Cybersecurity Network Systems

8630 36 weeks

Table of Contents

Acknowledgments ......................................................................................................................................... 1
Course Description ........................................................................................................................................ 2
Task Essentials List ....................................................................................................................................... 3
Curriculum Framework ................................................................................................................................. 6
Understanding Threats, Attacks, and Vulnerabilities ................................................................................... 6
Exploring Technologies and Tools ............................................................................................................. 11
Examining Architecture and Design .......................................................................................................... 21
Analyzing Identity and Access Management .............................................................................................. 29
Demonstrating Risk Management ............................................................................................................... 31
Examining Cryptography and Public Key Infrastructure (PKI) ........................................................................ 38
Understanding Ethical and Legal Considerations in Cybersecurity ............................................................ 43
SOL Correlation by Task ............................................................................................................................... 46
Teacher Resources ...................................................................................................................................... 51
Appendix: Credentials and Career Cluster Information .............................................................................. 52

Acknowledgments

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

Joseph Carter, Chief Executive Officer, R&K Cyber Solutions LLC
Joseph D. Chase, Professor, Radford University
Jeremiah Doucette, Washington County Career and Technical Education Center, Washington County Public Schools
Gail Drake, Battlefield High School, Prince William County Public Schools, and Associate Professor, Northern Virginia Community College
Jennifer Eller, Radford High School, Radford City Public Schools
Deb Garcia, Information Security Engineer, Lockheed Martin Integrated Technology
Course Description

Suggested Grade Level: 12
Prerequisites: 6306 or 8629 or 8545

This advanced-level course prepares students for postsecondary education and careers in the rapidly growing field of cybersecurity. Students gain competitive skills required to administer,
analyze, and secure applications, networks, and devices. Students perform threat analysis and participate in risk mitigation. Concepts include understanding threats, attacks, and vulnerabilities; exploring technology and tools; examining architecture and design; analyzing identity and access management; demonstrating risk management; and examining cryptography and public key management. Upon successful completion of this course, students may qualify for the CompTIA Security+ certification exam. Individuals with a Security+ credential are well-equipped to further develop their skills toward a CompTIA Cybersecurity Analyst (CSA+) credential.

**Task Essentials List**

- 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>Tasks/Competencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>39</td>
<td>Compare types of attacks.</td>
</tr>
<tr>
<td>40</td>
<td>Explain threat actor types and attributes.</td>
</tr>
<tr>
<td>41</td>
<td>Explain vulnerability scanning concepts.</td>
</tr>
<tr>
<td>42</td>
<td>Research ethical and legal issues related to penetration testing.</td>
</tr>
<tr>
<td>43</td>
<td>Explain penetration (pen) testing concepts.</td>
</tr>
<tr>
<td>44</td>
<td>Analyze indicators of compromise for the purpose of determining the type of malware in a given scenario.</td>
</tr>
<tr>
<td>45</td>
<td>Explore network infrastructure hardware and software-based components that support organizational security.</td>
</tr>
<tr>
<td>46</td>
<td>Explore host hardware- and software-based components that support organizational security.</td>
</tr>
<tr>
<td>Task Number</td>
<td>8630</td>
</tr>
<tr>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>47</td>
<td>+</td>
</tr>
<tr>
<td>48</td>
<td>+</td>
</tr>
<tr>
<td>49</td>
<td>+</td>
</tr>
<tr>
<td>50</td>
<td>+</td>
</tr>
<tr>
<td>51</td>
<td>+</td>
</tr>
<tr>
<td>52</td>
<td>+</td>
</tr>
<tr>
<td>53</td>
<td>+</td>
</tr>
<tr>
<td>54</td>
<td>+</td>
</tr>
</tbody>
</table>

**Examining Architecture and Design**

<table>
<thead>
<tr>
<th>Task Number</th>
<th>8630</th>
<th>Tasks/Competencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>55</td>
<td>+</td>
<td>Describe frameworks, best practices, and secure configuration guides and their purposes.</td>
</tr>
<tr>
<td>56</td>
<td>+</td>
<td>Implement secure network architecture concepts.</td>
</tr>
<tr>
<td>57</td>
<td>+</td>
<td>Implement secure systems design.</td>
</tr>
<tr>
<td>58</td>
<td>+</td>
<td>Explain the importance of secure staging deployment concepts.</td>
</tr>
<tr>
<td>59</td>
<td>+</td>
<td>Explain the security implications of embedded systems.</td>
</tr>
<tr>
<td>60</td>
<td>+</td>
<td>Summarize secure application development and deployment concepts.</td>
</tr>
<tr>
<td>61</td>
<td>+</td>
<td>Examine cloud computing concepts.</td>
</tr>
<tr>
<td>62</td>
<td>+</td>
<td>Outline virtualization concepts.</td>
</tr>
<tr>
<td>63</td>
<td>+</td>
<td>Explain how resiliency and automation strategies reduce risk.</td>
</tr>
<tr>
<td>64</td>
<td>+</td>
<td>Explain the importance of physical security controls.</td>
</tr>
<tr>
<td>Task Number</td>
<td>8630</td>
<td>Tasks/Competencies</td>
</tr>
<tr>
<td>-------------</td>
<td>------</td>
<td>--------------------</td>
</tr>
<tr>
<td><strong>Analyzing Identity and Access Management</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>65</td>
<td>+</td>
<td>Compare identity and access management concepts.</td>
</tr>
<tr>
<td>66</td>
<td>+</td>
<td>Install identity and access services.</td>
</tr>
<tr>
<td>67</td>
<td>+</td>
<td>Implement identity and access management controls.</td>
</tr>
<tr>
<td>68</td>
<td>+</td>
<td>Differentiate common account management practices.</td>
</tr>
<tr>
<td><strong>Demonstrating Risk Management</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>69</td>
<td>+</td>
<td>Explain the importance of policies, plans, and procedures related to organizational security.</td>
</tr>
<tr>
<td>70</td>
<td>+</td>
<td>Summarize business impact analysis concepts.</td>
</tr>
<tr>
<td>71</td>
<td>+</td>
<td>Explain risk management processes and concepts.</td>
</tr>
<tr>
<td>72</td>
<td>+</td>
<td>Describe appropriate incident response procedures.</td>
</tr>
<tr>
<td>73</td>
<td>+</td>
<td>Summarize basic concepts of forensics.</td>
</tr>
<tr>
<td>74</td>
<td>+</td>
<td>Explain disaster recovery and continuity of operation concepts.</td>
</tr>
<tr>
<td>75</td>
<td>+</td>
<td>Compare various types of controls.</td>
</tr>
<tr>
<td>76</td>
<td>+</td>
<td>Execute data security and privacy practices.</td>
</tr>
<tr>
<td><strong>Examining Cryptography and Public Key Infrastructure (PKI)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>77</td>
<td>+</td>
<td>Identify the states of the data that needs to be secured.</td>
</tr>
<tr>
<td>78</td>
<td>+</td>
<td>Explain the three main forms of cryptography.</td>
</tr>
<tr>
<td>79</td>
<td>+</td>
<td>Identify basic concepts of cryptography.</td>
</tr>
<tr>
<td>80</td>
<td>o</td>
<td>Explain common use cases for cryptography.</td>
</tr>
</tbody>
</table>
### Curriculum Framework

