Certified in Cybersecurity (CC)

Course Overview

As digital landscapes expand, safeguarding organizational assets requires a workforce grounded in standardized security fundamentals. The Certified in Cybersecurity (CC) credential proves to employers that you have the foundational knowledge, skills, and abilities necessary for an entry- or junior-level cybersecurity role. This course signals your clear understanding of fundamental security best practices, policies, and procedures, while validating your willingness and ability to learn more and grow on the job. Designed for entry-level practitioners, career changers, and IT professionals alike, this course deconstructs complex paradigms into clear operational frameworks. Through lectures those derive from real world case studies, and structured exam preparation, participants will master, security the essential vocabulary principles and practices required to protect assets under modern enterprise environments.

Course Objective:

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

- **Apply Information Assurance Frameworks:** Identify and enforce the core tenets of the CIA Triad (Confidentiality, Integrity, and Availability) alongside the IAAA Framework to support corporate governance and compliance requirements.
- **Evaluate and Treat Organizational Risk:** Categorize security threats, select appropriate administrative, physical, or technical controls, and apply the correct risk treatment strategy (Accept, Avoid, Mitigate, Transfer).
- **Execute Incident and Business Continuity Plans:** Differentiate between the operational goals of Incident Response (IR), Business Continuity (BC), and Disaster Recovery (DR) to maintain organizational resilience during disruptions.
- **Enforce Robust Access Management:** Implement the Principle of Least Privilege, enforce separation of duties, and deploy Discretionary (DAC), Mandatory (MAC), and Role-Based Access Control (RBAC) models.
- **Secure Modern Network Architectures:** Map network traffic patterns using the OSI and TCP/IP models, secure core protocols, and safely transition business assets across local, remote (VPN), and cloud environments (IaaS, PaaS, SaaS).
- **Mitigate Technical and Social Attacks:** Recognize indicators of compromise for common malware strains, counter network exploits like DDoS and Man-in-the-Middle attacks, and build human firewalls against advanced social engineering tactics.
- **Maintain Operational Security Baselines:** Standardize system configurations, govern data security lifecycle phases via encryption and hashing, manage patch cycles, and navigate formal Change Management protocols.
- **Take the Official ISC2 CC Exam:** Master question-deconstruction strategies, eliminate distractor options under timed conditions, and schedule the final examination with confidence through authorized Pearson VUE testing services.

Benefits:

- **Validate Job Readiness** – Prove to employers that you possess the precise skills required for cybersecurity starter roles.
- **Accelerate Career Growth** – Signal your personal motivation, technical aptitude, and long-term trainability to hiring teams.
- **Build Team Credibility** – By establishing a organizational security best practices.
- **Earn Professional Status** – Satisfy the academic requirements needed to join the globally recognized network of ISC2 professionals.

Course Outline:

Domain 1: Security Principles

Module 1.1: Information Assurance Fundamentals

- **The CIA Triad** – Core definitions of Confidentiality, Integrity, and Availability.
- **The IAAA Framework** – Practical implementation of Identification, Authentication, Authorization, and Accountability.
- **Non-Repudiation** – Using digital signatures and asymmetric cryptography to prevent denial of actions.
- **Privacy Principles** – Baseline definitions of PII (Personally Identifiable Information) and data ownership.

Module 1.2: Corporate Governance & Risk Management

- **The Risk Process** – Risk Identification, Risk Assessment, and Risk Treatment options (Accept, Avoid, Mitigate, Transfer).
- **Security Controls** – Implementing Physical, Administrative (Managerial), and Technical (Logical) countermeasures.
- **Defense-in-Depth** – Building layered security architectures using a combination of control categories.
- **Governance Frameworks** – The role of corporate policies, organizational standards, operational procedures, and baseline guidelines.
- **Ethical Conduct** – Deep dive into the four canons of the ISC2 Code of Ethics.

Domain 2: Incident Response, Business Continuity (BC) and Disaster Recovery (DR) Concepts

- **Incident Response (IR)** – The incident lifecycle: Detection, Containment, Eradication, Recovery, and Lessons Learned.
- **Business Continuity (BC)** – Preserving critical business operations during active disruptions.
- **Disaster Recovery (DR)** – Restoring supporting IT systems and infrastructures following catastrophic failures.

