Your Future. Secured.

Sample ISC2 Certified in Cybersecurity Certification Course Outline for OTPs
The course outline can be used as a customizable template

Official ISC2 Certified in Cybersecurity Entry-Level Certification Training

About Certification
To help close the workforce gap, ISC2 recently launched the Certified in Cybersecurity (CC) entry-level certification. With no experience required, it opens opportunities in the field to a much broader range of candidates, including recent graduates, career changers and IT professionals. CC starts newcomers on their path to advanced cybersecurity certifications like the CISSP and future leadership roles.

Official ISC2 Certified in Cybersecurity (CC) Entry-Level Certification Training will review the content covered in the exam. It prepares candidates by building a solid foundation of knowledge they need to pass the exam and ultimately land an entry- or junior-level cybersecurity role.

Participate in live sessions led by an authorized ISC2 instructor to build a solid foundation of knowledge tested on the entry-level Certified in Cybersecurity (CC) exam.

- 8 hours of live instruction
- Peer discussions
- Pre- and post-course assessments
- End-of-chapter study sheets and quizzes
- Online interactive flash cards
- Exam voucher

Exam Domains Covered

- Domain 1: Security Principles
- Domain 2: Business Continuity (BC), Disaster Recovery (DR), & Incident Response Concepts
- Domain 3: Access Controls Concepts
- Domain 4: Network Security
- Domain 5: Security Operations

Who is Training For?
CC training is for IT professionals, career changers, college students, recent college graduates, advanced high school students and recent high school graduates looking to start their path toward cybersecurity leadership by taking the Certified in Cybersecurity entry-level exam. There are no prerequisites.

Course Type
Blended approach to learning that includes live sessions led by an ISC2 Authorized Instructor and self-paced learning sessions.

Course Learning Objectives

After completing this course, learners will be able to:

- Discuss the foundational concepts of cybersecurity principles.
- Recognize foundational security concepts of information assurance.
- Define risk management terminology and summarize the process.
- Relate risk management to personal or professional practices.
- Classify types of security controls.
- Distinguish between policies, procedures, standards, regulations and laws.
- Demonstrate the relationship among governance elements.
- Analyze appropriate outcomes according to the canons of the ISC2 Code of Ethics when given examples.
- Practice the terminology of and review security policies.
- Explain how organizations respond to, recover from and continue to operate during unplanned disruptions.
- Recall the terms and components of incident response.
- Summarize the components of a business continuity plan.
- Identify the components of disaster recovery.
- Practice the terminology and review concepts of business continuity, disaster recovery and incident response.
- Select access controls that are appropriate in a given scenario.
- Relate access control concepts and processes to given scenarios.
- Compare various physical access controls.
- Describe logical access controls.
- Practice the terminology and review concepts of access controls.
- Explain the concepts of network security.
- Recognize common networking terms and models.
- Identify common protocols and port and their secure counterparts.
- Identify types of network (cyber) threats and attacks.
- Discuss common tools used to identify and prevent threats.
- Identify common data center terminology.
- Recognize common cloud service terminology.
- Identify secure network design terminology.
- Practice the terminology and review concepts of network security.
- Explain concepts of security operations.
- Discuss data handling best practices.
- Identify key concepts of logging and monitoring.
- Summarize the different types of encryption and their common uses.
- Describe the concepts of configuration management.
- Explain the application of common security policies.
- Discuss the importance of security awareness training.
- Practice the terminology and review concepts of network operations.

Domains/Modules/Chapters

This course covers the following chapters and modules:

Chapter 1: Security Principles

- Module 1: Understand the Security Concepts of Information Assurance
- Module 2: Understand the Risk Management Processes
- Module 3: Understand Security Controls

- Module 4: Understand Governance Elements
- Module 5: Understand ISC2 Code of Ethics

Chapter 2: Incident Response, Business Continuity and Disaster Recovery

- Module 1: Understand Incident Response
- Module 2: Understand Business Continuity
- Module 3: Understand Disaster Recovery

Chapter 3: Access Controls Concepts

- Module 1: Understand Access Control Concepts
- Module 2: Understand Physical Access Controls
- Module 3: Understand Logical Access controls

Chapter 4: Network Security

- Module 1: Understand Computer Networking
- Module 2: Understand Network (Cyber) Threats and Attacks
- Module 3: Understand Network Security Infrastructure

Chapter 5: Security Operations

- Module 1: Understand Data Security
- Module 2: Understand System Hardening
- Module 3: Understand Best Practice Security Policies
- Module 4: Understand Security Awareness Training

Chapter 6: Course Summary and Test Preparation

- Module 1: Certification Requirements
- Module 2: Scheduling the Exam
- Module 3: Before the Exam
- Module 4: Day of Exam
- Module 5: Tips for Reading the Questions
- Module 6: After the Exam

Note: Course materials are organized by chapter, not domain, which may result in domains or individual domain topics being covered in a different order than what appears in the exam outline. The chapter structure allows us to properly cover the exam domains while supporting a more cohesive learning experience.

www.ISC2.org p: +1.727.785.0189
625 N Washington Street, Suite 400, Alexandria, VA 22314, United States