#### Understanding Threats, Attacks, and Vulnerabilities

**Task Number 39**

**Compare types of attacks.**
Definition

Comparison should include the following:

- **Social engineering**
  - Phishing
  - Spear phishing
  - Whaling
  - Vishing
  - Tailgating
  - Impersonation
  - Dumpster diving
  - Shoulder surfing
  - Hoax
  - Watering hole attack
  - Principles (reasons for effectiveness)
    - Authority
    - Intimidation
    - Consensus
    - Scarcity
    - Familiarity
    - Trust
    - Urgency

- **Application/service attacks**
  - Denial of Service (DoS)
  - Distributed Denial of Service (DDoS)
  - Man-in-the-middle
  - Buffer overflow
  - Injection
  - Cross-site scripting
  - Cross-site request forgery
  - Privilege escalation
  - Address Resolution Protocol (ARP) poisoning
  - Amplification
  - Domain Name Service (DNS) poisoning
  - Domain hijacking
  - Man-in-the-browser
  - Zero day
  - Replay
  - Pass the hash
  - Hijacking and related attacks
    - Clickjacking
    - Session hijacking
    - Universal Resource Locator (URL) hijacking
    - Typo squatting
  - Driver manipulation
- Shimming
- Refactoring
  - Message Authentication Code (MAC) spoofing
  - Internet Protocol (IP) spoofing
- Wireless attacks
  - Replay
  - Initialization Vector (IV)
  - Evil twin
  - Rogue Access Point (AP)
  - Jamming
  - Wireless Fidelity (WiFi) Protected Setup (WPS)
  - Bluejacking
  - Bluesnarfing
  - Radio Frequency Identifier (RFID)
  - Near Field Communication (NFC)
  - Disassociation
- Cryptographic attacks
  - Birthday
  - Known plain text/cipher text
  - Rainbow tables
  - Dictionary
  - Brute force
    - Online vs. offline
  - Collision
  - Downgrade
  - Replay
  - Weak implementations

**Process/Skill Questions**

- What specific vulnerability is exploited by a social engineering attack?
- How is spear phishing different from vishing?
- What are the similarities among various application attacks?
- What might be done to prevent social engineering attacks?

---

**Task Number 40**

**Explain threat actor types and attributes.**

**Definition**

Explanation should include the following:
• Types of actors
  o Script kiddies
  o Hacktivist
  o Organized crime
  o Nation states/Advanced Persistent Threat (APT)
  o Insiders
  o Competitors
• Attributes of actors
  o Internal/external
  o Level of sophistication
  o Resources/funding
  o Intent/motivation
• Use of open-source intelligence

Process/Skill Questions

• What would constitute a misconfiguration?
• How can business processes help prevent vulnerabilities?
• How does one determine whether a website has a buffer vulnerability?
• What is an example of a historical misconfiguration vulnerability?

Task Number 41

Explain vulnerability scanning concepts.

Definition

Explanation should include the following:

• Passively test security controls
• Identify vulnerability
• Identify lack of security controls
• Identify common misconfigurations
• Intrusive vs. non-intrusive
• Credentialed vs. non-credentialed
• False positive

Process/Skill Questions

• What ethical concerns are related to vulnerability scanning?
• What techniques are commonly used in vulnerability scanning?
• Should users be allowed to configure workstation security? Explain.
Task Number 42

Research ethical and legal issues related to penetration testing.

Definition

Research should include

- evaluating Association for Computing Machinery (ACM) Code of Ethics and Professional Conduct
- local use policies.

Teacher resource: Association for Computing Machinery (ACM) Code of Ethics and Professional Conduct

Process/Skill Questions

- What is the purpose of a non-disclosure agreement with regard to penetration testing?
- Why would a penetration test need a “get out of jail free” card?
- Why would a business want to make sure that penetration testers comply with the ACM Code of Ethics and Professional Conduct?

Task Number 43

Explain penetration (pen) testing concepts.

Definition

Explanation should include the following:

- Active reconnaissance
- Passive reconnaissance
- Pivot
- Initial exploitation
- Persistence
- Escalation of privilege
- Black box
- White box
• Gray box
• Pen testing vs. vulnerability scanning

**Process/Skill Questions**

• What is the difference between active and passive reconnaissance?
• What are the differences among black box, white box, and gray box?
• What is a method by which one could escalate privileges?

---

**Task Number 44**

**Analyze indicators of compromise for the purpose of determining the type of malware in a given scenario.**

**Definition**

Analysis should include the following:

• Viruses
• Crypto-malware
• Ransomware
• Worm
• Trojan
• Rootkit
• Keylogger
• Adware
• Spyware
• Bots
• Remote Access Trojan (RAT)
• Logic bomb
• Backdoor

**Process/Skill Questions**

• What are some examples of ransomware attacks?
• What is the process used to uncover a rootkit?
• Which malware can be delivered via email?

**Exploring Technologies and Tools**

**Task Number 45**
Explore network infrastructure hardware and software-based components that support organizational security.

Definition

Exploration may include the following:

- **Firewall/Unified Threat Management (UTM)**
  - Access Control List (ACL)
  - Application-based vs. network-based
  - Stateful vs. stateless
  - Implicit deny
- **Switch**
  - Port security
  - Layer 2 vs. Layer 3
  - Loop prevention
  - Flood guard
- **Router**
  - ACLs
  - Anti-spoofing
- **Proxy**
  - Forward and reverse proxy
  - Transparent
  - Application/multipurpose
- **Load balancer**
  - Scheduling
    - Affinity
    - Round-robin
  - Active-passive
  - Active-active
  - Virtual IPs
- **Access point**
  - Service Set Identifier (SSID)
  - MAC filtering
  - Signal strength
  - Band selection/width
  - Antenna types and placement
  - Fat vs. thin
  - Controller-based vs. standalone Bridge
- **Network Access Control (NAC)**
  - Dissolvable vs. permanent
  - Host health checks
  - Agent vs. agentless

Process/Skill Questions
• What security features can be implemented on/with a firewall?
• How does the proxy protect the end user?
• How does load balancer introduce security into the organization?

