SSCP®
Candidate Information Bulletin
(Exam Outline)
Effective Date: February 1, 2012

Systems Security Certified Practitioner
ISSA Certified Practitioner

© 2012 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited.
Non-Discrimination

ISC² does not discriminate candidates based on their nationality, gender, religion, race, ethnicity, sexual orientation, age and disability. For further information on ISC²’s non-discrimination policy, please visit https://www.isc2.org/legal-info-policies.aspx.
1) ACCESS CONTROLS ............................................................................................................................................... 5
   Overview .......................................................................................................................................................... 5
   Key Areas of Knowledge ................................................................................................................................. 5
2) SECURITY OPERATIONS & ADMINISTRATION ......................................................................................... 7
   Overview ........................................................................................................................................................ 7
   Key Areas of Knowledge ................................................................................................................................. 7
3) MONITORING AND ANALYSIS ..................................................................................................................... 9
   Overview ........................................................................................................................................................ 9
   Key Areas of Knowledge ................................................................................................................................. 9
4) RISK, RESPONSE, AND RECOVERY ........................................................................................................... 10
   Overview ......................................................................................................................................................... 10
   Key Areas of Knowledge ................................................................................................................................. 11
5) CRYPTOGRAPHY .......................................................................................................................................... 12
   Overview ......................................................................................................................................................... 12
   Key Areas of Knowledge ................................................................................................................................. 12
6) NETWORKS & COMMUNICATIONS ............................................................................................................... 13
   Overview ......................................................................................................................................................... 13
   Key Areas of Knowledge ................................................................................................................................. 13
7) MALICIOUS CODE & ACTIVITY .................................................................................................................. 15
   Overview ......................................................................................................................................................... 15
   Key Areas of Knowledge ................................................................................................................................. 15
REFERENCES ......................................................................................................................................................... 17
GENERAL EXAMINATION INFORMATION .................................................................................................... 23
   Paper Based Test (PBT) .................................................................................................................................. 23
Any questions? .................................................................................................................................................... 26
GENERAL EXAMINATION INFORMATION .................................................................................................... 27
Computer Based Test (CBT) ............................................................................................................................... 27
Registering for the Exam ..................................................................................................................................... 27
Scheduling a Test Appointment .......................................................................................................................... 28
Non Disclosure .................................................................................................................................................... 31
Day of the Exam .................................................................................................................................................. 31
Any questions? .................................................................................................................................................... 35

© 2012 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1-10-14 - V17
The Systems Security Certified Practitioner (SSCP) certification measures the competence of a security professional against an internationally accepted common body of knowledge encompassing seven (7) security domains including Access Controls, Security Operations & Administration, Monitoring and Analysis, Risk Response and Recovery, Cryptography, Networks and Communications and Malicious Code and Activity.

The SSCP is geared toward individuals who may hold technical and engineering related information technology positions such as network security engineers, systems security analysts, security administrators as well as non-security specific technical positions that require an understanding of security concepts and of best security practices including system administrators, application programmers, database administrators and systems analysts.

This Candidate Information Bulletin provides:
- an exam blueprint to a limited level of detail that outlines major topics and sub-topics within the domains,
- suggested reference list,
- description of the format of the items on the exam, and
- basic registration/administration policies.

Before candidates are allowed to take the test at testing centers, they must respond “yes” or “No” to the following four questions regarding criminal history and related background:

1. Have you ever been convicted of a felony; a misdemeanor involving a computer crime, dishonesty, or repeat offenses; or a Court Martial in military service, or is there a felony charge, indictment, or information now pending against you? (Omit minor traffic violations and offenses prosecuted in juvenile court).
2. Have you ever had a professional license, certification, membership or registration revoked, or have you ever been censured or disciplined by any professional organization or government agency?
3. Have you ever been involved, or publicly identified, with criminal hackers or hacking?
4. Have you ever been known by any other name, alias, or pseudonym? (You need not include user identities or screen names with which you were publicly identified).

A candidate is required to have a minimum of one year of cumulative paid full-time work experience in one or more of the seven domains of the (ISC)^2 SSCP CBK®.

SSCP practitioner's experience includes:
- Work requiring special education or intellectual attainment, usually including a technical school, liberal education or college degree.
- Work requiring habitual memory of a body of knowledge shared with others doing similar work.
- Management of projects and/or other employees.
- Supervision of the work of others while working with a minimum of supervision of one's self.
- Work requiring the exercise of judgment, management decision-making, and discretion.
- Work requiring the exercise of ethical judgment (as opposed to ethical behavior).
- Creative writing and oral communication.
- Teaching, instructing, training and the mentoring of others.
- Research and development.

The specification and selection of controls and mechanisms (i.e. identification and authentication technology) (does not include the mere operation of these controls).
1) ACCESS CONTROLS

Overview

Tasks within the access controls domain permit management to specify what users are permitted to do, which resources they are allowed to access, and what operations they are able to perform on a system.

Access controls provide system managers with the ability to limit and monitor who has access to a system, and to restrain or influence the user’s behavior on that system. Access control systems define what level of access an individual has to the information contained within a system based upon predefined conditions such as authority level or group membership. Access control systems are based upon varying technologies including passwords, hardware tokens, biometrics, and certificates, to name just a few.

