Cybersecurity Operations, Advanced

6306/36 weeks

Table of Contents

Acknowledgments........................................................................................................................... 1
Course Description.......................................................................................................................... 2
Task Essentials Table..................................................................................................................... 2
Curriculum Frameworks .............................................................................................................. 5
Exploring Attacks, Threats, and Vulnerabilities............................................................................. 5
Exploring Architecture and Design .............................................................................................. 11
Implementing Security Operations ............................................................................................... 17
Exploring Operations and Incident Response................................................................................ 27
Understanding Governance, Risk, Ethics, and Compliance ......................................................... 32
Performing Legal and Ethical Functions ...................................................................................... 36
Preparing for Industry Certification............................................................................................. 38
Developing Employability Skills................................................................................................. 40
SOL Correlations to Task ............................................................................................................ 42
Instructional Scenarios................................................................................................................ 45
Entrepreneurship Infusion Units ................................................................................................. 45
Curriculum Resources................................................................................................................ 45
Appendix: Credentials, Course Sequences, and Career Cluster Information............................... 46

Acknowledgments

The components of this instructional framework were developed by the following curriculum development panelists:

- Julie Back, STEM Education Specialist, Department of Educational Foundations and Leadership, Old Dominion University, Norfolk
- Dr. Darrell Carpenter, Director, Century for Cyber Security Longwood University, Farmville
- Jeff Dingeldein, Network Administrator and Instructional Technology Resource Specialist, Cumberland County Public Schools
- Dr. Charles Gardner, Director of Curriculum, CYBER.ORG, Bossier City, Louisiana
- Jennifer Marden, Instructor, Loudoun County High School, Loudoun County Public Schools
- Karl Meister, Instructor, Norview High School, Norfolk Public Schools
- Dr. David Raymond, Director, Virginia Cyber Range, Virginia Tech, Blacksburg
- Kristi Rice, Instructor, Spotsylvania High School, Spotsylvania County Public Schools
- Katrina Riggleman, Instructor, Riverbend High School, Spotsylvania County Public Schools
- Beverly Ross, Internal Audit Manager, Telos Corporation, Ashburn

Correlations to the Virginia Standards of Learning were reviewed and updated by the following:
Leslie R. Bowers, English Teacher (ret.), Newport News Public Schools
Vickie L. Inge, Mathematics Committee Member, Virginia Mathematics and Science Coalition
Anne F. Markwith, New Teacher Mentor (Science), Gloucester County Public Schools
Michael L. Nagy, Social Studies Department Chair, Rustburg High School, Campbell County Public Schools

The framework was edited and produced by the CTE Resource Center:

Leanne Forbes Tipton, Writer/Editor
Kevin P. Reilly, Administrative Coordinator

Virginia Department of Education Staff
Judith Sams, Specialist, Business and Information Technology and Related Clusters
Dr. J. Anthony Williams, Curriculum and Instruction Coordinator
Dr. David S. Eshelman, Director, Workforce Development and Initiatives
George R. Willcox, Director, Operations and Accountability
Office of Career, Technical, and Adult Education
Virginia Department of Education

Copyright © 2021

Course Description

Suggested Grade Level: 11 & 12

In Cybersecurity Operations, Advanced, students explore security analysis and network security, monitoring and detecting security incidents in information systems and networks. The course introduces tools and tactics to manage cybersecurity risks, identify common threats, evaluate an organization's security, collect and analyze cybersecurity intelligence, and handle cybersecurity incidents. Students will understand threats, attacks and vulnerabilities, architecture and design considerations in a business environment, implementation of security operations, risk and incident response, ethics, and cryptography. Instruction will emphasize preparation for industry certification.

Recommended prerequisite: 6304 Cybersecurity Operations

Task Essentials Table

- Tasks/competencies designated by plus icons (++) in the left-hand column(s) are essential
- Tasks/competencies designated by empty-circle icons (○) are optional
- Tasks/competencies designated by minus icons (−) are omitted
- Tasks marked with an asterisk (*) are sensitive.

<table>
<thead>
<tr>
<th>Task Number</th>
<th>6306</th>
<th>Tasks/Competencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exploring Attacks, Threats, and Vulnerabilities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>++</td>
<td>Compare information security roles.</td>
</tr>
<tr>
<td>40</td>
<td>++</td>
<td>Explain threat actor types and attributes.</td>
</tr>
<tr>
<td>41</td>
<td>○</td>
<td>Explore social engineering attack types.</td>
</tr>
<tr>
<td>42</td>
<td>++</td>
<td>Identify the types of malicious software (malware).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>Identify the types of malicious network attacks.</td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>Identify the types of programming vulnerabilities and attacks.</td>
<td></td>
</tr>
<tr>
<td>45</td>
<td>Identify the types of cryptographic attacks.</td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>Explain penetration testing concepts.</td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>Identify vulnerability scanning and types.</td>
<td></td>
</tr>
</tbody>
</table>

**Exploring Architecture and Design**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>48</td>
<td>Explain the importance of security protocols in a business environment.</td>
</tr>
<tr>
<td>49</td>
<td>Explore virtualization and cloud computer concepts.</td>
</tr>
<tr>
<td>50</td>
<td>Summarize secure application development, deployment, and automation protocols.</td>
</tr>
<tr>
<td>51</td>
<td>Summarize authentication and authorization design protocols.</td>
</tr>
<tr>
<td>52</td>
<td>Identify concepts related to the implementation of cybersecurity resilience.</td>
</tr>
<tr>
<td>53</td>
<td>Explore the security implications of various networks, components, and systems.</td>
</tr>
<tr>
<td>54</td>
<td>Explore the importance of security controls.</td>
</tr>
<tr>
<td>55</td>
<td>Explore advanced cryptographic concepts.</td>
</tr>
</tbody>
</table>

**Implementing Security Operations**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>56</td>
<td>Explore secure network protocols.</td>
</tr>
<tr>
<td>57</td>
<td>Explore host or application security solutions.</td>
</tr>
<tr>
<td>58</td>
<td>Describe malware protection for clients and servers.</td>
</tr>
<tr>
<td>59</td>
<td>Describe system hardening techniques.</td>
</tr>
<tr>
<td>60</td>
<td>Develop a network security plan.</td>
</tr>
<tr>
<td>61</td>
<td>Identify methods of encryption.</td>
</tr>
<tr>
<td>62</td>
<td>Explain the basic network security systems and protocols.</td>
</tr>
<tr>
<td>63</td>
<td>Describe firewalls.</td>
</tr>
<tr>
<td>64</td>
<td>Implement secure network design.</td>
</tr>
<tr>
<td>65</td>
<td>Configure wireless security settings.</td>
</tr>
<tr>
<td>66</td>
<td>Explore secure mobile solutions.</td>
</tr>
<tr>
<td>67</td>
<td>Apply cybersecurity solutions to the cloud.</td>
</tr>
<tr>
<td>68</td>
<td>Describe identity and account management controls.</td>
</tr>
<tr>
<td>69</td>
<td>Explain concepts related to user authentication.</td>
</tr>
<tr>
<td>70</td>
<td>Explore a security certificate.</td>
</tr>
</tbody>
</table>

