk analysts, network support associates, and incident responders. Many of these individuals perform the tasks of practitioners. Practitioners generally work in the field and have detailed experience or knowledge of networking devices, situational monitoring, and operational software. The SSCP certification is designed for the IT security professional practitioner.

Those in managerial positions require a greater overview of corporate IT systems and must correlate the goals and mission of the enterprise with the design and security of the IT systems and information. Generally these individuals are less nuts and bolts oriented and much more policy driven in a large-scale environment. The CISSP certification is ideal for IT managers, consultants, and senior staff responsible for information security and assuredness within an organization.

Specialty Certifications

$(ISC)^2$ offers a number of specialty certifications for the IT professional.

Certified Authorization Professional (CAP) The Certified Authorization Professional certification recognizes the skills, knowledge, and abilities of individuals responsible for the process of authorizing and maintaining information systems. The certification is intended for those who regularly assess risk and establish documentation and security requirements for the enterprise. These individuals are responsible for the overall security of information systems and ensure that the system security is commensurate with the level of potential risk.

Certified Cyber Forensics Professional (CCFP) The Certified Cyber Forensics Professional demonstrates expertise in the area of forensics investigation and procedures, standards and practices, and ethical and legal knowledge to assure the accurate and complete processing of digital evidence so that it may be admissible in a court of law. The certification also establishes a baseline capability in other information security disciplines, such as e-discovery, incident response, and attack and malware analysis.

HealthCare Information Security and Privacy Practitioner (HCISPP) The HealthCare Information Security and Privacy Practitioner demonstrates knowledge in information governance and risk management, information risk assessment, and third-party risk management within the healthcare industry. These individuals have foundational knowledge and experience throughout the healthcare information security and privacy industry and utilize privacy best practices and techniques to protect organizations and sensitive patient data against breaches, data loss, and organizational threats. They are instrumental in establishing policies, controls, education and training, and risk evaluation throughout an IT organization within an healthcare enterprise.

Certified Secure Software Lifecycle Professional (CSSLP) The Certified Secure Software Lifecycle Professional is an industry leader in application security. This individual

develops application security programs within an enterprise and works to reduce production costs, application vulnerabilities, and delivery delays. This individual works within software production organizations and identifies application vulnerabilities and is knowledgeable of the entire security lifecycle of an application that guides the creation of controls that mitigate risk.

About the Systems Security Certified Practitioner Certification

The Systems Security Certified Practitioner (SSCP) certification is a foundational certification with an emphasis on technical or practical knowledge. For example, it is intended for the person in an active role of systems maintenance, incident detection and response, and other tasks involving equipment support and risk control. The SSCP certification documents the knowledge of an individual and can be displayed on business cards, resumes, and other promotional materials.

What Is the Objective of This Certification?

The SSCP certification demonstrates that the individual has proficiency with IT security knowledge. The certification ensures that the candidate has the requisite knowledge to apply security concepts, tools, and procedures required during security incidents and that the individual can monitor systems and establish safeguards against threats to an organization.

Who Should Take the Certification Exam?

The SSCP certification exam is open to all individuals who are working toward positions like the following within the IT security profession:

- Information assurance technician
- Security architect systems analyst
- Security consultant or specialist
- Database administrator
- Information systems auditor
- Network security engineer
- System administrator
- Network security administrator
- Information systems auditor
- Information systems assuredness specialist
- Security architect
- Information security engineer
- Enterprise security technician

The SSCP certification is an ideal beginning point for those seeking a career in information security technology. It is an ideal introduction to many of the subjects required on future exams, such as the CISSP. (For the knowledge requirements, see the section "Certification Qualification: The SSCP Common Body of Knowledge" earlier in this chapter.)

What If You Are New to IT Security?

The SSCP certification is ideal if you are seeking to improve your information security skills or seeking a position advancement or promotion. The seven SSCP CBK domains cover all of the major topics required by an entry-level IT security professional. These are the same topics covered in greater depth in much more advanced exams.

It is common for an IT security individual to be employed in a position that requires knowledge of only one or two of the domains. It is possible that several of the domains may be quite foreign. Studying for this certification establishes a foundation of knowledge that allows for career advancement, job rotation, management potential, and recognition as a well-rounded IT security professional.

How Much Information Should You Know?

