



## Certified Information Systems Security Professional (CISSP®) Candidate Information Bulletin

This Candidate Information Bulletin provides the following:

- exam blueprint to a limited level of detail that outlines major topics and sub-topics within the domains which are listed in alphabetical order,
- suggested reference list,
- description of the format of the items on the exam, and
- basic registration/administration policies

Applicants must have a minimum of four years of direct full-time security professional work experience in one or more of the ten domains of the (ISC)<sup>2</sup> CISSP® CBK® or three years of direct full-time security professional work experience in one or more of the ten domains of the CISSP® CBK® with a four-year college degree. Additionally, a Master's Degree in Information Security from a National Center of Excellence can substitute for one year toward the four-year requirement.

CISSP professional experience includes:

- Work requiring special education or intellectual attainment, usually including a 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).
- Applicable titles such as officer, director, manager, leader, supervisor, analyst, designer, cryptologist, cryptographer, cryptanalyst, architect, engineer, instructor, professor, investigator, consultant, salesman, representative, etc. Title may include programmer. It may include administrator, except where it applies to one who simply operates controls under the authority and supervision of others. Titles with the words "coder" or "operator" are likely excluded.

---

## Access Control

---

### Overview

Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It permits management to specify what users can do, which resources they can access, and what operations they can perform on a system.

The candidate should fully understand access control concepts, methodologies and implementation within centralized and decentralized environments across the enterprise's computer systems. Access control techniques, detective and corrective measures should be studied to understand the potential risks, vulnerabilities, and exposures.

### Key Areas of Knowledge

- Control access by applying the following concepts/methodologies/techniques
- Identify, evaluate and respond to access control attacks (e.g., Brute Force, Dictionary, Spoofing, Denial of Service)
- Design, coordinate, and evaluate penetration test(s)
- Design, coordinate, and evaluate vulnerability test(s)

**SITC The best choice for CISSP candidate to study at**  
For more information about CISSP training&exam please contact  
Mr Liao TEL:021-62126633-6022 MAIL:liaoash@sh.cei.gov.cn

---

## Application Security

---

### Overview

Application security refers to the controls that are included within systems and applications software and the steps used in their development. Applications refer to agents, applets, software, databases, data warehouses, and knowledge-based systems. These applications may be used in distributed or centralized environments.

The candidate should fully understand the security and controls of the systems development process, system life cycle, application controls, change controls, data warehousing, data mining, knowledge-based systems, program interfaces, and concepts used to ensure data and application integrity, security, and availability.

### Key Areas of Knowledge

- Understand the role of security in the system life cycle
- Understand the application environment and security controls
- Understand databases and data warehousing and protect against vulnerabilities and threats
- Understand application & system development knowledge security-based systems (e.g., expert systems)
- Understand application and system vulnerabilities and threats

---

## Business Continuity and Disaster Recover Planning

---

### Overview

The Business Continuity and Disaster Recovery Planning domain addresses the preservation of the business in the face of major disruptions to normal business operations. BCP and DRP involve the preparation, testing and updating of specific actions to protect critical business processes from the effect of major system and network failures.

Business Continuity Plans counteract interruptions to business activities and should be available to protect critical business processes from the effects of major failures or disasters. It deals with the natural and man-made events and the consequences if not dealt with promptly and effectively.

Business Impact Assessment determines the proportion of impact an individual business unit would sustain subsequent to a significant interruption of computing or telecommunication services. These impacts may be financial, in terms of monetary loss, or operational, in terms of inability to deliver.

Disaster Recovery Plans contain procedures for emergency response, extended backup operation and post-disaster recovery should a computer installation experience a partial or total loss of computer resources and physical facilities. The primary objective of the Disaster Recovery Plan is to provide the capability to process mission-essential applications, in a degraded mode, and return to normal mode of operation within a reasonable amount of time.

The candidate will be expected to know the difference between business continuity planning and disaster recovery; business continuity planning in terms of project scope and planning, business impact analysis, recovery strategies, recovery plan development, and implementation. The candidate should understand disaster recovery in terms of recovery plan development, implementation and restoration.

