CISSP®

Certified Information Systems Security Professional

Exam Outline

Candidate Information Bulletin

Effective Date: April 15, 2015

(ISC)²®

Non-Discrimination

ISC)² does not discriminate against candidates on the basis of nationality, gender, religion, race, ethnicity, sexual orientation, age or disability. For further information on (ISC)²'s non-discrimination policy, please visit https://www.isc2.org/legal-info-policies.aspx.

The Certified Information Systems Security Professional (CISSP) is an ISO/IEC 17024 ANSI accredited, internationally recognized benchmark information security certification designed for information security professionals with five or more years of experience in the field. The CISSP examination measures the competence of candidates against an internationally accepted common body of knowledge encompassing eight (8) security domains which include Security and Risk Management, Asset Security, Security Engineering, Communication and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security.

The eight (8) domains of the (ISC)² CISSP CBK® provide a vendor neutral and internationally understood common framework upon which the practice of information security can be discussed, taught and otherwise advanced across geographic and geopolitical boundaries. The broad spectrum of topics included in the CISSP CBK® ensure its relevancy across all disciplines in the field of information security and the high level of detail provided in each domain ensures that credential holders possess the depth of skills and knowledge expected of a seasoned security professional. (ISC)²'s CISSP credential holders may further elevate their standing through one of the CISSP concentrations in management, architecture or engineering. They can also deepen their knowledge beyond the CISSP by coupling credentials such as Digital Forensics (CCFP), Software Development (CSSLP), System Authorization (CAP), and/or the Certified Cloud Security Professional (CCSP).

This Candidate Information Bulletin includes;

- an exam blueprint that outlines major topics and sub- topics within the eight (8) domains,
- a suggested reference list,
- a description of the format of the items on the exam,
- and general examination registration and administration policies.

In order to be considered for the CISSP® credential, candidates are required to have a minimum of five (5) years of cumulative paid full-time security professional work experience in two or more of the eight domains of the (ISC)² CISSP® CBK®. Candidates who presently hold an active certification that appears on the (ISC)² approved list (visit www.isc2.org/credential waiver for a complete list) may receive a one year experience waiver. Alternatively, a four-year Baccalaureate degree, or the regional equivalent, may be substituted for one year of experience. **No more than 1 year of total experience may be waived.**

Candidates must also respond to the following four (4) questions regarding criminal history and related background information and provide an explanation for any questions answered in the affirmative (any such explanations will be evaluated during the endorsement process).

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).*

CISSP Candidates must also attest to the truth of their assertions regarding professional experience, and legally commit to abide by the (ISC)² Code of Ethics (Section 3).

1) Security and Risk Management (e.g., Security, Risk, Compliance, Law, Regulations, Business Continuity)

Overview

The first domain of the CISSP examination, Security and Risk Management, addresses a broad spectrum of general information security and risk management topics beginning with coverage of the fundamental security principles of confidentiality, availability and integrity upon which all information security functions are based. The Security and Risk management Domain then builds upon these concepts in the areas of security governance and compliance and candidates will be tested on both.

As is the case with all (ISC)² examinations, CISSP candidates will tested on ethical considerations in general, and the (ISC)² code of ethics in particular. The unique position of trust from which information security professionals apply their craft must be rooted in an ethically sound and consistently applied code of ethics.

The information security function will not be very successful without carefully constructed and uniformly applied security policies and procedures and candidates will be tested on their ability to develop and implement policies and procedures within an information security context. The security and risk management domain also include coverage of all aspects of business continuity planning including information and requirements gathering, business impact analysis and recovery point objectives.

Risk management constitutes an integral part of the security and risk management domain and CISSP candidates should have a thorough understanding of risk management concepts. Covered individual risk management topics include risk analysis, countermeasure selection and implementation, risk monitoring, reporting, and risk frameworks. This domain further builds upon risk management concepts with the introduction of threat modeling and the integration of risk management into the acquisition and management of hardware, software and service contracts.

CISSP candidates will also be tested in the area of personnel security policies and are expected to be capable of establishing and maintaining security education, training and awareness programs.

Key Areas of Knowledge

A. *Understand and apply concepts of confidentiality, integrity and availability*

B. *Apply security governance principles through:*

B.1 Alignment of security function to strategy, goals, mission, and objectives (e.g., business case, budget and resources)

B.2 Organizational processes (e.g., acquisitions, divestitures, governance committees)

B.3 Security roles and responsibilities

B.4 Control frameworks

B.5 Due care

B.6 Due diligence

C. *Compliance*

C.1 Legislative and regulatory compliance

C.2 Privacy requirements compliance

D. *Understand legal and regulatory issues that pertain to information security in a global context*

D.1 Computer crimes

D.2 Licensing and intellectual property (e.g., copyright, trademark, digital-rights management)

D.3 Import/export controls

D.4 Trans-border data flow

D.5 Privacy

D.6 Data breaches

E. Understand professional ethics

E.1 Exercise (ISC)² Code of Professional Ethics

E.2 Support organization's code of ethics

F. Develop and implement documented security policy, standards, procedures, and guidelines

G. Understand business continuity requirements

G.1 Develop and document project scope and plan

G.2 Conduct business impact analysis

H. Contribute to personnel security policies

H.1 Employment candidate screening (e.g., reference checks, education verification)

H.2 Employment agreements and policies

H.3 Employment termination processes

H.4 Vendor, consultant, and contractor controls

H.5 Compliance

H.6 Privacy

I. Understand and apply risk management concepts

I.1 Identify threats and vulnerabilities

I.2 Risk assessment/analysis (qualitative, quantitative, hybrid)

I.3 Risk assignment/acceptance (e.g., system authorization)

I.4 Countermeasure selection

I.5 Implementation

I.6 Types of controls (preventive, detective, corrective, etc.)