---

**Task Number 46**

**Explore host hardware- and software-based components that support organizational security.**

**Definition**

Exploration may include the following:

- Mail gateway
  - Spam filter
  - Data Loss Prevention (DLP)
  - Encryption
- Media gateway
- Security Information and Event Management (SIEM)
  - Aggregation
  - Correlation
  - Automated alerting and triggers
  - Time synchronization
  - Event deduplication
  - Logs/Write Once Read Many (WORM)
- Network-based Intrusion Prevention System (NIPS)/Network-based Intrusion Detection System (NIDS)/Host-based Intrusion Detection System (HIDS)
  - Signature-based
  - Heuristic/behavioral
  - Anomaly
  - Inline vs. passive
  - In-band vs. out-of-band
  - Rules
  - Analytics
    - False positive
    - False negative
- Virtual Private Network (VPN) Concentrator
  - Remote access vs. site-to-site
  - Internet Protocol Security (IPSec)
    - Tunnel mode
    - Transport mode
    - Authentication Header (AH)
    - Encapsulated Security Payload (ESP)
- Split tunnel vs. full tunnel
- Transport Layer Security (TLS)
- Always-on VPN
- Secure Sockets Layer (SSL)/TLS accelerators
- SSL decryptors
- DLP
  - Universal Serial Bus (USB) blocking
  - Cloud-based
  - Email
- Hardware security module

**Process/Skill Questions**

- How does a VPN device ensure security between two end points?
- How does a SIEM ease a security engineer’s responsibilities?
- What is the difference between a NIPS and NIDS?

---

**Task Number 47**

**Assess the network security posture of an organization in a given scenario.**

**Definition**

Assessment should use appropriate software tools and include the following:

- Protocol analyzer
- Network scanners
  - Rogue system detection
  - Network mapping
- Command line tools
  - ping
  - netstat
  - tracert
  - nslookup/dig
  - arp
  - ipconfig/ip/ifconfig
  - tcpdump
  - nmap
  - netcat
- Wireless scanners / crackers
- Passive vs. active
- Web application firewall
Task Number 48

Assess the host security posture of an organization in a given scenario.

Definition

Assessment should use appropriate software tools and include the following:

- Configuration compliance scanner
- Backup utilities
- Honeypot
- Banner grabbing
- Password cracker
- Vulnerability scanner
- Exploitation frameworks
- Host-based Intrusion Detection System (HIDS)/Host-based Intrusion Prevention System (HIPS)
- Host-based firewall
- Antivirus
- File integrity check
- Application whitelisting
- Advanced malware tools
- Patch management tools
- Removable media control

Process/Skill Questions

- What are the main differences between HIDS and HIPS?
- How can a “honeypot” be used to increase security for an organization?
- What is the purpose of backup utilities in determining the overall security health of an organization?
Assess the data security posture of an organization in a given scenario.

Definition

Assessment should use appropriate software tools and include the following:

- Data sanitization tools
- Steganography
- Data Execution Prevention
- Data Loss Prevention (DLP)

Process/Skill Questions

- How is steganography used in the digital era?
- How does DLP software help in safeguarding an organization’s data?
- Why do organizations need to use data sanitization tools when disposing of obsolete technology?

Task Number 50

Troubleshoot common security issues in a given scenario.

Definition

Troubleshooting should include the following:

- Unencrypted credentials/clear text
- Logs and events anomalies
- Permission issues
- Access violations
- Certificate issues
- Data exfiltration
- Misconfigured devices
  - Firewall
  - Content filter
  - Access points
- Weak security configurations
- Personnel issues
  - Policy violation
  - Insider threat
  - Social engineering
• Social media
  • Personal email
• Unauthorized software
• Baseline deviation
• License compliance violation (availability/integrity)
• Asset management
• Authentication issues

Process/Skill Questions

• What logs can be evaluated for security issues?
• Where would one locate evidence of an access violation?
• Why must a security portal with a mantrap still be supervised or observed by security personnel?

Task Number 51

Evaluate the output from security technologies.

Definition

Evaluation of output from security technologies may include:

• Network tools
  • Protocol analyzer
  • Network Scanners
  • Wireless scanners / crackers
  • Web application firewall
• Host tools
  • Configuration compliance scanner
  • Backup utilities
  • Honeypot
  • Banner grabbing
  • Password cracker
  • Vulnerability scanner
  • Exploitation frameworks
  • HIDS/HIPS
  • Host-based firewall
  • Antivirus
  • File integrity check
  • Application whitelisting
  • Advanced malware
  • Patch management
• Removable media control
  • Data tools
    o Data sanitization tools
    o DLP
    o Data execution prevention violations

Process/Skill Questions

• What tool/s would you use to investigate issues on a user workstation?
• Which tools logs will show out-of-date patching?
• Why tool would show you blocked sites?

Task Number 52

Describe mobile connection methods and deployment models.

Definition

Description may include the following:

• Connection methods
  o Cellular
  o WiFi
  o Satellite communications (SATCOM)
  o Bluetooth
  o NFC
  o ANT
  o Infrared
  o USB
• Deployment models
  o Bring Your Own Device (BYOD)
  o Corporate Owned, Personally Enabled (COPE)
  o Choose Your Own Device (CYOD)
  o Corporate-owned
  o Virtual Desktop Infrastructure (VDI)

Process/Skill Questions

• How would an organization ensure that a BYOD device would not compromise their network?
• How can an individual ensure that their BYOD device will not be compromised?
• What security technologies are deployed in WiFi?
• Which connection methods can be used to access the organization remotely?

---

**Task Number 53**

**Discuss device management and enforcement concepts.**

**Definition**

Discussion of device management and enforcement concepts may include the following:

- Mobile device management concepts
  - Application management
  - Content management
  - Remote wipe
  - Geofencing
  - Geolocation
  - Screen locks
  - Push notification services
  - Passwords and pins
  - Biometrics
  - Context-aware authentication
  - Containerization
  - Storage segmentation
  - Full device encryption

- Enforcement and monitoring
  - Third-party app stores
  - Rooting/jailbreaking
  - Sideload
  - Custom firmware
  - Carrier unlocking
  - Firmware over-the-air (OTA) updates
  - Camera use
  - Short Message Service (SMS)/Multimedia Message Service (MMS)
  - External media
  - USB on-the-go (OTG)
  - Recording microphone
  - Global Positioning System (GPS) tagging
  - WiFi direct/ad hoc
  - Tethering
  - Payment methods

**Process/Skill Questions**
• What is full device encryption?
• What security methods support screen locking?
• How does geolocation present a security risk for portable devices?