### Key Areas of Knowledge

- Develop and document project scope and plan
- Conduct Business Impact Analysis
- Develop recovery strategy
- Incorporate the following elements into the plan
  - 1 Emergency response
  - 2 Notification (e.g., calling tree)
  - 3 Personnel safety
  - 4 Communications
  - 5 Public utilities
  - 6 Logistics and supplies
  - 7 Fire and water protection
  - 8 Business resumption planning
  - 9 Damage assessment
  - 10 Restoration (e.g., cleaning, data recovery, relocation to primary site)
- Training
- Plan Maintenance

**SITC The best choice for CISSP candidate to study at**

For more information about CISSP training&exam please contact

Mr Liao TEL:021-62126633-6022 MAIL:liaosh@sh.cei.gov.cn

---

## Cryptography

---

### Overview

The Cryptography domain addresses the principles, means, and methods of disguising information to ensure its integrity, confidentiality, and authenticity.

The candidate will be expected to know basic concepts within cryptography; public and private key algorithms in terms of their applications and uses; algorithm construction, key distribution and management, and methods of attack; and the applications, construction and use of digital signatures to provide authenticity of electronic transactions, and nonrepudiation of the parties involved.

### Key Areas of Knowledge

- Understand the application and use of cryptography (e.g., confidentiality, availability and integrity)
- Understand methods of encryption (e.g., one-time pads, substitutions, permutations)
- Understand types of encryption (e.g., stream, block)
- Understand initialization vectors (IV)
- Understand cryptographic systems
- Understand the use of and employ key management techniques
- Understand message digests/ hashing (e.g., MD5, SHA, HMAC)
- Understand digital signatures
- Understand non-repudiation
- Understand methods of cryptanalytic attacks
- Employ cryptography in network security (e.g., SSL)
- Use cryptography to maintain e-mail security (e.g., PGP, S/MIME)
- Understand Public Key Infrastructure (PKI) (e.g. certification authorities, etc.)
- Understand alternatives (e.g., steganography, watermarking)

---

## Information Security and Risk Management

---

### Overview

Information Security and Risk Management entails the identification of an organization's information assets and the development, documentation, and implementation of policies, standards, procedures and guidelines that ensure confidentiality, integrity, and availability. Management tools such as data classification, risk assessment, and risk analysis are used to identify the threats, classify assets, and to rate their vulnerabilities so that effective security controls can be implemented.

Risk management is the identification, measurement, control, and minimization of loss associated with uncertain events or risks. It includes overall security review, risk analysis; selection and evaluation of safeguards, cost benefit analysis, management decision, safeguard implementation, and effectiveness review.

The candidate will be expected to understand the planning, organization, and roles of individuals in identifying and securing an organization's information assets; the development and use of policies stating management's views and position on particular topics and the use of guidelines, standards, and procedures to support the policies; security awareness training to make employees aware of the importance of information security, its significance, and the specific security-related requirements relative to their position; the importance of confidentiality, proprietary and private information; employment agreements; employee hiring and termination practices; and risk management practices and tools to identify, rate, and reduce the risk to specific resources.

### Key Areas of Knowledge

- Understand and document goals, mission, and objectives of the Organizations)
- Establish governance
- Understand concepts of availability, integrity and confidentiality
- Apply the following security concepts in planning
  - 1 Defense-in-depth
  - 2 Avoid single points of failure
- Develop and implement Security Policy
- Define the Organization's security roles and responsibilities
- Secure outsourcing
- Develop and maintain internal service level agreements
- Integrate and support identity management
- Understand and apply risk management concepts
- Evaluate personnel security
- Develop and conduct security education, training and awareness
- Understand data classification concepts
- Evaluate information system security strategies
- Support certification and accreditation efforts
- Design, conduct, and evaluate security assessment
- Report security issues to management
- Understand professional ethics

**SITC The best choice for CISSP candidate to study at**

For more information about CISSP training&exam please contact

Mr Liao TEL:021-62126633-6022 MAIL:liaosh@sh.cei.gov.cn

---

## Legal, Regulations, Compliance and Investigations

---

### Overview

The Legal, Regulations, Compliance and Investigations domain addresses computer crime laws and regulations; the investigative measures and techniques which can be used to determine if a crime has been committed, methods to gather evidence if it has, as well as the ethical issues and code of conduct for the security professional.