I.7 Control assessment

I.8 Monitoring and measurement

I.9 Asset valuation

I.10 Reporting

I.11 Continuous improvement

I.12 Risk frameworks

J. Understand and apply threat modeling

J.1 Identifying threats (e.g., adversaries, contractors, employees, trusted partners)

J.2 Determining and diagramming potential attacks (e.g., social engineering, spoofing)

J.3 Performing reduction analysis

J.4 Technologies and processes to remediate threats (e.g., software architecture and operations)

K. Integrate security risk considerations into acquisition strategy and practice

K.1 Hardware, software, and services

K.2 Third-party assessment and monitoring (e.g., on-site assessment, document exchange and review, process/policy review)

K.3 Minimum security requirements

K.4 Service-level requirements

L. Establish and manage information security education, training, and awareness

L.1 Appropriate levels of awareness, training, and education required within organization

L.2 Periodic reviews for content relevancy

2) Asset Security (Protecting Security of Assets)

Overview

Asset Security, within the context of the second domain of the (ISC)² CISSP examination, addresses the collection, handling and protection of information throughout its lifecycle. The classification of information and supporting assets forms the basis for all covered topics within this domain and candidates are expected to be well versed in this area. Ownership, as it relates to information, systems, and business processes, goes hand in hand with classification and is the second covered topic in the asset security domain.

The rapid expansion in the collection and storage of digitized personal information has resulted in a corresponding increase in the importance of privacy considerations, and privacy protection constitutes an important part of the asset security domain. Individual privacy protection topics covered on the CISSP examination include the concepts of data owners, data processors, data remanence, and limitations on collection and storage. Any discussion regarding the collection and storage of information must include data retention. Retention must be considered in light of organizational, legal and regulatory requirements and candidates will be tested on each.

Having considered all factors discussed above, the responsibility for the selection of appropriate data security controls then falls upon the information security professional, and CISSP candidates will be tested on this area in some detail. Covered topics in this area include baselines, scoping and tailoring, standards selection and cryptography.

The final topic in the asset security domain addresses data handling requirements and includes data storage, labeling and destruction. CISSP candidates are expected to be capable of evaluating data handling requirements and of developing appropriate policies and procedures based on that evaluation.

Key Areas of Knowledge

A. Classify information and supporting assets (e.g., sensitivity, criticality)

B. Determine and maintain ownership (e.g., data owners, system owners, business/mission owners)

C. Protect privacy

C.1 Data owners

C.2 Data processers

C.3 Data remanence

C.4 Collection limitation

D. Ensure appropriate retention (e.g., media, hardware, personnel)

E. Determine data security controls (e.g., data at rest, data in transit)

E.1 Baselines

E.2 Scoping and tailoring

E.3 Standards selection

E.4 Cryptography

F. Establish handling requirements (markings, labels, storage, destruction of sensitive information)

3) Security Engineering (Engineering and Management of Security)

Overview

Security engineering makes up the third domain of the CISSP examination and it is also the second largest in terms of the number of covered topics. Security engineering may be defined as the practice of building information systems and related architecture that continue to deliver the required functionality in the face of threats that may be caused by malicious acts, human error, hardware failure and natural disasters. It is the natural expression of the underlying security principles of confidentiality, integrity and availability in systems engineering and involves the incorporation and integration of security controls, behaviors and capabilities into information systems and enterprise architecture.

CISSP candidates will be tested on their ability to implement and manage security engineering processes using secure design principles. They must understand the fundamental concepts of security models and be capable of developing design requirements based on organization requirements and security policies and of selecting controls and countermeasures that satisfy those design requirements. All of this is made possible by the security professional's in depth knowledge and understanding of the security limitations and capabilities of information systems and candidates will tested in this area.

Information security professionals must continuously assess and mitigate vulnerabilities in security architectures, designs and solution elements and CISSP candidates will be tested on this area in some detail. Individual topics covered under this task include client and server-side vulnerabilities, database security, distributed systems and cloud security, cryptographic systems and industrial controls. Web application vulnerabilities, mobiles devices and embedded systems are also covered.

Cryptography involves the protection of information, both while in motion and at rest, by altering that information to ensure its integrity, confidentiality and authenticity and is covered in some detail in the security engineering domain. CISSP candidates will be tested on general cryptographic concepts, the cryptographic lifecycle, cryptographic systems, public key infrastructure, key management practices, digital signatures, and digital rights management. Candidates must also have a thorough understanding of cryptanalytic attack vectors including social engineering, brute force, cipher-text only, known plaintext, frequency analysis, chosen cipher-text and implementation attacks.