**Exploring Operations and Incident Response**

| 71 | Explore tools to assess organizational security. |
| 72 | Apply mitigation techniques or controls to secure an environment. |
| 73 | Summarize the importance of policies, processes, and procedures for incident response. |
| 74 | Explore data sources to support a security incident investigation. |
| 75 | Develop a plan to avoid data loss. |
| 76 | Explain the key aspects of digital forensics. |

**Understanding Governance, Risk, Ethics, and Compliance**

| 77 | Compare types of controls. |
| 78 | Review organizational security posture. |
| 79 | Identify the importance of policies to organizational security. |
| 80 | Summarize risk management processes and concepts. |
| 81 | Identify privacy and sensitive data issues in relation to security. |
| 82 | Summarize basic concepts of forensics. |

**Performing Legal and Ethical Functions**

| 83 | Identify ethical behavior. |
| 84 | Identify copyright and licensing laws that apply to computer use and network administration. |
| 85 | Ensure the proper licensing of a client-server OS and applications. |

**Preparing for Industry Certification**

| 86 | Describe the process and requirements for obtaining industry certifications related to the Cybersecurity Operations, Advanced, course. |
| 87 | Identify testing skills/strategies for a certification examination. |
| 88 | Demonstrate the ability to complete selected practice examinations (i.e., practice questions similar to those on certification exams). |
| 89 | Complete an industry certification examination representative of skills learned in this course. |

**Developing Employability Skills**

| 90 | Update résumé. |
Update a professional portfolio that contains representative samples of student work.

Identify potential employment barriers for nontraditional groups and ways to overcome these barriers.

**Curriculum Frameworks**

**Exploring Attacks, Threats, and Vulnerabilities**

**Task Number 39**

**Compare information security roles.**

**Definition**

Comparison should include

- information security
- assets and liabilities
- confidentiality, integrity, and availability (CIA Triad)
- security policies.

**FBLA Competitive Events and Activities Areas**

Business Knowledge and Skills

Business Ethics

Cyber Security

Healthcare Administration

Hospitality and Event Management

Introduction to Information Technology

Management Information Systems

Network Design

Networking Infrastructures

**Task Number 40**

**Explain threat actor types and attributes.**

**Definition**

Explanation should include

- differentiating between threats, vulnerability, and risks
- identifying attributes of threat actors
  - script kiddies
  - hackers
- hacktivists
- organized crime
- competitors
- nation state actors and/or advanced persistent threats
- malicious insider threats
  - identifying the cyber kill chain
  - identifying indicators of compromise
  - identifying open source intelligence
  - identifying deep web vs. dark web.

**FBLA Competitive Events and Activities Areas**

Business Knowledge and Skills

Business Ethics

Cyber Security

Healthcare Administration

Hospitality and Event Management

Introduction to Information Technology

Management Information Systems

Network Design

Networking Infrastructures

---

**Task Number 41**

**Explore social engineering attack types.**

**Definition**

Exploration should include

- comparing the types of social engineering
  - impersonation
  - dumpster diving
  - shoulder surfing
  - lunchtime attack
  - tailgating
  - phishing
  - whaling
  - vishing
  - pharming
  - hoaxing

- identifying ways to troubleshoot social engineering attacks.
FBLA Competitive Events and Activities Areas

Business Knowledge and Skills
Business Ethics
Cyber Security
Healthcare Administration
Hospitality and Event Management
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

Task Number 42
Identify the types of malicious software (malware).

Definition
Identification should include

- viruses (e.g., boot sector, program, script, macro, multipartite)
- worms
- trojans, bots, backdoors, and remote access trojans (RATs)
- spyware, adware, and keyloggers
- rootkits
- ransomware, crypto-malware, and logic bombs.

Teacher resource:
[CYBER.ORG](https://cyber.org/cybersecurity/threats-attacks-and-vulnerabilities)

FBLA Competitive Events and Activities Areas

Business Knowledge and Skills
Business Ethics
Cyber Security
Healthcare Administration
Hospitality and Event Management
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

Task Number 43
Identify the types of malicious network attacks.

Definition

Identification should include

- disk operating system (DoS) (e.g., flood, fraggle, synchronize flood, ping of death, teardrop, fork)
- distributed denial of service (DDOS)
- domain name system (DNS)
- amplification attacks
- spoofing
- session hijacking (i.e., Transmission Control Protocol/Internet Protocol [TCP/IP], blind and clickjacking, man-in-the-middle, watering hole)
- replay
- Address Resolution Protocol poisoning
  - wireless network attacks (i.e., rogue access points, evil twin, worker protection standards attacks, wireless jamming)
  - Bluetooth attacks (i.e., bluejacking, bluesnarfing)
- radio frequency identification (RFID) and near field communication (NFC) attacks.

Teacher resources:

- [CYBER.ORG, Case Study -Wireless Jamming](https://cyber.org/cybersecurity/threats-attacks-and-vulnerabilities)
- [CYBER.ORG, Lab – Clickjacking](https://cyber.org/cybersecurity/threats-attacks-and-vulnerabilities)

FBLA Competitive Events and Activities Areas

Business Knowledge and Skills
Business Ethics
Cyber Security
Healthcare Administration
Hospitality and Event Management
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

Task Number 44

Identify the types of programming vulnerabilities and attacks.

Definition

Identification should include

- backdoors
buffer overflows
- Structured Query Language (SQL) injections
- cross-site scripting
- zero day.

**FBLA Competitive Events and Activities Areas**

Business Knowledge and Skills

Business Ethics

Cyber Security

Healthcare Administration

Hospitality and Event Management

Introduction to Information Technology

Management Information Systems

Network Design

Networking Infrastructures

---

**Task Number 45**

**Identify the types of cryptographic attacks.**

**Definition**

Identification should include

- brute force
- dictionary attacks
- rainbow tables.

---

**FBLA Competitive Events and Activities Areas**

Business Knowledge and Skills

Business Ethics

Cyber Security

Healthcare Administration

Hospitality and Event Management

Introduction to Information Technology

Management Information Systems

Network Design

Networking Infrastructures

---

**Task Number 46**

**Explain penetration testing concepts.**
**Definition**

Explanation should include

- differentiating between penetration testing and ethical hacking
- reviewing steps taken by a penetration tester
  - verifying a threat exists
  - bypassing security controls
  - testing security controls
  - exploiting vulnerabilities
- reviewing penetration testing techniques
  - reconnaissance phase techniques
  - initial exploitation
  - persistence
  - escalation of privileges and pivot.

