Certified in Cybersecurity

ISC2 Certification

Certification **Exam Outline**

Effective Date: September 1, 2026

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
- Security Governance
- Identity And Access Management (IAM) Concepts
- Networking and Cloud Security Concepts
- Security Operations and Incident Response

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.

Accreditation

CC is in compliance with the stringent requirements of the ANSI National Accreditation Board (ANAB) ISO/IEC Standard 17024.

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 CAT Examination Information

The CC exam uses Computerized Adaptive Testing (CAT) for all English, Simplified Chinese, Japanese, German, Spanish-Modern exams. You can learn more about CC CAT at **ISC2.org/certifications/computerized-adaptive-testing**.

Length of exam	2 hours
Number of items	100 - 125
Item format	Multiple choice and advanced item types
Passing grade	700 out of 1000 points
Exam availability	English, Chinese, Japanese, German, Spanish
Testing center	Pearson VUE Testing Center

CC CAT Examination Weights

Domains	Average Weight
1. Security Principles	24%
2. Security Governance	17.3%
3. Identity And Access Management (IAM) Concepts	20%
4. Networking and Cloud Security Concepts	21.3%
5. Security Operations and Incident Response	17.3%
	Total: 100%

Domain 1: Security Principles

1.1 Understand cybersecurity concepts

- Confidentiality
- Integrity
- Availability
- Authentication, Authorization, Accounting (AAA)
- Non-repudiation
- Privacy

1.2 Understand risk management concepts

- Risk management lifecycle
- Risk management processes

1.3 Understand governance concepts

- Regulations and laws
- Frameworks and guidelines
- Policies, standards (e.g., International Organization for Standardization (ISO), Center for Internet Security), procedures

1.4 Understand cybersecurity controls

- Technical controls
- Administrative controls
- Physical controls

1.5 Maintain professional and ethical conduct

- Professional code of conduct
- Due care and due diligence
- ISC2 Code of Ethics

Domain 2: Security Governance

2.1 Plan Governance, Risk, and Compliance (GRC)

- Purpose
- Importance
- Frameworks and tools

2.2 Understand redundancy

- Business Continuity (BC)
- Disaster Recovery (DR)

2.3 Understand security awareness

- Organizational culture (e.g., importance of security, security leadership)
- Concepts (e.g., social engineering, password protection, phishing)

2.4 Measure cybersecurity effectiveness

- Key metrics, Key Risk Indicators (KRI)
- Dashboards, score cards, reports

Domain 3: Identity And Access Management (IAM) Concepts

3.1 Understand identity life cycle management

- Roles definition
- Provision
- Review
- Deprovision
- Frameworks and tools

3.2 Understand logical access controls

- Principle of Least Privilege (PoLP)
- Separation of Duties (SoD)
- Access control models

Domain 4: Networking and Cloud Security Concepts

4.1 Understand network security

- Concepts (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), Virtual Private Network (VPN))
- Firewalls (e.g., ports, applications)
- Wireless (e.g., Wi-Fi, Bluetooth)
- Embedded systems (e.g., Industrial Control System (ICS)), Internet Of Things (IoT)

4.2 Understand network security architecture

- Comprehending network segmentation (e.g., Firewall zones, Virtual Local Area Network (VLAN), micro-segmentation)
- Defense in Depth
- Zero Trust (ZT)

4.3 Understand cloud security

- Characteristics (e.g., Broad network access, rapid elasticity, measured service, on-demand self-service, resource pooling)
- Service models
- Deployment models
- Shared security model (e.g., roles and responsibilities)

Domain 5: Security Operations and Incident Response

5.1 Understand data security

- Data handling (e.g., classification, labeling, masking, and sanitization)
- Encryption (e.g., symmetric, asymmetric, hashing, quantum resistant cryptography)

5.2 Understand security operations

- Logging and monitoring security events
- Security event triage (e.g., incident use cases, prioritization, correlation)
- Threat actors (e.g., types, motivations)
- Cyber threat intelligence
- Threat frameworks

5.3 Understand Incident Response (IR)

- Data handling policy implementing Incident Response Plan (IRP)
- Incident Response (IR) exercises (e.g., testing, tabletop)

5.4 Understand asset protection

- Asset lifecycle management (e.g., End Of Life (EOL) software and devices)
- Configuration and change management

5.5 Understand security testing

- Security readiness testing (e.g., blue teaming, purple teaming, red teaming)
- Application testing (e.g., vulnerability scanning, static analysis, dynamic analysis, threat modeling)
- Physical penetration testing (e.g., phishing, tailgating, impersonation)

Additional Exam Information

Supplementary References

Candidates are encouraged to supplement their education and experience by reviewing relevant resources that pertain to the CC Exam Outline and identifying areas of study that may need additional attention.

View the full list of supplementary references at ISC2.org/certifications/References.

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 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), press 1
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