Security engineering is not limited to information systems development and additional topics in the security engineering domain include the application of secure design principles to site and facility design and physical security.

Key Areas of Knowledge

A. Implement and manage engineering processes using secure design principles

B. Understand the fundamental concepts of security models (e.g., Confidentiality, Integrity, and Multi-level Models)

C. Select controls and countermeasures based upon systems security evaluation models

D. Understand security capabilities of information systems (e.g., memory protection, virtualization, trusted platform module, interfaces, fault tolerance)

E. Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

- E.1 Client-based (e.g., applets, local caches)
- E.2 Server-based (e.g., data flow control)
- E.3 Database security (e.g., inference, aggregation, data mining, data analytics, warehousing)
- E.4 Large-scale parallel data systems
- E.5 Distributed systems (e.g., cloud computing, grid computing, peer to peer)
- E.6 Cryptographic systems
- E.7 Industrial control systems (e.g., SCADA)

F. Assess and mitigate vulnerabilities in web-based systems (e.g., XML, OWASP)

G. Assess and mitigate vulnerabilities in mobile systems

H. Assess and mitigate vulnerabilities in embedded devices and cyber-physical systems (e.g., network-enabled devices, Internet of things (IoT))

I. Apply cryptography

- I.1 Cryptographic life cycle (e.g., cryptographic limitations, algorithm/protocol governance)
- I.2 Cryptographic types (e.g., symmetric, asymmetric, elliptic curves)
- I.3 Public Key Infrastructure (PKI)
- I.4 Key management practices
- I.5 Digital signatures

I.6 Digital rights management

I.7 Non-repudiation

I.8 Integrity (hashing and salting)

I.9 Methods of cryptanalytic attacks (e.g., brute force, cipher-text only, known plaintext)

J. Apply secure principles to site and facility design

K. Design and implement physical security

K.1 Wiring closets

K.2 Server rooms

K.3 Media storage facilities

K.4 Evidence storage

K.5 Restricted and work area security (e.g., operations centers)

K.6 Data center security

K.7 Utilities and HVAC considerations

K.8 Water issues (e.g., leakage, flooding)

K.9 Fire prevention, detection and suppression

4) Communication and Network Security (Designing and Protecting Network Security)

Overview

The communication and network security domain encompasses the network architecture, transmission methods, transport protocols, control devices, and the security measures used to maintain the confidentiality, integrity and availability of information transmitted over both private and public communication networks.

The CISSP candidate is expected to demonstrate a thorough understanding of network fundamentals including network topologies, IP addressing, network segmentation, switching and routing, wireless networking, the OSI and TCP models and the TCP/IP protocol suite. Candidates will also be tested on cryptography as it relates to secure network communication. The communication and network security domain also includes a broad range of topics under the heading of securing network devices. CISSP candidates will be tested on their knowledge of, and ability to, securely operate and maintain network control devices including switches, routers and wireless access points. Candidates must be familiar with the security considerations inherent in the various forms of transmission media. Network access control, endpoint security, and content distribution networks are also covered.

CISSP candidates are expected to be capable of designing and implementing secure communication channels using a wide range of technologies to facilitate a number of applications including data, voice, remote access, multimedia collaboration and virtualized networks. Candidates will also be tested on their knowledge of network attack vectors and on their ability to prevent or mitigate those attacks.

Key Areas of Knowledge

A. Apply secure design principles to network architecture (e.g., IP & non-IP protocols, segmentation)

A.1 OSI and TCP/IP models

A.2 IP networking

A.3 Implications of multilayer protocols (e.g., DNP3)

A.4 Converged protocols (e.g., FCoE, MPLS, VoIP, iSCSI)

A.5 Software-defined networks

A.6 Wireless networks

A.7 Cryptography used to maintain communication security

B. Secure network components

B.1	Operation of hardware (e.g., modems, switches, routers, wireless access points, mobile devices)
B.2	Transmission media (e.g., wired, wireless, fiber)
B.3	Network access control devices (e.g., firewalls, proxies)
B.4	Endpoint security
B.5	Content-distribution networks
B.6	Physical devices

C. Design and establish secure communication channels

C.1	Voice
C.2	Multimedia collaboration (e.g., remote meeting technology, instant messaging)
C.3	Remote access (e.g., VPN, screen scraper, virtual application/desktop, telecommuting)
C.4	Data communications (e.g., VLAN, TLS/SSL)
C.5	Virtualized networks (e.g., SDN, virtual SAN, guest operating systems, port isolation)

D. Prevent or mitigate network attacks

5) Identity and Access Management (Controlling Access and Managing Identity)

Overview

Identity and access management is an essential component of information security in general and the CISSP examination in particular. It involves provisioning and managing the identities and access used in the interaction of humans and information systems, of disparate information systems, and even between individual components of information systems. Compromising an identity or an access control system to gain unauthorized access to systems and information also happens to be the net goal of almost all attacks involving the confidentiality of data so it is an area where information security professionals should invest a considerable amount of time.

The identity and access management domain addresses the identification and authorization of users, systems and services. CISSP candidates will be tested on identity management systems, single and multi-factor authentication, accountability, session management, registration and proofing, federated identity management, and credential management systems.