Ideally, the SSCP candidate has at least one year cumulative work experience in one or more of the seven SSCP CBK domains. After the candidate passes the examination, however, this work experience is not necessary to immediately become a member of $(ISC)^2$. Individuals may become an Associate of $(ISC)^2$ until they gain the necessary one year of work experience.

Generally, an interest and a desire to become involved in the fastest-growing segment of the IT industry is all that is necessary to pursue certification. Any prior experience with programming, networking, hardware or software, databases, software applications, or general computer use within an organization is all that is required or desired as a launching point for the SSCP credential.

You will find that the SSCP CBK domains encompass a broad range of topics. What is required is that you have a general understanding of the subject matter and be able to answer examination questions as to the application and definitions of these concepts.

What Do I Have to Do after I Pass the Exam?

The SSCP candidate must complete the endorsement process after successfully completing the examination. The endorsement process has an time limit of nine months after the date of the exam or after the individual becomes an Associate of $(ISC)^2$. If you do not obtain an endorsement within the nine-month endorsement time limit, you will be required to retake the exam in order to become certified.

The following steps are required for endorsement:

Create a Resume This resume should indicate job positions that you have held where you have performed activities supporting any of the SSCP domains. The structure may be simple. This is different than a job-seeking resume. On this type of resume, the $(ISC)^2$

organization wants to identify the job positions you have held and the number of months in each position. Therefore, list the company name, the job position title, and a very brief description of the job responsibilities. Clearly state the beginning and ending dates of this position. For instance, specify May 2007 to December 2007. (ISC)^2 will compute this as May 1 to December 31. Also, it is important to list one or more of the SSCP domains used within this period of time.

Complete the Endorsement Form An SSCP Applicant Endorsement Assistance Form may be downloaded from the (ISC)^2 website. The form must be completed and signed by an (ISC)^2 certified professional who is an active member and who can attest to your professional experience. This member may be located through any one of the numerous (ISC)^2 chapters around the world or possibly through your current employment or a website such as LinkedIn.com. In the event you cannot find an (ISC)^2 certified individual to act as an endorser, (ISC)^2 can act as an endorser for you. Please see the endorsement assistant guidelines on the (ISC)^2 website for additional information about the endorsement requirements.

The resume that you present to the endorser or (ISC)^2 should clearly indicate the number of months you were employed in one or more of the SSCP certification domains.

How Do I Maintain My SSCP Certification?

Credentials are maintained in good standing by participating in various activities and gaining professional continuing professional education credits (CPEs). CPEs are obtained through numerous methods such as reading books, attending seminars, writing papers or articles, teaching classes, attending security conventions, and participating in many other qualifying activities. For additional information concerning the definition of CPEs, visit the (ISC)^2 website.

Individuals are required to post a minimum of 20 CPE credits each year on the (ISC)^2 member website. Generally, the CPE credit posted will be recognized immediately by the system, but it's also subject to random audit. Please note that any CPEs accomplished prior to being awarded the SSCP certification may not be claimed. If an individual accomplishes more than 20 CPEs during one year, the remainder may be carried forward to the following year. The (ISC)^2 website describes CPEs as items gained external to your current employment duties.

An annual membership fee (AMF) of US$65 is required each year. The membership time frame is an annual cycle beginning on the member's certification anniversary date.

What Is My Next (ISC)^2 Certification?

A great many people use the SSCP certification as a stepping stone in their IT security career. In many cases, this may be the first certification obtained. Each of the SSCP CBK

domains is foundational information that will show up in greater depth or granularity in many other IT security certifications. Depending upon the current career track, you may pursue vendor-specific certifications or vendor-neutral certifications to further your knowledge and recognition within the IT security industry. After obtaining the requisite years of work experience, you are encouraged to seek the prestigious CISSP credential from (ISC)^2.

How Do I Use My SSCP Knowledge on the Job?

The Systems Security Certified Practitioner will have the knowledge and awareness of many aspects of protecting and defending cyber systems. This will include an awareness of access control, risk mitigation, change control, and network protection as well as many other knowledge areas that may be employed on the job.

It is important for the SSCP to understand the methods of security protection, hardware, and software systems involved and the tasks and procedures that the practioner may be assigned to perform. The use of your SSCP training will provide you with the skills to be able to confidently and competently perform duties in a professional manner.

