Certaining Cybersecurity Fundamentals

Exam Code- CCYF™

Table of Contents

Introduction

The CCYF certificate ensures that the candidates achieve a good understanding of the essential parts of cybersecurity without requiring them to be hardcore coders or have advanced technical skills. This credential adds up the first principles of safety in software, be it a threat landscape or risk trend, whether by following compliance frameworks or secure cloud practices.

Certaining's Cybersecurity Fundamentals certification is compatible with international standards, for instance, ISO/IEC 27001, NIST Cybersecurity Framework (CSF), and CIS Critical Security Controls. As a result, it offers an initial point to comprehend how vital cybersecurity is in IT operations and enterprise digital systems.

This certificate helps candidates connect IT knowledge and the skillset of the cybersecurity domain. It enables professionals to become part of the secure working infrastructure. Perhaps it equips them with the necessary skills for further certifications in the Certaining Cybersecurity series.

Core Competencies

- Study the basics of cybersecurity, the major concepts, principles, and terminology used.
- Know the features, breaches, vulnerabilities, and security threats of IT.
- Take part in compliance, risk, and management activities.
- Security and identity management (IAM).
- First-hand knowledge of secure protocols, VPNs, firewalls, and network security.
- Know the architectures of cloud security and the shared responsibility model.
- Security operations and incident handling at the beginner's level.

Suitable Professionals for the CCYF Certification

- **IT Support** and **System Administrators** who have decided to start their journey into cybersecurity.
- **Network Engineers** and **Cloud professionals** seeking foundational knowledge in security.
- **Project Managers** and **IT executives** who are inclined toward knowing the essentials of cybersecurity.
- **Students** and those who are on a different career path, but are now thinking about getting into cybersecurity.

Exam Information

Field	Details
Exam Code	CCYF
Delivery Mode	Online Proctored / Authorized Test Center
Exam Format	MCQ and MR
No. of Questions	65
Duration	90 minutes
Passing Score	70%
Language	English
Validity	Lifetime

EXAMINATION DOMAINS & WEIGHTAGE

S.No.	Domain Name	Weightage
1	Security Concepts & Principles	20%
2	Threats, Attacks & Vulnerabilities	20%
3	Network Security & Infrastructure	20%
4	Identity, Access & Cryptography	20%
5	Security Operations & Risk Management	20%

1. SECURITY CONCEPTS & PRINCIPLES

This domain establishes the foundational understanding of key cybersecurity principles and governance frameworks. Candidates learn the importance of the **CIA Triad**—Confidentiality, Integrity, and Availability—and how it guides all security objectives. The course covers essential principles such as **least privilege**, **defense in depth**, **separation of duties**, and the **AAA framework** (Authentication, Authorization, Accounting). Learners also explore major **security frameworks** like NIST CSF and ISO 27001/27002, along with governance fundamentals that ensure consistent policy enforcement. Additional topics include **physical security controls**, **non-repudiation**, **accountability**, and the hierarchy of **policies, standards, and procedures**. Emphasis is placed on **security awareness training**, risk terminology, and the structured documentation that underpins an organization's cybersecurity posture.

- **1.1. CIA Triad and security objectives**
- **1.2. Security principles (least privilege, defense in depth, separation of duties, need-to-know)**
- **1.3. AAA framework**
- **1.4. Security frameworks (NIST, ISO)**
- **1.5. Security governance basics**
- **1.6. Physical security (badges, locks, surveillance, environmental controls)**
- **1.7. Security awareness training**
- **1.8. Security terminology (threat, vulnerability, risk, exploit, asset)**
- **1.9. Security documentation (policies, standards, procedures, guidelines)**

2. THREATS, ATTACKS & VULNERABILITIES

This domain equips candidates with the knowledge to identify, classify, and respond to a wide range of cybersecurity threats. Learners explore different **malware types**—including viruses, ransomware, trojans, and botnets—alongside **social engineering attacks** such as phishing, pretexting, and tailgating. The course covers **network-based attacks** like DDoS, DNS poisoning, and session hijacking, as well as **application-level exploits** including SQL injection and Cross-Site Scripting (XSS). Wireless and physical security threats are examined to provide holistic awareness. Candidates also study **vulnerability assessment**, **patch management**, and the role of **threat intelligence** in proactive defense. Understanding various **threat actors** and their motivations helps learners anticipate risks and strengthen organizational resilience against evolving cyber threats.

2.1. **Malware:** Virus, worm, trojan, ransomware, spyware, adware, rootkit, botnet
2.2. **Social Engineering:** Phishing, spear phishing, whaling, vishing, smishing, pretexting, baiting, tailgating, shoulder surfing, dumpster diving
2.3. **Network Attacks:** DDoS, DoS, Man-in-the-Middle (MitM), session hijacking, DNS poisoning, ARP poisoning, IP spoofing
2.4. **Application Attacks:** SQL injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), buffer overflow (basic concept)
2.5. **Wireless Attacks:** Evil twin, rogue access point, WEP/WPA attacks, deauthentication attacks
2.6. **Vulnerabilities:** Zero-day, unpatched systems, misconfigurations, weak credentials
2.7. **Threat Actors:** Nation-states, hacktivists, cybercriminals, script kiddies, insiders, competitors
2.8. **Patch Management:** Vulnerability scanning, patch testing, deployment, verification

3. NETWORK SECURITY & INFRASTRUCTURE

This domain focuses on the essential principles and technologies that secure modern network environments. Candidates begin by understanding **network fundamentals**, including the OSI and TCP/IP models, and the security implications of common **network protocols**. The course explores **network security devices**—routers, switches, firewalls, proxies, and load balancers—along with **IDS/IPS systems**, **VPN technologies**, and **secure network design** concepts such as segmentation, DMZs, and isolation. Learners gain insight into **wireless security protocols** like WPA3 and 802.1X, as well as **network monitoring** and **logging** through SIEM tools and NetFlow. Emphasis is placed on designing resilient, defense-in-depth architectures that ensure confidentiality, integrity, and availability across both on-premise and cloud-based infrastructures.

