

# Career & Technical Education | Information Technology

## Cybersecurity Testing & Response

**Subject Code: 146015**

### Outcome & Competency Descriptions

#### Course Description:

Students will apply the skills of systematic testing and planned response to mitigate security concerns in information technology systems. They will describe the need for security, identify and explain security risks, and implement security safeguards. Students will manage threats, deploy countermeasures, and establish strategies to protect business information using risk and incident management.

#### Strand 1. Business Operations/21st Century Skills

Learners apply principles of economics, business management, marketing, and employability in an entrepreneur, manager, and employee role to the leadership, planning, developing, and analyzing of business enterprises related to the career field.

#### Outcome: 1.2. Leadership and Communications

Process, maintain, evaluate, and disseminate information in a business.  
Develop leadership and team building to promote collaboration.

##### Competencies

- 1.2.1. Extract relevant, valid information from materials and cite sources of information.
- 1.2.4. Use negotiation and conflict-resolution skills to reach solutions.
- 1.2.7. Use problem-solving and consensus-building techniques to draw conclusions and determine next steps.

#### Outcome: 1.3. Business Ethics and Law

Analyze how professional, ethical, and legal behavior contributes to continuous improvement in organizational performance and regulatory compliance.

##### Competencies

- 1.3.1. Analyze how regulatory compliance affects business operations and organizational performance.
- 1.3.2. Follow protocols and practices necessary to maintain a clean, safe, and healthy work environment.
- 1.3.4. Identify how federal and state consumer protection laws affect products and services.
- 1.3.5. Access and implement safety compliance measures (e.g., quality assurance information, safety data sheets [SDSs], product safety data sheets [PSDSs], United States Environmental Protection Agency [EPA], United States Occupational Safety

and Health Administration [OSHA]) that contribute to the continuous improvement of the organization.

- 1.3.8. Verify compliance with computer and intellectual property laws and regulations.

**Outcome: 1.4. Knowledge Management and Information Technology**

Demonstrate current and emerging strategies and technologies used to collect, analyze, record, and share information in business operations.

**Competencies**

- 1.4.3. Verify compliance with security rules, regulations and codes (e.g., property, privacy, access, accuracy issues, client and patient record confidentiality) pertaining to technology specific to the industry pathway.

**Outcome: 1.5. Global Environment**

Evaluate how beliefs, values, attitudes and behaviors influence organizational strategies and goals.

**Competencies**

- 1.5.1. Describe how cultural understanding, cultural intelligence skills and continual awareness are interdependent.
- 1.5.2. Describe how cultural intelligence skills influence the overall success and survival of an organization.
- 1.5.3. Use cultural intelligence to interact with individuals from diverse cultural settings.
- 1.5.4. Recognize barriers in cross-cultural relationships and implement behavioral adjustments.
- 1.5.5. Recognize the ways in which bias and discrimination may influence productivity and profitability.

**Outcome: 1.6. Business Literacy**

Develop foundational skills and knowledge in entrepreneurship, financial literacy and business operations.

**Competencies**

- 1.6.1. Identify business opportunities.
- 1.6.2. Assess the reality of becoming an entrepreneur, including advantages and disadvantages (e.g., risk versus reward, reasons for success and failure).
- 1.6.3. Explain the importance of planning your business.
- 1.6.4. Identify types of businesses, ownership and entities (i.e., individual proprietorships, partnerships, corporations, cooperatives, public, private, profit, not-for-profit).
- 1.6.5. Describe organizational structure, chain of command, the roles and responsibilities of the organizational departments and interdepartmental interactions.
- 1.6.6. Identify the target market served by the organization, the niche that the organization fills and an outlook of the industry.

- 1.6.8. Identify the features and benefits that make an organization's product or service competitive.
- 1.6.11. Describe how all business activities of an organization work within the parameters of a budget.
- 1.6.12. Describe classifications of employee benefits, rights, deductions and compensations.

**Outcome: 1.8.      Operations Management**

Plan, organize and monitor an organization or department to maximize contribution to organizational goals and objectives.

**Competencies**

- 1.8.1. Forecast future resources and budgetary needs using financial documents (e.g., balance sheet demand forecasting, financial ratios).
- 1.8.4. Identify alternative actions to take when goals are not met (e.g., changing goals, changing strategies, efficiencies).

**Outcome: 1.12.      Cyber Hygiene**

Apply digital information security principles to keep information secure.