Incident handling provides the ability to react quickly and efficiently to malicious technical threats or incidents.

The candidate will be expected to know the methods for determining whether a computer crime has been committed; the laws that would be applicable for the crime; laws prohibiting specific types of computer crime; methods to gather and preserve evidence of a computer crime, investigative methods and techniques; and ways in which RFC 1087 and the (ISC) 2<sup>TM</sup> Code of Ethics can be applied to resolve ethical dilemmas.

### Key Areas of Knowledge

- Understand common elements of international laws that pertain to information systems security
- Understand and support investigations
- Understand forensic procedures

---

## Operations Security

---

### Overview

Operations Security is used to identify the controls over hardware, media, and the operators with access privileges to any of these resources. Audit and monitoring is the mechanisms, tools and facilities that permit the identification of security events and subsequent actions to identify the key elements and report the pertinent information to the appropriate individual, group, or process.

The candidate will be expected to know the resources that must be protected, the privileges that must be restricted, the control mechanisms available, the potential for abuse of access, the appropriate controls, and the principles of good practice.

### Key Areas of Knowledge

- Apply the following security concepts to activities
  - 1 Need-to-know/ least privilege
  - 2 Separation of duties & responsibilities
  - 3 Monitor special privileges (e.g., operators, administrators)
  - 4 Job rotation
  - 5 Marking, handling, storing, and destroying of sensitive information & media
  - 6 Record retention
  - 7 Backup critical information
  - 8 Anti-virus management
  - 9 Remote working
  - 10 Malware management
- Employ resource protection
- Handle violations, incidents, and breaches and report when necessary
- Support high availability (e.g., fault tolerance, Denial of Service prevention)
- Implement & Support Patch and Vulnerability Management
- Ensure administrative management and control
- Understand Configuration Management Concepts (e.g., Hardware/ Software)
- Respond to attacks and other vulnerabilities (e.g., spam, virus, spyware, phishing)

**SITC The best choice for CISSP candidate to study at**

For more information about CISSP training&exam please contact

Mr Liao TEL:021-62126633-6022 MAIL:liaosh@sh.cei.gov.cn

---

## Physical (Environmental) Security

---

### Overview

The Physical (Environmental) Security domain addresses the threats, vulnerabilities, and countermeasures that can be utilized to physically protect an enterprise's resources and sensitive information. These resources include people, the facility in which they work, and the data, equipment, support systems, media, and supplies they utilize.

The candidate will be expected to know the elements involved in choosing a secure site, its design and configuration, and the methods for securing the facility against unauthorized access, theft of equipment and information, and the environmental and safety measures needed to protect people, the facility, and its resources.

### Key Areas of Knowledge

- Participate in site and facility design considerations
  - Support the implementation and operation of perimeter security
  - Support the implementation and operation of interior security
  - Support the implementation and operation of operations/facility security
  - Participate in the protection and securing equipment
- 

---

## Security Architecture and Design

---

### Overview

The Security Architecture and Design domain contains the concepts, principles, structures, and standards used to design, implement, monitor, and secure, operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity, and availability.

The candidate should understand security models in terms of confidentiality, integrity, information flow, commercial vs. government requirements; system models in terms of the Common Criteria, international (ITSEC), United States Department of Defense (TCSEC), and Internet (IETF IPSEC); technical platforms in terms of hardware, firmware, and software; and system security techniques in terms of preventative, detective, and corrective controls.

