ISC2 Certified in Cybersecurity Training

Duration: **3 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

The official **ISC2 Certified in Cybersecurity (CC)** training course is an entry-level programme designed to introduce learners to the core concepts and principles of cyber security.

The course provides a structured foundation across key areas such as information security principles, risk management, access control, network security, security operations, incident response, business continuity, and disaster recovery.

It is designed for learners with little or no previous cyber security experience and provides a strong starting point for entering the profession or progressing towards more advanced certifications.

A blended learning approach combines live instructor-led sessions with self-paced study materials, giving participants both guided learning and the flexibility to review content independently.

The programme is aligned with the **ISC2 Certified in Cybersecurity exam** and is designed to help learners approach certification with greater confidence and a clearer understanding of the core domains.

Prerequisites

No previous cyber security experience or formal technical prerequisites are required.

Who Should Attend

This course is particularly suitable for individuals who want to begin a career in cyber security.

Typical participants include:

- IT professionals looking to move into cyber security,
- Adjacent technical teams wanting to build cyber security awareness,
- Career changers,
- College and university students,
- Recent graduates,
- Individuals exploring cyber security career pathways.

ISC2 Certified in Cybersecurity Training

Duration: **3 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

By the end of this course, participants will be able to:

- Explain foundational cyber security concepts and principles,
- Understand basic Risk Management terminology and processes,
- Identify and classify different types of Security Controls,
- Distinguish between Policies, Standards, Procedures, Regulations, and Laws,
- Understand Governance and ethical responsibilities in cyber security,
- Explain Incident Response, Business Continuity, and Disaster Recovery concepts,
- Apply basic Access Control principles in practical scenarios,
- Understand networking fundamentals and common security threats,
- Identify key Security Operations concepts including Monitoring and Encryption,
- Recognise best practices for secure data handling and system protection.

Training Outline

Module 1 – Security Principles

- Information Assurance concepts
- Core security principles
- Risk Management processes
- Security Controls
- Governance elements
- Differences between Policies, Standards, Procedures, Regulations, and Laws
- ISC2 Code of Ethics
- Ethical responsibilities in cyber security

Module 2 – Business Continuity, Disaster Recovery and Incident Response

- Incident Response processes
- Recognising and responding to security incidents
- Business Continuity Planning
- Maintaining critical business services
- Disaster Recovery components
- Restoring systems and services
- Post-incident recovery concepts

Module 3 – Access Control Concepts

- Fundamental Access Control principles
- Access Control Models
- Managing user and resource access
- Physical Access Controls
- Logical Access Controls
- Authorisation and access restriction approaches
- Applying access security in basic scenarios

Module 4 – Network Security

- Networking fundamentals
- Core network components and communication concepts
- Common Threats
- Common Attack Types
- Network Security Infrastructure
- Basic approaches for protecting traffic and connectivity
- Key elements of a secure network environment

Module 5 – Security Operations

- Data Security best practices
- Secure data handling and protection
- System Hardening techniques
- Security Policies and Procedures
- Monitoring concepts
- Introduction to Encryption
- Security Awareness Training
- Supporting a stronger security culture

Module 6 – Exam Preparation and Course Summary

- Understanding ISC2 CC certification requirements
- Exam scheduling and registration
- Understanding the exam format
- Exam techniques and strategies
- Reviewing key concepts across all domains
- Identifying areas that require further study
- Assessing readiness before certification

Hands-On Learning

This course supports not only theoretical understanding, but also practical application of foundational cyber security knowledge.

Participants take part in:

- Scenario-based discussions,
- Practice questions aligned to exam topics,
- Instructor-led walkthroughs of key concepts,
- Guided review sessions for certification preparation.

This practical approach helps reinforce learning and builds confidence in applying basic cyber security principles to realistic situations.

Exams and Assessments

The programme includes structured assessments and preparation activities aligned with the ISC2 Certified in Cybersecurity (CC) exam.

- Official ISC2 Certified in Cybersecurity exam included,
- Delivered using a Computer Adaptive Testing format,
- Approximate exam duration of two hours,

ISC2 Certified in Cybersecurity Training

Duration: **3 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

- Between 100 and 125 questions,
- Question formats may include Multiple Choice and Advanced Item Types,
- Passing score of 700 out of 1000.

By the end of the course, learners should have a clearer understanding of their certification readiness and a stronger foundation for pursuing entry-level cyber security roles.