**Competencies**

- 1.12.3. Interpret security policies through job specific training and training updates.
- 1.12.4. Apply secure password behavior.
- 1.12.5. Apply physical and virtual situational awareness (e.g., clean desk policies, shoulder surfing, social engineering, tailgating).

## **Strand 2. IT Fundamentals**

Learners apply fundamental principles of IT, including the history of IT and its impact on society, common industry terms, systems theory, information storage and retrieval, database management, and computer hardware, software, and peripheral device configuration and installation. This base of knowledge and skills may be applied across the career field.

### **Outcome: 2.1. Security, Risks, and Safeguards**

Describe the need for security and explain security risks and security safeguards.

#### **Competencies**

- 2.1.1. Explain the need for confidentiality, integrity, and availability (CIA) of information.
- 2.1.2. Describe authentication, authorization, and auditing.
- 2.1.3. Describe multilevel security.
- 2.1.4. Identify security risks and describe associated safeguards and methodologies (e.g., auditing).
- 2.1.5. Describe major threats to computer systems (e.g., internal threats, viruses, malware, ransomware, spoofing, hacking, social engineering, phishing, Denial of Service, web application attacks, network-based attacks).
- 2.1.10. Describe computer forensics, its importance in information security and cybersecurity, and its relevance to law enforcement.
- 2.1.11. Identify the need for information security and implement best practices for maintaining cyber hygiene (e.g. personal identifiable information, private financial documents, corporate records).
- 2.1.12. Describe privacy security compliance on systems (e.g., Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry [PCI], Sarbanes Oxley Act [SOX], Americans with Disabilities Act [ADA], General Data Protection Regulation [GDPR], European Union Data Protection Regulation [EUDPR]).

### **Outcome 2.4. Emerging Technologies**

Identify trending technologies, their fundamental architecture, and their value in the marketplace.

### **Competencies**

- 2.4.1. Identify emerging technologies that are applicable to the marketplace.
- 2.4.2. Describe the fundamental architectures of emerging technologies and how they are integrating into the existing systems of information technology.
- 2.4.3. Research the value of emerging technologies on the marketplace.
- 2.4.4. Describe emerging technologies (e.g., Bring your Own Device [BYOD], Services Virtualization, Mixed Reality [MR], SMART Devices, Additive Manufacturing [3D Printing], Internet of Things, Large Language Models, Machine Learning, and Artificial Intelligence).

## **Strand 3. Information Security**

Learners apply principles of information security to implement and maintain security compliance and network security. Learners select components and mechanisms required for a multilayer defense structure and evaluate and minimize security risks to wired and wireless networks and devices.

### **Outcome: 3.1. Components of Information Security**

Describe the components associated with information security systems.

### **Competencies**

- 3.1.1. Differentiate between authentication and authorization.
- 3.1.2. Compare and contrast authentication techniques (e.g., single factor, multifactor, passwords, biometrics, certificates, Radio Frequency Identification [RFID] cards).
- 3.1.4. Describe Virtual Private Networks (VPNs) using tunneling protocols (e.g., Layer 2 Tunneling Protocol [L2TP], Secure Socket Tunneling Protocol [SSTP], Point-to-Point Tunneling Protocol [PPTP]) and encrypting techniques).

### **Outcome: 3.2. General Security Compliance**

Implement and maintain general security compliance.

### **Competencies**

- 3.2.1. Identify and implement data and application security.
- 3.2.8. Identify the need for disaster recovery policies and procedures (e.g., business continuity plans, scenario testing).

### **Outcome: 3.4. Multilayer Defense Structure**

Explain information technology mechanisms as they apply to a multilayer defense structure.

## Competencies

- 3.4.3. Compare and contrast network analysis software (e.g., network analyzer) and hardware tools to identify security risks and vulnerabilities.
- 3.4.4. Identify the components of human security (e.g., social engineering) and techniques to mitigate human security threats (e.g., policies, procedures, training).

## Outcome: 3.5. Wireless Security

Implement secure wireless networks.

## Competencies

- 3.5.1. Describe wireless security risks (e.g., unauthorized access) and how to mitigate them.
- 3.5.2. Compare methods of increasing the security of wireless networks and devices (e.g., Media Access Control [MAC] address filtering, Wi-Fi Protected Access [WPA], 802.1x, Remote Authentication Dial In User Service [RADIUS]).
- 3.5.3. Research security standards provided by Institute of Electrical and Electronics Engineers (IEEE).
- 3.5.4. Describe practices and policies for preventing and detecting installation of rogue networks.
- 3.5.5. Describe security practices and policies for personal devices.
- 3.5.6. Implement and test the security of a wireless network.