**FBLA Competitive Events and Activities Areas**

Business Knowledge and Skills

Business Ethics

Cyber Security

Healthcare Administration

Hospitality and Event Management

Introduction to Information Technology

Management Information Systems

Network Design

Networking Infrastructures

---

**Task Number 47**

**Identify vulnerability scanning and types.**

**Definition**

Identification should include assessing the vulnerability with security tools, including

- network mapping
- vulnerability scanning
- network sniffing
- password analysis.

**FBLA Competitive Events and Activities Areas**

Business Knowledge and Skills

Business Ethics

Cyber Security
Exploring Architecture and Design

Task Number 48

Explain the importance of security protocols in a business environment.

Definition

Explanation should include

- configuration management
  - standard naming convention
  - IP
- data protection
  - data loss prevention (DLP)
  - masking, encryption
  - at rest
  - in transit and/or motion
  - in processing
  - tokenization
  - right’s management
- response and recovery controls
- Secure Sockets Layer (SSL)/Transport Layer Security (TSL) inspection
- hashing
- site resiliency
  - hot, cold, and warm sites
- deception and disruption
  - honeypots
  - honeyfiles
  - honeynets
  - fake telemetry
  - DNS sinkhole.

FBLA Competitive Events and Activities Areas

Business Knowledge and Skills
Business Ethics
Cyber Security
Healthcare Administration
Hospitality and Event Management
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures
Task Number 49
Explore virtualization and cloud computer concepts.

Definition
Exploration should include
- summarizing different cloud models
  - infrastructure-as-a service (IaaS)
  - platform-as-a service (PaaS)
  - software-as-a service (SaaS)
  - anything-as-a service (XaaS)
- identifying cloud service providers
- defining managed service provider (MSP)/managed security service provider (MSSP)
- exploring benefits and drawbacks of on-premise vs. off-premise computing
- exploring virtualization
  - virtual machines (VM)
  - sprawl avoidance
  - VM escape protection.

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Business Ethics
Cyber Security
Healthcare Administration
Hospitality and Event Management
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

Task Number 50
Summarize secure application development, deployment, and automation protocols.

Definition
Summarization should include
- identifying the environment
  - development
  - testing
  - staging
  - production
  - quality assurance
- identifying secure coding techniques
● normalization
● stored procedures
● obfuscation and camouflage
● code reuse and dead code
● server-side vs. client-side execution and validation
● memory management
● use of third-party libraries and software development kits (SDK)
● data exposure

identifying the Open Web Application Security Project (OWASP).

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Business Ethics
Cyber Security
Healthcare Administration
Hospitality and Event Management
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

Task Number 51
Summarize authentication and authorization design protocols.

Definition
Summarization could include

● identifying authentication methods (e.g., technologies)
  ○ time-based one-time password (TOTP)
  ○ hash-based message authentication code (HMAC)/hash-based one-time password (HOTP)
  ○ short message service (SMS)
  ○ token key
  ○ static codes
  ○ authentication applications
  ○ push notifications
  ○ smart card authentication
  ○ biometrics
  ○ multifactor authentication (MFA) factors and attributes
o authentication, authorization, and accounting (AAA)

o cloud vs. on-premise requirements.

FBLA Competitive Events and Activities Areas

Business Knowledge and Skills

Business Ethics

Cyber Security

Healthcare Administration

Hospitality and Event Management

Introduction to Information Technology

Management Information Systems

Network Design

Networking Infrastructures

---

**Task Number 52**

**Identify concepts related to the implementation of cybersecurity resilience.**

**Definition**

Identification should include

- exploring redundancy concepts
  - geographical dispersal
  - network (e.g., load balancer, network interface card teaming)
  - power (e.g., uninterruptible power supply [UPS], generator, dual supply, managed power distribution units [PDU])

- exploring replication
  - storage area network

- exploring backup types
  - full
  - incremental
  - snapshot
  - differential
  - tape
  - disk
  - copy
  - network-attached storage (NAS)
  - storage area network (SAN)
  - cloud
  - image
○ online vs. offline
○ onsite storage
○ distance considerations
● exploring diversity
  ○ technologies
  ○ vendors
  ○ crypto
  ○ controls.

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Business Ethics
Cyber Security
Healthcare Administration
Hospitality and Event Management
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

Task Number 53
Explore the security implications of various networks, components, and systems.

Definition
Exploration should include security implications of various residential, commercial, and industrial

● network components
  ○ hardware devices (e.g., Raspberry Pi, Arduino, micro:bit)
  ○ Internet of things (IoT) devices (e.g., sensors, meters, smart devices, wired and wireless automation components)
  ○ manned and unmanned specialized devices (e.g., medical, vehicular, aircraft, habitation, heating, ventilation, and air conditioning [HVAC])

● network communications (e.g., baseband signal, fifth generation technology [5G], analog vs. digital, voice over IP [VOIP], real-time operating system [RTOS]).

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Business Ethics
Cyber Security
Healthcare Administration
Task Number 54
Explore the importance of security controls.

Definition
Exploration should include how security controls work to reduce or mitigate the risks to an asset(s) through methods that are designed to help accomplish the goal.

Security controls include those that are

- physical (e.g., fences, gates, guards, badges, biometrics, cameras, closed-circuit television [CCTV], data destruction, air gap)
- technical or logical (e.g., hardware or software including firewalls, antivirus, intrusion detection systems [IDS], intrusion protection systems [IPS], access control lists [ACL], data destruction)
- administrative (e.g., logs, policies, procedures, guidelines).

Task Number 55
Explore advanced cryptographic concepts.

Definition
Exploration can include

- cryptographic systems (e.g., elliptic-curve, cipher suites, lightweight, homomorphic, steganography)
- cryptographic concepts (e.g., symmetric vs. asymmetric, hashing and salting, blockchain and public ledgers, digital signatures, key length, key stretching, and key exchange)
- limitations (e.g., speed, size, weak keys, time, predictability, reuse, entropy)
• research of use-case examples that support the CIA triad components of confidentiality, integrity, availability, and non-repudiation.

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Business Ethics
Cyber Security
Healthcare Administration
Hospitality and Event Management
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

Implementing Security Operations

Task Number 56
Explore secure network protocols.

Definition
Exploration should include

• DNS Security Extension (DNSSEC)
• Secure Shell (SSH)
• Secure/Multipurpose Internet Mail Extension (S/MIME)
• Simple Network Management Protocol, version 3 (SNMPv3)
• Hypertext Transfer Protocol (HTTPS) over Secure Sockets Layer (SSL)/Transport Layer Security (TLS)
• IP Security (IPSec)
  ○ authentication header (AH)
  ○ encapsulating security payloads (ESP)
  ○ tunnel/transport
• Secure Post Office Protocol (POP)
• Internet Message Access Protocol (IMAP).

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Business Ethics
Cyber Security
Healthcare Administration
Hospitality and Event Management
Introduction to Information Technology
Task Number 57
Explore host or application security solutions.