### Key Areas of Knowledge

- Understand the theoretical concepts of security models
- Understand the Components of Information Systems Evaluation Models
- Understand security capabilities of computer systems
- Understand how the security architecture is affected by
  - 1 Covert channels
  - 2 States attacks (e.g., time of check / time of use)
  - 3 Emanations
  - 4 Maintenance hooks and privileged programs
  - 5 Countermeasures
  - 6 Assurance, trust, and confidence
  - 7 Trusted computer base (TCB), reference monitors and kernels

**SITC The best choice for CISSP candidate to study at**  
For more information about CISSP training&exam please contact  
Mr Liao TEL:021-62126633-6022 MAIL:liaosh@sh.cei.gov.cn

---

## Telecommunications and Network Security

---

### Overview

Telecommunications and Network Security domain encompasses the structures, transmission methods, transport formats, and security measures used to provide integrity, availability, authentication, and confidentiality for transmissions over private and public communications networks and media.

The candidate is expected to demonstrate an understanding of communications and network security as it relates to voice communications; data communications in terms of local area, wide area, and remote access; Internet/Intranet/Extranet in terms of Firewalls, Routers, and TCP/IP; and communications security management and techniques in terms of preventive, detective and corrective measures.

In today's global marketplace, the ability to communicate with others is a mandatory requirement. The data 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 demonstrate an understanding of communications and network security as it relates to data communications in local area and wide area networks; remote access; internet/intranet/extranet configurations, use of firewalls, network equipment and protocols (such as TCP/IP), VPNs, and techniques for preventing and detecting network based attacks.

### Key Areas of Knowledge

- Establish secure data communications
- Establish secure multimedia communications
- Develop and maintain secure networks
- Prevent attacks and control potential attack threats (e.g., Malicious Code, Flooding, Spamming)
- Remote access protocols (e.g., CHAP, EAP)

**SITC The best choice for CISSP candidate to study at**

For more information about CISSP training&exam please contact

Mr Liao TEL:021-62126633-6022 MAIL:liaosh@sh.cei.gov.cn

**GENERAL EXAMINATION INFORMATION**

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

The CISSP® exam will end at approximately 3:00 p.m. All other exams will end at approximately 12:00 noon.

Please note there will be no lunch break during the testing period of 9:00 a.m. to 3:00 p.m. 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.

2. **Examination Admittance.** Please arrive at 8:00 a.m. when the doors open. Please bring your admission letter to the examination. In order to be admitted, a 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.

3. **Examination Security.** Failure to follow oral and written instructions will result in your application being voided and forfeiture of your application fee. Conduct that results in a violation of security or disrupts the administration of the examination could result in the confiscation of your test and 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.

4. **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 copy 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.

5. **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 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 SMT 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.

6. **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.

**SITC The best choice for CISSP candidate to study at**  
For more information about CISSP training&exam please contact  
Mr Liao TEL:021-62126633-6022 MAIL:liaoash@sh.cei.gov.cn

7. **Examination Format and Scoring.**

- The CISSP examination consists of 250 multiple choice questions with four (4) choices each.
- The SSCP® exam contains 125 multiple choice questions with four (4) choices each.
- The ISSAP®, ISSEP®, and ISSMP® exams contain 125, 150, 125 multiple choice questions respectively with four (4) choices each.
- The Certification and Accreditation Professional (CAP) exam contains 125 multiple choice questions with four (4) choices each.

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. 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. Expert certified information security professionals 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 is used to make the scores 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.

8. **Examination Results.** Examination results will normally be released, via U.S. first class mail, within 4 to 6 weeks of the examination date. A comprehensive statistical and psychometric analysis of the score data is conducted for each spring and fall testing cycle 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 4-6 week time frame in order to complete this critical process. Results WILL NOT be released over the phone. In order to receive your results, your address must be current and any address change must be submitted to SMT in writing.

9. **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 should be directed to:

(ISC)<sup>2</sup>  
c/o Schroeder Measurement Technologies, Inc.  
2494 Bayshore Blvd., Suite 201  
Dunedin, FL 34698  
(888) 333-4468 (U.S. only) (727) 738-8857

**SITC -----The Best Choice  
for CISSP candidate to study at**

**Latest CISSP training course**

**08.01.21-25 AT SHANGHAI**

**08.04.21-25 AT BEIJING**

**SITC The best choice for CISSP candidate to study at**

**For more information about CISSP training&exam please contact**

**Mr Liao TEL:021-62126633-6022 MAIL:liaosh@sh.cei.gov.cn**