INFOSECTRAIN

ISC² Certified in Cybersecurity (CC)

Online Training Courses

CC Course Highlights

- 16 Hours LIVE Instructor-Led Training
- Full 5 Domain Exam Practice
- Career Guidance and Mentorship
- Post Training Support
- Learn from Industry Experts

100% Satisfaction Guarantee

Not satisfied with your training on Day 1?
You can get a refund or enroll in a different course.

Access Recorded Sessions

Revisit your lectures, revise your concepts, and retain your knowledge
From anywhere, whenever you want

Extended Post Training

Get extended support even after you finish your training.
We're here for you until you reach your certification goals.

Introduction

The Certified in Cybersecurity (CC) training course from InfosecTrain offers a comprehensive introduction to the field of cybersecurity, aligned with (ISC)² standards. This foundational course covers five key domains: Security Principles, Business Continuity and Disaster Recovery, Access Controls, Network Security, and Security Operations. Participants will understand essential topics such as risk management, ethical guidelines, physical and logical access controls, networking, and system hardening.

Certified in Cybersecurity (CC) training program equips both new entrants and seasoned professionals with the knowledge to tackle cybersecurity challenges and prepares them for the Certified in Cybersecurity exam. Ideal for IT professionals, career changers, and students, this course is a critical step toward a successful career in cybersecurity.

Why Certified in Cybersecurity (CC) Training Course with InfosecTrain?

InfosecTrain is a leading IT security training and consulting organization offering best-in-class yet cost-effective, customized training programs to enterprises and individuals across the globe. We offer role-specific certification training programs and prepare professionals for the future. Our Certified in Cybersecurity (CC) training course will equip you with a comprehensive overview of essential topics in the field of cybersecurity.

Here's what you get when you choose InfosecTrain as your learning partner:

Flexible Schedule

Training sessions to match your schedule and accommodate your needs.

Post Training Support with No Expiry Date

Ongoing assistance and support until the learners achieve their certification goals.

Recorded Sessions

Access to LMS or recorded sessions for post-training reference.

Customized Training

A training program that caters to your specific learning needs.

Knowledge Sharing Community

Collaborative group discussions to facilitate knowledge sharing and learning.

Certificate

Each candidate receives a certificate of participation as a testament to their accomplishment.

Expert Career Guidance

Free career guidance and support from industry experts.