**Definition**

Exploration should include

- **boot integrity**
  - boot security and/or Unified Extensible Firmware Interface (UEFI)
  - measured boot
  - boot attestation
- **application security**
  - input validations
  - secure cookies
  - HTTP headers
  - code signing
  - whitelisting
  - blocklisting
  - static code analysis
  - manual code review
  - dynamic code analysis
  - fuzzing
- **self-encrypting drive (SED) and/or full-disk encryption (FDE)**
- **trusted platform module (TPM)**
- **sandboxing.**

---

**FBLA Competitive Events and Activities Areas**

- Business Knowledge and Skills
- Business Ethics
- Cyber Security
- Healthcare Administration
- Hospitality and Event Management
- Introduction to Information Technology
- Management Information Systems
- Network Design
- Networking Infrastructures

---

Task Number 58
Describe malware protection for clients and servers.

**Definition**

Descriptions should include

- **forms**
○ antivirus software
○ spyware filtering
○ patch management

• characteristics
  ○ function
  ○ cost
  ○ upkeep
  ○ reliability
  ○ reporting

• deployed systems
  ○ email security gateways
  ○ web security gateways
  ○ endpoints (workstations or servers).

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Business Ethics
Business Procedures
Cyber Security
Healthcare Administration
Hospitality and Event Management
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

Task Number 59
Describe system hardening techniques.

Definition
Description should include OS, application, and hardware, including

• identifying and removing unneeded items (e.g., software, open ports, accounts, roles, services)
• identifying vulnerability scans
• identifying endpoint security software.

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Business Ethics
Cyber Security
Healthcare Administration
Hospitality and Event Management
Introduction to Information Technology
Task Number 60

**Develop a network security plan.**

**Definition**

Development should include explaining and enforcing well-documented usage policies that ensure network security, including

- Internet security software
- antivirus or antimalware software
- network segmentation
- principle of least privilege implementation
- acceptable use policies (AUP)
- intrusion detection systems (host- and network-based)
- intrusion prevention systems (host- and network-based).

FBLA Competitive Events and Activities Areas

Business Knowledge and Skills
Business Ethics
Cyber Security
Healthcare Administration
Hospitality and Event Management
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

Task Number 61

**Identify methods of encryption.**

**Definition**

Identification should include

- asymmetric encryption
- symmetric encryption
- secure hashing
- salted hashes.

FBLA Competitive Events and Activities Areas

Business Knowledge and Skills
Business Ethics
Task Number 62

Explain the basic network security systems and protocols.

Definition
Explanation should include
- firewalls
- port security
- router access lists
- network intrusion detection systems (NIDS)
- authentication protocols
- public key infrastructure (PKI)
- virtual private network (VPN)
- IPSec
- virtual local area network (VLAN)
- security zones.

Task Number 63

Describe firewalls.

Definition
Description should include
- identification of types of firewalls
  - web-application firewall (WAF)
• next-generation firewall (NGFW)
• stateful
• stateless
• unified threat management (UTM)
• network address translation (NAT) gateway
• content and/or uniform resource locator (URL) filter
• open-source vs. proprietary
• hardware vs. software
• appliance vs. host-based vs. virtual comparison
• characteristics, uses, performance, and benefits of each type of firewall
• software and hardware firewalls comparison
• host-based and network comparison.

**FBLA Competitive Events and Activities Areas**

Business Knowledge and Skills

Business Ethics
Cyber Security
Healthcare Administration
Hospitality and Event Management
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

**Task Number 64**

**Implement secure network design.**

**Definition**

Implementation should include

• access control list (ACL)
• implications of IP version 6 (IPv6)
• port spanning and/or port mirroring
• monitoring services
• file integrity monitors
• network appliances
• jump servers
• proxy servers.

**FBLA Competitive Events and Activities Areas**

Business Knowledge and Skills

Business Ethics
Cyber Security
Healthcare Administration
Hospitality and Event Management
Task Number 65
Configure wireless security settings.

Definition
Configuration should include utilization of the concepts needed to install and configure wireless configuration settings such as

- cryptographic protocols
  - Wireless Fidelity (WiFi) Protected Access II (WPA2)
  - WiFi Protected Access III (WPA3)
- authentication protocols
  - Institution of Electrical and Electronics Engineers (IEEE) 802.1X
  - Remote Authentication Dial-in User Service (RADIUS) federation
- methods
  - pre-shared key (PSK) vs. enterprise vs. open
  - WiFi Protected Setup (WPS)
  - captive portals
- installation considerations
  - site surveys
  - heat maps
  - WiFi analyzers
  - channel overlays
  - wireless access point (WAP) placement.

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Business Ethics
Cyber Security
Healthcare Administration
Hospitality and Event Management
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

Task Number 66
Explore secure mobile solutions.

Definition
Exploration should include
connection methods and receivers
  ○ cellular
  ○ WiFi
  ○ Bluetooth
  ○ Near Field Communication (NFC)
  ○ infrared
  ○ Global Positioning System (GPS)
  ○ radio frequency identification (RFID)

mobile device management

enforcement and monitoring of
  ○ third-party application stores
  ○ rooting and/or jailbreaking
  ○ sideloading
  ○ custom firmware
  ○ carrier unlocking
  ○ firmware over-the-air (OTA) updates
  ○ camera use
  ○ SMS and/or Multimedia Messaging Service (MMS) and/or Rich Communication Services (RCS)
  ○ external media
  ○ USB on-the-go (OTG)
  ○ recording microphone
  ○ GPS tagging
  ○ WiFi direct/ad hoc
  ○ tethering hotspot
  ○ payment methods.

FBLA Competitive Events and Activities Areas

Business Knowledge and Skills

Business Ethics

Cyber Security

Healthcare Administration

Hospitality and Event Management

Introduction to Information Technology

Management Information Systems

Network Design

Networking Infrastructures

Task Number 67

Apply cybersecurity solutions to the cloud.

Definition

Application should include
  • cloud security controls
  • third-party cloud security solutions.
Task Number 68
Describe identity and account management controls.

Definition
Description should include

- identity
  - identity provider (IdP)
  - attributes
  - certificates
  - tokens
  - SSH keys
  - smart cards
- account types
  - user account
  - shared and generic accounts and credentials
  - guest accounts
  - service accounts
- account policies
  - password complexity
  - password history
  - password reuse
  - time of day
  - network location
  - geofencing
  - geotagging
  - geolocation
  - time-based logins
  - access policies
  - account permissions
  - account audits
  - impossible travel time and/or risky login
  - disablement.
Task Number 69

Explain concepts related to user authentication.

Definition

Explanation should include

- single and multi-factor (e.g., security tokens, smart cards, biometrics)
- types (e.g., anonymous, basic, form-based, secure, integrated, multi-factor)
- management
  - password vaults
  - knowledge-based authentication.

FBLA Competitive Events and Activities Areas

Business Knowledge and Skills

Business Ethics
Cyber Security
Healthcare Administration
Hospitality and Event Management
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

Task Number 70

Explore a security certificate.

