CC℠

Certified in Cybersecurity

ISC2 Certification

Certification Exam Outline

Effective Date: August 29, 2022

ISC2™

About Certified in Cybersecurity Certification

Certified in Cybersecurity (CC) will prove to employers you have the foundational knowledge, skills and abilities necessary for an entry- or junior-level cybersecurity role. It will signal your understanding of fundamental security best practices, policies and procedures, as well as your willingness and ability to learn more and grow on the job.

There are five domains covered on the exam.

- Security Principles
- Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts
- Access Controls Concepts
- Network Security
- Security Operations

Experience Requirements

There are no specific prerequisites to take the exam. It is recommended that candidates have basic information technology (IT) knowledge. No work experience in cybersecurity or any formal educational diploma/degree is required. The next step in the candidate's career would drive to earning ISC2 expert-level certifications, which require experience in the field.

Job Task Analysis (JTA)

ISC2 has an obligation to its membership to maintain the relevancy of the CC. Conducted at regular intervals, the Job Task Analysis (JTA) is a methodical and critical process of determining the tasks that are performed by security professionals who are engaged in the profession defined by the CC. The results of the JTA are used to update the examination. This process ensures that candidates are tested on the topic areas relevant to the roles and responsibilities of today's practicing information security professionals.

CC Examination Information

Length of exam	2 hours
Number of items	100
Item format	Multiple choice
Passing grade	700 out of 1000 points
Exam availability	English, Chinese, Japanese, German
Testing center	Pearson VUE Testing Center

CC Examination Weights

Domains	Average Weight
1. Security Principles	26%
2. Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts	10%
3. Access Controls Concepts	22%
4. Network Security	24%
5. Security Operations	18%
Total	**100%**

Domain 1:
Security Principles

1.1 Understand the security concepts of information assurance

- Confidentiality
- Integrity
- Availability
- Authentication (e.g., methods of authentication, multi-factor authentication (MFA))
- Non-repudiation
- Privacy

1.2 Understand the risk management process

- Risk management (e.g., risk priorities, risk tolerance)
- Risk identification, assessment and treatment

1.3 Understand security controls

- Technical controls
- Administrative controls
- Physical controls

1.4 Understand (ISC)^2 Code of Ethics

- Professional code of conduct

1.5 Understand governance processes

- Policies
- Procedures
- Standards
- Regulations and laws

Domain 2:
Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts

2.1 Understand business continuity (BC)

- Purpose
- Importance
- Components

2.2 Understand disaster recovery (DR)

- Purpose
- Importance
- Components

2.3 Understand incident response

- Purpose
- Importance
- Components

Domain 3:
Access Controls Concepts

3.1 Understand physical access controls

- Physical security controls (e.g., badge systems, gate entry, environmental design)
- Monitoring (e.g., security guards, closed-circuit television (CCTV), alarm systems, logs)
- Authorized versus unauthorized personnel

3.2 Understand logical access controls

- Principle of least privilege
- Segregation of duties
- Discretionary access control (DAC)
- Mandatory access control (MAC)
- Role-based access control (RBAC)

Domain 4:
Network Security

4.1 Understand computer networking

- Networks (e.g., Open Systems Interconnection (OSI) model, Transmission Control Protocol/Internet Protocol (TCP/IP) model, Internet Protocol version 4 (IPv4), Internet Protocol version 6 (IPv6), WiFi)
- Ports
- Applications

4.2 Understand network threats and attacks

- Types of threats (e.g., distributed denial-of-service (DDoS), virus, worm, Trojan, man-in-the-middle (MITM), side-channel)
- Identification (e.g., intrusion detection system (IDS), host-based intrusion detection system (HIDS), network intrusion detection system (NIDS))
- Prevention (e.g., antivirus, scans, firewalls, intrusion prevention system (IPS))

4.3 Understand network security infrastructure

- On-premises (e.g., power, data center/closets, Heating, Ventilation, and Air Conditioning (HVAC), environmental, fire suppression, redundancy, memorandum of understanding (MOU)/memorandum of agreement (MOA))
- Design (e.g., network segmentation (demilitarized zone (DMZ), virtual local area network (VLAN), virtual private network (VPN), micro-segmentation), defense in depth, Network Access Control (NAC) (segmentation for embedded systems, Internet of Things (IoT))
- Cloud (e.g., service-level agreement (SLA), managed service provider (MSP), Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), hybrid)

Domain 5: Security Operations

5.1 Understand data security

- » Encryption (e.g., symmetric, asymmetric, hashing)
- » Data handling (e.g., destruction, retention, classification, labeling)
- » Logging and monitoring security events

5.2 Understand system hardening

- » Configuration management (e.g., baselines, updates, patches)

5.3 Understand best practice security policies

- » Data handling policy
- » Password policy
- » Acceptable Use Policy (AUP)
- » Bring your own device (BYOD) policy
- » Change management policy (e.g., documentation, approval, rollback)
- » Privacy policy

5.4 Understand security awareness training

- » Purpose/concepts (e.g., social engineering, password protection)
- » Importance

Additional Exam Information

Examination Policies and Procedures

ISC2 recommends that candidates review exam policies and procedures prior to registering for the examination. Read the comprehensive breakdown of this important information at www.isc2.org/Register-for-Exam.

Legal Information

For any questions related to ISC2's legal policies, please contact the ISC2 Legal Department at legal@isc2.org.

Any Questions?

Contact ISC2 Candidate Services in your region:

Americas

Phone: +1-866-331-ISC2 (4722)
Email: membersupport@isc2.org

Asia-Pacific

Phone: +852-5803-5662
Email: isc2asia@isc2.org

Europe, Middle East and Africa

Phone: +44-203-960-7800
Email: info-emea@isc2.org