Each access control system offers different levels of confidentiality, integrity and availability to the user, system and stored information.

The candidates are expected to demonstrate their knowledge of how different access control systems operate and how they are implemented to protect the system and its stored data. In addition, they must demonstrate knowledge in account management, access control concepts, and attack methods that are used to defeat access control systems.

Key Areas of Knowledge

A. Implement Logical Access Controls in Terms of Subjects
   A.1 Requirements for access controls

B. Implement Logical Access Controls in Terms of Objects
   B.1 Requirements for access controls
   B.2 Object groups

C. Implement Authentication Mechanisms (e.g., single/multi-factor authentication, single sign-on, offline authentication)

D. Apply Access Control Concepts (e.g., least privilege, and separation of duties)
   D.1 Discretionary Access Control (DAC)
   D.2 Non-discretionary Access Control
E. **Manage Internetwork Trust Architectures** (e.g., extranet, third party connections, federated access)

F. **Implement identity management**
   
   F.1 Provisioning
   
   F.2 Maintenance
   
   F.3 Entitlement

G. **Understand basic security concepts related to cloud computing** (e.g., virtualization, data control, storage, privacy, compliance)
2) SECURITY OPERATIONS & ADMINISTRATION

Overview

Security operations & administration domain entails the identification of an organization’s information assets and the documentation required for the implementation of policies, standards, procedures and guidelines that ensure confidentiality, integrity and availability. Working with management, information owners, custodians and users, the appropriate data classification scheme is defined for proper handling of both hardcopy and electronic information.

The candidates are expected to demonstrate knowledge in privacy issues, data classification, data integrity, audit, organization roles and responsibilities, policies, standards, guidelines, procedures, security awareness and configuration controls and the application of accepted industry practices.

Key Areas of Knowledge

A. Adhere to Code of Ethics
   A.1 Understand and comply with ISC² code of ethics
   A.2 Understand and comply with the organizational code of ethics

B. Perform Security Administrative Duties
   B.1 Maintain adherence to security policies, baselines, standards and procedures
   B.2 Validate security controls
   B.3 Data classification (e.g., control, handling, categorization)
   B.4 Asset Management (e.g., hardware, software, data)
   B.5 Develop and maintain systems and security control documentation

C. Perform Change Management Duties
   C.1 Assist with implementation of Configuration Management Plan
   C.2 Understand the impact of the changes to the environment
   C.3 Test patches, fixes and updates (e.g., operating system, applications, SDLC)

D. Provide security evaluation and assistance to the organization (e.g., product evaluation, data flow management)
   D.1 Support certification and accreditation (i.e., security authorization)

E. Participate in Security Awareness Education
F. Assess the information communication technology infrastructure using appropriate tools (e.g., discovery, security)

F.1 Understand impact of security testing

G. Understand concepts of endpoint device security (e.g., virtualization, thin clients, thick clients, USB devices, mobile devices)

H. Comply with data management policies (e.g., storage media (paper or electronic), transmission archiving, retention requirements, destruction, deduplication, data loss prevention, social network usage, information rights management (IRM))

I. Understand security concepts (e.g., confidentiality, integrity, availability, privacy)
3) MONITORING AND ANALYSIS

Overview

Within the monitoring and analysis domain, monitoring deals with activities that are accountable for collecting information, providing methods of identifying security events, assigning priority to these events, taking the appropriate actions to maintain the security of the system, and reporting the pertinent information to the appropriate individual, group, or process.

Analysis function provides the security manager with the ability to determine if the system is being operated in accordance with accepted industry practices, and in compliance with any specific organization policies and procedures.

Understanding the audit components prepares the candidate to work with either internal or external auditors during a formal audit review. The candidate is expected to demonstrate knowledge in the various methods of data collection, including data logging, sampling and reporting, in addition to analysis and audit review, and compliance check techniques. An understanding of the legal requirements for monitoring and audit activities is essential.

Key Areas of Knowledge

A. Maintain Effective Monitoring Systems (e.g., continuous monitoring)
   A.1 Monitor Intrusion Detection/Prevention Systems
   A.2 Monitor event correlation systems (e.g., SIM, SEM, SIEM)
      Review systems for unauthorized changes (e.g., file integrity checkers, honeypots, unauthorized connections)
   A.3 Monitor deviations from normal activity (e.g., white lists, anomaly detection, profiling)
   A.4 Install and configure agents and management systems

B. Analyze Monitoring Results (e.g., review and analysis of logs and reports, false positives, communicate findings)
4) RISK, RESPONSE, AND RECOVERY

Overview

The risk, response and recovery domain covers multiple aspects of existing threats, and mitigating and developing plans to deal with those threats.

Risk management is the identification, measurement and control of loss associated with adverse events. It includes overall security review, risk analysis, selection and evaluation of safeguards, cost benefit analysis, management decisions, safeguard implementation, and effectiveness review.

The candidate is expected to understand risk management including risk analysis, threats and vulnerabilities, asset identification and risk management tools and techniques.

Incident handling provides the ability to react quickly by putting highly trained people at the forefront of an incident and allows for a consistently applied approach to resolving incidents. Investigations include data collection and integrity preservation; seizure of hardware and software; evidence collection, handling, and storage; and reporting.