Candidates will also be tested on the integration of third party cloud based and on premise identity services. CISSP candidates are expected to be capable of implementing and managing authorization mechanisms including those based on role-based, rule-based, mandatory and discretionary access control. Topics in the identity and access management domain also include the prevention and mitigation of attacks targeting access control systems and on the identity management lifecycle.

Key Areas of Knowledge

A. Control physical and logical access to assets

A.1 Information

A.2 Systems

A.3 Devices

A.4 Facilities

B. Manage identification and authentication of people and devices

B.1 Identity management implementation (e.g., SSO, LDAP)

B.2 Single/multi-factor authentication (e.g., factors, strength, errors, biometrics)

B.3 Accountability

B.4 Session management (e.g., timeouts, screensavers)

B.5 Registration and proofing of identity

B.6 Federated identity management (e.g., SAML)

B.7 Credential management systems

C. Integrate identity as a service (e.g., cloud identity)

D. Integrate third-party identity services (e.g., on-premise)

E. Implement and manage authorization mechanisms

E.1 Role-Based Access Control (RBAC) methods

E.2 Rule-based access control methods

E.3 Mandatory Access Control (MAC)

E.4 Discretionary Access Control (DAC)

F. Prevent or mitigate access control attacks

G. Manage the identity and access provisioning lifecycle (e.g., provisioning, review)

6) Security Assessment and Testing (Designing, Performing, and Analyzing Security Testing)

Overview

Security assessment and testing involves the evaluation of information assets and associated infrastructure using various tools and techniques for the purposes of identifying and mitigating risk due to architectural issues, design flaws, configuration errors, hardware and software vulnerabilities, coding errors, and any other weaknesses that may affect an information system's ability to deliver its intended functionality in a secure manner. For the purposes of the CISSP examination, it also includes the continuous validation of the application of organizational information security plans, policies, processes and procedures.

CISSP candidates should be capable of validating assessment and test strategies and of carrying out those strategies using various techniques. Candidates will be tested on vulnerability assessments, penetration testing, synthetic transactions, code review and testing, misuse case, and interface testing.

Information security professionals must ensure that security policies and procedures are continuously and uniformly applied. They must also ensure that disaster recovery and business continuity plans are maintained, updated, and will function as intended in the event of a disaster. To this end, the security assessment and testing domain includes topics in the collection of security process data. Candidates will be tested on account management, management review, key performance and risk indicators, verification of backups, training and awareness, and disaster recovery and business continuity.

Security assessment and testing has little value in the absence of the careful analysis and reporting of assessment results such that appropriate mitigation strategies can be developed and implemented. CISSP candidates will be tested on their ability to analyze and report on test outputs. Candidates will also be tested on their ability to conduct or facilitate internal and third party audits.

Key Areas of Knowledge

A. Design and validate assessment and test strategies

B. Conduct security control testing

- B.1 Vulnerability assessment
- B.2 Penetration testing
- B.3 Log reviews
- B.4 Synthetic transactions
- B.5 Code review and testing (e.g., manual, dynamic, static, fuzz)
- B.6 Misuse case testing
- B.7 Test coverage analysis
- B.8 Interface testing (e.g., API, UI, physical)

C. Collect security process data (e.g., management and operational controls)

- C.1 Account management (e.g., escalation, revocation)
- C.2 Management review
- C.3 Key performance and risk indicators
- C.4 Backup verification data
- C.5 Training and awareness
- C.6 Disaster recovery and business continuity

D. Analyze and report test outputs (e.g., automated, manual)

E. Conduct or facilitate internal and third party audits

7) Security Operations (e.g., Foundational Concepts, Investigations, Incident Management, Disaster Recovery)

Overview

The security operations domain represents a broad range of topics involving the application of information security concepts and best practices to the operation of enterprise computing systems. It is practical in nature and intended to cover the tasks and situations that information security professionals are expected to perform or are presented with on a daily basis. It is also representative of the areas where security professionals spend most of their time so it is no surprise that the security operations domain is the largest in terms of individual topics on the CISSP examination.

The security operations domain includes topics intended to assess the CISSP candidate's knowledge of and ability to orchestrate and otherwise support forensic investigations. Candidates will be tested on various investigative concepts including evidence collection and handling, documentation and reporting, investigative techniques and digital forensics. CISSP candidates must also understand investigation requirements from an operational, criminal, civil, and regulatory perspective.

Effective logging and monitoring mechanisms are an essential security function. In addition to supporting forensic investigations, logging and monitoring provide visibility into the day to day operation of the information technology infrastructure. Individual topics in this area include intrusion detection and prevention, security information and event monitoring systems, and data leakage protection.

The security operations domain also addresses the provisioning of resources and the management and protection of those resources throughout their lifecycle and it is the protection of those resources upon which security operations is predicated. CISSP candidates will be tested on their ability to operate and maintain protective controls including firewalls, intrusion prevention systems, application whitelisting, anti-malware, honeypots and honeynets and sandboxing as well manage third party security contracts and services. Candidates will also be tested on patch, vulnerability and change management.

Additional topics covered under the security operations domain include incident response and recovery, disaster recovery, and business continuity. Candidates will be tested on their ability to conduct all aspects of incident management and on their ability to implement and test disaster recovery processes and participate in business continuity planning. The security operations domain concludes with topics in physical security and personal safety.