---

**Task Number 54**

**Explain secure protocols and their use cases.**

**Definition**

Explanation of secure protocols and their use cases may include the following:

- **Protocols**
  - DNS Security Extensions (DNSSEC)
  - Secure Shell (SSH)
  - Secure/Multipurpose Internet Mail Extensions (S/MIME)
  - Secure Real-Time Protocol (SRTP)
  - Lightweight Directory Access Protocol (LDAP)
  - Secure File Transfer Protocol (FTPS)
  - Secure File Transfer Protocol (SFTP)
  - Simple Network Management Protocol, version 3 (SNMPv3)
  - SSL/TLS
  - Hypertext Transfer Protocol over SSL/TLS (HTTPS)
  - Secure Post Office Protocol (POP)/Internet Message Access Protocol (IMAP)

- **Use cases**
  - Voice and video
  - Time synchronization
  - Email
  - Web
  - File transfer
  - Directory services
  - Remote access
  - Domain name resolution
  - Routing and switching
  - Network address allocation
  - Subscription services

*Note: Be sure to look for newest protocols and implementations.*

**Process/Skill Questions**

- What protocols are used to secure file transfers?
- What protocols are used to secure email?
• How can DNS be secured?

Examining Architecture and Design

Task Number 55

Describe frameworks, best practices, and secure configuration guides and their purposes.

Definition

Description should include the following:

• Industry-standard frameworks and reference architectures
  o Regulatory
  o Non-regulatory
  o National vs. international
  o Industry-specific frameworks
• Benchmarks/secure configuration guides
  o Platform/vendor-specific guides
    ▪ Web server
    ▪ Operating system
    ▪ Application server
    ▪ Network infrastructure devices
  o General purpose guides
• Defense-in-depth/layersed security
  o Vendor diversity
  o Control diversity
    ▪ Administrative
    ▪ Technical
  o User training

Process/Skill Questions

• Why is one layer of security not effective enough?
• Why is there a need for multiple layers?
• Why must vendors provide proprietary configuration guides?
• What is the difference between national and international architectures?

Task Number 56
Implement secure network architecture concepts.

Definition

Implementation should include the following:

- Zones/topologies
  - Demilitarized zone (DMZ)
  - Extranet
  - Intranet
  - Wireless
  - Guest
  - Honeynets
  - Network Address Translation (NAT)
  - Ad hoc
- Segregation/segmentation/isolation
  - Physical
  - Logical (Virtual Local Area Network [VLAN])
  - Virtualization
  - Air gaps
- Tunneling/VPN
  - Site-to-site
  - Remote access
- Security device/technology placement
  - Sensors
  - Collectors
  - Correlation engines
  - Filters
  - Proxies
  - Firewalls
  - VPN concentrators
  - SSL accelerators
  - Load balancers
  - DDoS mitigator
  - Aggregation switches
  - Taps and port mirror
- Software Defined Network (SDN)

Process/Skill Questions

- What is the purpose of an SDN?
- What are the differences between a virtual switch and a physical switch?
- What are the components of a secure network?
Task Number 57

Implement secure systems design.

Definition

Implementation should include the following:

- Hardware/firmware security
  - Full Disk Encryption (FDE)/Self-Encrypting Drive (SED)
  - Trusted Platform Module (TPM)
  - Hardware Security Module (HSM)
  - Unified Extensible Firmware Interface (UEFI)/Basic Input-Output System (BIOS)
  - Secure boot and attestation
  - Supply chain
  - Hardware root of trust
  - Electromagnetic Interference (EMI)/Electro Magnetic Pulse (EMP)
- Operating systems
  - Types
    - Network
    - Server
    - Workstation
    - Appliance
    - Kiosk
    - Mobile operating system (OS)
  - Patch management
  - Disabling unnecessary ports and services
  - Least functionality
  - Secure configurations
  - Trusted operating system
  - Application whitelisting/blacklisting
  - Disable default accounts/passwords
- Peripherals
  - Wireless keyboards
  - Wireless mice
  - Displays
  - WiFi-enabled Micro Secure Digital (MicroSD) cards
  - Printers/Multi-function Devices (MFDs)
  - External storage devices
  - Digital cameras

Process/Skill Questions

- How can you detect a nonsecure systems design?
- What are the differences in security considerations between servers and workstations?
What security considerations are imperative in a BYOD/BYOT environment?

Task Number 58

Explain the importance of secure staging deployment concepts.

Definition

Explanation should include the following:

- Sandboxing
- Environment
  - Development
  - Test
  - Staging
  - Production
- Secure baseline
- Integrity measurement

Process/Skill Questions

- What are the differences in the staging deployment?
- What is the significance of sandboxing?
- How can the establishment of a demilitarized zone (DMZ) in the network improve sandboxing security?

Task Number 59

Explain the security implications of embedded systems.

Definition

Explanation should include the following:

- System Control and Data Acquisition (SCADA)/Industrial Control System (ICS)
- Smart devices/Internet of Things (IoT)
  - Wearable technology
  - Home automation
• Heating, ventilation, and air conditioning (HVAC)
• System on Chip (SoC)
• Real-Time Operating System (RTOS)
• Printers/MFDs
• Camera systems
• Special purpose
  o Medical devices
  o Vehicles
  o Aircraft/unmanned aerial vehicle (UAV)

Process/Skill Questions

• What are the advantages and disadvantages of wearable technology?
• What would happen if home automation or security systems were compromised?
• What degree of remote-control capability can you have with a medically implanted device?

Task Number 60

Summarize secure application development and deployment concepts.

Definition

Summary should include the following:

• Development life-cycle models
  o Waterfall vs. Agile
• Secure DevOps
  o Security automation
  o Continuous integration
  o Baselining
  o Immutable systems
  o Infrastructure as code
• Version control and change management
• Provisioning and de-provisioning
• Secure coding techniques
  o Proper error handling
  o Proper input validation
  o Normalization
  o Stored procedures
  o Code signing
  o Encryption
Obfuscation/camouflage
- Code reuse/dead code
- Server-side vs. client-side execution and validation
- Memory management
- Use of third-party libraries and Software Development Kits (SDKs)
- Data exposure

- Code quality and testing
  - Static code analyzers
  - Dynamic analysis (e.g., fuzzing)
  - Stress testing
  - Sandboxing
  - Model verification

- Compiled vs. runtime code

Process/Skill Questions

- Why is version control and change management critical to secure application development?
- What are secure coding techniques?
- Why are code walk-throughs and code quality assurance testing so important?

Task Number 61

Examine cloud computing concepts.

Definition

Examination should include the following:

- Cloud storage
- Cloud deployment models
  - Software as a Service (SaaS)
  - Platform as a Service (PaaS)
  - Infrastructure as a Service (IaaS)
  - Private
  - Public
  - Hybrid
  - Community
- On-premise vs. hosted vs. cloud
- VDI/Virtual Desktop Environment (VDE)
- Cloud access security broker
- SaaS
Process/Skill Questions

- What are advantages of on-premises vs. hosted?
- How are security threats reduced in a private cloud?
- What services overlap in SaaS, PaaS, and IaaS?