## **Strand 4. Infrastructure Systems**

Learners apply principles of networking and infrastructure related to the installation, administration, and maintenance of computer networks and components. Knowledge and skills may be applied to network connectivity, cabling, protocols, architecture, classification, topologies, operating systems, Open Systems Interconnection (OSI) standards, data encoding, Quality of Service (QoS), Internet Protocol (IP) addressing, and wide area network (WAN) design.

### **Outcome: 4.1. Network Infrastructure** Build a multinode network.

#### **Competencies**

- 4.1.1. Determine the basic point-to-point (PTP) and point-to-multipoint (PTMP) network topologies (e.g., star, ring, tree, mesh, hybrid) and identify broadband and baseband (e.g., Ethernet) transmission methods and standards.
- 4.1.4. Identify standard and emerging network technologies (e.g., broadband, satellite, optic, cellular, Local-Area Network (LAN) and WiFi).
- 4.1.6. Configure and build a network.

### **Outcome: 4.3. Network Media** Select, assemble, terminate, and test media.

#### **Competencies**

- 4.3.1. Identify the criteria used in selecting media (e.g., physical properties, transmission technologies, transmission span, bandwidth, topology, security, noise immunity, installation considerations, cost).
- 4.3.2. Differentiate between media types (e.g., coaxial, twisted pair, fiber optic) and interfaces.
- 4.3.3. Compare media categories (e.g., fiber (single mode vs. multimode), CAT5, CAT5E, CAT6+).
- 4.3.4. Describe types of media connectors (e.g., Bayonet Neill-Concelman [BNC], RJ-11, RJ-45, LC, ST, SC, Duplex Multimode LC) and grounding and bonding techniques.
- 4.3.6. Identify the advantages and disadvantages of cabling systems.

### **Outcome: 4.4. Wireless Communications** Explain wireless communications.

#### **Competencies**

- 4.4.1. Compare wireless standards in common use (e.g., Institute of Electrical and Electronics Engineers [IEEE] 802.11, Cellular, Bluetooth, Worldwide Interoperability for Microwave Access [WiMAX], Radio Frequency Identification [RFID], Near Field Communication [NFC]).

## **Outcome: 4.5.      Wireless Network Solutions**

Design and implement wireless network solutions.

### **Competencies**

- 4.5.3.    Describe the Service Set Identifier (SSID) as used in wireless communications.
- 4.5.4.    Select and install access points, wireless Network Interface Cards (NICs), antennas, and other hardware and software components to provide a wireless networking solution as determined by a site and customer survey.
- 4.5.6.    Secure the wireless network.



## **Strand 9. Cybersecurity**

Learners apply principles of Cybersecurity to secure and defend information technology systems, selection and implementation of methods and tools to secure physical and digital assets, manage threats, deploy countermeasures, and establish strategies to protect business information using risk and incident management.

### **Outcome: 9.1. Cybersecurity**

Examine and employ principles of Cybersecurity.

#### **Competencies**

- 9.1.1. Identify the goals, objectives and purposes of cybersecurity.
- 9.1.2. Describe the threats, vulnerabilities, threat actors and their capabilities to mitigate risk in cyber security.
- 9.1.5. Identify types of controls (e.g., Deterrent, Preventive, Detective, Compensating, Technical, and Administrative).

### **Outcome: 9.3. Application Development Security**

Develop and maintain application security.

#### **Competencies**

- 9.3.1. Identify application vulnerabilities (e.g., Cross-site scripting, SQL injection, LDAP injection, XML injection, Directory traversal/command injection, Buffer overflow, Integer overflow, Zero-day, Cookies and attachments, Locally Shared Objects (LSOs), Flash cookies, Malicious add-ons, Session hijacking, Header manipulation, Arbitrary code execution/remote code execution).
- 9.3.5. Discover and mitigate common database vulnerabilities and attacks.
- 9.3.6. Differentiate between Server-side vs. client-side validation.

#### **Outcome: 9.4. Set up a secure network**

Set up and maintain network security.