Definition

Exploration should include

- understanding the purpose and benefits of certificates and PKI
- describing how a certificate affects user security
- identifying how a certificate is used to encrypt data
- identifying how a certificate and/or key combination is used to decrypt a certificate file
- identifying types of certificates
differentiating among certificate formats.

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Business Ethics
Cyber Security
Healthcare Administration
Hospitality and Event Management
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

Exploring Operations and Incident Response
Task Number 71
Explore tools to assess organizational security.
Definition
Exploration should include using

- network reconnaissance and discovery
  - tracert and traceroute
  - name server lookup (nslookup)/domain information groper (dig)
  - IP configuration (ipconfig)/interface configuration (ifconfig)
  - network mapper (Nmap)
  - ping/pathping
  - network statistics (netstat)
  - netcat
  - route
  - DNS enumeration (DNSenum)

- shell and script environments
  - SSH
  - PowerShell
  - Python

- packet capture and replay
  - tcpreplay
  - tcpdump
  - Wireshark

- exploitation frameworks
- password crackers.

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Task Number 72

Apply mitigation techniques or controls to secure an environment.

Definition

Application should include

- reconfiguring endpoint security solutions
  - application whitelisting
  - application blocklisting
  - device quarantine
- making configuration changes
  - firewall rules
  - mobile device management (MDM)
  - DLP
  - content filter and/or URL filter
  - certificate updates or revocations
- implementing network segmentation
- creating security, orchestration, automation, and response (SOAR)
  - runbooks
  - playbooks.

FBLA Competitive Events and Activities Areas

Business Knowledge and Skills

Business Ethics

Cyber Security

Healthcare Administration

Hospitality and Event Management

Introduction to Information Technology

Management Information Systems

Network Design

Networking Infrastructures

Task Number 73
Summarize the importance of policies, processes, and procedures for incident response.

Definition

Summarization should include

- incident response plans
- incident response processes
  - preparation
  - identification
  - containment
  - eradication
  - recovery
  - lessons learned
- exercises
  - tabletop exercises
  - walkthroughs
  - simulations
- attack frameworks
  - MITRE Att&ck
  - Cyber Kill Chain
- communication plan
- disaster recovery plan
- business continuity plan
- Continuity of Operations Planning (COOP)
- incident response team.

FBLA Competitive Events and Activities Areas

Business Knowledge and Skills
- Business Ethics
- Cyber Security
- Healthcare Administration
- Hospitality and Event Management
- Introduction to Information Technology
- Management Information Systems
- Network Design
- Networking Infrastructures

Task Number 74

Explore data sources to support a security incident investigation.

Definition

Exploration should include

- vulnerability scan output
- security information and event management (SIEM) dashboards
- log files
  - network device logs
○ system logs
○ application logs
○ security logs
○ web server logs
○ DNS logs
○ log retention
○ NetFlow/sFlow.

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Business Ethics
Cyber Security
Healthcare Administration
Hospitality and Event Management
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

Task Number 75
Develop a plan to avoid data loss.

Definition
Development should include
- determining what data should be backed up
- choosing the type and frequency of backups
- establishing a policy for restoring data and testing backup
- selecting a remote storage facility
- determining a retention period
- determining DLP tools and techniques.
Task Number 76

Explain the key aspects of digital forensics.

Definition

Explanation should include

- documentation and evidence
  - legal hold
  - admissibility
  - chain of custody
  - timelines of sequence of events
  - time stamps
  - reports
  - event logs
  - interviews

- acquisition
  - order of volatility
  - secondary storage
  - primary storage and random access memory (RAM)
  - swap and page file
  - firmware
  - cache
  - network

- data integrity
  - hashing
  - checksums
  - provenance

- software for digital forensics investigation
  - dd
  - memdump
  - WinHex
  - forensic toolkit (FTK) imager
  - autopsy

- electronic discovery (e-discovery), including identifying, collecting, and producing electronically stored information (ESI).

FBLA Competitive Events and Activities Areas

Business Knowledge and Skills

Business Ethics

Cyber Security

Healthcare Administration

Hospitality and Event Management

Introduction to Information Technology

Management Information Systems

Network Design

Networking Infrastructures
Understanding Governance, Risk, Ethics, and Compliance

Task Number 77
Compare types of controls.

Definition

Comparison includes

- identifying the categories
  - managerial
  - operational
  - technical
- identifying the types
  - preventative
  - detective
  - corrective
  - deterrent
  - compensating
  - physical.

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Business Ethics
Cyber Security
Healthcare Administration
Hospitality and Event Management
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

Task Number 78
Review organizational security posture.

Definition

Review should include

- regulations, standards, and legislation associated with
  - general data protection regulation
  - national, territorial, or state laws
  - payment card industry data
Payment Card Industry Data Security Standard (PCI DSS)

- key frameworks
  - Center for Internet Security (CIS) (https://www.cisecurity.org/)
  - National Institute of Standards and Technology (NIST) (https://www.nist.gov/)
  - International Organization for Standardization (ISO) (https://www.iso.org/home.html)
  - Statement on Standards for Attestation Engagements (SSAE) 16 SOC 2 Type I and II
  - Cloud Security Alliance (CSA) https://cloudsecurityalliance.org/

- benchmarks and secure configuration guides
  - platform or vendor specific guides
    - web server
    - OS
    - application server
    - network infrastructure devices.

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Business Ethics
Cyber Security
Healthcare Administration
Hospitality and Event Management
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

Task Number 79
Identify the importance of policies to organizational security.

Definition
Identification should include examining the importance of personnel

- AUP
- job rotation
- mandatory vacations
- non-disclosure agreement
- onboarding and offboarding
- user training
o principle of least privilege
o background checks
o separation of duties
● diversity of training techniques
● third party risk management
  o vendors
  o supply chain
  o business partners
  o service level agreements (SLA)
  o memorandum of understanding (MOU)
  o business partnership agreement (BPA)
  o end of life or service
● data
● credential policies
● organizational policies
  o change management
  o change control
  o asset management.

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Business Ethics
Business Procedures
Cyber Security
Healthcare Administration
Hospitality and Event Management
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

Task Number 80
Summarize risk management processes and concepts.
Definition
Summarization should include identifying
  ● risks types
  ● risk management strategies


- risk analysis
- disasters
  - natural
  - human caused
  - other incidents of mass trauma (i.e., COVID-19, community unrest)
- business impact analysis.

**FBLA Competitive Events and Activities Areas**

Business Knowledge and Skills

Business Ethics

Cyber Security

Healthcare Administration

Hospitality and Event Management

Introduction to Information Technology

Management Information Systems

Network Design

Networking Infrastructures

**Task Number 81**

**Identify privacy and sensitive data issues in relation to security.**

**Definition**

Identification should include

- organizational consequences of privacy breaches
- notifications of breaches
- data types and classification of data
- privacy enhancing technologies
- roles and responsibilities of data
  - owners
  - controllers
  - processors
  - custodians and/or steward
  - protection officer
- information life cycle
- impact assessment
- terms of agreement
- privacy notices.
Task Number 82
Summarize basic concepts of forensics.

