## CC: Certified in CyberSecurity

Course Code: CC
Duration: 2 days
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

### OVERVIEW

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.

### SKILLS COVERED

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?

**WHO SHOULD ATTEND?**

CC training is for:

- IT professionals
- career changers
- college students
- recent college graduates
- advanced high school students
- recent high school graduates

**PREREQUISITES**

There are no prerequisites required to attend this course.

**MODULES**

**Module 1: Security Principles**

- Understand the Security Concepts of Information Assurance
- Understand the Risk Management Processes
- Understand Security Controls
- Understand Governance Elements
- Understand ISC2 Code of Ethics

**Module 2: Incident Response, Business Continuity and Disaster Recovery**

- Understand Incident Response
- Understand Business Continuity
- Understand Disaster Recovery

**Module 3: Access Controls Concepts**

- Understand Access Control Concepts
- Understand Physical Access Controls
- Understand Logical Access controls

**Module 4: Network Security**

- Understand Computer Networking
- Understand Network (Cyber) Threats and Attacks
- Understand Network Security Infrastructure

**Module 5: Security Operations**

- Understand Data Security
- Understand System Hardening
- Understand Best Practice Security Policies
- Understand Security Awareness Training

**Module 6: Course Summary and Test Preparation**

- Certification Requirements
- Scheduling the Exam
- Before the Exam
- Day of Exam
- Tips for Reading the Questions
- After the Exam

**END OF PAGE**