Display Your Certification with Pride

The (ISC)^2 organization is recognized worldwide as offering the most prestigious IT security certifications. Through the requisite learning process, extensive examination, work history evaluation, subscription to the (ISC)^2 ethics statement, and annual maintenance through continuing education, employers and others throughout the industry recognize and revere the certifications.

Obtaining the SSCP certification is a career milestone. Once awarded, the SSCP letter designation may follow your name on business cards, stationery, and signature lines. You may proudly display the (ISC)^2 SSCP logo and have it associated with your professional work. You will receive a signed, full-color, gold-foil-embossed certificate as illustrated in Figure 1.2, which may be framed and proudly displayed in your office or work area. You will be further identified by an (ISC)^2 member number, which is printed on your certificate. At any time, employers may validate your certifications through the (ISC)^2 organization.

Actively Participate

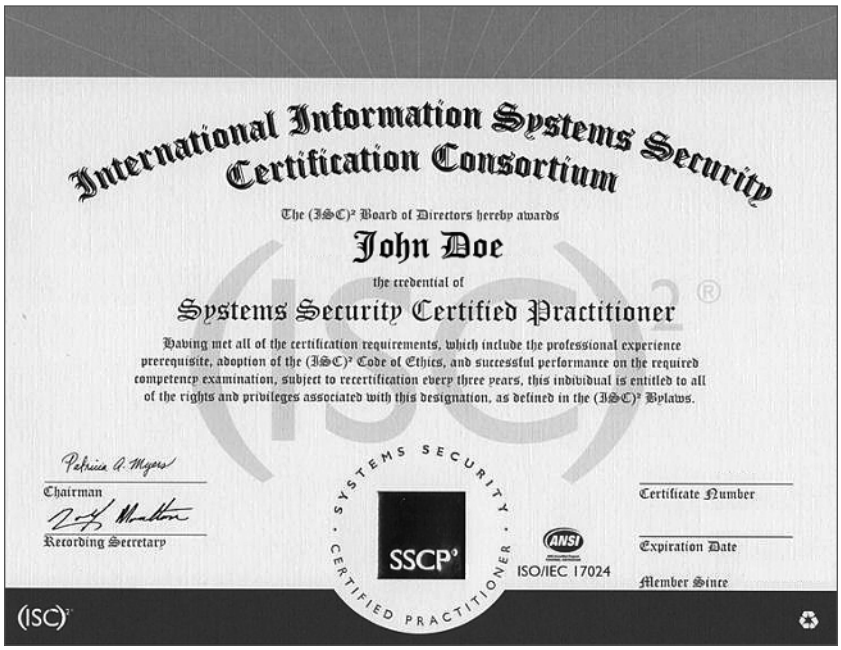
All (ISC)^2 members are encouraged to actively participate within their organization and throughout their community. (ISC)^2 offers numerous training opportunities such as webinars, magazines, and emails as well as seminars, symposiums, and a security congress. There are think-tank roundtables, local events, and the Global Academic Program (GAP). All of these activities are explained on the (ISC)^2 website.

Demonstrate Your Knowledge at Every Opportunity

As an SSCP, you will be recognized as having attained a certain level of expertise and IT security knowledge. Company managers, supervisors, team leaders, and other individuals

may seek you out for insight on how IT security impacts their specific projects or duties in the enterprise as a whole.

FIGURE 1.2 A typical framed SSCP certification



(ISC)² members are also encouraged to participate in community programs by spreading the word of IT security. Each member is encouraged to participate in the (ISC)² sponsored Safe and Secure Online Program. The Safe and Secure program features a security seminar that can be presented to schoolchildren, churches, organizations, and other general groups of people interested in IT and online security. (ISC)² supplies all of the manuals and booklets and facilitator guides required to conduct the seminars.

Join a Local (ISC)² Chapter

The (ISC)² organization has numerous local chapters around the world. You can locate them by accessing the chapter directory on the (ISC)² website. Various chapters may be titled as an (ISC)² CISSP chapter, but do not let that deter you. Feel free to contact the chapter manager or membership manager and invite yourself to their meeting. Participating in (ISC)² chapter meetings will allow you to meet and network with many of the top IT security professionals in the area. Organization dues are minimal, and usually each chapter offers a speaker or a program at each meeting. You do not have to hold a current credential prior to visiting a chapter meeting. Chapter meetings are a great place to learn about the IT security industry, and many of the individuals within a chapter can be approached for study suggestions, subject questions, or even mentoring or tutoring.