Key Areas of Knowledge

A. Understand and support investigations

A.1 Evidence collection and handling (e.g., chain of custody, interviewing)

A.2 Reporting and documenting

A.3 Investigative techniques (e.g., root-cause analysis, incident handling)

A.4 Digital forensics (e.g., media, network, software, and embedded devices)

B. Understand requirements for investigation types

B.1 Operational

B.2 Criminal

B.3 Civil

B.4 Regulatory

B.5 Electronic discovery (eDiscovery)

C. Conduct logging and monitoring activities

C.1 Intrusion detection and prevention

C.2 Security information and event management

C.3 Continuous monitoring

C.4 Egress monitoring (e.g., data loss prevention, steganography, watermarking)

D. Secure the provisioning of resources

D.1 Asset inventory (e.g., hardware, software)

D.2 Configuration management

D.3 Physical assets

D.4 Virtual assets (e.g., software-defined network, virtual SAN, guest operating systems)

D.5 Cloud assets (e.g., services, VMs, storage, networks)

D.6 Applications (e.g., workloads or private clouds, web services, software as a service)

E. Understand and apply foundational security operations concepts

E.1 Need-to-know/least privilege (e.g., entitlement, aggregation, transitive trust)

E.2 Separation of duties and responsibilities

E.3 Monitor special privileges (e.g., operators, administrators)

E.4 Job rotation

E.5 Information lifecycle

E.6 Service-level agreements

F. Employ resource protection techniques

F.1 Media management

F.2 Hardware and software asset management

G. Conduct incident management

G.1 Detection

G.2 Response

G.3 Mitigation

G.4 Reporting

G.5 Recovery

G.6 Remediation

G.7 Lessons learned

H. Operate and maintain preventative measures

H.1 Firewalls

H.2 Intrusion detection and prevention systems

H.3 Whitelisting/Blacklisting

H.4 Third-party security services

H.5 Sandboxing

H.6 Honeypots/Honeynets

H.7 Anti-malware

I. Implement and support patch and vulnerability management

J. Participate in and understand change management processes (e.g., versioning, baselining, security impact analysis)

K. Implement recovery strategies

K.1 Backup storage strategies (e.g., offsite storage, electronic vaulting, tape rotation)

K.2 Recovery site strategies

K.3 Multiple processing sites (e.g., operationally redundant systems)

K.4 System resilience, high availability, quality of service, and fault tolerance

L. Implement disaster recovery processes

L.1 Response

L.2 Personnel

L.3 Communications

L.4 Assessment

L.5 Restoration

L.6 Training and awareness

M. Test disaster recovery plans

M.1 Read-through

M.2 Walkthrough

M.3 Simulation

M.4 Parallel

M.5 Full interruption

N. Participate in business continuity planning and exercises

O. Implement and manage physical security

O.1 Perimeter (e.g., access control and monitoring)

O.2 Internal security (e.g., escort requirements/visitor control, keys and locks)

P. Participate in addressing personnel safety concerns (e.g., duress, travel, monitoring)

8) Software Development Security (Understanding, Applying, and Enforcing Software Security)

Overview

The last domain of the CISSP examination, software development security, involves the application of security concepts and best practices to production and development software environments. CISSP's are not, generally speaking, software developers or software security engineers; however, it is incumbent upon them to assess and enforce security controls on software being operated within their environments.

To achieve this end, information security professionals must understand and apply security in the context of the software development lifecycle. CISSP candidates will be tested on software development methodologies, maturity models, operations and maintenance and change management as well as understand the need for an integrated product development team.

Information security professionals must also be capable of enforcing security controls in software development environments. Candidates will be tested on several topics in this area including the security of software development tools, source code weaknesses and vulnerabilities, configuration management as it relates to source code development, the security of code repositories and the security of application programming interfaces.

CISSP candidates will also be tested in the area of software security control assessment. Topics in this area include auditing and logging as it relates to change management, risk analysis and mitigation as it relates to software security and the security impact of acquired software.

Key Areas of Knowledge

A. Understand and apply security in the software development lifecycle

A.1 Development methodologies (e.g., Agile, Waterfall)

A.2 Maturity models

A.3 Operation and maintenance

A.4 Change management

A.5 Integrated product team (e.g., DevOps)

B. Enforce security controls in development environments

B.1 Security of the software environments

B.2 Security weaknesses and vulnerabilities at the source-code level (e.g., buffer overflow, escalation of privilege, input/output validation)

B.3 Configuration management as an aspect of secure coding

B.4 Security of code repositories

B.5 Security of application programming interfaces

C. Assess the effectiveness of software security

C.1 Auditing and logging of changes

C.2 Risk analysis and mitigation

C.3 Acceptance testing

D. Assess security impact of acquired software

REFERENCES

The CISSP exam is based on a common body of knowledge that is recognized internationally and the exam content is based on a job task analysis conducted as recommended by ISO/IEC/ANSI 17024 standards. Questions included in the examination are developed by item writers who are subject matter experts in the field from information gained through their practical experience. Such information is validated against reference materials including (ISC)²'s own common body of knowledge, textbooks, articles, standards and regulations. The following supplemental reference list is not intended to be all inclusive and (ISC) ² makes no assertion that the use of this list or knowledge of the subject matter within will result in the successful completion of the examination. Nor does (ISC) ² endorse any particular text or author. Candidates are encouraged to supplement their education and experience by reviewing relevant resources that pertain to the common body of knowledge and finding information for areas in which they find themselves to be deficient.