The candidate is expected to demonstrate knowledge in event identification, damage recovery, data integrity and preservation, evidence collection and handling, reporting, and prevention.

Business Continuity Planning (BCP) facilitates the rapid recovery of business operations to reduce the overall impact of the disaster, through ensuring continuity of the critical business functions. Disaster Recovery Planning includes procedures for emergency response, extended backup operations and post-disaster recovery when the computer installation suffers loss of computer resources and physical facilities.

The candidate is expected to understand how to prepare business continuity or disaster recovery plan, techniques and concepts, identification of critical data and systems, and finally the recovery of the lost data.
Key Areas of Knowledge

A. Understand Risk Management Process
   A.1 Understand risk management concepts (e.g., impacts, threats, vulnerabilities)
   A.2 Participate in risk assessment
   A.3 Support mitigation activity (e.g., safeguards, countermeasures)
   A.4 Address audit findings

B. Perform Security Assessment Activities
   B.1 Scan for vulnerabilities
   B.2 Participate in penetration testing
   B.3 Review security configurations of infrastructure
   B.4 Interpret results of scanning and testing

C. Participate in incident handling analysis
   C.1 Understand the concepts of incident handling (e.g., discovery, escalation reporting)
   C.2 Understand the concept of forensic investigations (e.g., first responder, evidence handling, chain of custody, preservation of scene)
   C.3 Participate in the implementation of countermeasures

D. Understand and Support Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)
   D.1 Understand the Components of a Business Continuity Plan (BCP)
   D.2 Understand and support Disaster Recovery Plan (DRP)
5) CRYPTOGRAPHY

Overview

Cryptography domain deals with the protection of information by modifying the information to ensure its integrity, confidentiality, authenticity and non-repudiation. Cryptanalysis deals with defeating the cryptosystem and violating the confidentiality or integrity of the protected data. The ability of any organization to protect its information from unauthorized access or modification is critical. The application of cryptography for the storage and transmission of information attempts to address these concerns.

The candidate is expected to understand basic concepts in cryptography; public and private key algorithms, key distribution and management, methods of attack; the application, construction and use of digital signatures, and the principles of public key infrastructure and certification.

Key Areas of Knowledge

A. Understand basic concepts of Cryptography (e.g., hashing, encryption, mechanisms, performance)
   A.1 Install and maintain cryptographic systems

B. Understand Requirements for Cryptography (e.g., data sensitivity, regulatory requirements, end-user training)

C. Support Certificate and Key Management
   C.1 Understand basic key management concepts (e.g., public key infrastructure)
   C.2 Administration and validation (e.g., key creation, exchange, revocation, escrow)

D. Understand the use of Secure Protocols (e.g., differences in implementation, appropriate use)
   D.1 Support the implementation of secure protocols (e.g., IPSec, SSL/TLS, S/MIME)
6) NETWORKS & COMMUNICATIONS

Overview

The networks and communications domain encompasses the network structure, transmission methods, transport formats and security measures used to maintain the integrity, availability, authentication and confidentiality of the transmitted information over both private and public communication networks.

The candidate is expected to understand communications and network security as it relates to data and telecommunications in local area and wide area networks; remote access; internet/intranet/extranet configurations, use of firewalls, network equipment and protocols (such as TCP/IP), VPN’s, and techniques for preventing and detecting network based attacks.

Key Areas of Knowledge

A. Understand Security issues related to Networks
   A.1 OSI and TCP/IP models
   A.2 Network topographies and relationships (e.g., token ring, star, bus, Ethernet)
   A.3 Commonly used ports and protocols
   A.4 Admission control (e.g., NAC, remediation, quarantine)
   A.5 Network security concepts (e.g., address translation, defense in depth, IP addressing)

B. Understand Telecommunications
   B.1 Technology (e.g., VoIP, facsimile, PSTN)
   B.2 Common Vulnerabilities

C. Understand Remote Access
   C.1 Technology (e.g., thin client, SSL/VPN)
   C.2 Common Vulnerabilities

D. Understand Firewalls & Proxies
   D.1 Methods (e.g., application filtering, packet filtering, stateful/stateless inspection)
   D.2 Types (e.g., host based, network based)
   D.3 Common Vulnerabilities
E. Understand Wireless and Cellular Technologies

E.1 Protocols (e.g., WPA, WPA2, TKIP)
E.2 Technology (e.g., Bluetooth, RFID, 802.11, WiMax, GSM, 3G, NFC)
E.3 Common Vulnerabilities
7) MALICIOUS CODE & ACTIVITY

Overview

The malicious code & activity domain addresses computer code that can be described as being harmful or destructive to the computing environment. This includes viruses, worms, logic bombs, the Trojan horse and other technical and non-technical attacks. The number and types of attacks using malicious code is increasing. The requirement for an individual or an organization to protect themselves from these attacks is extremely important.

While there are a variety of methods available to build a virus, many viruses are still targeted at a specific computing platform. With the availability of platform independent languages, it is becoming easier to write malicious code that can be run across different platforms.

The candidate is expected to understand the concepts of malicious and mobile code, types of malicious code threats, how malicious code is introduced into the environment, and various protection and recovery methods.