The SSCP Exam

The SSCP exam is a skills and knowledge security exam sponsored by (ISC)^2. The exam is focused on understanding key security concepts.

Exam Type The exam is what's called a proctored examination, which means that an individual will be available in the testing room at all times. In some test centers, each test booth will usually be monitored by closed-circuit TV camera.

Number of Questions The SSCP exam consists of 125 multiple-choice questions. Only 100 of the questions are graded, and 25 of the questions are evaluated for future tests. The 25 test questions will not be marked. Therefore, you must answer all 125 questions as if they are all graded.

Question Description Exam questions will have four possible answers. There are no true or false questions. There will be no blanket scenario questions in which a scenario is stated and several following questions refer to the scenario.

You may expect some situation questions, which describe a situation and ask for the action that you would take in this situation. All acronyms will be spelled out, such as, for instance, access control list (ACL). Many questions will ask for the MOST correct or LEAST correct or use logical operators such as NOT, ALWAYS, BEST, TRUE, or FALSE. You should carefully read and understand any questions that contain any qualifier word. In most cases, this word with be in all capital letters, but carefully read any question, whether or not there are capitalized words.

It is important to remember that you are not penalized for wrong answers. Even if it is a guess, make sure every question has a marked answer.

Passing Score Passing score is 700 out of a possible 1,000. It is reported that the questions are weighted values. This means you may be required to have more or less than 70 correct to pass the exam. The examination is pass/fail.

Preparing for the Exam

You can prepare for the SSCP examination through a variety of activities and techniques:

- Referring to the candidate information bulletin
- Reading this book
- Attending (ISC)^2 classroom-based training
- Attending (ISC)^2 online training
- Attending (ISC)^2 private, onsite training (usually sponsored by a company)

For additional information concerning classroom-based training, online training, or private training, email `education@(ISC)².org` or call 1.866.462.4777 or +1.703.781.6781 outside the United States.

Although it's nice to use the (ISC)^2 training products, please do not think that they are necessary. The majority of individuals who have passed the SSCP exam have done so by self-studying and reading.

Study Time

As you may remember from high school or college, studying for any exam takes time and diligence. Not only must you read through the material, but you must be able to understand the topics and concepts to adequately be able to answer the questions. The challenge on a certification exam such as the SSCP is the broad scope of the information contained in seven domains. While some of the material will seem easy and logical, it may be very easy to become bogged down in other topics.

Finding a location to study is not always easy in our busy lives. The place you select should be private and quiet. This examination is not something that you can study for in a local coffee shop. If you find yourself easily distracted by sounds, many sporting goods stores offer inexpensive earplugs or hearing protection headphones that may reduce the distraction from noise in your study location. If you must select between a location with noise and a location with people coming and going, choose the noisy location with privacy and use earplugs rather than being tempted to look up every time somebody passes by.

Study Techniques, Habits, and Methods

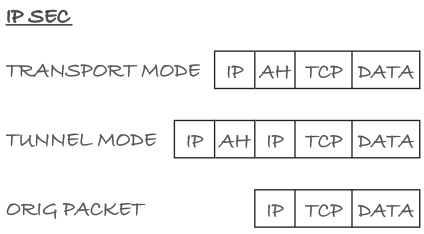
Through our high school and college years, many of us developed a variety of study techniques, habits, and learning methods, some better than others. It is a proven fact that we learn differently. We all have five senses, and some of us make use of these senses in different ways. The following list includes some personal study techniques shared over the years by college students who were studying technical or complex subjects.

Read and Mark While reading the text, mark, highlight, underline, or make comments in the margin.

Read and Rewrite While reading the text, rewrite or summarize the concept on a notepad in your own words. Writing things down in our own words reinforces what we are reading.

Read and Draw While reading the text, draw a rough picture or illustration of the concept. This takes a little more creative thinking, and some of us see concepts as pictures or illustrations. Figure 1.3 illustrates a typical hand-drawn rough sketch of an SSCP topic. This is also a handy memory technique because in some cases, an illustration or picture is easier to recall than text.

