Training: ISC2
# ISC2 CC Certification Prep Course

## TRAINING GOALS:

Official ISC2 Certified in Cybersecurity (CC) Training Seminar

The Certified in Cybersecurity℠ (CC) is for anyone interested in gaining a basic understanding of cybersecurity concepts. This course covers the content tested in ISC2's entry-level Certified in Cybersecurity (CC) exam helping to build a solid foundation of knowledge tested on the exam and needed to be successful in an entry-level cybersecurity role. The topics covered include:

- Security Principles
- Incident Response, Business Continuity, and Disaster Recovery
- Access Controls Concepts
- Network Security
- Security Operations

*Each participant in an authorized training **CC Certification Prep Course** held in Compendium CE will receive a free CC Certification Exam voucher.*

Course objectives

At the end of 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.



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- 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.

Intended audience

Students, prospective employees, entry-level professionals and career-changers wishing to start their path toward cybersecurity leadership by taking the ISC2’s Certified in Cybersecurity (CC) exam.

## CONSPECT:

- Security Principles
  - Understand the Security Concepts of Information Assurance
  - Understand the Risk Management Process
  - Understand Security Controls



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Understand Governance Elements and Processes
- Understand ISC2 Code of Ethics

- Incident Response, Business Continuity and Disaster Recovery Concepts
  - Understand Incident Response
  - Understand Business Continuity
  - Understand Disaster Recovery
- Access Controls Concepts
  - Understand Access Control Concepts
  - Understand Physical Access Controls
  - Understand Logical Access Controls
- Network Security
  - Understand Computer Networking
  - Understand Network (Cyber) Threats and Attacks
  - Understand Network Security Infrastructure
- Security Operations
  - Understand Data Security
  - Understand System Hardening
  - Understand Best Practice Security Policies
  - Understand Security Awareness Training

## REQUIREMENTS:

There are no prerequisites for this program.

## Difficulty level

## CERTIFICATE:

The participants will obtain certificates signed by ISC2 (course completion).

In order to complete the course, receive a certificate of completion and earn ISC2 continuing professional education (CPE) credits, learners must:

- Complete all learning activities within the course.
- Complete a course evaluation.

An electronic Certificate of Completion will be provided once you have completed the course by



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

meeting all the requirements. We recommend that you download and retain the certificate of completion as proof of credits earned.

This course will help prepare you also for the CC certification exam available at Pearson VUE test centers.

*Each participant in an authorized training **CC Certification Prep Course** held in Compendium CE will receive a free CC Certification Exam voucher.*

## TRAINER:

ISC2 Authorized Instructor



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007