# CC - Certified in Cybersecurity Certification Prep

**Category:** Networking & Security | **Vendor:** ISC2

**Duration:** 2.00 hours (1 days) **1.6 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

## Course Information

| | |
|---|---|
| **Delivery Format:** | vILT |
| **Certification:** | Certified in Cybersecurity (CC) |
| **Related Exam:** | CC |

## Course Overview

Learn cybersecurity fundamentals and prepare for an entry-level role in the domain. CC - Certified in Cybersecurity course includes cybersecurity principles, risk management, security controls, governance, Code of Ethics, incident response, disaster recovery, and other vital cybersecurity topics.

## About This Course

Learn cybersecurity fundamentals and prepare for an entry-level role in the domain. CC - Certified in Cybersecurity course includes cybersecurity principles, risk management, security controls, governance, Code of Ethics, incident response, disaster recovery, and other vital cybersecurity topics.

# Learning Outcomes

**Upon successful completion of this course, participants will be able to:**

Course ObjectivesDiscuss the foundational concepts of cybersecurity principlesRecognize foundational security concepts of information assuranceDefine risk management terminology and summarize the processRelate risk management to personal or professional practicesClassify types of security controlsDistinguish between policies, procedures, standards, regulations and lawsDemonstrate the relationship among governance elementsAnalyze appropriate outcomes according to the canons of the (ISC)² Code of Ethics when given examplesPractice the terminology of and review security policiesExplain how organizations respond to, recover from and continue to operate during unplanned disruptionsRecall the terms and components of incident responseSummarize the components of a business continuity planIdentify the components of disaster recoveryPractice the terminology and review concepts of business continuity, disaster recovery and incident responseSelect access controls that are appropriate in a given scenarioRelate access control concepts and processes to given scenariosCompare various physical access controlsDescribe logical access controlsPractice the terminology and review concepts of access controlsExplain the concepts of network securityRecognize common networking terms and modelsIdentify common protocols and port and their secure counterpartsIdentify types of network (cyber) threats and attacksDiscuss common tools used to identify and prevent threatsIdentify common data center terminologyRecognize common cloud service terminologyIdentify secure network design terminologyPractice the terminology and review concepts of network securityExplain concepts of security operationsDiscuss data handling best practicesIdentify key concepts of logging and monitoringSummarize the different types of encryption and their common usesDescribe the concepts of configuration managementExplain the application of common security policiesDiscuss the importance of security awareness trainingPractice the terminology and review concepts of network operations, Course ObjectivesDiscuss the foundational concepts of cybersecurity principlesRecognize foundational security concepts of information assuranceDefine risk management terminology and summarize the processRelate risk management to personal or professional practicesClassify types of security controlsDistinguish between policies, procedures, standards, regulations and lawsDemonstrate the relationship among governance elementsAnalyze appropriate outcomes according to the canons of the (ISC)² Code of Ethics when given examplesPractice the terminology of and review security policiesExplain how organizations respond to, recover from and continue to operate during unplanned disruptionsRecall the terms and components of incident responseSummarize the components of a business continuity planIdentify the components of disaster recoveryPractice the terminology and review concepts of business continuity, disaster recovery and

incident responseSelect access controls that are appropriate in a given scenarioRelate access control concepts and processes to given scenariosCompare various physical access controlsDescribe logical access controlsPractice the terminology and review concepts of access controlsExplain the concepts of network securityRecognize common networking terms and modelsIdentify common protocols and port and their secure counterpartsIdentify types of network (cyber) threats and attacksDiscuss common tools used to identify and prevent threatsIdentify common data center terminologyRecognize common cloud service terminologyIdentify secure network design terminologyPractice the terminology and review concepts of network securityExplain concepts of security operationsDiscuss data handling best practicesIdentify key concepts of logging and monitoringSummarize the different types of encryption and their common usesDescribe the concepts of configuration managementExplain the application of common security policiesDiscuss the importance of security awareness trainingPractice the terminology and review concepts of network operations, Course ObjectivesDiscuss the foundational concepts of cybersecurity principlesRecognize foundational security concepts of information assuranceDefine risk management terminology and summarize the processRelate risk management to personal or professional practicesClassify types of security controlsDistinguish between policies, procedures, standards, regulations and lawsDemonstrate the relationship among governance elementsAnalyze appropriate outcomes according to the canons of the (ISC)² Code of Ethics when given examplesPractice the terminology of and review security policiesExplain how organizations respond to, recover from and continue to operate during unplanned disruptionsRecall the terms and components of incident responseSummarize the components of a business continuity planIdentify the components of disaster recoveryPractice the terminology and review concepts of business continuity, disaster recovery and incident responseSelect access controls that are appropriate in a given scenarioRelate access control concepts and processes to given scenariosCompare various physical access controlsDescribe logical access controlsPractice the terminology and review concepts of access controlsExplain the concepts of network securityRecognize common networking terms and modelsIdentify common protocols and port and their secure counterpartsIdentify types of network (cyber) threats and attacksDiscuss common tools used to identify and prevent threatsIdentify common data center terminologyRecognize common cloud service terminologyIdentify secure network design terminologyPractice the terminology and review concepts of network securityExplain concepts of security operationsDiscuss data handling best practicesIdentify key concepts of logging and monitoringSummarize the different types of encryption and their common usesDescribe the concepts of configuration managementExplain the application of common security policiesDiscuss the importance of security awareness trainingPractice the terminology and review concepts of network operations, Course ObjectivesDiscuss the foundational concepts of cybersecurity principlesRecognize foundational security concepts of information assuranceDefine risk management terminology and

