COURSE OUTLINE

TRENDS Academy
Learning | Evolving | Empowering

CC – Certified in Cybersecurity

Duration: **2 Days**

Course Description:

The Certified in Cybersecurity (CC) credential was developed for newcomers to the field, to recognize the growing trend of people entering the cybersecurity workforce without direct IT experience. Getting Certified in Cybersecurity provides employers with the confidence that you have a solid grasp of the right technical concepts, and a demonstrated aptitude to learn on the job. As a recognized certification, those who hold the CC are backed by the world's largest network of certified cybersecurity professionals helping them continue their professional development and earn new achievements and qualifications throughout their career.

Prerequisites:

There are no specific prerequisites to take the exam. It is recommended that candidates have basic information technology (IT) knowledge. No work experience in cybersecurity or any formal educational diploma/degree is required. The next step in the candidate's career would drive to earning ISC2 expert-level certifications, which require experience in the field.

Course Outlines:

Domain 1. Security Principles

Understand the security concepts of information assurance
- Confidentiality
- Integrity
- Availability
- Authentication (e.g., methods of authentication, multi-factor authentication (MFA))
- Non-repudiation
- Privacy

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

Understand security controls
- Technical controls
- Administrative controls
- Physical controls

Understand ISC2 Code of Ethics
- Professional code of conduct

Understand governance processes
- Policies
- Procedures
- Standards
- Regulations and laws

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

Understand business continuity (BC)
- Purpose
- Importance
- Components

Understand disaster recovery (DR)
- Purpose
- Importance
- Components

Understand incident response
- Purpose
- Importance
- Components

Domain 3. Access Controls Concepts

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

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. Network Security

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

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))

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. Security Operations

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

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

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

Understand security awareness training
- Purpose/concepts (e.g., social engineering, password protection)
- Importance