COURSE SYLLABUS

ISC2 CC Exam Preparation Course (Self-Paced)

Learn all five domains of the current ISC2 Certified in Cybersecurity exam and get ready to sit it, with no experience needed.

> Group classes (Live Online) and onsite training are available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/courses/isc2-cc-exam-prep-course-self-paced



support@graduateschool.edu •
(888) 744-4723

Course Outline

Module 1: Security Principles

- Lessons:
  - Confidentiality, Integrity, and Availability
  - Authentication, Authorization, Accounting, Non-repudiation, and Privacy
  - The Risk Management Lifecycle
  - Governance Concepts: Laws, Frameworks, Policies, Standards, and Procedures
  - Control Types and Professional Ethics
- Applied activity: Learners review a short description of a small company that has just discovered customer records were exposed, and identify which part of the CIA triad was affected, which control types were missing, and which risk treatment option the company chose after the fact.

Module 2: Security Governance

- Lessons:
  - Governance, Risk, and Compliance: Purpose and Frameworks
  - Redundancy: Business Continuity and Disaster Recovery
  - Security Awareness and Organizational Culture
  - Measuring Cybersecurity Effectiveness
- Applied activity: Learners review a short scenario describing an organization whose staff reuse passwords and click simulated phishing messages, and choose the awareness and measurement changes that would address the behavior, including which metric would show whether the change worked.

Module 3: Identity and Access Management (IAM) Concepts

- Lessons:
  - The Identity Life Cycle: Roles, Provisioning, Review, and Deprovisioning
  - Least Privilege and Separation of Duties

- Access Control Models

- Applied activity: Learners review a short scenario describing an employee who has changed jobs three times inside the same company and still holds every permission ever granted, and identify which life cycle step failed, what an access review should have caught, and which principle was violated.

Module 4: Networking and Cloud Security Concepts

- Lessons:
  - Network Concepts: OSI and TCP/IP Models, IPv4, IPv6, and VPNs
  - Firewalls, Wireless, and Embedded Systems
  - Network Security Architecture: Segmentation, Defense in Depth, and Zero Trust
  - Cloud Security: Characteristics, Models, and Shared Responsibility

- Applied activity: Learners review a short description of a small office network that has moved its file storage to a cloud service, and identify which protections belong to the provider, which remain the customer's, and where segmentation would limit the damage from one compromised laptop.

Module 5: Security Operations and Incident Response

Lessons:

- Data Security: Handling and Encryption
- Security Operations: Logging, Monitoring, Triage, and Threat Actors
- Incident Response Plans, Exercises, and Asset Protection
- Security Testing: Team Colors and Application Testing