**Definition**
Summarization should include gathering and using forensic data.

Performing Legal and Ethical Functions

Task Number 83
Identify ethical behavior.

**Definition**
Identification should include

- ethical concerns that an administrator might encounter
- email privacy issues
- nondisclosure of confidential information
- ethical and fair use of copyrighted material.
Task Number 84

Identify copyright and licensing laws that apply to computer use and network administration.

Definition

Identification should include laws that govern the use of software, information, and graphics.

FBLA Competitive Events and Activities Areas

Business Knowledge and Skills
3D Animation
American Enterprise Project
Broadcast Journalism
Business Communication
Business Ethics
Business Financial Plan
Business Law
Business Plan
Business Procedures
Community Service Project
Coding and Programming
Computer Applications
Computer Game & Simulation Programming
Digital Video Production
E-business
Electronic Career Portfolio
Graphic Design
Introduction to Business Communication
Introduction to Business Presentation
Introduction to Social Media Strategy
Journalism
Local Chapter Annual Business Report
Mobile Application Development
Network Design
Networking Infrastructures
Partnership with Business Project
Task Number 85
Ensure the proper licensing of a client-server OS and applications.
Definition
Ensuring should include steps for
- tracking server connections (i.e., physical, virtual)
- monitoring software licenses
- searching for unlicensed software.

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Business Ethics
Business Procedures
Cyber Security
Healthcare Administration
Hospitality and Event Management
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

Preparing for Industry Certification
Task Number 86
Describe the process and requirements for obtaining industry certifications related to the Cybersecurity Operations, Advanced, course.
Definition
Description should include a list of industry certifications related to the Cybersecurity Operations, Advanced, course and the process/requirements for obtaining the certifications from
- official websites of the testing organization and/or vendor
● materials from publishers that have developed practice materials and tests based on information from the testing organization and/or vendor
● information from certified instructors or industry-certified professionals
● information in the "Introduction/Course Description" section of this document.

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Cyber Security
Electronic Career Portfolio
Job Interview

Task Number 87
Identify testing skills/strategies for a certification examination.

Definition
Identification of testing skills and strategies should be undertaken by
● conducting an Internet research project
● reviewing materials from exam and practice-exam publishers
● interviewing certified instructors and/or industry-certified professionals.

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Cyber Security
Electronic Career Portfolio
Job Interview

Task Number 88
Demonstrate the ability to complete selected practice examinations (i.e., practice questions similar to those on certification exams).

Definition
Demonstration should include completing practice examinations for selected certifications obtained from vendor sites and/or materials from publishers. The level of performance on a practice examination serves as a gauge of the applicant's readiness for formal industry testing.

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Cyber Security
Electronic Career Portfolio
Task Number 89

Complete an industry certification examination representative of skills learned in this course.

Definition

Completion of an industry certification examination is achieved when the student applicant earns an examination score deemed "passing" by the testing organization. Qualifying examinations are those currently approved at the state level as representative of Cybersecurity Operations, Advanced skills.

Students should be encouraged to attain industry certification as evidence of their computer network software operations skill level and general employability.

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Cyber Security
Electronic Career Portfolio
Job Interview

Developing Employability Skills

Task Number 90

Update résumé.

Definition

Updating the résumé should include

- educational background
- work history
- honors and awards
- membership in club and/or community activities
  - leadership positions held
  - community service.

Students should know how to convert a résumé created in a word processing application into ASCII or plain text format with line breaks, so it can be posted on the Internet, placed into an employer’s résumé bank on a company website, or scanned by an optical character recognition (OCR) scanner.

Students should be encouraged to keep a résumé current and updated to reflect their education and experience, even if they are not currently involved in a job search.

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Task Number 91
Update a professional portfolio that contains representative samples of student work.

Definition
Updating the portfolio should include

- résumé (electronic and non-electronic documents)
- representations of the student’s qualifications and work (e.g., program design, source code, technical documentation, output).

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Business Communications
Computer Applications
Electronic Career Portfolio
Future Business Leader
Introduction to Business Communications
Job Interview
Scholarships
Word Processing

Task Number 92
Identify potential employment barriers for nontraditional groups and ways to overcome these barriers.

Definition
Identification of potential employment barriers should include

- gender
- ethnicity
- age
- discrimination in hiring or promoting practices.
Identification of ways to overcome the barriers should include

- scholarships
- job training programs
- mentorships
- minority assistance programs.

