

TestOut[®]

TestOut Security Pro – English 7.0.x

Objective Mappings:

TestOut Security Pro
CompTIA Security+ SY0-601

Contents

This document contains four objective mappings. Click on a mapping to view its contents.

Objective Mapping: LabSim Section to TestOut Security Pro Objective	3
Objective Mapping: TestOut Security Pro Objective to LabSim Section	11
Objective Mapping: LabSim Section to CompTIA SY0-601 Objective.....	14
Objective Mapping: CompTIA SY0-601 Objective to LabSim Section	83

Objective Mapping: LabSim Section to TestOut Security Pro Objective

Section	Title	TestOut Security Pro Objectives
1.0	Introduction	
1.1	Security Overview	
1.2	Defense Planning	
1.3	Using the Simulator	
2.0	Threats, Attacks, and Vulnerabilities	
2.1	Understanding Attacks	
2.2	Malware	3.1 Harden Computer Systems <ul style="list-style-type: none"> • 3.1.2 Configure Anti-virus Protection
2.3	Social Engineering	5.2 Assessment Techniques Assessment Techniques <ul style="list-style-type: none"> • 5.2.2 Identify Social Engineering
2.4	Vulnerability Concerns	
3.0	Physical	
3.1	Physical Threats	2.1 Harden Physical Access <ul style="list-style-type: none"> • 2.1.1 Implement Physical Security
3.2	Device and Network Protection	
3.3	Environmental Controls	
4.0	Networks and Hosts Design and Diagnosis	

4.1	Manageable Network Plan	
4.2	Windows System Hardening	<p>3.1 Harden Computer Systems</p> <ul style="list-style-type: none"> • 3.1.1 Configure File system Inheritance • 3.1.2 Configure Anti-virus Protection • 3.1.3 Configure NTFS Permissions • 3.1.4 Configure Windows Update
4.3	File Server Security	<p>3.1 Harden Computer Systems</p> <ul style="list-style-type: none"> • 3.1.1 Configure File system Inheritance • 3.1.3 Configure NTFS Permissions
4.4	Linux Host Security	
5.0	Devices and Infrastructure	
5.1	Security Appliances	<p>2.1 Harden Physical Access</p> <ul style="list-style-type: none"> • 2.1.2 Install and Configure a Security Appliance • 2.1.4 Create and Configure a Demilitarized Zone (DMZ)
5.2	Demilitarized Zones	<p>2.1 Harden Physical Access</p> <ul style="list-style-type: none"> • 2.1.4 Create and Configure a Demilitarized Zone (DMZ)
5.3	Firewalls	<p>2.1 Harden Physical Access</p> <ul style="list-style-type: none"> • 2.1.3 Install and Configure a Firewall
5.4	Network Address Translation	<p>2.1 Harden Physical Access</p> <ul style="list-style-type: none"> • 2.1.5 Configure Network Address Translation (NAT)
5.5	Virtual Private Networks	<p>2.2 Harden Network Devices</p> <ul style="list-style-type: none"> • 2.2.3 Configure and Access a Virtual Private Network (VPN) • 2.2.4 Harden a Wireless Network

5.6	Web Threat Protection	3.2 Implement Application Defenses <ul style="list-style-type: none"> 3.2.3 Configure Web Application Security 3.2.4 Configure Email Filters and Settings
5.7	Network Access Control	
5.8	Network Threats	
5.9	Network Device Vulnerabilities	2.2 Harden Network Devices <ul style="list-style-type: none"> 2.2.1 Configure and Access a Switch
5.10	Network Applications	
5.11	Switch Security and Attacks	2.1 Harden Physical Access <ul style="list-style-type: none"> 2.1.1 Implement Physical Security 2.2 Harden Network Devices <ul style="list-style-type: none"> 2.2.1 Configure and Access a Switch
5.12	Using VLANs	2.2 Harden Network Devices <ul style="list-style-type: none"> 2.2.7 Create and Connect to a Virtual Local Area Network (VLAN)
5.13	Router Security	2.2 Harden Network Devices <ul style="list-style-type: none"> 2.2.5 Configure Router Security
6.0	Identity, Access, and Account Management	
6.1	Access Control Models	
6.2	Authentication	
6.3	Authorization	
6.4	Windows User Management	