FIGURE 1.3 An example of a hand-drawn rough sketch

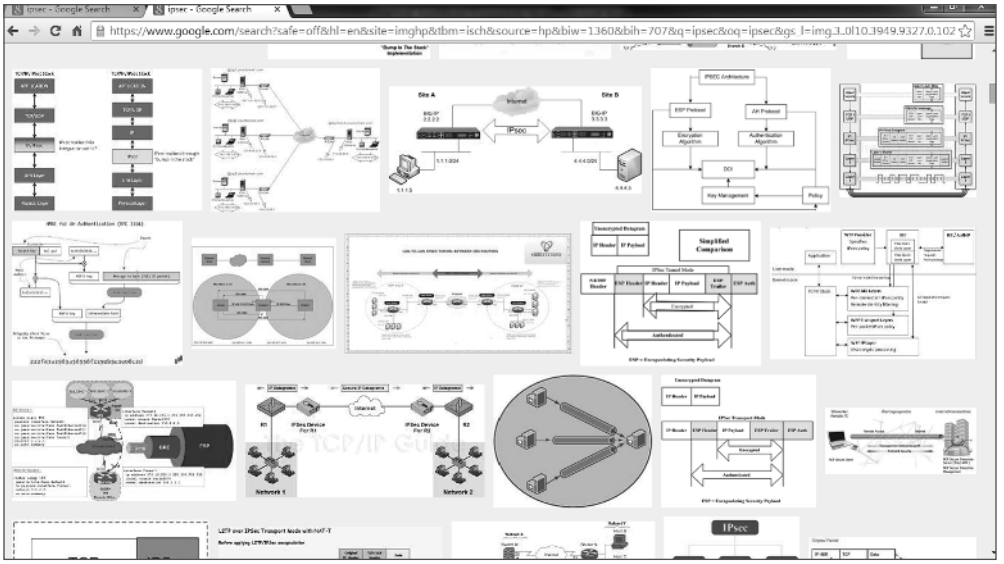


Read and Look Up Some students like to read different authors' explanations of a concept. In this case, some use two books and refer to the exact same subject in both books, or they utilize an online search, dictionary, or encyclopedia for further research on the subject.

Read and View a Video Over recent years, video-sharing sites such as YouTube.com have allowed the ability to view a short presentation on a specific subject. These presentations can last from a few minutes to an hour or more. While some presenters are better than others, the ability to view a presentation, especially a short one, has its advantages as a learning technique. A typical YouTube video on IPsec is at `www.youtube.com/watch?v=rwu8__GG_rw`.

Read and View a Picture A similar technique to viewing a video is to view a picture or illustration of the subject. Several students utilize the technique of using Google images, Yahoo! images, or other search engines to find pictures or illustrations of concepts. For instance, complex subjects such as Public Key Infrastructure, Kerberos, and IPsec are depicted in dozens of drawings and illustrations gathered from websites around the Internet. Within the search results, you can click an image to be directed to the site containing it. In many cases, there is an explanation of the concept and the image. Figure 1.4 illustrates the results of a Google Images search for images on IPsec.

FIGURE 1.4 An example of a Google Images search on the term *IPsec*



Read, Record, and Listen Many of us learn by listening. The read-record-listen technique is a method used by some students to study materials while on the go. The student first reads the material in the book out loud in a normal tone of voice while recording it onto their electronic device such as a phone, pad, tablet, or laptop. Then, as time permits, they

play back their recording as many times as they wish. Students have expressed that this works great when running or exercising or when driving or commuting.

Read and Explain A favorite of college graduate students is the read-and-explain study concept. In many universities, some grad students assist professors by stepping in, sometimes at the last minute, and teaching part of an undergraduate class. Using this technique, they read the book material in order to explain it to somebody else.

If you use this technique, envision reading material as if you had to explain the concept to your boss, a committee at work, or even a family member. This allows you to dissect the information and then reform it in your own words so that you can verbally explain it. While you're doing this, jot down some talking points or "lecture notes" on your notepad for your made-up presentation.

Read and Form a Question Critical thinking has always been part of the learning process. The "read and form a question" concept is a very efficient way of understanding the material. When you read a block of information, stop and ask yourself, "How could I form an examination question based on this information?" In this exercise, place the topic or subject of the information somewhere in your question and create a multiple-choice answer out of the remaining information that refers to or defines the topic or subject. Then switch it around so that the subject is actually one of the answer selections and the description is the question.

When studying, it is easy to become immersed in the subject, especially if you are researching or watching a video. It is important to remember the scope of the SSCP exam subject matter. The exam covers only the terms and definitions of security concepts. This is an entry-level examination in IT security for individuals with one year of experience. It is very easy to find an incredible amount of very detailed information on any IT security subject and become very frustrated.