**FBLA Competitive Events and Activities Areas**

Business Knowledge and Skills

Business Communications

Computer Applications

Electronic Career Portfolio

Future Business Leader

Introduction to Business Communications

Job Interview

Scholarships

Word Processing

---

**SOL Correlations to Task**

<table>
<thead>
<tr>
<th>Activity</th>
<th>English:</th>
<th>Social Studies:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Compare information security roles.</td>
<td>11.5, 12.5</td>
<td>VUS 14; Govt 9, 14, 15</td>
<td></td>
</tr>
<tr>
<td>Explain threat actor types and attributes.</td>
<td>11.5, 12.5</td>
<td>VUS 14; Govt 9, 14, 15</td>
<td></td>
</tr>
<tr>
<td>Explore social engineering attack types.</td>
<td>11.5, 12.5</td>
<td>VUS 14; Govt 9, 14, 15</td>
<td></td>
</tr>
<tr>
<td>Identify the types of malicious software (malware).</td>
<td>11.5, 12.5</td>
<td>VUS 14; Govt 9, 14, 15</td>
<td></td>
</tr>
<tr>
<td>Identify the types of malicious network attacks.</td>
<td>11.5, 12.5</td>
<td>VUS 14; Govt 9, 14, 15</td>
<td></td>
</tr>
<tr>
<td>Identify the types of programming vulnerabilities and attacks.</td>
<td>11.5, 12.5</td>
<td>VUS 14; Govt 9, 14, 15</td>
<td></td>
</tr>
<tr>
<td>Identify the types of cryptographic attacks.</td>
<td>11.5, 12.5</td>
<td>VUS 14; Govt 9, 14, 15</td>
<td></td>
</tr>
<tr>
<td>Explain penetration testing concepts.</td>
<td>11.5, 12.5</td>
<td>VUS 14; Govt 9, 14, 15</td>
<td></td>
</tr>
<tr>
<td>Identify vulnerability scanning and types.</td>
<td>11.5, 12.5</td>
<td>VUS 14; Govt 9, 14, 15</td>
<td></td>
</tr>
<tr>
<td>Explain the importance of security protocols in a business environment.</td>
<td>11.5, 12.5</td>
<td>VUS 14; Govt 9, 14, 15</td>
<td></td>
</tr>
<tr>
<td>Explore virtualization and cloud computer concepts.</td>
<td>11.3, 11.5, 12.3, 12.5</td>
<td>VUS 14; Govt 9, 14, 15</td>
<td></td>
</tr>
<tr>
<td>Activity</td>
<td>Language:</td>
<td>English:</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Summarize secure application development, deployment, and automation protocols.</td>
<td></td>
<td>11.5, 12.5</td>
<td></td>
</tr>
<tr>
<td>Summarize authentication and authorization design protocols.</td>
<td></td>
<td>11.5, 12.5</td>
<td></td>
</tr>
<tr>
<td>Identify concepts related to the implementation of cybersecurity resilience.</td>
<td></td>
<td>11.5, 12.5</td>
<td></td>
</tr>
<tr>
<td>Explore the security implications of various networks, components, and systems.</td>
<td></td>
<td>11.5, 12.5</td>
<td></td>
</tr>
<tr>
<td>Explore the importance of security controls.</td>
<td></td>
<td>11.5, 12.5</td>
<td></td>
</tr>
<tr>
<td>Explore advanced cryptographic concepts.</td>
<td></td>
<td>11.5, 12.5</td>
<td></td>
</tr>
<tr>
<td>Explore secure network protocols.</td>
<td></td>
<td>11.5, 12.5</td>
<td></td>
</tr>
<tr>
<td>Explore host or application security solutions.</td>
<td></td>
<td>11.5, 11.8, 12.5, 12.8</td>
<td></td>
</tr>
<tr>
<td>Describe malware protection for clients and servers.</td>
<td></td>
<td>11.5, 12.5</td>
<td></td>
</tr>
<tr>
<td>Describe system hardening techniques.</td>
<td></td>
<td>11.5, 12.5</td>
<td></td>
</tr>
<tr>
<td>Develop a network security plan.</td>
<td></td>
<td>11.1, 11.5, 12.1, 12.5</td>
<td></td>
</tr>
<tr>
<td>Identify methods of encryption.</td>
<td></td>
<td>11.5, 12.5</td>
<td></td>
</tr>
<tr>
<td>Explain the basic network security systems and protocols.</td>
<td></td>
<td>11.5, 12.5</td>
<td></td>
</tr>
<tr>
<td>Describe firewalls.</td>
<td></td>
<td>11.5, 12.5</td>
<td></td>
</tr>
<tr>
<td>Implement secure network design.</td>
<td></td>
<td>11.5, 12.5</td>
<td></td>
</tr>
<tr>
<td>Configure wireless security settings.</td>
<td></td>
<td>11.5, 12.5</td>
<td></td>
</tr>
<tr>
<td>Explain secure mobile solutions.</td>
<td></td>
<td>11.5, 11.8, 12.5, 12.8</td>
<td></td>
</tr>
<tr>
<td>Apply cybersecurity solutions to the cloud.</td>
<td></td>
<td>11.5, 12.5</td>
<td></td>
</tr>
<tr>
<td>Describe identity and account management controls.</td>
<td></td>
<td>11.5, 11.8, 12.5, 12.8</td>
<td></td>
</tr>
<tr>
<td>Explain concepts related to user authentication.</td>
<td></td>
<td>11.5, 12.5</td>
<td></td>
</tr>
<tr>
<td>Explore a security certificate.</td>
<td></td>
<td>11.5, 11.8, 12.5, 12.8</td>
<td></td>
</tr>
<tr>
<td>Explore tools to assess organizational security.</td>
<td></td>
<td>11.5, 11.8, 12.5, 12.8</td>
<td></td>
</tr>
<tr>
<td>Apply mitigation techniques or controls to secure an environment.</td>
<td></td>
<td>11.5, 12.5</td>
<td></td>
</tr>
<tr>
<td>Summarize the importance of policies, processes, and procedures for incident response.</td>
<td></td>
<td>11.5, 12.5</td>
<td></td>
</tr>
<tr>
<td>Explore data sources to support a security incident investigation.</td>
<td></td>
<td>11.5, 11.8, 12.5, 12.8</td>
<td></td>
</tr>
<tr>
<td>Develop a plan to avoid data loss.</td>
<td></td>
<td>11.1, 11.5, 12.1, 12.5</td>
<td></td>
</tr>
<tr>
<td>Explain the key aspects of digital forensics.</td>
<td></td>
<td>11.5, 11.6, 11.7, 12.5, 12.6, 12.7</td>
<td></td>
</tr>
<tr>
<td>Compare types of controls.</td>
<td></td>
<td>11.5, 12.5</td>
<td></td>
</tr>
<tr>
<td>Review organizational security posture.</td>
<td></td>
<td>11.5, 12.5</td>
<td></td>
</tr>
<tr>
<td>Identify the importance of policies to organizational security.</td>
<td></td>
<td>11.5, 12.5</td>
<td></td>
</tr>
<tr>
<td>Summarize risk management processes and concepts.</td>
<td></td>
<td>11.5, 12.5</td>
<td></td>
</tr>
<tr>
<td>Task</td>
<td>Difficulty</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify privacy and sensitive data issues in relation to security.</td>
<td>English: 11.5, 12.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Summarize basic concepts of forensics.</td>
<td>English: 11.5, 12.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify ethical behavior.</td>
<td>English: 11.5, 12.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify copyright and licensing laws that apply to computer use and network administration.</td>
<td>English: 11.5, 12.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure the proper licensing of a client-server OS and applications.</td>
<td>English: 11.5, 12.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Describe the process and requirements for obtaining industry certifications related to the Cybersecurity Operations, Advanced, course.</td>
<td>English: 11.5, 12.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify testing skills/strategies for a certification examination.</td>
<td>English: 11.5, 12.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Demonstrate the ability to complete selected practice examinations (i.e., practice questions similar to those on certification exams).</td>
<td>English: 11.5, 12.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Complete an industry certification examination representative of skills learned in this course.</td>
<td>English: 11.5, 12.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update résumé.</td>
<td>English: 11.5, 11.6, 11.7, 12.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update a professional portfolio that contains representative samples of student work.</td>
<td>English: 11.5, 11.6, 11.7, 12.5, 12.6, 12.7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify potential employment barriers for nontraditional groups and ways to overcome these barriers.</td>
<td>English: 11.5, 12.5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Instructional Scenarios

Lockdown at International Hotel

Duty Area(s): Exploring Operations and Incident Response

Scenario:
Please refer to the resource link below for more information.
https://cyber.instructure.com/courses/6/pages/aics
Module 1: International Hotel Lockdown

Big Question:
How do agencies like the Department of Homeland Security investigate an incident using digital forensics and various media?

Focused Questions:
- Based on the evidence, how might you go about constructing a list of key names or groups that can be responsible for the incident?
- Based on the evidence gathered, what is the timeline of events?
- What type of information did you glean from the .txt file?

Based on the evidence, were you able to identify connections between any of the key figures involved?

