

Four-Week Pre-Recorded ISC2 CC Curriculum

This accelerated course delivers the core concepts of the ISC2 Certified in Cybersecurity (CC) exam over four weeks. It consists of eight modules, each released every three days. Students watch pre-recorded video lectures, read transcripts, complete labs and take module quizzes. A final exam at the end of week four simulates the certification test.

Module Overview

Module 1: Introduction & Security Principles

Explain the cyber security profession, CIA triad (confidentiality, integrity, availability), risk management basics, security controls and governance.

Module 2: Risk Management & Governance

Deep dive into risk identification, assessment and treatment. Discuss threat actors, vulnerabilities, and policy frameworks.

Module 3: Business Continuity, Disaster Recovery & Incident Response

Explore incident response phases, BC/DR plans, team roles and communication strategies.

Module 4: Access Control Concepts

Cover subjects, objects and rules; principle of least privilege; defense-in-depth; privileged access management; physical vs logical controls.

Module 5: Computer Networking Fundamentals

Introduce network types (LAN, WAN, WLAN, VPN), devices (routers, switches, firewalls), OSI vs TCP/IP models, IPv4 vs IPv6, and Wi-Fi security.

Module 6: Network Threats & Security Infrastructure

Describe common attacks (DDoS, spoofing, malware), threat identification tools (IDS, SIEM), prevention mechanisms, on-premise/cloud infrastructure, and network segmentation.

Module 7: Security Operations

Explain data handling and classification, encryption methods, system hardening, configuration management, policies (password, acceptable use, BYOD) and security awareness training.

Module 8: Review & Practice Exam

Revisit all domains, conduct capstone lab, take practice exam, and receive feedback.

Schedule

Modules are released every three days over four weeks. The final exam and capstone project occur in the last week.