3.1. **Network Fundamentals:** OSI model (7 layers), TCP/IP model, IP addressing, subnetting basics
3.2. **Protocols:** HTTP/HTTPS, FTP/SFTP, SSH, Telnet, DNS, DHCP, SMTP, SNMP
3.3. **Network Devices:** Routers, switches, hubs, bridges, firewalls, proxies, load balancers
3.4. **Firewalls:** Packet filtering, stateful inspection, application-level, next-gen firewalls (NGFW)
3.5. **IDS/IPS:** Intrusion detection vs prevention, signature-based vs anomaly-based
3.6. **VPN:** IPSec, SSL/TLS VPN, site-to-site vs remote access
3.7. **Network Segmentation:** VLANs, DMZ, subnetting for security
3.8. **Wireless Security:** WEP, WPA, WPA2, WPA3, 802.1X, SSID hiding, MAC filtering
3.9. **Network Monitoring:** SIEM basics, log aggregation, NetFlow
3.10. **Secure Design:** Defense in depth, redundancy, fail-safe defaults

4. IDENTITY, ACCESS & CRYPTOGRAPHY

This domain focuses on securing digital identities and protecting information through robust authentication, authorization, and encryption mechanisms. Candidates explore **authentication methods**, **Multi-Factor Authentication (MFA)**, and **Single Sign-On (SSO)** to ensure secure user verification and access management. The course covers **access control models**—MAC, DAC, RBAC, and ABAC—along with **Privileged Access Management (PAM)** and **identity lifecycle management**. Learners also study **authentication protocols** such as Kerberos, LDAP, and RADIUS. In the cryptography section, the focus shifts to **encryption, hashing, and digital signatures**, emphasizing both **symmetric** (AES, DES) and **asymmetric** (RSA, ECC) techniques. Topics include **PKI fundamentals**, **digital certificates**, **key management**, and cryptographic protocols like **TLS** and **IPSec** that secure data in transit and storage.

4.1. **Authentication Methods:** Passwords, biometrics (fingerprint, facial, iris), tokens, smart cards, certificates
4.2. **MFA/2FA:** Something you know, something you have, something you are
4.3. **SSO & Federation:** SAML, OAuth, OpenID Connect
4.4. **Access Control Models:** MAC (Mandatory), DAC (Discretionary), RBAC (Role-Based), ABAC (Attribute-Based)
4.5. **PAM:** Privileged account management, just-in-time access
4.6. **Authentication Protocols:** Kerberos, LDAP, RADIUS, TACACS+
4.7. **Cryptography:** Encryption (making data unreadable), hashing (one-way function), digital signatures (verification)
4.8. **Symmetric Encryption:** AES, DES, 3DES (same key for encrypt/decrypt)
4.9. **Asymmetric Encryption:** RSA, ECC (public/private key pairs)
4.10. **Hashing:** MD5, SHA-1, SHA-256, SHA-3
4.11. **PKI:** Public Key Infrastructure, Certificate Authority (CA), digital certificates, certificate lifecycle
4.12. **Cryptographic Protocols:** TLS/SSL, IPSec, PGP

5. SECURITY OPERATIONS & RISK MANAGEMENT

This domain emphasizes the processes, teams, and frameworks essential for maintaining operational security and managing risk effectively. Candidates learn **Security Operations Center (SOC)** fundamentals, including monitoring, logging, and incident detection using **SIEM platforms**. The course covers the **incident response lifecycle**—from preparation to recovery—and introduces **digital forensics** concepts such as evidence handling and chain of custody. Learners also study **business continuity** and **disaster recovery** planning to ensure organizational resilience. The risk management section focuses on identifying, analyzing, and treating risks through mitigation, transfer, or avoidance. Additional topics include **data classification**, **security audits**, **policy enforcement**, and compliance with major frameworks like **GDPR**, **HIPAA**, and **PCI DSS**, ensuring alignment with regulatory and operational best practices.

5.1. **SOC:** Security Operations Center roles, functions, tiers (Tier 1/2/3 analysts)
5.2. **Security Monitoring:** Log collection, correlation, alerting
5.3. **SIEM:** Security Information and Event Management - centralized logging and analysis
5.4. **Incident Response:** Preparation → Detection → Containment → Eradication → Recovery → Lessons Learned
5.5. **Forensics:** Chain of custody, evidence handling, preservation, analysis basics
5.6. **BC/DR:** Business Continuity Plan, Disaster Recovery Plan, RTO/RPO concepts
5.7. **Risk Management:** Risk = Threat × Vulnerability × Impact
5.8. **Risk Assessment:** Identifying assets, threats, vulnerabilities, calculating risk
5.9. **Risk Treatment:** Mitigation, acceptance, transfer (insurance), avoidance
5.10. **Compliance Frameworks:** GDPR (EU privacy), HIPAA (healthcare), PCI DSS (payment cards), SOX (financial)
5.11. **Security Policies:** Acceptable Use Policy (AUP), Password Policy, Data Handling Policy
5.12. **Data Classification:** Public, Internal, Confidential, Restricted
5.13. **Security Audits:** Compliance audits, vulnerability assessments, penetration testing (awareness)