Key Areas of Knowledge

A. Identify Malicious Code (e.g., virus, worms, Trojan horses, logic bombs)
   A.1 Understand concepts of rootkits
   A.2 Understand types of malware (e.g., spyware, scareware, ransomware)
   A.3 Understand concepts of Trapdoors & Backdoors
   A.4 Understand concepts of Botnets
   A.5 Understand concepts of Mobile Code

B. Implement Malicious Code Countermeasures
   B.1 Scanners (e.g., heuristic, integrity checker, signatures)
   B.2 Deploy and manage anti-malware
   B.3 Containment & Remediation
      Software Security (e.g., code signing, application review, server side input validation)
   B.4

C. Identify Malicious Activity (e.g., social engineering, insider threat, data theft, DDoS, spoofing, phishing, pharming, spam)
C.1 Understand malicious web activity (e.g., cross site scripting, cross site request forgery, injection, social networking attacks)
C.2 Understand the concept of zero day exploits
C.3 Understand the concept of Advanced Persistent Threat (APT)

D. Implement Malicious Activity Countermeasures (e.g., user awareness, system hardening)
REFERENCES

(ISC)² does not intend that candidates purchase and read all of the books and articles listed in this reference list. Since most of the information tested in the examination pertains to a common body of knowledge, this additional information serves only as a supplement to one’s understanding of basic knowledge. A reference list is not intended to be inclusive but is provided to allow flexibility. The candidate is encouraged to supplement his or her education and experience by reviewing other resources and finding information in areas which he or she may consider himself or herself not as skilled or experienced. (ISC)² does not endorse any particular text or author. Although the list may include more than one reference that covers a content area, one such reference may be enough. The candidate may also have resources available that are not on the list but which will adequately cover the content area. The list does not represent the only body of information to be used as study material.

Questions in the examination are also developed from information gained through practical experience. This reference list is not intended to be all-inclusive, but rather, a useful list of references used to support the test question development process. Use of the references does not guarantee successful completion of the test.

Below is the suggested reference list:

<table>
<thead>
<tr>
<th>Domain</th>
<th>Supplementary Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Operations &amp; Administration</td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Johnson, M., (2011). It Asset Management: What you Need to Know For It Operations Management</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Monitoring and Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kruegel, C., F. Valeur, G. Vigna, (2010). Intrusion Detection and</td>
</tr>
</tbody>
</table>
| Monitoring and Analysis | Correlation: Challenges and Solutions  
|----------------------------|-------------------------------------------------------------------------------------------------|
Buffington, J., (2010). Data Protection for Virtual Data Centers  
## Risk, Response, and Recovery

(Continued)

<table>
<thead>
<tr>
<th>Author(s)</th>
<th>Title</th>
</tr>
</thead>
</table>
| Networks and Communications (Continued) | Nam-Kee, T., (2003). **Building VPNs: with IPsec and MPLS**  
Noonan, W. I., Dubrawsky, (2006). **Firewall Fundamentals**  
Prowell, S., R. Kraus, M. Borkin, (2010). **Seven Deadliest Network Attacks**  
SAMPLE EXAM QUESTIONS

1. When properly installed, which type of card/badge reader is MOST tamper resistant?

   (A) Card swipe device
   (B) Optical reader
   (C) Proximity reader
   (D) Card insertion device

   Answer: C

2. Which one of the following describes how a polymorphic virus attempts to hide from antivirus software?

   (A) By repeatedly changing the boot record of the host disk
   (B) By changing the routines that encrypt the body of the virus
   (C) By directly attacking the antivirus software
   (D) By directly attaching itself to an email

   Answer: B

3. Which one of the following is the technique used to prevent inference violations by allowing different versions of the same information item to exist at different classification levels?

   (A) Appropriate labeling
   (B) Query restriction
   (C) Auditing
   (D) Polyinstantiation

   Answer: D
GENERAL EXAMINATION INFORMATION

Paper Based Test (PBT)

General Information  The doors to all examination rooms will open at 8:00a.m. Examination instructions will begin promptly at 8:30a.m.  All examinations will begin at approximately 9:00a.m.

The maximum duration of the CISSP® exam is 6 hours. The maximum duration of all other exams except the CSSLP® is 3 hours. The CSSLP® candidates are allowed a maximum of 4 hours to complete the exam.

Please note there will be no lunch break during the testing period.  However, you are permitted to bring a snack with you.  You may, at your option, take a break and eat your snack at the back of the examination room.  No additional time will be allotted for breaks.

Examination Admittance  Please arrive at 8:00a.m. when the doors are opened. Please bring your admission letter to the examination site. In order to be admitted, photo identification is also required. You will not be admitted without proper identification. The only acceptable forms of identification are a driver’s license, government-issued identification card, or passport. No other written forms of identification will be accepted.

Examination Security  Failure to follow oral and written instructions will result in your application being voided and application fee being forfeited. Conduct that results in a violation of security or disrupts the administration of the examination could result in the confiscation of your test and your dismissal from the examination. In addition, your examination will be considered void and will not be scored. Examples of misconduct include, but are not limited to, the following: writing on anything other than designated examination materials, writing after time is called, looking at another candidate’s examination materials, talking with other candidates at any time during the examination period, failing to turn in all examination materials before leaving the testing room.