Domain	Supplementary Reference
Security and Risk Management (e.g., Security, Risk, Compliance, Law, Regulations, Business Continuity)	(ISC)², *Code of Ethics (https://www.isc2.org/ethics/default.aspx)*
	Bacik, S., (2008). *Building an Effective Information Security Policy Architecture*
	Bowman, R.H., (2008). *Business Continuity Planning for Data Centers and Systems: A Strategic Implementation Guide*
	Brotby, K., (2010). *Information Security Governance*
	Calder, A., S. Watkins, (2012). *IT Governance: A Manager's Guide to Data Security and ISO 27001/ISO 27002, (5th Edition)*
	Ermann, M.D., M.S. Shauf, (2002). *Computers, Ethics, and Society, (3RD Edition)*
	Garner, B.A., (2009). *Black's Law Dictionary,(9th edition)*
	Hayden, L., (2010). *IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data*
	Herold, R., (2010). *Managing an Information Security and Privacy Awareness and Training Program, (2nd Edition)*
	Hiles, A., P. Barnes, (2010). *The Definitive Handbook of Business Continuity Management, (3rd Edition)*
	Jaquith, A., (2007). *Security Metrics: Replacing Fear, Uncertainty, and Doubt*
	Kuner, C., (2007). *European Data Protection Law: Corporate Regulation and Compliance*
	Landoll, D.J., (2011). *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments, (2nd Edition)*

	National Fire Protection Association, (2013). *NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity*
	Nissenbaum, H., (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*
	PCI Security Standards Council, (2013). Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures, Version 3.0
	Thomas L. Norman, (2009). *Risk Analysis and Security Countermeasure Selection*
	Hernandez, S., (2012). *Official (ISC)² Guide to the CISSP CBK, (3rd Edition)*
	Whitman, M.E., H.J. Mattord, (2013). *Management of Information Security (4th Edition)*
Asset Security (Protecting Security of Assets)	Alger, D., (2012). *Build the Best Data Center Facility for Your Business*
	Al homaidi, O., Boldt, M., (2010). Data Remanence: Secure Deletion of data in Solid State Drives
	Arata, A., (2005). *Perimeter Security*
	Damjanovski, V., (2013). *CCTV, Third Edition: From Light to Pixels*
	Davis, C., Schiller, M., (2011). IT Auditing Using Controls to Protect Information Assets, (2nd Edition)
	Fennelly, L., (2012). *Effective Physical Security, (4th Edition)*
	Garcia, M.L., (2005). *Vulnerability Assessment of Physical Protection Systems*
	Johnson, M., (2011). *It Asset Management: What you Need to Know For It Operations Management*
	Khairallah, M., (2005). *Physical Security Systems Handbook: The Design and Implementation of Electronic Security Systems*
	Knoke, M., (2012). Protection of Assets: Security management
	Nilsson, F., (2008). *Intelligent Network Video: Understanding Modern Video Surveillance Systems*
	Schulz, G., (2009). *The Green and Virtual Data Center*
	Snevely, R. (2002). *Enterprise Data Center Design and Methodology*
Security Engineering (Engineering and Management of Security)	Anderson, R.J., (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems*
	Challener, C., K. Yoder, R. Catherman, D. Safford, L.V. Doorn, (2008). *A Practical Guide to Trusted Computing*
	Cole, E., (2003). *Hiding in Plain Sight: Steganography and the Art of Covert Communication*
	D. Hankerson, A.J. Menezes, S. Vanstone, (2010). *Guide to Elliptic Curve Cryptography*
	Daemen, J., V. Rijmen, (2002). *The Design of RijndaeL: AES - The Advanced Encryption Standard*