Task Number 62

Outline virtualization concepts.

Definition

Outline should include the following:

- Hypervisor
  - Type I
  - Type II
  - Application cells/containers
- Virtual Machine (VM) sprawl avoidance
- VM escape protection

Process/Skill Questions

- What is a hypervisor?
- How do you maintain the functionality of a VM?
- What system resources are required for a VM?

Task Number 63

Explain how resiliency and automation strategies reduce risk.

Definition

Explanation should include the following:

- Automation/scripting
  - Automated courses of action
  - Continuous monitoring
• Configuration validation
  • Templates
  • Master image
  • Non-persistence
    • Snapshots
    • Revert to known state
    • Rollback to known configuration
    • Live boot media
  • Elasticity
  • Scalability
  • Distributive allocation
  • Redundancy
  • Fault tolerance
  • High availability
  • Redundant Array of Inexpensive Disks (RAID)

Process/Skill Questions

• What is the relationship between redundancy and high availability?
• How does automating courses of action reduce risk?
• Why would an organization find a master image valuable?

Task Number 64

Explain the importance of physical security controls.

Definition

Explanation should include the following:

• Lighting
• Signs
• Fencing/gate/cage
• Security guards
• Alarms
• Safe
• Secure cabinets/enclosures
• Protected distribution/Protected cabling
• Airgap
• Mantrap
• Faraday cage
• Lock types
• Biometrics
• Barricades/bollards
• Tokens/cards
• Environmental controls
  o HVAC
  o Hot and cold aisles
  o Fire suppression
• Cable locks
• Screen filters
• Cameras
• Motion detection
• Logs
• Infrared detection
• Key management

Process/Skill Questions

• To gain access to the environment, which security controls should be used?
• What is the purpose of a Faraday cage?
• What are the security implications of automated environmental controls?

Analyzing Identity and Access Management

Task Number 65

Compare identity and access management concepts.

Definition

Comparison should include the following:

• Identification, authentication, authorization, and accounting (AAA)
• Multifactor authentication
  o Something you are
  o Something you have
  o Something you know
  o Somewhere you are
  o Something you do
• Federation
• Single sign-on
• Transitive trust

Process/Skill Questions

• What is the difference between authentication and authorization?
• What are the elements of multifactor authentication?
• What are the strengths and weaknesses of multi-factor authentication?
• How does the principle of least privilege mitigate the dangers of single sign-on?
• What is the danger of single sign-on?
• Why might a transitive trust domain design create a security concern for shared files?

---

**Task Number 66**

**Install identity and access services.**

**Definition**

Installation should include configuration and the following:

- LDAP
- Kerberos
- Terminal Access Controller Access Control System Plus (TACACS+)
- Challenge Handshake Authentication Protocol (CHAP)
- Password Authentication Protocol (PAP)
- Microsoft CHAP (MSCHAP)
- Remote Authentication Dial-in User Server (RADIUS)
- Security Assertions Markup Language (SAML)
- OpenID Connect
- Open Authorization (OAUTH)
- Shibboleth
- Secure token
- New Technology LAN Manager (NTLM)

**Process/Skill Questions**

- How does a three-way handshake enhance secure communications?
- What is the difference between the TACACS+ system and a server?
- What would happen if a secure router had open authentication enabled for guest accounts?

---

**Task Number 67**

**Implement identity and access management controls.**

**Definition**
Implementation should include the following:

- Access control models
- Physical access control
- Biometric factors
- Tokens
- Certificate-based authentication
- File system security
- Database security

Process/Skill Questions

- What are the implications and limitations of biometric controls?
- What are the various file systems security protocols?

Task Number 68

Differentiate common account management practices.

Definition

Differentiation should include the following:

- Account types
- General account management Concepts
- Account policy enforcements

Process/Skill Questions

- What are the various account types?
- What are some of the privilege accounts?
- What should happen to a person’s account when he/she changes jobs?
- What should happen to a person’s account when he/she is terminated?

Demonstrating Risk Management

Task Number 69

Explain the importance of policies, plans, and procedures related to organizational security.
Definition

Explanation should include the following:

- Standard operating procedure
- Agreement types
  - Business partners agreement (BPA)
  - Service-level agreement (SLA)
  - Interconnection security agreement (ISA)
  - Memorandum of understanding (MOU)/Memorandum of agreement (MOA)
- Personnel management
  - Mandatory vacations
  - Job rotation
  - Separation of duties
  - Clean desk
  - Background checks
  - Exit interviews
  - Role-based awareness training
    - Data owner
    - System administrator
    - System owner
    - User
    - Privileged user
    - Executive user
  - Non-disclosure agreement (NDA)
  - Onboarding
  - Continuing education
  - Acceptable use policy/rules of behavior
  - Adverse actions
- General security policies
  - Social media networks/applications
  - Personal email

Process/Skill Questions

- How can organizational policies affect your job?
- Why are employees required to use their work-assigned email?
- Why is it imperative that different people are aware of policies, plans, and procedures?

Task Number 70

Summarize business impact analysis concepts.
Definition

Summary should include the following:

- Recovery Time Objective (RTO)/Recovery Point Objective (RPO)
- Mean Time Between Failures (MTBF)
- Mean Time to Recover (MTTR)
- Mission-essential functions
- Identification of critical systems
- Single point of failure
- Impact
  - Life
  - Property
  - Safety
  - Finance
  - Reputation
- Privacy impact assessment
- Privacy threshold assessment

Process/Skill Questions

- How has cloud services impacted companies?
- What historical cloud services events have impacted company-based relations?
- What is the difference between MTBF and MTTR?

Task Number 71

Explain risk management processes and concepts.

Definition

Explanation should include the following:

- Threat assessment
  - Environmental
  - Manmade
  - Internal vs. external
- Risk assessment
  - Single Loss Expectancy (SLE)
  - Annualized Loss Expectancy (ALE)
  - Annualized Rate of Occurrence (ARO)
  - Asset value
  - Risk register
- Likelihood of occurrence
- Supply chain assessment
- Impact
- Quantitative
- Qualitative
- Testing
  - Penetration testing authorization
  - Vulnerability testing authorization
- Risk response techniques
  - Accept
  - Transfer
  - Avoid
  - Mitigate
- Change management

**Process/Skill Questions**

- What is the difference between a threat and a risk?
- What is the difference between quantitative and qualitative risk assessment?
- What are the differences between risk response techniques?