You must not discuss or share reference materials or any other examination information with any candidate during the entire examination period. You are particularly cautioned not to do so after you have completed the exam and checked out of the test room, as other candidates in the area might be taking a break and still not have completed the examination. You may not attend the examination only to review or audit test materials. You may not copy any portion of the examination for any reason. No examination materials may leave the test room under any circumstances and all examination materials must be turned in and accounted for before leaving the testing room. No unauthorized persons will be admitted into the testing area.

Please be further advised that all examination content is strictly confidential. You may only communicate about the test, or questions on the test, using the appropriate comment forms provided by the examination staff at the test site. At no other time, before, during or
after the examination, may you communicate orally, electronically or in writing with any person or entity about the content of the examination or individual examination questions.

Reference Material Candidates writing on anything other than examination materials distributed by the proctors will be in violation of the security policies above. Reference materials are not allowed in the testing room. Candidates are asked to bring as few personal and other items as possible to the testing area.

Hard copies of language translation dictionaries are permitted for the examination, should you choose to bring one to assist you with language conversions. Electronic dictionaries will not be permitted under any circumstances. The Examination Supervisor will fully inspect your dictionary at check-in. Your dictionary may not contain any writing or extraneous materials of any kind. If the dictionary contains writing or other materials or papers, it will not be permitted in the examination room. Additionally, you are not permitted to write in your dictionary at any time during the examination, and it will be inspected a second time prior to dismissal from the examination. Finally, (ISC)² takes no responsibility for the content of such dictionaries or interpretations of the contents by a candidate.

Examination Protocol While the site climate is controlled to the extent possible, be prepared for either warm or cool temperatures at the testing center. Cellular phones and beepers are prohibited in the testing area. The use of headphones inside the testing area is prohibited. Electrical outlets will not be available for any reason. Earplugs for sound suppression are allowed. No smoking or use of tobacco products will be allowed inside the testing area. Food and drinks are only allowed in the snack area located at the rear of the examination room. You must vacate the testing area after you have completed the examination. If you require special assistance, you must contact (ISC)² Candidate Services (see address at the bottom of this document) at least one week in advance of the examination date and appropriate arrangements will be made. Due to limited parking facilities at some sites, please allow ample time to park and reach the testing area.

Admission Problems A problem table for those candidates who did not receive an admission notice or need other assistance will be available 30 minutes prior to the opening of the doors.

Examination Format and Scoring

- The CISSP® examination consists of 250 multiple choice questions with four (4) choices each.
- The CSSLP® examination consists of 175 multiple choice questions with four (4) choices each.
- The SSCP® examination contains 125 multiple choice questions with four (4) choices each.
- The ISSAP®, ISSEP®, and ISSMP® concentration examinations contain 125, 150, 125 multiple choice questions respectively with four (4) choices each.
- The Certified Authorization Professional (CAP®) examination contains 125 multiple choice questions with four (4) choices each. Also, administered in computers.
There may be scenario-based items which may have more than one multiple choice question associated with it. These items will be specifically identified in the test booklet.

Each of these exams contains 25 questions which are included for research purposes only. The research questions are not identified; therefore, answer all questions to the best of your ability. There is no penalty for guessing, so candidates should not leave any item unanswered. Examination results will be based only on the scored questions on the examination. There are several versions of the examination. It is important that each candidate have an equal opportunity to pass the examination, no matter which version is administered. Subject Matter Experts (SMEs) have provided input as to the difficulty level of all questions used in the examinations. That information is used to develop examination forms that have comparable difficulty levels. When there are differences in the examination difficulty, a mathematical procedure called equating is used to make the difficulty level of each test form equal. Because the number of questions required to pass the examination may be different for each version, the scores are converted onto a reporting scale to ensure a common standard. The passing grade required is a scale score of 700 out of a possible 1000 points on the grading scale.

**Examination Results**  Examination results will normally be released, via email, within 6 to 8 weeks of the examination date. A comprehensive statistical and psychometric analysis of the score data is conducted prior to the release of scores. A minimum number of candidates must have taken the examination for the analysis to be conducted. Accordingly, depending upon the schedule of test dates for a given cycle, there may be occasions when scores are delayed beyond the 6-8 week time frame in order to complete this critical process. If the test is administered via computers, candidates’ pass/fail status is provided at the end of the testing on the site. Results WILL NOT be released over the telephone. In order to receive your results, your primary email address must be current and any email address changes must be submitted to (ISC)² Customer Support via email customersupport@isc2.org, or may be updated online in your candidate profile.

**Exam Response Information**  Your answer sheet MUST be completed with your name and other information as required. The answer sheet must be used to record all answers to the multiple-choice questions. Upon completion, you are to wait for the proctor to collect your examination materials. Answers marked in the test booklet will not be counted or graded, and additional time will not be allowed in order to transfer answers to the answer sheet. All marks on the answer sheet must be made with a No. 2 pencil. You must blacken the appropriate circles completely and completely erase any incorrect marks. Only your responses marked on the answer sheet will be considered. An unanswered question will be scored as incorrect. Dress is “business casual” (neat…but certainly comfortable).
Any questions?