Project-Based Assessment:

Groups can be graded on the following:

- Opening Statements (clear, well organized, and relevant)
- Addressed Issues (coverage of topic)
- Supporting Facts (provided facts that support the topic)
- Persuasiveness (arguments are clear and convincing)
- Teamwork (all members contributed to briefing)
- Organization (addressed likely culprit and gave clear recommended response)
- Overall preparedness, effectiveness, and professionalism

Resources: Cyber.org/Cyber Society/AICS
https://cyber.instructure.com/courses/6/pages/aics


Entrepreneurship Infusion Units

Entrepreneurship Infusion Units may be used to help students achieve additional, focused competencies and enhance the validated tasks/competencies related to identifying and starting a new business venture. Because the unit is a complement to certain designated courses and is not mandatory, all tasks/competencies are marked “optional.”

Curriculum Resources

The Academic Initiative of the Cyber Innovation Center offers access to its curricula at no cost to K-12 teachers. These lessons could be used to supplement the following tasks:

- Task 40: Describe cybersecurity threats to an organization. (How Businesses Secure Information)
- Task 43: Describe the cyberattack surface of various organizations (How Businesses Secure Information)
• Task 64: Distinguish among types of ethical concerns. (Privacy vs. Security)
• Task 73: Explain the concept of "personally identifiable information." (You are the Data)
• Task 74: Explain how and why personal data is valuable to both an individual and to the organizations. (You are the Data)
• Task 75: Identify ways to control and protect personal data. (You are the Data)
• Task 77: Analyze the social and legal significance of the ongoing collection of personal digital information. (Your Permanent Electronic Record)

The National Institute of Standards and Technology has published the Glossary of Key Information Security Terms, which has been extracted from federal standards, publications, reports, and instructions.

The SANS Institute offers free professional development curricula focused on the fundamentals of cybersecurity. The course covers operating systems, networking, and systems administration.

The Virginia Cyber Range is a Commonwealth of Virginia initiative with a mission to enhance cybersecurity education for students in the Commonwealth’s public high schools, colleges, and universities. The Virginia Cyber Range seeks to increase the number of fully prepared students entering the cybersecurity workforce in operations, development, and research. The Virginia Cyber Range provides an extensive Courseware Repository for educators and a cloud-hosted Exercise Area environment for hands-on cybersecurity labs and exercises for students.

AFA CyberPatriot is the National Youth Cyber Education Program created by the Air Force Association to inspire K-12 students toward careers in cybersecurity or other science, technology, engineering, and mathematics (STEM) disciplines critical to our nation's future. At the core of the program is the National Youth Cyber Defense Competition, the nation's largest cyber defense competition that puts high school and middle school students in charge of securing virtual networks.

Net Etiquette

"What do I need to know about technology?" Northern Virginia Community College

"Netiquette," Justice Institute of British Columbia

Coding Standards

"SEI CERT Coding Standards," Software Engineering Institute, Carnegie-Mellon University

Open Web Application Security Project (OWASP), focused on improving the security of software.

Job-related Tools and Data

CyberSeek: Provides detailed data about supply and demand in cybersecurity fields, including an interactive state-by-state map which shows the field where demand is highest. For job seekers, educators, school counselors, and students.

Burning Glass Technologies: Job market analytics firm which looks at trends in hiring. Includes research about the cybersecurity job market.

“Breaking the Code on a Career in Cybersecurity”: Virginia Space Grant Consortium’s free video series, which features interviews with cyber professionals about their career pathways.

Appendix: Credentials, Course Sequences, and Career Cluster Information

Industry Credentials: Only apply to 36-week course
• A+ Certification Examination
• Business Information Processing Assessment
• Certified Associate in Python Programming (PCAP) Examination
• Certified Entry-Level Python Programmer (PCEP) Examination
• Certified Internet Web (CIW) Advanced HTML 5 and CSS 3 Specialist Examination
• Certified Internet Web (CIW) Data Analyst Examination
• Certified Internet Web (CIW) Database Design Specialist Examination
• Certified Internet Web (CIW) E-Commerce Services Specialist Examination
• Certified Internet Web (CIW) Internet Business Associate Examination
• Certified Internet Web (CIW) JavaScript Specialist Examination
• Certified Internet Web (CIW) Network Technology Associate Examination
• Certified Internet Web (CIW) Site Development Associate Examination
• Certified Internet Web (CIW) Social Media Strategist Examination
• Certified Internet Web (CIW) User Interface Designer Examination
• Certified Internet Web (CIW) Web Design Specialist Examination
• Certified Internet Web (CIW) Web Security Specialist Examination
• Cloud Essentials Certification Examination
• College and Work Readiness Assessment (CWRA+)
• Computer Networking Fundamentals Assessment
• Computer Repair Technology Assessment
• Computer Technology Assessment
• Cyber Forensics Associate Examination
• Ethical Hacking Associate Examination
• IC3 Digital Literacy Certification Examination
• Internetworking Examination
• IT Fundamentals+ Certification Examination
• Linux+ Certification Examination
• Microsoft 365 Fundamentals Examination
• Microsoft Certified Azure Fundamentals Examination
• Microsoft Dynamics 365 Fundamentals Examination
• Microsoft Office Specialist (MOS) Examinations
• Microsoft Technology Associate (MTA) Examinations
• National Career Readiness Certificate Assessment
• Network Administration Certification Tests
• Network Pro Certification Examination
• Network+ Certification Examination
• Oracle Certified Associate Examinations
• Oracle Certified Junior Associate Examinations
• PC Pro Certification Examination
• Security Pro Certification Examination
• Security+ Certification Examination
• Technical Support Certification Tests
• Workplace Readiness Skills for the Commonwealth Examination

Concentration sequences: A combination of this course and those below, equivalent to two 36-week courses, is a concentration sequence. Students wishing to complete a specialization may take additional courses based on their career pathways. A program completer is a student who has met the requirements for a CTE concentration sequence and all other requirements for high school graduation or an approved alternative education program.

• Cybersecurity Fundamentals (6302/36 weeks)
• Cybersecurity Operations (6304/36 weeks)

<table>
<thead>
<tr>
<th>Career Cluster: Information Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pathway</strong></td>
</tr>
<tr>
<td>Information Support and Services</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Network Systems</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
| Programming and Software Development | Computer Support Specialist  
Network and Computer Systems Administrator  
Network Systems and Data Communication Analyst  
Telecommunications Specialist |
|--------------------------------------|-------------------------------------------------------------------------------|
|                                      | Game Designer, Programmer  
Multimedia Artist, Animator  
Network Systems and Data Communication Analyst  
Software Applications Engineer  
Web Developer |

### Career Cluster: Science, Technology, Engineering and Mathematics

<table>
<thead>
<tr>
<th>Pathway</th>
<th>Occupations</th>
</tr>
</thead>
</table>
| Engineering and Technology   | Computer Hardware Engineer  
Computer Programmer  
Computer Software Engineer  
Network and Computer Systems Administrator  
Network Systems and Data Communication Analyst  
Power Systems Engineer  
Production, Planning, Expediting Clerk  
Stockroom, Warehouse, or Storage Yard Stock Clerk  
Technical Writer  
Telecommunications Specialist  
Transportation Manager |