---

**Task Number 72**

**Describe appropriate incident response procedures.**

**Definition**

Description should include the following:

- Incident response plan
  - Documented incident types/category definitions
  - Roles and responsibilities
  - Reporting requirements/escalation
  - Cyber-incident response teams
  - Exercise
- Incident response process
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Lessons learned
Process/Skill Questions

- What is the difference between an incident response plan and an incident response process?
- Why is it important to have incident response exercises?
- How does chain of custody apply to the incident response process?

Task Number 73

Summarize basic concepts of forensics.

Definition

Summary should include the following:

- Order of volatility
- Chain of custody
- Legal hold
- Data acquisition
  - Capture system image
  - Network traffic and logs
  - Capture video
  - Record time offset
  - Take hashes
  - Screenshots
  - Witness interviews
- Preservation
- Recovery
- Strategic intelligence/counterintelligence gathering
  - Active logging
- Track man-hours

Process/Skill Questions

- Why is it important to save your volatile information?
- Why are procedures necessary when collecting information?
- What are the legal implications of a failed chain of custody?
Explain disaster recovery and continuity of operation concepts.

Definition

Explanation should include the following:

- Recovery sites
  - Hot site
  - Warm site
  - Cold site
- Order of restoration
- Backup concepts
  - Differential
  - Incremental
  - Snapshots
  - Full
- Geographic considerations
  - Off-site backups
  - Distance
  - Location selection
  - Legal implications
  - Data sovereignty
- Continuity of operation planning
  - Exercises/tabletop
  - After-action reports
  - Failover
  - Alternate processing sites
  - Alternate business practices

Process/Skill Questions

- What are the differences between hot, cold, and warm sites?
- What are the strengths and weaknesses of differential, incremental, and full backups?
- What could happen if a company failed to identify a preferred order of restoration?

Task Number 75

Compare various types of controls.

Definition
Comparison should include the following:

- Deterrent
- Preventive
- Detective
- Corrective
- Compensating
- Technical
- Administrative
- Physical

**Process/Skill Questions**

- What are the differences between the various types of controls?
- How are detective and corrective controls similar and different?
- What is a physical control?

---

**Task Number 76**

**Execute data security and privacy practices.**

**Definition**

Execution should include the following:

- Data destruction and media sanitization
  - Burning
  - Shredding
  - Pulping
  - Pulverizing
  - Degaussing
  - Purging
  - Wiping
- Data sensitivity labeling and handling
  - Confidential
  - Private
  - Public
  - Proprietary
  - Personally identifiable information (PII)
  - Personal health information (PHI)
- Data roles
  - Owner
  - Steward/custodian
Process/Skill Questions

- What are the limitations of the various physical data-destruction practices?
- What are the implications of the different data roles?
- What can happen when company’s policies lead to your personal identity being compromised?

Examining Cryptography and Public Key Infrastructure (PKI)

Task Number 77

Identify the states of the data that needs to be secured.

Definition

Identification should include

- data in transit
- data in use
- data at rest.

Process/Skill Questions

- What are the examples of the different states of data?
- How do the cryptographic needs of different states of data differ from each other?
- What is the primary security concern for data in transit compared to data at rest?

Task Number 78

Explain the three main forms of cryptography.

Definition

Explanation should include the definitions and uses of these three classes of cryptography: symmetric algorithms, asymmetric algorithms, and hashing.
Process/Skill Questions

- What are the primary uses of each of the three forms of cryptography?
- What are the differences between asymmetric and symmetric algorithms?
- What is the purpose of hashing?

Task Number 79

Identify basic concepts of cryptography.

Definition

Identification should include the following:

- Key strength
- Stream vs. block
- Diffusion
- Confusion
- Random/pseudo-random number generation
- Session keys and perfect forward secrecy
- Ephemeral key
- Collision
- Steganography
- Salt, IV, nonce
- Weak/deprecated algorithms
- Key exchange
- Digital signatures
- Obfuscation
- Key stretching
- Implementation vs. algorithm selection
- Security through obscurity

Process/Skill Questions

- How can you prevent two passwords from hashing to the same value?
- What are the factors that make a strong key?
- What is the difference between confusion and obfuscation?
- What are the different methods to exchange a secret key?

Task Number 80
Explain common use cases for cryptography.

Definition

Explanation may include the following:

- Modes of operation
- Low-power devices
- Low latency
- High resiliency
- Supporting confidentiality
- Supporting integrity
- Supporting obfuscation
- Supporting authentication
- Supporting nonrepudiation
- Resource vs. security constraints

Process/Skill Questions

- What are the different modes of operation?
- Which cryptographic technique would you use to support integrity?
- Why must more efficient cryptography methods be implemented for low-power devices?

Task Number 81

Explain algorithms and their basic characteristics in cryptography.

Definition

Explanation should include standard examples for each of the following:

- Symmetric algorithms
- Cipher modes
- Asymmetric algorithms
- Hashing algorithms
- Key-stretching algorithms
- Obfuscation

Process/Skill Questions
• What are the difference between Advanced Encryption Standard (AES) and Digital Encryption Standard (DES)?
• What is the purpose of a key-stretching algorithm?
• What are the strengths and weaknesses of the most common cipher modes?

Task Number 82

Configure wireless security settings in a given scenario.

Definition

Configuration should include the following:

• Cryptographic protocols
  o WiFi Protected Access (WPA)
  o WPA2
  o Counter-Mode/Cipher Block Chaining-Mac Protocol (CCMP)
  o Temporal Key Integrity Protocol (TKIP)

• Authentication protocols
  o Extensible Authentication Protocol (EAP)
  o Protected EAP (PEAP)
  o EAP-FAST
  o EAP-TLS
  o EAP-TTLS
  o Institute of Electrical and Electronic Engineers (IEEE) 802.1x
  o RADIUS Federation

• Methods
  o Pre-shared Key (PSK) vs. Enterprise vs. Open
  o WPS
  o Captive portals

Process/Skill Questions

• What is the difference in keys between WPA and WPA2?
• What is the context in which you would use RADIUS?
• What are the differences among PSK, Enterprise, and Open authentication?

Task Number 83

Implement public key infrastructure in a given scenario.
Definition

Implementation should include the following:

- **Components**
  - Certificate Authority (CA)
  - Intermediate CA
  - Certificate Revocation List (CRL)
  - Online Certificate Status Protocol (OCSP)
  - Certificate Signing Request (CSR)
  - Certificate
  - Public key
  - Private key
  - Object identifiers (OID)

- **Concepts**
  - Online vs. offline CA
  - Stapling
  - Pinning
  - Trust model
  - Key escrow
  - Certificate chaining

- **Types of certificates**
  - Wildcard
  - Subject Alternative Name (SAN)
  - Code signing
  - Self-signed
  - Machine/computer
  - Email
  - User
  - Root
  - Domain validation
  - Extended validation

- **Certificate formats**
  - Distinguished Encoding Rules (DER)
  - Privacy-enhanced Electronic Mail (PEM)
  - Perfect Forward Secrecy (PFX)
  - Certificate (CER)
  - PKCS #12 (P12)
  - P7B

**Process/Skill Questions**

- What are the different formats of standard certificates?
- What is the difference between self-signed and code-signed certificates?
- When a browser claims that a website is not secured, what does this mean?
Task Number 84

Research legal issues in the use of cryptography.

