ISC2 CC Certified in Cybersecurity

Duration: 3 Days Course Code: CC Delivery Method: Virtual Learning

Overview:

The CC ISC2 Certified in Cybersecurity course validates the competencies required to establish a strong foundation in cybersecurity knowledge, aligned with employer expectations and backed by a trusted association.
The ISC2 Certified in Cybersecurity (CC) course provides a comprehensive introduction to the core principles and practices of modern cybersecurity. Designed for individuals starting their careers in the field, this course equips learners with the foundational knowledge and practical understanding required to support and secure IT systems and environments.
During this training, Participants will gain insight into essential security concepts, including security principles, governance, identity and access management (IAM), networking and cloud security, and security operations.
By the end of the course, learners will be prepared to confidently pursue the ISC2 Certified in Cybersecurity (CC) certification exam while building a strong foundation for future career growth in cybersecurity.

Updated 9/2026

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

Target Audience:

This course is ideal for Entry-level cybersecurity job roles, including:
- Security Analyst
- Security Specialist
- Security Architect
- Security Auditor
- Forensic Specialist/Analyst
- Junior Penetration Tester
- Security Engineer
- IT Auditor
- IT Security Manager
- Systems Administrator

Objectives:

- Understand fundamental cybersecurity concepts
- Understand risk management, governance, security policies, standards, regulations, and compliance requirements Understand key cybersecurity principles and frameworks
- Describe cybersecurity controls, including administrative, technical, and physical controls.
- Understand Identity and Access Management (IAM) concepts, authentication methods, access control models, and least privilege principles
- Understand security operations, system monitoring, asset protection, vulnerability management, and security best practices
- Describe incident response processes and the role of business continuity and disaster recovery in maintaining organizational resilience.
- Prepare for the ISC² Certified in Cybersecurity (CC) exam

Prerequisites:

No prerequisites required However it is recommended to have the following knowledge & skills:

Testing and Certification

The ISC2 Certified in Cybersecurity (CC) certification is ISC2 the global leader in information security credentials, this certification

- Basic understanding of IT concepts
- Familiarity with networking fundamentals
- Administrative experience with Windows-based TCP/IP networks
- Awareness of other operating systems, such as macOS, Unix, or Linux

creates a clear pathway to an exciting and rewarding career in cybersecurity. It breaks down traditional barriers to entry, enabling you to build confidence and enter your first cybersecurity role ready for what's next.

The exam covers the following domains:

- Domain 1: Security Principles
- Domain 2: Security Governance
- Domain 3: Identity and Access Management (IAM) Concepts
- Domain 4: Network and Cloud Security Concepts
- Domain 5: Security Operations and Incident Response

Certification Title: **ISC2 Certified in Cybersecurity (CC) certification**

Follow-on-Courses:

Learners can progress depending on career goals.

- CCSP - Official ISC2 Certified Cloud Security Professional (CCSP) Training
- CISSP - Official ISC2 Certified Information Systems Security Professional Training (CISSP)
- SSCP - Official ISC2 Systems Security Certified Practitioner (SSCP) Training

Content:

Domain 1: Security Principles

- Module 1: Understand Security Concepts
- Module 2: Understand the Risk Management concepts
- Module 3: Understand governance concepts
- Module 4: Understand cybersecurity controls
- Module 5: Maintain professional and ethical conduct

Domain 2: Security Governance

- Module 1: Plan Governance, Risk and Compliance (GRC)
- Module 2: Understand redundancy
- Module 3: Understand security awareness
- Module 4: Measure cybersecurity effectiveness
- Module 3: Understand Disaster Recovery

Domain 3: Identify and Access Management (IAM) Concepts

- Module 1: Understand identity life cycle management
- Module 2: Understand logical access controls

Domain 4: Networking and Cloud Security Concepts

- Module 1: Understand network security
- Module 2: Understand network security architecture
- Module 3: Understand cloud security

Domain 5: Security Operations and Incident Response

- Module 1: Understand Data Security
- Module 2: Understand security operations
- Module 3: Understand incident response
- Module 4: Understand asset protection
- Module 5: Understand security testing

Further Information:

For More information, or to book your course, please call us on 00 20 (0) 2 2269 1982 or 16142

training@globalknowledge.com.eg

www.globalknowledge.com/en-eg/

Global Knowledge, 16 Moustafa Refaat St. Block 1137, Sheraton Buildings, Heliopolis, Cairo