	Garfinkel, S., (1994). *PGP: Pretty Good Privacy*
	Gillis, T., (2010). *Securing the Borderless Network: Security for the Web 2.0 World*
	Higaki, W.H., Y. Higaki, (2010). *Successful Common Criteria Evaluations: A Practical Guide for Vendors*
	Kanneganti, R., P.R. Chodavarapu, (2008). *SOA Security*
	Karamanian, A., S. Tenneti, (2011). *PKI Uncovered: Certificate-Based Security Solutions for Next-Generation Networks*
	Kenan, K., (2005). *Cryptography in the Database: The Last Line of Defense*
	Menezes, A.J., P. van Oorschot, S. Vanstone, (1996). *Handbook of Applied Cryptography (Discrete Mathematics and Its Applications)*
	Petkovic, M., W. Jonker, (2007). *Security, Privacy, and Trust in Modern Data Management*
	Santos, O., (2007). *End-to-End Network Security: Defense-in-Depth*
	Schneier, B., (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C (2nd Edition)*
	Shimonski, R., W. Schmied, V. Chang, T.W. Shinder, (2006). *Building DMZs For Enterprise Networks*
	W. Stallings, (2013). *Cryptography and Network Security: Principles and Practice (6th Edition)*
Communications and Network Security (Designing and Protecting Network Security)	Boudriga, N., (2009). *Security of Mobile Communications*
	Cheswick, W.R., S.M. Bellovin, A.D. Rubin, (2003). *Firewalls and Internet Security: Repelling the Wily Hacker (2nd Edition)*
	Daniel V. Hoffman, D.V., (2008). *Implementing NAP and NAC Security Technologies: The Complete Guide to Network Access Control*
	Davis, C., (2001). *IPSec: Securing VPNs*
	Hogg, S., E. Vyncke, (2008). *IPv6 Security*
	Kadrich, M., (2007). *Endpoint Security*
	Luotonen, A., (1997). *Web Proxy Servers*
	Porter, T., J. Kanclirz, B. Baskin, (2006). *Practical VoIP Security*
	Prowell, S., R.Kraus, M. Borkin, (2010). *Seven Deadliest Network Attacks*
	Stevens, W.R., G.R. Wright, (2001). *TCP/IP Illustrated (3 Volume Set)*
	Wetteroth, D., (2001). *OSI Reference Model for Telecommunications*
Identity and Access Management (Controlling Access and Managing Identity)	Bertino, E., K. Takahashi, (2011). *Identity Management: Concepts, Technologies, and Systems*
	Chin, S-K., S.B. Older (2010). *Access Control, Security, and Trust: A Logical Approach*
	Ferraiolo, D.F., D.R. Kuhn, R. Chandramouli, (2007). *Role-Based Access Control (2nd Edition)*
	Kayem, A.V., S.G. Akl, P. Martin, (2010). *Adaptive Cryptographic Access Control*

	Konicek, J., (1997). *Security, ID Systems and Locks: The Book on Electronic Access Control*
	Links, C.L., (2008). *IAM Success Tips (Volumes 1-3)*
	Newman, R., (2009). *Security and Access Control Using Biometric Technologies: Application, Technology, and Management*
	Rankl, W., W. Effing, (2010). *Smart Card Handbook*
	Tipton, H.F., M.K. Nozaki, (2012). *Information Security Management Handbook (2012 CD-ROM Edition)*
	Vacca, J.R., (2010). *Biometric Technologies and Verification Systems*
Security Assessment and Testing (Designing, Performing, and Analyzing Security Testing)	Ali, S., T. Heriyanto, (2011). *BackTrack 4: Assuring Security by Penetration Testing*
	Babbin, J., D. Kleiman, E.F. Carter Jr., J. Faircloth, (2006). *Security Log Management: Identifying Patterns in the Chaos*
	Engebretson, P., (2013). The Basics of Hacking and Penetration Testing, Second Edition
	Foreman, P., (2009). *Vulnerability Management*
	Hope, P. B. Walther, (2008). *Web Security Testing Cookbook: Systematic Techniques to Find Problems Fast*
	Kanneganti, R., P.R. Chodavarapu, (2008). *SOA Security*
	Andrews, M., J.A. Whittaker, (2006). How to Break Web Software: Functional and Security Testing of Web Applications and Web Services
	Swiderski, F., W. Snyder, (2004). *Threat Modeling*
	Trost, R., (2009). *Practical Intrusion Analysis: Prevention and Detection for the Twenty-First Century*
Security Operations (e.g., Foundational Concepts, Investigations, Incident Management, Disaster Recovery)	Aiello, R., (2010). *Configuration Management Best Practices: Practical Methods that Work in the Real World*
	Buffington, J., (2010). *Data Protection for Virtual Data Centers*
	Bejtlich, R., (2005). *Extrusion Detection: Security Monitoring for Internal Intrusions*
	Bosworth, S., M. E. Kabay, E. Whyne, (2009). *Computer Security Handbook (2 Volume Set)*
	Casey, E., (2011). *Digital Evidence and Computer Crime, Forensic Science, Computers, and the Internet (3rd Edition)*
	Clark, T., (2005). Storage Virtualization: Technologies for Simplifying Data Storage and Management
	Cloud Security Alliance, (2011). Security Guidance For Critical Areas Of Focus In Cloud Computing V3.0
	Cole, E., S. Ring, (2006). *Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft*
	Foreman, P. (2009). *Vulnerability Management*
	Fry, C., M. Nystrom, (2009). *Security Monitoring: Proven Methods for Incident Detection on Enterprise Networks*