Many of us learn by using different styles and techniques. Some of us learn by reading, listening, visualizing, and doing something in connection with the subject. Use the study techniques outlined in this chapter not only to prepare for the SSCP exam but also while studying for any future exams.

Setting Goals

It is easy to become distracted in our everyday lives. There are always demands from our jobs, family matters, personal problems, and even procrastination. As with any project, it's always beneficial to create a time frame for accomplishing a project or activities within the project. You might start by establishing an examination date. If you're prone to procrastination, even go so far as to book the exam and pay for the examination voucher. Once you have set the examination date, you have the ability to work backward to schedule your study activities. This may assist you in keeping focused on the task of becoming an SSCP.

Booking the Exam

The SSCP examination may be scheduled and taken at a Pearson VUE professional testing center. To schedule an exam, go to the (ISC)^2 website. You will then be redirected to the Pearson VUE scheduling site. Please note that the (ISC)^2 utilizes the Pearson Professional Centers. The Pearson Professional Centers provide for greater security and candidate authentication. In any metropolitan area, there may be only a few of the Professional Centers compared to many regular Pearson VUE testing centers.

Make sure you read and understand the cancellation, reschedule, and refund policy concerning the examination. Since this is a three-hour examination, exams will begin at only certain times during the day, and in some testing locations, exams may be offered only a few times each month. In the event that you have difficulty finding a Pearson Professional Center, click the Pearson VUE customer service link on the Pearson VUE scheduling website.

While on the Pearson VUE exam scheduling website, you'll see that the SSCP examination is offered in a number of languages. You may select the language of your choice. The examination is available in the following languages:

- English
- Indonesian
- Japanese
- Portuguese – Brazilian

Exam Fees and Payment

An exam voucher may be attained and fees paid during the scheduling process on the Pearson VUE website. Vouchers may be obtained in bulk on the (ISC)^2 website. This is ideal for companies that are scheduling a number of people for various exams. Of course, the more vouchers purchased, the greater the discount.

Exam Reschedule and Cancellation policy

It is very important to understand the Pearson VUE exam reschedule and cancellation policy. This policy is stated on the Pearson VUE website and is reiterated after you have scheduled the exam and purchased the voucher. It's advisable to immediately contact Pearson VUE if you have a conflict with the exam date and/or time.

Reschedule Policy If you wish to reschedule your exam, you must contact Pearson VUE at least 24 hours prior to your exam appointment. If you reschedule an exam less than 24 hours prior to your appointment, you will be subject to a same-day forfeit exam fee. Exam fees are also forfeited for no-shows. There is a $50 fee to reschedule an exam.

Cancellation Policy If you wish to cancel your exam, you must contact Pearson VUE 24 hours prior to your scheduled appointment. If you cancel an exam less than 24 hours prior to your appointment or miss your exam, the result may be forfeiting your exam fees. There is a $100 fee for cancellations.

These policies were in effect at the date of publication of this text. You are advised to contact the Pearson VUE website for up-to-date information.

(ISC)² Code of Ethics and NDA

You will be asked to read the (ISC)² Candidate Background Qualifications. The acknowledgement question on the website is as follows:

> *I have read and acknowledge that I am eligible for certification with (ISC)² based on the criteria outlined on https://www.isc2.org/candidate-background.aspx
>
> ○ I am eligible for certification

(ISC)² requires that the examination candidate agree to and sign the Code of Ethics and a nondisclosure agreement (NDA). The NDA is on the Pearson VUE website at `www.pearsonvue.com/isc2/isc2_nda.pdf`. It is highly recommended that you read it prior to getting to the exam location. At the very beginning of the exam, you will be presented with the NDA, and you will have 5 minutes to read and accept the agreement. If the 5-minute time limit expires, you will not be able to take the exam and all exam fees will be forfeited.

Taking the Exam

Many of us like to plan ahead. We like to know what to expect. When taking exams, it is important to not create added stress through surprises. In the following sections, you will learn about some best practices and what to expect during your visit to the examination center.

It is often comforting to have a plan for what to do and how to relax the evening before an exam and what to do the morning or afternoon of exam day. For example, you can plan for unusual traffic delays or take into account the time involved locating the exam center in an unfamiliar part of the city.