Domain 3 Access Control Concepts

Module 3.1: Access Control Basic

- **Least Privilege** – Restricting asset access to the absolute minimum required to perform a job function.
- **Separation of Duties** – Dividing high-risk tasks among multiple personnel to prevent fraud or collusion.
- **Access Models** – Structural differences between Discretionary (DAC), Mandatory (MAC), and Role-Based Access Control (RBAC).

Module 3.2: Authentication & Physical Security

- **Authentication Factors** – Multi-Factor Authentication (MFA) variables: Something you know, have, are, or do.
- **Physical Protections** – Deploying perimeter barriers, fences, locks, badge readers, environmental controls, and CCTV.

Domain 4: Network Security

Module 4.1: Computer Networking Fundamentals
- **The OSI Reference Model** – Analyzing the 7 conceptual layers from Physical to Application.
- **The TCP/IP Suite** – Mapping the 4-layer internet protocol architecture against real-world operations.
- **Core Network Protocols** – Understanding TCP vs. UDP, IPv4 vs. IPv6 address formatting, DNS, and DHCP.
- **Ports and Services** – Recognizing common transport vectors (HTTP/80, HTTPS/443, SSH/22, RDP/3389).

Module 4.2: Infrastructure & Cloud Architecture
- **Network Segmentation** – Isolating workloads via Virtual Local Area Networks (VLANs) and Demilitarized Zones (DMZs).
- **Secure Transit Vectors** – Deploying Virtual Private Networks (VPNs) for remote workers and branch sites.
- **Cloud Service Models** – Security boundaries in Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

Module 4.3: Network Threats & Defenses
- **Malicious Vectors** – Identifying indicators of compromise for Viruses, Worms, Trojans, and Ransomware.
- **Network Attacks** – Mitigating Denial of Service (DoS/DDoS), Man-in-the-Middle (MITM), and On-Path eavesdropping.
- **Active Defense Tools** – Deploying Firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS).

Domain 5: Security Operations

Module 5.1: Data Security & System Hardening
- **Cryptography Basics** – Differentiating Symmetric (secret key) from Asymmetric (public-private key pairs) algorithms.
- **Hashing Functions** – Utilizing MD5, SHA-256, and SHA-3 to verify data integrity without encryption.
- **Configuration Baselines** – Hardening operating systems by disabling unused ports, protocols, and default accounts.
- **Patch Management** – Structuring software updates and vulnerability remediation workflows.

Module 5.2: Operational Policies & Awareness Training
- **Organizational Policies** – Writing and enforcing Acceptable Use Policies (AUP) and Bring Your Own Device (BYOD) mandates.
- **Change Management** – Utilizing formal request, approval, testing, and rollback documentation to prevent outages.
- **Social Engineering** – Educating workforces against Phishing, Vishing, Spear Phishing, and Tailgating threats.

Module 5.3: Review & Test Strategies
- **Exam Logistics** – Booking, scheduling, and identifying authorized centers using Pearson VUE Testing Services.
- **Question Analysis** – Breaking down trick scenarios and word stems under timed conditions.
- **Comprehensive Practice Assessment** – 100-questions mock exam practice run.

Who should attend?

This course is strategically designed for individuals seeking to enter the information security workforce, as well as organizations aiming to build a security-aware culture. Ideal candidates include:

- **Career Changers & Non-Technical Professionals** – Individuals transitioning from fields like retail, hospitality, finance, legal, or military service into tech.
- **Information Technology Support Staff** – Help Desk technicians, desktop support specialists, and field engineers seeking upward mobility into specialized security roles working under Security Operations Center (SOC).
- **Junior System & Network Administrators** – Infrastructure professionals aiming to formalize their understanding of baseline system hardening and modern network segment security.
- **Recent Graduates & Students** – University or college students looking for a globally recognized, industry-vetted credential to pair with their academic degrees.
- **Risk, Audit, and Compliance Officers** – Business professionals who collaborate closely with security teams and need a foundational grasp of standard security controls and corporate governance models.
- **Enterprise Teams & New Hires** – Corporate cohorts requiring a standardized, baseline technical security orientation to satisfy onboarding or compliance mandates.

Course Length: 3 days

- 2 days lecture (5 domains)
- 1 day mock exam practice run