Definition

Research should include examples of import/export controls for different countries.

Process/Skill Questions

• Distinguish U.S. export regulations with another country of your choice.
• Distinguish U.S. import regulations with another country of your choice.
• What is an example of a country that is similar to, and one that is different from, the U.S. in import/export regulations?

Understanding Ethical and Legal Considerations in Cybersecurity

Task Number 85

Summarize the code of ethics by various standards for cybersecurity/computing professionals.

Definition

Summary should include:

• ACM Code of Ethics
• IEEE Code of Ethics
• Information Systems Security Association (ISSA) Code of Ethics

Process/Skill Questions

• What are the differences between any two standard codes of computer ethics, such as IEEE and ACM?
• Why is ethics a topic of study in computing and cybersecurity?
• What department in an enterprise environment is responsible for ensuring compliance with the appropriate code of ethics?
Task Number 86

Identify laws related to intellectual property.

Definition

Identification should include copyright, patent, and trademark laws.

Process/Skill Questions

- What types of digital objects are protected by each of these three laws?
- What are the exceptions to copyright under fair use?
- Why can Coca-Cola’s formula not be copyrighted?

Task Number 87

Summarize the acceptable use policy (AUP) for your school.

Definition

Summary should include examples of behaviors that are prohibited by the AUP.

Process/Skill Questions

- What are the similarities between a white hat agreement and the school AUP?
- What is an example of an allowable activity under the AUP?
- What are the most common prohibited behaviors in a school-based AUP?

Task Number 88

Differentiate between ethics and laws.

Definition

Differentiation should include the following:

- Ethics are the moral principles that guide a person’s conduct.
• Laws are the set of accepted rules and regulations created by appropriate authorities, such as national, state, or local governments.
• Legal issues can include significant privacy and data security concerns, which can open up an organization to potential legal and liability risks.
• Examine the rights and protections for owners of intellectual property.

Process/Skill Questions

• Can ethical violations be punishable by law? Explain.
• What is the distinction between unethical and illegal behaviors?
• How can an organization or individual protect intellectual property?

Task Number 89

Distinguish among types of ethical concerns.

Definition

Distinction should include

• describing ethical and unethical behaviors
• understanding that organizations must balance “reasonable security” with reasonable access.

Process/Skill Questions

• What are the repercussions of unethical behavior in a corporate environment?
• What does an organization use to determine the best balance of reasonable access vs. reasonable security?
• What can lead someone to behave unethically toward an employer?

Task Number 90

Identify laws applicable to cybersecurity.

Definition

Identification should include, but not be limited to

• national laws, regulations, policies, and/or standards
- Privacy Act of 1974
- Electronic Communications Privacy Act of 1986
- Counterfeit Access Device and Computer Fraud and Abuse Act of 1984
- Cyber Security Information Sharing Act of 2015 (CISA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Telecommunications Act of 1996
- Gramm-Leach-Bliley Act
- Family Educational Rights and Privacy Act (FERPA)
- Sarbanes-Oxley Act of 2002
- international laws and standards (e.g., European Union and Information Security Directive).

**Process/Skill Questions**

- What event(s) led to the enactment of the Sarbanes-Oxley Act of 2002?
- What is FERPA? Under FERPA, does the education agency get to determine what education records to create and keep? Explain.
- Do HIPAA security rules apply to information transmitted by non-technological means?