	Hadnagy, C., (2010). *Social Engineering: The Art of Human Hacking*
	Koren, I., C.M. Krishna, (2007). *Fault-Tolerant Systems*
	Little, D.B., D.A. Chapa, (2003). *Implementing Backup and Recovery: The Readiness Guide for the Enterprise*
	Mather, T., S. Kumaraswamy, S. Latif, (2009). *Cloud Security and Privacy*
	Moeller, R.R., (2010). *IT Audit, Control, and Security (2 Edition)*
	Preston, C., (2007). *Backup & Recovery: Inexpensive Backup Solutions for Open Systems*
	Prosise, C., K. Mandia, (2014). *Incident Response and Computer Forensics (3rd Edition)*
	Rajnovic, D., (2010). *Computer Incident Response and Product Security*
	Schmidt, K., (2006). *High Availability and Disaster Recovery: Concepts, Design, Implementation*
	Snedaker, S., (2013). *Business Continuity and Disaster Recovery Planning for IT Professionals, (2nd Edition)*
	Toigo, J.W., (2014). *Disaster Recovery Planning: getting to Business-Savvy Business Continuity (4th Edition)*
	Trost, R., (2009). *Practical Intrusion Analysis: Prevention and Detection for the Twenty-First Century*
Software Development Security (Understanding, Applying, and Enforcing Software Security)	Allen, J.A., S.J. Barnum, R.J. Ellison, G. McGraw, N.R. Mead, (2008). *Software Security Engineering: A Guide for Project Managers*
	Chess, B., J. West, (2007). *Secure Programming with Static Analysis*
	Clarke, J., (2012). *SQL Injection Attacks and Defense, (2nd Edition)*
	Dowd, M., J. McDonald, J. Schuh, (2006). *The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities*
	Dwivedi, H., (2010). *Mobile Application Security*
	Howard, M., D. LeBlanc, J. Viega, (2009). *24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them*
	Howard, M., S. Lipner, (2006). *The Security Development Lifecycle: SDL: A Process for Developing Demonstrably More Secure Software*
	Ligh, M., S. Adair, B. Hartstein, M. Richard, (2010). *Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code*
	Stuttard, D., M. Pinto, (2011). *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, (2nd Edition)*

SAMPLE EXAM QUESTIONS

CISSP® Exam Questions

Innovative Drag & Drop and Hotspot CISSP Questions

Beginning in 2014, (ISC)²® will introduce new innovative Drag & Drop and Hotspot in its flagship CISSP certification examination. Innovative question types provide several benefits over simple four-option multiple choice items. Benefits of the new CISSP questions include:

- Measures knowledge at higher cognitive levels
- Measures a broader range of skills
- Provides more realistic simulation of practice in the field
- Provides opportunities for broader content coverage than may be possible with multiple choice questions

How the New CISSP Questions be scored?

Innovative questions will be scored in the same way that a multiple-choice question is scored because there is only one right answer to each item. All questions, both multiple choice and innovative types will be equally weighted when determining scores. The total testing time for the CISSP examination will remain the same. Addition of such items should not impact candidates' ability to complete the examination within the time limit.

What will the New CISSP Questions look like?

Candidates are encouraged to view the Tutorial **(**https://www.isc2.org/innovative-cissp-questions/default.aspx**)** in order to become familiar with samples of each item type being used on the examination.

Drag & Drop Sample CISSP Question ***(please note:*** *in order to score a correct answer, both correct answers must be pulled into the box on the right hand side - partial score will not be awarded, if only one correct answer is pulled into the box).*

Hot Spot Sample CISSP Question

SAMPLE EXAM QUESTIONS (continued)

1. Which one of the following is the MOST important security consideration when selecting a new computer facility?

   (A) Local law enforcement response times

   (B) Adjacent to competitors' facilities

   (C) Aircraft flight paths

   (D) Utility infrastructure

   Answer - D

2. Which one of the following describes a SYN flood attack?

   (A) Rapid transmission of Internet Relay Chat (IRC) messages

   (B) Creating a high number of half-open connections

   (C) Disabling the Domain Name Service (DNS) server

   (D) Excessive list linking of users and files

   Answer - B

3. Which of the following is a limitation of fuzzing, as it relates to secure software development best practices?

   (A) Access to the source code is required.

   (B) Not all discovered issues are exploitable.

   (C) Issues must be accessible through an open interface.

   (D) Is not suitable where code development is outsourced.

   Answer - C

GENERAL EXAMINATION INFORMATION

Computer Based Testing (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 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 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), 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) 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.

Accepted Primary ID (photograph and signature, not expired)
• Government issued Driver's License or Identification Card
• U.S. Dept of State Drivers License
• U.S. Learner's Permit (card only with photo and signature)
• National/State/Country Identification Card
• Passport
• Passport Cards
• Military ID
• Military ID for spouses and dependents
• Alien Registration Card (Green Card, Permanent Resident Visa)
• Government Issued local language ID (plastic card with photo and signature
• Employee ID
• School ID
• 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.
Accepted Secondary ID (contains signature, not expired)
• U.S. Social Security Card
• Debit/(ATM) Card
• Credit Cards
• Any form of ID on the primary list

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.

Exam Irregularities and Test Invalidation

(ISC)² exams are intended to be delivered under standardized conditions. If any irregularity or fraud is encountered before, during, or after the administration of the exam, (ISC)² will examine the situation and determine whether action is warranted. If (ISC)² determines that any testing irregularity or fraud has happened, it may choose not to score the answer documents of the affected test taker(s), or it may choose to cancel the scores of the affected test taker(s).

(ISC)² may at its sole discretion revoke any and all certifications a candidate may have earned and ban the candidate from earning future (ISC)² certifications, and decline to score or cancel any Exam under any of the circumstances listed in the (ISC)² Examination Agreement. Please refer to the (ISC)² Examination Agreement for further details.

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/LogoGuidleines.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

(ISC)²®