(ISC)² Candidate Services
311 Park Place Blvd, Suite 400
Clearwater, FL 33759
Phone: 1.866.331.ISC2 (4722) in the United States
1.727.785.0189 all others
Fax: 1.727.683.0785
GENERAL EXAMINATION INFORMATION

Computer Based Test (CBT)

Registering for the Exam

Process for Registration Overview

This section describes procedures for candidates registering to sit for a Computer Based Test (CBT). The test is administered at Pearson VUE Testing centers in the US, Canada, and other parts of the world.

1. Go to [www.pearsonvue.com/isc2](http://www.pearsonvue.com/isc2) to register for a test appointment.
2. Select the most convenient test center
3. Select an appointment time.
4. Pay for your exam appointment.
5. Receive confirmation from Pearson VUE with the appointment details, test center location and other relevant instructions, if any.

Please note that your registration information will be transferred to (ISC)² and all communication about the testing process from (ISC)² and Pearson VUE will be sent to you via email.

Fees

Please visit the (ISC)² website [https://www.isc2.org/certification-register-now.aspx](https://www.isc2.org/certification-register-now.aspx) for the most current examination registration fees.
U.S. Government Veteran’s Administration G.I. Bill

The U.S. Department of Veterans Affairs has approved reimbursement to veterans under the G.I. Bill for the cost of the Certified Information System Security Professional (CISSP), the CISSP Concentrations (ISSAP, ISSEP, ISSMP), the Certification and Accreditation Professional (CAP), and the System Security Certified Practitioner (SSCP) examinations. Please refer to the U.S. Department of Veterans Affairs Website at www.va.gov for more details.

CBT Demonstration
Candidates can experience a demonstration and tutorial of the CBT experience on our Pearson VUE web page. The tutorial may be found at www.pearsonvue.com/isc2.

Scheduling a Test Appointment

Process for Registration Overview

Candidates may register for a testing appointment directly with Pearson VUE (www.pearsonvue.com/isc2). Candidates who do not pass the test will be subject to the retake policy and must wait the applicable time before they are allowed to re-sit for the examination.

Exam Appointment

Test centers may fill up quickly because of high volume and previously scheduled special events. Pearson VUE testing centers also serve candidates from other entities; thus waiting to schedule the testing appointment may significantly limit the options for candidate’s desired testing dates at the closest center available.

Scheduling for a Testing Appointment

Candidates may schedule their appointment online at (ISC)² CBT Website located at www.pearsonvue.com/isc2. Candidates will be required to create a Pearson VUE account in order to complete registration. Candidates profile will be transferred to (ISC)² and becomes part of the candidate’s permanent record. Candidates will be able to locate test centers and select from a choice of available examination appointment times at the Pearson VUE website.

Candidates may also register over the telephone with a CBT registration specialist. Please refer to ‘Contact Information’ for local telephone numbers for your region.
Rescheduling or Cancellation of a Testing Appointment

If you wish to reschedule or cancel your exam appointment, you must contact Pearson VUE at least **48 hours** before the exam date by contacting Pearson VUE online ([www.pearsonvue.com/isc2](http://www.pearsonvue.com/isc2)), OR at least **24 hours** prior to exam appointment time by contacting Pearson VUE **over the phone**. Canceling or rescheduling an exam appointment less than 24 hours via phone notification, or less than 48 hours via online notification is subject to a forfeit of exam fees. Exam fees are also forfeited for no-shows. Please note that Pearson VUE charges a 50 USD/35 £/40 € fee for reschedules, and 100 USD/70 £/80 € fee for cancellations.

Reschedules and cancellations may be done at the (ISC)² CBT Candidate Website ([www.pearsonvue.com/isc2](http://www.pearsonvue.com/isc2)) or via telephone. Please refer to ‘Contact Information’ for more information and local telephone numbers for your region.

Late Arrivals or No Shows

If the candidate does not arrive within 15 minutes of the scheduled exam starting time, he or she has technically forfeited his or her assigned seat.

If the candidate arrives late (after 15 minutes of his/her scheduled appointment), it is up to the discretion of the testing center as to whether or not the candidate may still take the exam. If the test administrator at the testing location is able to accommodate a late arriving candidate, without affecting subsequent candidates’ appointments, he/she will let the candidate to sit for the exam and launch his/her exam.

Any/all attempts are made to accommodate candidates who arrive late. However, if the schedule is such that the test center is not able to accommodate a late arrival, the candidate will be turned away and his/her exam fees will be forfeited.

If a candidate fails to appear for a testing appointment, the test result will appear in the system as a No-Show and the candidate’s exam fees will be forfeited.

Procedure for Requesting Special Accommodations

Pearson VUE Professional Centers can accommodate a variety of candidates’ needs, as they are fully compliant with the Americans with Disability Act (ADA), and the equivalent requirements in other countries.

Requests for accommodations should be made to (ISC)² in advance of the desired testing appointment. Once (ISC)² grants the accommodations request, the candidate may schedule the testing appointment using Pearson VUE’s special accommodations number. From there, a Pearson VUE coordinator will handle all of the arrangements.
PLEASE NOTE: Candidates that request special accommodations should not schedule their appointment online or call the main CBT registration line.