**SOL Correlation by Task**

<table>
<thead>
<tr>
<th>Task</th>
<th>English</th>
<th>History and Social Science</th>
<th>Mathematics</th>
</tr>
</thead>
<tbody>
<tr>
<td>39</td>
<td>11.5, 12.5</td>
<td>VUS.14</td>
<td>COM.16, COM.18</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>11.5, 12.5</td>
<td>VUS.14</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>41</td>
<td>11.5, 12.5</td>
<td>VUS.14</td>
<td>COM.17, COM.18</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>11.5, 11.8, 12.5, 12.8</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
</tbody>
</table>
| 43 | Explain penetration (pen) testing concepts. | English: 11.5, 12.5  
Mathematics: COM.17 |
| 44 | Analyze indicators of compromise for the purpose of determining the type of malware in a given scenario. | English: 11.5, 12.5  
History and Social Science: VUS.14  
Mathematics: COM.16, COM.17, COM.18 |
| 45 | Explore network infrastructure hardware and software-based components that support organizational security. | English: 11.5, 12.5  
History and Social Science: VUS.14 |
| 46 | Explore host hardware- and software-based components that support organizational security. | English: 11.5, 12.5 |
| 47 | Assess the network security posture of an organization in a given scenario. | English: 11.5, 12.5  
History and Social Science: VUS.14 |
| 48 | Assess the host security posture of an organization in a given scenario. | English: 11.5, 12.5  
History and Social Science: VUS.14 |
| 49 | Assess the data security posture of an organization in a given scenario. | English: 11.5, 12.5  
History and Social Science: VUS.14 |
| 50 | Troubleshoot common security issues in a given scenario. | English: 11.5, 12.5  
History and Social Science: VUS.14  
Mathematics: COM.17, COM.18 |
| 51 | Evaluate the output from security technologies. | Mathematics: COM.11 |
| 52 | Describe mobile connection methods and deployment models. | English: 11.5, 12.5  
History and Social Science: VUS.14 |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th>Language</th>
<th>History and Social Science:</th>
<th>Mathematics:</th>
</tr>
</thead>
<tbody>
<tr>
<td>53</td>
<td>Discuss device management and enforcement concepts.</td>
<td>English: 11.5, 12.5</td>
<td>VUS.14</td>
<td></td>
</tr>
<tr>
<td>54</td>
<td>Explain secure protocols and their use cases.</td>
<td>English: 11.5, 12.5</td>
<td>VUS.14</td>
<td>COM.16</td>
</tr>
<tr>
<td>55</td>
<td>Describe frameworks, best practices, and secure configuration</td>
<td>English: 11.5, 12.5</td>
<td>VUS.14</td>
<td></td>
</tr>
<tr>
<td></td>
<td>guides and their purposes.</td>
<td>History and Social Science:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>56</td>
<td>Implement secure network architecture concepts.</td>
<td>History and Social Science:</td>
<td>VUS.14</td>
<td></td>
</tr>
<tr>
<td>57</td>
<td>Implement secure systems design.</td>
<td>History and Social Science:</td>
<td>VUS.14</td>
<td></td>
</tr>
<tr>
<td>58</td>
<td>Explain the importance of secure staging deployment concepts.</td>
<td>English: 11.5, 12.5</td>
<td>VUS.14</td>
<td>GOVT.16, VUS.14</td>
</tr>
<tr>
<td>59</td>
<td>Explain the security implications of embedded systems.</td>
<td>English: 11.5, 12.5</td>
<td>History and Social Science:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>VUS.14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>Summarize secure application development and deployment concepts.</td>
<td>English: 11.5, 12.5</td>
<td>History and Social Science:</td>
<td>COM.10, COM.11, COM.16</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VUS.14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>61</td>
<td>Examine cloud computing concepts.</td>
<td>English: 11.5, 12.5</td>
<td>History and Social Science:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>VUS.14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>62</td>
<td>Outline virtualization concepts.</td>
<td>English: 11.5, 12.5</td>
<td>History and Social Science:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>VUS.14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>63</td>
<td>Explain how resiliency and automation strategies reduce risk.</td>
<td>English: 11.5, 12.5</td>
<td>History and Social Science:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>VUS.14</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>64</strong></td>
<td>Explain the importance of physical security controls.</td>
<td>English: 11.5, 12.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>65</strong></td>
<td>Compare identity and access management concepts.</td>
<td>History and Social Science: VUS.14</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>66</strong></td>
<td>Install identity and access services.</td>
<td>English: 11.5, 12.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>67</strong></td>
<td>Implement identity and access management controls.</td>
<td>English: 11.5, 12.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>68</strong></td>
<td>Differentiate common account management practices.</td>
<td>English: 11.5, 12.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>69</strong></td>
<td>Explain the importance of policies, plans, and procedures related to organizational security.</td>
<td>History and Social Science: VUS.14</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>70</strong></td>
<td>Summarize business impact analysis concepts.</td>
<td>English: 11.5, 12.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>71</strong></td>
<td>Explain risk management processes and concepts.</td>
<td>History and Social Science: VUS.14</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>72</strong></td>
<td>Describe appropriate incident response procedures.</td>
<td>English: 11.5, 12.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>73</strong></td>
<td>Summarize basic concepts of forensics.</td>
<td>English: 11.5, 12.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>74</strong></td>
<td>Explain disaster recovery and continuity of operation concepts.</td>
<td>English: 11.5, 12.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>75</strong></td>
<td>Compare various types of controls.</td>
<td>English: 11.5, 12.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>76</strong></td>
<td>Execute data security and privacy practices.</td>
<td>English: 11.5, 12.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>77</strong></td>
<td>Identify the states of the data that needs to be secured.</td>
<td>History and Social Science: VUS.14</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>78</strong></td>
<td>Explain the three main forms of cryptography.</td>
<td>English: 11.3, 11.5, 12.3, 12.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
|79| Identify basic concepts of cryptography. | History and Social Science: VUS.14  
Mathematics: COM.2, COM.3, COM.4  
English: 11.5, 12.5 |
|80| Explain common use cases for cryptography. | History and Social Science: VUS.14  
English: 11.5, 12.5 |
|81| Explain algorithms and their basic characteristics in cryptography. | History and Social Science: VUS.14  
Mathematics: COM.2, COM.3, COM.4  
English: 11.5, 12.5 |
|82| Configure wireless security settings in a given scenario. | History and Social Science: VUS.14  
English: 11.5, 12.5 |
|83| Implement public key infrastructure in a given scenario. | History and Social Science: VUS.14  
English: 11.5, 12.5 |
|84| Research legal issues in the use of cryptography. | History and Social Science: GOVT.1, VUS.1  
English: 11.5, 11.8, 12.5, 12.8 |
|85| Summarize the code of ethics by various standards for cybersecurity/computing professionals. | History and Social Science: GOVT.16  
English: 11.5, 12.5 |
|86| Identify laws related to intellectual property. | History and Social Science: VUS.1  
English: 11.5, 12.5 |
|87| Summarize the acceptable use policy (AUP) for your school. | History and Social Science: VUS.14  
English: 11.5, 12.5 |
|88| Differentiate between ethics and laws. | History and Social Science: VUS.14  
English: 11.5, 12.5 |
Teacher Resources

CompTIA

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 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.
Appendix: Credentials and Career Cluster Information

Industry Credentials: Only apply to 36-week courses

- Cisco Certified CyberOps Associate Examination
- Cisco Certified DevNet Associate Examination
- Cisco Certified Networking Associate (CCNA) Examination
- Cisco Certified Networking Professional (CCNP) Automation for Cisco Enterprise Solutions Examination
- Cisco Certified Networking Professional (CCNP) Cisco Enterprise Networks Examination
- Cisco Certified Networking Professional (CCNP) Cisco SD-WAN Solutions Examination
- Cisco Certified Networking Professional (CCNP) Designing Enterprise Wireless Networks Examination
- Cisco Certified Networking Professional (CCNP) Enterprise Advanced Routing and Services Examination
- Cisco Certified Networking Professional (CCNP) Enterprise Network Core Technologies Examination
- Cisco Certified Networking Professional (CCNP) Implementing Enterprise Wireless Networks Examination
- College and Work Readiness Assessment (CWRA+)
- Customer Service Examination
- Customer Service Specialist (CSS) Examination
- Cybersecurity Analyst (CSA+) Examination
- National Career Readiness Certificate Assessment
- Network+ Certification Examination
- Security+ Certification Examination
- Workplace Readiness Skills for the Commonwealth Examination

Career Cluster: Information Technology

<table>
<thead>
<tr>
<th>Pathway</th>
<th>Occupations</th>
</tr>
</thead>
</table>
| Information Support and Services| Computer Support Specialist  
Computer Systems Engineer, Architect  
Information Systems Analyst  
Network Systems and Data Communication Analyst  
Systems Analyst |
| Network Systems                 | Computer and Information Systems Administrator  
Computer Operator  
Computer Security Specialist  
Computer Software Engineer  
Computer Support Specialist  
Computer Systems Engineer, Architect  
Database Analyst  
Information Security Analyst  
Network and Computer Systems Administrator  
Network Architect  
Network Systems and Data Communication Analyst  
Systems Analyst  
Telecommunications Equipment Installer, Repairer  
Telecommunications Specialist |
| Programming and Software        | Computer Software Engineer  
Network Systems and Data Communication Analyst |
<table>
<thead>
<tr>
<th>Pathway</th>
<th>Occupations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web and Digital Communications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Computer Support Specialist</td>
</tr>
<tr>
<td></td>
<td>Computer Systems Engineer, Architect</td>
</tr>
<tr>
<td></td>
<td>Systems Analyst</td>
</tr>
</tbody>
</table>