Evening before the Exam

It may have worked for some people when they were in college, but the SSCP exam is not something that you can cram for the evening before. As mentioned earlier, you should establish a study regime that allows you adequate time to read and reflect on the material. The evening before the exam, you might do a very brief review, have a good dinner, and get plenty of rest. Although you may not need all of the time allotted, it is a three-hour exam.

Day of the Exam

It is important to plan the day of your exam. Here are some best practices to keep in mind:

Scheduling and Arrival Allow yourself plenty of time. Depending on the testing center location, monitor the distance and traffic so that you arrive in plenty of time. It is highly

suggested that you arrive at least a minimum of 30 minutes prior to your scheduled examination time. There are two reasons for this:

- You may have a few forms to complete and various security steps to authenticate your identity.
- The Pearson Professional Centers test a large number of individuals in a wide array of certifications, from pharmacy tech to real estate, and there could easily be a dozen people ahead of you arriving for the same time period.

What to Bring When you register and pay your examination fee, you'll receive a confirmation email. It is highly suggested that you print this email and bring with you. You also need to bring two pieces of identification, and one must have your picture on it and both must have your signature. There are a number of items that qualify as personal authentication listed on the Pearson VUE website.

What to Expect upon Arrival Pearson Professional Centers follow thorough procedures prior to allowing someone to sit for an exam. You will be asked to fill out various forms and provide certain information, present your identification, and be subjected to several palm scans or other security identification procedures prior to entrance into the examination room. Lockers will be provided for all of your personal effects. Everything, including cell phones, watches, wallets, and all assorted pocket items, must be placed in the locker.

In the Testing Room Most of the Pearson Professional Centers feature a large number of 4-foot-wide testing cubicles. Of course, each cubicle contains an individual computer workstation. Most of the testing centers offer noise-reduction headphones at each workstation. If they do not have the headphones, you may request or be offered noise-canceling earplugs. Because other individuals come and go or are being set up on their workstations, it is highly advised that you use the noise-canceling earplugs or headphones to reduce distracting noise.

Plastic Worksheet Each exam candidate will be issued a plastic worksheet and an erasable marker pen. The worksheets are specifically used during the examination in lieu of scrap paper to make computations or notes.

An ideal use for the plastic worksheet is for a memory dump. Upon beginning the examination, many examination candidates write down on the plastic worksheet information they memorized, including items that might be confusing or detailed, such as the layers of the OSI model, the names of various protocols, cryptography algorithms, and risk formulas. This may be done prior to answering the first test question when the information is fresh in your mind.

In the Testing Room This is a three-hour examination. You will be instructed to raise your hand if you need assistance from the proctor—for example, if you need to use the restroom, take medications, eat something, or for any other activity. If you need to bring medications or bottled water into the testing room, you are advised to discuss this at the front desk when signing in.

Taking a Break It is possible for you to take a break during the exam. You are advised to raise your hand to summon the exam proctor. Advise the proctor of your desires, such as, for instance, to take a restroom break or just to leave the room for a little bit. The proctor will make the necessary arrangements. You will not be able to leave the immediate premises to smoke.

Because this is a three-hour exam, you may take a break. This might encompass sitting back in your seat and relaxing for a few minutes, standing at your place and stretching quietly, or taking a few steps. When standing, stretching, or communicating with the proctor, it is important to not create any distraction for other exam takers.

Many exam takers use a break as a stopping point or goal. For instance, you might take a first pass through the exam, answering questions that you recognize and marking those that you wish to return to. At the end of the first pass, you might take a short break. You would then proceed through a second pass, reviewing the questions that were marked during the first pass.

Using the Testing Exam Engine At the beginning of the examination, you will be asked to read and authorize the $(ISC)^2$ Code of Ethics and nondisclosure agreement. Remember, you should read this prior to entering the examination room. You will have 5 minutes at the beginning of the exam to do this.

When the exam begins, you will observe a multiple-choice question and four possible answers. In the upper-right portion of your screen, you will see a Mark For Review button. This allows you to return to questions you had a problem with or would like to review at the end of the exam. In the lower section of the screen, you will see forward and back buttons so that you can navigate through the exam. At the end of the exam, you will see a page listing the questions you have marked for review. You can access and review any of the questions prior to submitting your final exam result. At the end of the exam, there will be a Finish And Submit button, which ends the exam.