##### **Competencies**

- 9.4.1. Setup and maintain secure roles and system management techniques (e.g., password, group, and user privilege policies and monitoring).
- 9.4.2. Secure use of network Protocols (e.g., IPSec, SNMP, SSH, DNS, TLS, SSL, TCP/IP, FTPS, HTTPS, SCP, ICMP).
- 9.4.3. Apply principles of IPv4 and IPv6 securely.
- 9.4.4. Apply wireless security configurations (e.g., Disable SSID broadcast, TKIP, CCMP, Antenna placement, Power level controls).
- 9.4.5. Manage PKI and certificates (Transport encryption, Non-repudiation, Hashing, Key escrow, Steganography, Digital signatures).
- 9.4.6. Use algorithms/protocols with transport encryption (e.g., SSL, TLS, IPSec, SSH, HTTPS).
- 9.4.7. Install and configure network devices (firewalls, switches, load balancers, proxies, web security gateways, VPN concentrators).
- 9.4.8. Install and configure network security devices. (Protocol analyzers, UTM security appliances, URL filter, Content inspection, Malware inspection, Web Application Firewall (WAF)).
- 9.4.9. Implement port security.
- 9.4.10. Define Unified Threat Management and how to monitor a network.
- 9.4.11. Mitigate network threats (e.g., Flood guards, Loop protection, Implicit deny, Network separation, Log analysis, peripheral and removable media, DOS and DDOS).
- 9.4.12. Apply the principles of secure Network Design (e.g., DMZ, Subnetting, NAT/PAT, Remote access, Telephony, Virtualization, proxy servers, segmentation).

#### **Outcome: 9.5. Threat Management**

Mitigate common threats.

##### **Competencies**

- 9.5.1. Describe, locate, and mitigate security threats (e.g., Adware, Viruses, Spyware, Trojan, Rootkits, Botnets, Ransomware).
- 9.5.2. Describe and discover vulnerabilities to and mitigate network attacks. (e.g., Man-in-the-middle, DDoS, DoS, Replay, Smurf attack, Spoofing, and other attacks).
- 9.5.3. Configure defenses for Password attacks (e.g., Brute Force, Dictionary attacks, Hybrid, Birthday attacks, Rainbow tables).
- 9.5.4. Describe, appraise for, and mitigate Social Engineering attacks (e.g., Shoulder surfing, Dumpster diving, Tailgating, Impersonation, Hoaxes, Phishing, Spear Phishing, Whaling, Vishing, Principles, URL hijacking, Watering Hole, Spam, Spim, and Spit).
- 9.5.5. Perform penetration testing.

**Outcome: 9.7. Digital Forensics**

Capture and analyze information using digital tools.

**Competencies**

- 9.7.1. Recognize digital reconnaissance techniques (e.g., packet capture, OS fingerprinting, topology discovery, DNS harvesting).
- 9.7.2. Use tools and procedures for digital reconnaissance (e.g., host scanning, network mapping, NMAP, packet analyzer, vulnerability scanner).
- 9.7.3. Analyze reconnaissance results (data correlation, data analytics, point-in-time, data logs, packet captures).
- 9.7.4. Collect digital evidence according to established policies and protocols (e.g., system image, packet captures).
- 9.7.5. Maintain chain of custody on evidence.
- 9.7.6. Generate file hash.

**Outcome: 9.8. Countermeasures**

Use countermeasures to monitor systems and reduce risk.

**Competencies**

- 9.8.2. Differentiate between detection controls and prevention controls (e.g., IDS vs. IPS, Camera vs. guard).
- 9.8.3. Use discovery tools and utilities to identify threats (e.g., Protocol analyzer, Vulnerability scanner, Honeypots, Honeynets, Port scanner).
- 9.8.9. Interpret alarms and alert trends.
- 9.8.10. Apply Incident response procedures (e.g., Preparation, Incident identification, Escalation and notification, Mitigation steps, Lessons learned, Reporting, Recovery procedures, First responder, Incident isolation, Quarantine, Device removal, Data breach).

- 9.8.11. Differentiate between types of Penetration testing (e.g., Black box, White box, Gray box).

**Outcome: 9.10. Risk Management**

Apply concepts of risk management.

**Competencies**

- 9.10.1. Enforce concepts related to threat vectors and probability/threat likelihood).
- 9.10.2. Identify concepts of risk calculation (Likelihood, Fair Risk Model, Impact, SLE, ARO, MTTR, MTTF, MTBF).