6.5	Active Directory Overview	<p>1.1 Manage Identity</p> <ul style="list-style-type: none"> • 1.1.1 Manage Windows Local and Domain Users and Groups • 1.1.3 Manage Active Directory OUs <p>1.2 Harden Authentication</p> <ul style="list-style-type: none"> • 1.2.5 Configure and Link Group Policy Objects (GPO)
6.6	Hardening Authentication	<p>1.2 Harden Authentication</p> <ul style="list-style-type: none"> • 1.2.1 Configure Account Policies • 1.2.3 Secure Default and local accounts • 1.2.4 Enforce User Account Control (UAC) • 1.2.5 Configure and Link Group Policy Objects (GPO)
6.7	Linux Users	<p>1.1 Manage Identity</p> <ul style="list-style-type: none"> • 1.1.2 Manage Linux Users and Groups <p>1.2 Harden Authentication</p> <ul style="list-style-type: none"> • 1.2.2 Manage account password
6.8	Linux Groups	<p>1.1 Manage Identity</p> <ul style="list-style-type: none"> • 1.1.2 Manage Linux Users and Groups
6.9	Remote Access	
6.10	Network Authentication	<p>1.2 Harden Authentication</p> <ul style="list-style-type: none"> • 1.2.5 Configure and Link Group Policy Objects (GPO)

7.0	Cryptography and PKI	
7.1	Cryptography	4.2 Implement Encryption Technologies <ul style="list-style-type: none"> • 4.2.1 Encrypt Data Communications
7.2	Cryptography Implementations	
7.3	Hashing	4.2 Implement Encryption Technologies <ul style="list-style-type: none"> • 4.2.1 Encrypt Data Communications
7.4	File Encryption	4.2 Implement Encryption Technologies <ul style="list-style-type: none"> • 4.2.2 Encrypt Files
7.5	Public Key Infrastructure	4.2 Implement Encryption Technologies <ul style="list-style-type: none"> • 4.2.3 Manage Certificates
8.0	Wireless Threats	
8.1	Wireless Overview	2.2 Harden Network Devices <ul style="list-style-type: none"> • 2.2.2 Configure and Access a Wireless Network
8.2	Wireless Attacks	2.2 Harden Network Devices <ul style="list-style-type: none"> • 2.2.2 Configure and Access a Wireless Network
8.3	Wireless Defenses	2.2 Harden Network Devices <ul style="list-style-type: none"> • 2.2.4 Harden a Wireless Network
9.0	Virtualization, Cloud Security, and Securing Mobile Devices	
9.1	Host Virtualization	3.3 Implement Virtualization <ul style="list-style-type: none"> • 3.3.1 Create Virtual Machines

9.2	Virtual Networking	3.3 Implement Virtualization <ul style="list-style-type: none">• 3.3.2 Create Virtual Switches
9.3	Software-Defined Networking	
9.4	Cloud Services	
9.5	Cloud Security	
9.6	Mobile Devices	
9.7	Mobile Device Management	
9.8	BYOD Security	2.2 Harden Network Devices <ul style="list-style-type: none">• 2.2.6 Bring Your Own Device (BYOD) Security
9.9	Embedded and Specialized Systems	
10.0	Securing Data and Applications	
10.1	Data Transmission Security	3.2 Implement Application Defenses <ul style="list-style-type: none">• 3.2.3 Configure Web Application Security
10.2	Data Loss Prevention	
10.3	Web Application Attacks	3.2 Implement Application Defenses <ul style="list-style-type: none">• 3.2.3 Configure Web Application Security
10.4	Application Development and Security	3.2 Implement Application Defenses <ul style="list-style-type: none">• 3.2.1 Implement Application Whitelisting• 3.2.2 Implement Data Execution Prevention (DEP)
11.0	Security Assessments	
11.1	Penetration Testing	
11.2	Monitoring and Reconnaissance	