Stress and Relaxation Techniques It's a proven fact that lots of oxygen will help your brain cells. During any kind of examination, it's recommended that you breathe deeply from time to time. Feel free at any time to stand up, shake it out, or walk around a little. If you have any difficulties at all, raise your hand and ask for the proctor.

Answering Questions Wrong answers do not count against you. Therefore, it is important that you mark every question with an answer, even if it is a guess. *Do not leave anything blank*. At the end of this book there is a complete section about the techniques of taking multiple-choice tests.

Upon Exam Completion Your exam will end either at the end of the allotted time or when you click the finish or submit button. You will not be told immediately if you pass or fail the exam. Raise your hand and the proctor will escort you out of the room. You'll receive a printed copy of your examination report at the front desk. Expect either a "Congratulations; you have passed" or a listing of the domains you must study in more detail for your next examination attempt.

Certifications, (ISC)^2 Website, and Members Login

(ISC)^2 is very good about responding to you by email with the expected number of weeks it requires to complete the procedures prior to issuing you a certificate. Upon submission of your resume and endorsement form, you'll receive an email specifying the amount of time required to review the materials. Once your resume and endorsement form have been approved, you'll receive an email congratulating you for having been awarded the SSCP certification. The same email also specifies that you will receive your certification certificate within four to six weeks.

Each member of (ISC)^2 receives a member number. Once you receive your member number, you may access the (ISC)^2 website, establish login credentials, and view members-only information. While on the (ISC)^2 member website, you may also complete your member profile, view open jobs and positions, and subscribe to various periodicals and webinars.

Summary

In this chapter, you became familiar with the (ISC)^2 organization and its history and the certifications it offers. Various corporate, industrial, and government organizations either require certifications or will state that they prefer candidates for employment to have acquired various certifications.

The SSCP exam is based upon the SSCP Common Body of Knowledge, which has been established as including the knowledge and skills an SSCP should possess. Examination vendors are typically vendor neutral, vendor specific, or a professional association. (ISC)^2 is a professional association offering premier certifications that are recognized worldwide.

Most successful exam candidates plan their study time and use various methods such as marking the textbook, drawing a concept, or viewing pictures or videos. It is also important to relax and not cram the evening before the exam. Planning for the exam day is also important. The examination centers are busy places. At Pearson Professional Centers, you should register no later than 15 minutes prior to exam time, but it is suggested that you arrive 30 to 45 minutes prior to the exam because other folks will be registering before you. In many centers, expect to "take a number." As an exam taker, you may take a break, call the exam proctor, and make use of a plastic marker sheet and erasable pen during the exam.

I discussed various strategies for taking the exam, such as making an initial pass through the exam and answering questions you recognize first and then returning to those you have marked to review at a later time. All answers count, so do not leave any blank.

Exam Essentials

Common Body of Knowledge The SSCP certification was based upon a Common Body of Knowledge (CBK). The original CBK was intended to be all-encompassing, taking into consideration every aspect of information security, including technical networking,

information security models and theory, and physical security such as fire extinguishers, perimeter lighting, and fences.

Department of Defense Directive 8570.1 and Department of Defense Directive 8140 The US Department of Defense Directive 8570.1, signed in August 2004, requires every full- and part-time military service member, defense contractor, civilian, and foreign employee with privileged access to a DoD system, regardless of job series or occupational specialty, to obtain a commercial certification credential that has been accredited by the American National Standards Institute (ANSI).

Department of Defense Directive 8140 replaces 8570.1, which has been retired. DODD 8140 encompasses a much broader scope based upon job tasks rather than position titles.

Work Experience Requirement To qualify for the SSCP certification, a candidate must have at least one year of cumulative paid full-time work experience in one or more of the seven domains.

Endorsement Requirement An endorsement form may be downloaded from the $(ISC)^2$ website. This form must be completed and signed by an $(ISC)^2$ certified professional who is an active member and who can attest to your professional experience. In the event that an $(ISC)^2$ certified professional is not available, $(ISC)^2$ may act as the endorser.

SSCP Exam Description The SSCP exam consists of 125 questions, of which only 100 are graded. The exam must be completed within 3 hours and features only multiple-choice questions. A passing score of 700/1,000 is required. You either pass or fail the examination; no score is given.

Answering Test Questions Wrong answers do not count against you. Mark every question with an answer, even if it is a guess. Do not leave any answers blank.