**What to Bring to the Test Center**

**Proper Identification**

(ISC)² requires two forms of identification, a primary and a secondary, when checking in for a CBT test appointment at a Pearson VUE Test Center. All candidate identification documents must be valid (not expired) and must be an original document (not a photocopy or a fax).

**Primary IDs:** Must contain a permanently affixed photo of the candidate, along with the candidate’s signature.

**Secondary IDs:** Must have the candidate’s signature.

<table>
<thead>
<tr>
<th><strong>Accepted Primary ID (photograph and signature, not expired)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Government issued Driver’s License or Identification Card</td>
</tr>
<tr>
<td>- U.S. Dept of State Drivers License</td>
</tr>
<tr>
<td>- U.S. Learner’s Permit (card only with photo and signature)</td>
</tr>
<tr>
<td>- National/State/Country Identification Card</td>
</tr>
<tr>
<td>- Passport</td>
</tr>
<tr>
<td>- Passport Cards</td>
</tr>
<tr>
<td>- Military ID</td>
</tr>
<tr>
<td>- Military ID for spouses and dependents</td>
</tr>
<tr>
<td>- Alien Registration Card (Green Card, Permanent Resident Visa)</td>
</tr>
<tr>
<td>- Government Issued local language ID (plastic card with photo and signature)</td>
</tr>
<tr>
<td>- Employee ID</td>
</tr>
<tr>
<td>- School ID</td>
</tr>
<tr>
<td>- Credit Card* (A credit card can be used as a primary form of ID only if it contains both a photo and a signature and is not expired. Any credit card can be used as a secondary form of ID, as long as it contains a signature and is not expired. This includes major credit cards, such as VISA, MasterCard, American Express and Discover. It also includes department store and gasoline credit cards.)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Accepted Secondary ID (contains signature, not expired)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>- U.S. Social Security Card</td>
</tr>
<tr>
<td>- Debit/(ATM) Card</td>
</tr>
<tr>
<td>- Credit Cards</td>
</tr>
<tr>
<td>- Any form of ID on the primary list</td>
</tr>
</tbody>
</table>

© 2012 International Information Systems Security Certification Consortium, Inc. All Rights Reserved. Duplication for commercial purposes is prohibited. 1-10-14 - V17
Name Matching Policy

Candidate’s first and last name on the presented identification document must exactly match the first and last name on the registration record with Pearson VUE. If the name the candidate has registered with does not match the name on the identification document, proof of legal name change must be brought to the test center on the day of the test. The only acceptable forms of legal documentation are marriage licenses, divorce decrees, or court sanctioned legal name change documents. All documents presented at the test center must be original documents. If a mistake is made with a name during the application process, candidates should contact (ISC)² to correct the information well in advance of the actual test date. Name changes cannot be made at the test center or on the day of the exam. Candidates who do not meet the requirements presented in the name matching policy on the day of the test may be subject to forfeiture of testing fees and asked to leave the testing center.

Non Disclosure

Prior to starting the exam, all candidates are presented with (ISC)² non-disclosure agreement (NDA), and are required in the computer to accept the agreement prior to being presented with exam questions. If the NDA is not accepted by the candidate, or refused to accept within the time allotted, the exam will end, and the candidate will be asked to leave the test center. No refund of exam fees will be given. For this reason, all candidates are strongly encouraged to review the non-disclosure agreement prior to scheduling for, or taking the exam. The agreement is located at www.pearsonvue.com/isc2/isc2_nda.pdf.

Day of the Exam

Check-In Process

Plan to arrive at the Pearson VUE testing center at least 30 minutes before the scheduled testing time. If you arrive more than 15 minutes late to your scheduled appointment, you may lose your examination appointment. For checking-in:

- You will be required to present two acceptable forms of identification.
- You will be asked to provide your signature, submit to a palm vein scan, and have your photograph taken. Hats, scarves and coats may not be worn in the testing room, or while your photograph is being taken.
- You will be required to leave your personal belongings outside the testing room. Secure storage will be provided. Storage space is small, so candidates should plan appropriately. Pearson Professional Centers assume no responsibility for candidates’ personal belongings.
- The Test Administrator (TA) will give you a short orientation, and then will escort you to a computer terminal. You must remain in your seat during the examination, except
when authorized to leave by test center staff. You may not change your computer terminal unless a TA directs you to do so.

Raise your hand to notify the TA if you

- believe you have a problem with your computer.
- need to change note boards.
- need to take a break.
- need the administrator for any reason.

**Breaks**

You will have up to **six hours** to complete the **CISSP**, and up to **four hours** to complete the **CSSLP** and **CCFP** up to **three hours** to complete the following examinations:

- SSCP
- CAP
- HCISPP
- ISSAP
- ISSEP
- ISSMP

Total examination time includes any unscheduled breaks you may take. All breaks count against your testing time. You must leave the testing room during your break, but you may not leave the building or access any personal belongings unless absolutely necessary (e.g. for retrieving medication). Additionally, when you take a break, you will be required to submit to a palm vein scan before and after your break.