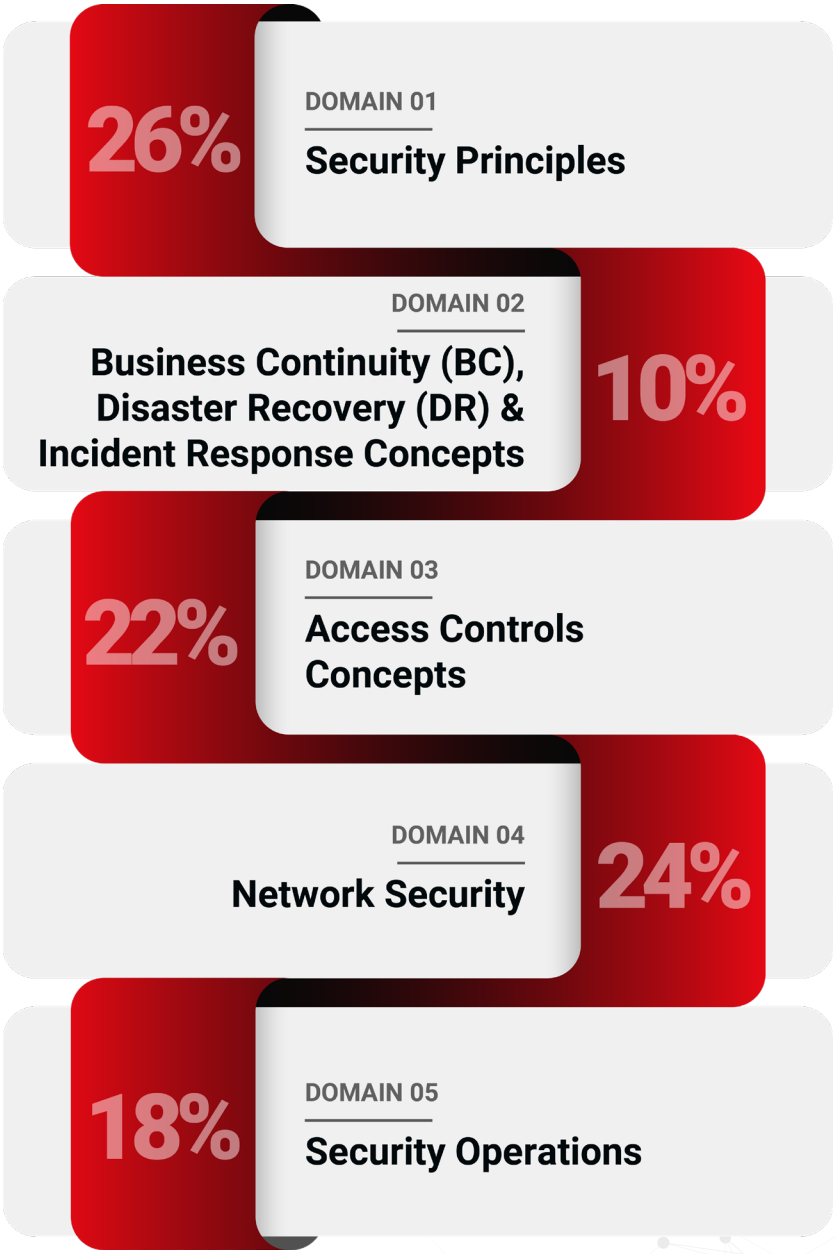
Who Should Attend

- IT Managers
- Security Managers
- System Analysts
- Individuals willing to learn Information Systems Auditing
- Professionals working in an Audit team
- Auditors

Exam Information

Duration of the Exam	2 Hours
Number of questions	100
Question format	Multiple Choice Questions
Passing Score	700 out of 1000
Exam language	English
Testing Center	Pearson VUE Testing Center

Domains Weightage Covered by Certified in Cybersecurity (CC)



CC Course Content

Domain 1 (26%)
Security Principles

1.1: Understand the security concepts of information assurance

- Confidentiality
- Integrity
- Availability
- Authentication (e.g., methods of authentication, multi-factor authentication (MFA))
- Non-repudiation
- Privacy

1.2: Understand the risk management process

- Risk management (e.g., risk priorities, risk tolerance)
- Risk identification, assessment, and treatment

1.3: Understand security controls

- Technical controls
- Administrative controls
- Physical controls

1.4: Understand (ISC)² Code of Ethics

- Professional code of conduct

1.5: Understand governance processes

- Policies
- Procedures
- Standards
- Regulations and laws

Domain 2 (10%)
Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts

2.1: Understand business continuity (BC)

- Purpose
- Importance
- Components

2.2: Understand disaster recovery (DR)

- Purpose
- Importance
- Components

2.3: Understand incident response

- Purpose
- Importance
- Components

Domain 3 (22%)
Access Controls Concepts

3.1: Understand physical access controls

- Physical security controls (e.g., badge systems, gate entry, environmental design)
- Monitoring (e.g., security guards, closed-circuit television (CCTV), alarm systems, logs)
- Authorized versus unauthorized personnel

3.2: Understand logical access controls

- Principle of least privilege
- Segregation of duties
- Discretionary access control (DAC)
- Mandatory access control (MAC)
- Role-based access control (RBAC)

Domain 4 (24%)
Network Security

4.1: Understand computer networking

- Networks (e.g., Open Systems Interconnection (OSI) model, Transmission Control Protocol/Internet Protocol (TCP/IP) model, Internet Protocol version 4 (IPv4), Internet Protocol version 6 (IPv6), WiFi)
- Ports
- Applications

4.2: Understand network threats and attacks

- Types of threats (e.g., distributed denial-of-service (DDoS), virus, worm, Trojan, man-in-the-middle (MITM), side-channel)
- Identification (e.g., intrusion detection system (IDS), host-based intrusion detection system (HIDS), network intrusion detection system (NIDS))
- Prevention (e.g., antivirus, scans, firewalls, intrusion prevention system (IPS))

4.3: Understand network security infrastructure

- On-premises (e.g., power, data center/closets, Heating, Ventilation, and Air Conditioning (HVAC), environmental, fire suppression, redundancy, memorandum of understanding (MOU)/memorandum of agreement (MOA))
- Design (e.g., network segmentation (demilitarized zone (DMZ), virtual local area network (VLAN), virtual private network (VPN), micro-segmentation), defense in depth, Network Access Control (NAC) (segmentation for embedded systems, Internet of Things (IoT))
- Cloud (e.g., service-level agreement (SLA), managed service provider (MSP), Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), hybrid)

Domain 5 (18%)
Security Operations

5.1: Understand data security

- Encryption (e.g., symmetric, asymmetric, hashing)
- Data handling (e.g., destruction, retention, classification, labeling)
- Logging and monitoring security events

5.2: Understand system hardening

- Configuration management (e.g., baselines, updates, patches)

5.3: Understand best practice security policies

- Data handling policy
- Password policy
- Acceptable Use Policy (AUP)
- Bring your own device (BYOD) policy
- Change management policy (e.g., documentation, approval, rollback)
- Privacy policy

5.4: Understand security awareness training

- Purpose/concepts (e.g., social engineering, password protection)
- Importance

INFOSECTRAIN

www.infosectrain.com | sales@infosectrain.com