summarize the processRelate risk management to personal or professional practicesClassify types of security controlsDistinguish between policies, procedures, standards, regulations and lawsDemonstrate the relationship among governance elementsAnalyze appropriate outcomes according to the canons of the (ISC)² Code of Ethics when given examplesPractice the terminology of and review security policiesExplain how organizations respond to, recover from and continue to operate during unplanned disruptionsRecall the terms and components of incident responseSummarize the components of a business continuity planIdentify the components of disaster recoveryPractice the terminology and review concepts of business continuity, disaster recovery and incident responseSelect access controls that are appropriate in a given scenarioRelate access control concepts and processes to given scenariosCompare various physical access controlsDescribe logical access controlsPractice the terminology and review concepts of access controlsExplain the concepts of network securityRecognize common networking terms and modelsIdentify common protocols and port and their secure counterpartsIdentify types of network (cyber) threats and attacksDiscuss common tools used to identify and prevent threatsIdentify common data center terminologyRecognize common cloud service terminologyIdentify secure network design terminologyPractice the terminology and review concepts of network securityExplain concepts of security operationsDiscuss data handling best practicesIdentify key concepts of logging and monitoringSummarize the different types of encryption and their common usesDescribe the concepts of configuration managementExplain the application of common security policiesDiscuss the importance of security awareness trainingPractice the terminology and review concepts of network operations, Course ObjectivesDiscuss the foundational concepts of cybersecurity principlesRecognize foundational security concepts of information assuranceDefine risk management terminology and summarize the processRelate risk management to personal or professional practicesClassify types of security controlsDistinguish between policies, procedures, standards, regulations and lawsDemonstrate the relationship among governance elementsAnalyze appropriate outcomes according to the canons of the (ISC)² Code of Ethics when given examplesPractice the terminology of and review security policiesExplain how organizations respond to, recover from and continue to operate during unplanned disruptionsRecall the terms and components of incident responseSummarize the components of a business continuity planIdentify the components of disaster recoveryPractice the terminology and review concepts of business continuity, disaster recovery and incident responseSelect access controls that are appropriate in a given scenarioRelate access control concepts and processes to given scenariosCompare various physical access controlsDescribe logical access controlsPractice the terminology and review concepts of access controlsExplain the concepts of network securityRecognize common networking terms and modelsIdentify common protocols and port and their secure counterpartsIdentify types of network (cyber) threats and attacksDiscuss common tools used to identify and prevent threatsIdentify common data center

terminologyRecognize common cloud service terminologyIdentify secure network design terminologyPractice the terminology and review concepts of network securityExplain concepts of security operationsDiscuss data handling best practicesIdentify key concepts of logging and monitoringSummarize the different types of encryption and their common usesDescribe the concepts of configuration managementExplain the application of common security policiesDiscuss the importance of security awareness trainingPractice the terminology and review concepts of network operations

## Detailed Course Outline

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

### □□ Certification Path

Certified in Cybersecurity (CC)

Exam: CC

# Frequently Asked Questions

### Q: What delivery options are available for CC - Certified in Cybersecurity Certification Prep?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

---

### Q: What certification does this course prepare me for?

The CC - Certified in Cybersecurity Certification Prep course helps prepare you for the Certified in Cybersecurity (CC) certification path.

---

### Q: Which exam does this course prepare me for?

This course prepares you for the CC official exam. You can take this exam at any exam center across United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online wherever you are located.

---

### Q: How many CPD hours does this course provide?

The 1-day CC - Certified in Cybersecurity Certification Prep course provides up to 1.6 CPD hours of structured learning. CPD certificates can be provided upon request.

---

### Q: What is the duration of the CC - Certified in Cybersecurity Certification Prep training?

The training takes place over 1 day(s), with each day lasting approximately 2.00 hours including breaks for lunch and refreshments.

---

### Q: Do you provide corporate training for CC - Certified in Cybersecurity Certification Prep?

Yes, we provide corporate training, dedicated training, and closed classes for CC - Certified in Cybersecurity Certification Prep. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

---

### Q: What related terms do people search for?

Popular related searches include: CC - Certified in Cybersecurity Certification Prep, ISC2, vILT

---

### Q: Why choose Nexus Human for CC - Certified in Cybersecurity Certification Prep?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

---

### Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your CC - Certified in Cybersecurity Certification Prep training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.


## Nexus Human

**Professional Training & Development**

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)