**Examination Format and Scoring**

- The **CISSP** examination consists of 250 multiple choice questions with four (4) choices each.
- The **CSSLP** examination consists of 175 multiple choice questions with four (4) choices each.
- The **HCISPP** examination contains 125 multiple choice questions with four (4) choices each.
- The **CCFP** examination contains 125 multiple choice questions with four (4) choices each.
- The **SSCP** examination contains 125 multiple choice questions with four (4) choices each.
- The **ISSAP**, **ISSEP**, and **ISSMP** concentration examinations contain 125, 150, 125 multiple choice questions respectively with four (4) choices each.
- The Certified Authorization Professional (CAP®) examination contains 125 multiple choice questions with four (4) choices each. Also, administered in computers.
There may be scenario-based items which may have more than one multiple choice question associated with it. These items will be specifically identified in the test booklet. Each of these exams contains 25 questions which are included for research purposes only. The research questions are not identified; therefore, answer all questions to the best of your ability. There is no penalty for guessing, so candidates should not leave any item unanswered. Examination results will be based only on the scored questions on the examination. There are several versions of the examination. It is important that each candidate have an equal opportunity to pass the examination, no matter which version is administered. Subject Matter Experts (SMEs) have provided input as to the difficulty level of all questions used in the examinations. That information is used to develop examination forms that have comparable difficulty levels. When there are differences in the examination difficulty, a mathematical procedure called equating is used to make the difficulty level of each test form equal. Because the number of questions required to pass the examination may be different for each version, the scores are converted onto a reporting scale to ensure a common standard. The passing grade required is a scale score of 700 out of a possible 1000 points on the grading scale.

**Technical Issues**

On rare occasions, technical problems may require rescheduling of a candidate’s examination. If circumstances arise causing you to wait more than 30 minutes after your scheduled appointment time, or a restart delay lasts longer than 30 minutes, you will be given the choice of continuing to wait, or rescheduling your appointment without an additional fee.

- If you choose to wait, but later change your mind at any time prior to beginning or restarting the examination, you will be allowed to take exam at a later date, at no additional cost.
- If you choose not to reschedule, but rather test after a delay, you will have no further recourse, and your test results will be considered valid.
- If you choose to reschedule your appointment, or the problem causing the delay cannot be resolved, you will be allowed to test at a later date at no additional charge. Every attempt will be made to contact candidates if technical problems are identified prior to a scheduled appointment.
Testing Environment

Pearson Professional Centers administer many types of examinations including some that require written responses (essay-type). Pearson Professional Centers have no control over typing noises made by candidates sitting next to you while writing their examination. Typing noise is considered a normal part of the computerized testing environment, just as the noise of turning pages is a normal part of the paper-and-pencil testing environment. Earplugs are available upon request.

When the Exam is Finished

After you have finished the examination, raise your hand to summon the TA. The TA will collect and inventory all note boards. The TA will dismiss you when all requirements are fulfilled.

If you believe there was an irregularity in the administration of your test, or the associated test conditions adversely affected the outcome of your examination, you should notify the TA before you leave the test center.

Results Reporting

Candidates will receive their unofficial test result at the test center. The results will be handed out by the Test Administrator during the checkout process. (ISC)² will then follow up with an official result via email.

In some instances, real time results may not be available. A comprehensive statistical and psychometric analysis of the score data is conducted during every testing cycle before scores are released. A minimum number of candidates are required to take the exam before this analysis can be completed. Depending upon the volume of test takers for a given cycle, there may be occasions when scores are delayed for approximately 6-8 weeks in order to complete this critical process. Results WILL NOT be released over the phone. They will be sent via email from (ISC)² as soon as the scores are finalized. If you have any questions regarding this policy, you should contact (ISC)² prior to your examination.

Retake Policy

Test takers who do not pass the exam the first time will be able to retest after 30 days. Test takers that fail a second time will need to wait 90 days prior to sitting for the exam again. In the unfortunate event that a candidate fails a third time, the next available time to sit for the exam will be 180 days after the most recent exam attempt. Candidates are eligible to sit for (ISC)² exams a maximum of 3 times within a calendar year.
Recertification by Examination

Candidates and members may recertify by examination for the following reasons ONLY:

- The candidate has become decertified due to reaching the expiration of the time limit for endorsement.
- The member has become decertified for not meeting the number of required continuing professional education credits.

Logo Usage Guidelines

(ISC)² is a non-profit membership organization identified as the leader in certifying individuals in information security.

Candidates who successfully complete any of the (ISC)² certification requirements may use the appropriate Certification Mark or the Collective Mark, where appropriate, and the logo containing the Certification Mark or the Collective Mark, where appropriate (the “Logo”) to identify themselves as having demonstrated the professional experience and requisite knowledge in the realm of information system security. Please visit the following link (URL) for more information on logo use:

https://www.isc2.org/uploadedfiles/(ISC)_2_Public_Content/Legal_and_Policies/LogoGuidelines.pdf

Any questions?

(ISC)² Candidate Services
311 Park Place Blvd, Suite 400
Clearwater, FL 33759
Phone: 1.866.331.ISC2 (4722) in the United States
1.727.785.0189 all others
Fax: 1.727.683.0785
Systems Security Certified Practitioner SSCP®

Candidate Information Bulletin

Effective Date: February 2012