

(ISC)² CC – Certified in Cybersecurity

This (ISC)² CC – Certified in Cybersecurity training covers how to perform the basic and essential tasks of an entry-level cybersecurity analyst without supervision or guidance. This Certified in Cybersecurity training prepares you for the foundational (ISC)² certification, a valuable tool for proving your familiarity with the tech you'll use on a daily basis in your first few years in an IT security job.

[CBT Nuggets course material](#) →

WEEK 1

Understanding Information Assurance

156 min.

The CIA Triad and Nonrepudiation	16
Methods of Authentication	11
Multi-Factor Authentication (MFA)	6
Biometrics Factors	5
Data Privacy	8

Discussing Risk Management, Controls, Ethics and Governance

Overview	1
Risk Management	8
Risk Treatment	6
Security Controls	8
Security Control Categories	7
ISC2 Code of Ethics	5
Policies and Procedures	7
Standards, Regulations and Laws	5

Exploring BC, DR & IR Concepts

Overview	1
Intro	3
Business Continuity	4
Business Continuity Planning	9
Disaster Recovery	4
Disaster Recovery Planning	8
Incident Response	11
After Action and Training	6

Reviewing Access Control Concepts

Overview	1
Physical Security Controls	5
Monitoring Controls	8

WEEK 2

154 min.

Authorized Personnel vs Unauthorized Personnel	5
Principle of Least Privilege	6
Segregation of Duties	6
Types of Access Control	9
Data and Media Access Control	9

Exploring Security Policies and Training

Overview	1
Data Handling Policy	7
Password Policy	5
Acceptable Use Policy	6
Bring Your Own Device (BYOD) Policy	7
Change Management Policy	6
Privacy Policy	8
Security Awareness Training	12

Understanding Data Security and System Hardening

Overview	1
Encryption Basics	3
Types of Encryption	11
Data Hashing with Encryption	7
Digital Signatures with Hashing	5
Data Handling	9

Data Logging	6
Configuration Management	10

Discussing Network Security Infrastructure

Overview	1
Network Segmentation	11

WEEK 3

151 min.

Embedded System Security	7
Virtual Private Networks (VPNs)	5
Defense In Depth and Zero Trust	7
Network Access Control (NAC)	4
SLAs and MSPs	7
The Cloud	9

Exploring Network Threats and Attacks

Overview	1
Types of Threats - DoS, DDoS and Malware	8
Types of Threats - Man-in-the-middle and Side Channel	4
Intrusion Detection / Prevention Systems (IDS/IPS)	13
Endpoint Protection and Management	7
Vulnerability Scanning	11
Firewalls	12

Understanding Computer Networking

Overview	1
Computer Networking Basics	7
OSI Model	5

TCP/IP Model	9
IP Addresses	11
Wireless Networking	4
Networking Ports	9
Common Applications	7

WEEK 4**Exploring On-Premise Network Infrastructure 52 min.**

Overview	1
Power	15
Data Centers and Closets	7
Heating, Ventilation and Air Conditioning (HVAC)	10
Dealing with Fire	6
Redundancy	9
Working with 3rd Parties	3