11.3	Intrusion Detection	5.2 Assessment Techniques Assessment Techniques <ul style="list-style-type: none"> 5.2.1 Implement Intrusion Detection
11.4	Security Assessment Techniques	5.2 Assessment Techniques Assessment Techniques <ul style="list-style-type: none"> 5.2.3 Scan for Vulnerabilities
11.5	Protocol Analyzers	
11.6	Analyzing Network Attacks	5.2 Assessment Techniques Assessment Techniques <ul style="list-style-type: none"> 5.2.4 Analyze Network Attacks
11.7	Password Attacks	5.2 Assessment Techniques Assessment Techniques <ul style="list-style-type: none"> 5.2.5 Analyze Password Attacks
12.0	Incident Response, Forensics, and Recovery	
12.1	Incident Response	
12.2	Mitigation of an Incident	
12.3	Log Management	
12.4	Windows Logging	
12.5	Digital Forensics	
12.6	File and Packet Manipulation	
12.7	Redundancy	4.1 Protect and Maintain Data files <ul style="list-style-type: none"> 4.1.1 Perform data backups and recovery
12.8	Backup and Restore	4.1 Protect and Maintain Data files <ul style="list-style-type: none"> 4.1.1 Perform data backups and recovery

13.0	Risk Management	
13.1	Organizational Security Policies	
13.2	Risk Management	
13.3	Email	3.2 Implement Application Defenses <ul style="list-style-type: none"> • 3.2.4 Configure Email Filters and Settings
14.0	Governance and Compliance	
14.1	Audits	5.1 Implement Logging and Auditing <ul style="list-style-type: none"> • 5.1.1 Configure Advanced Audit Policy • 5.1.2 Enable Device Logs
14.2	Controls and Frameworks	
14.3	Sensitive Data and Privacy	
A.0	TestOut Security Pro - Practice Exams	
A.1	Prepare for TestOut Security Pro Certification	
A.2	TestOut Security Pro Domain Review	
B.0	CompTIA Security+ SY0-601 - Practice Exams	
B.1	Prepare for CompTIA Security+ SY0-601 Certification	
B.2	CompTIA Security+ Domain Review (20 Questions)	
B.3	CompTIA Security+ Domain Review (All Questions)	

Objective Mapping: TestOut Security Pro Objective to LabSim Section

#	Domain	Module.Section
1.0	Identity Management and Authentication	
1.1	Manage Identity 1.1.1 Manage Windows Local and Domain Users and Groups 1.1.2 Manage Linux Users and Groups 1.1.3 Manage Active Directory OUs	6.5, 6.7, 6.8
1.2	Harden Authentication 1.2.1 Configure Account Policies 1.2.2 Manage account password 1.2.3 Secure Default and local accounts 1.2.4 Enforce User Account Control (UAC) 1.2.5 Configure and Link Group Policy Objects (GPO)	6.5, 6.6, 6.7, 6.10
2.0	Physical and Network Security	
2.1	Harden Physical Access 2.1.1 Implement Physical Security 2.1.2 Install and Configure a Security Appliance 2.1.3 Install and Configure a Firewall 2.1.4 Create and Configure a Demilitarized Zone (DMZ) 2.1.5 Configure Network Address Translation (NAT)	3.1 5.1, 5.2, 5.3, 5.4, 5.11
2.2	Harden Network Devices 2.2.1 Configure and Access a Switch 2.2.2 Configure and Access a Wireless Network 2.2.3 Configure and Access a Virtual Private Network (VPN)	5.5, 5.9, 5.11, 5.12, 5.13 8.1, 8.2, 8.3 9.8

	<ul style="list-style-type: none"> 2.2.4 Harden a Wireless Network 2.2.5 Configure Router Security 2.2.6 Bring Your Own Device (BYOD) Security 2.2.7 Create and Connect to a Virtual Local Area Network (VLAN) 	
3.0	Host and Application Defense	
3.1	<p>Harden Computer Systems</p> <ul style="list-style-type: none"> 3.1.1 Configure File system Inheritance 3.1.2 Configure Anti-virus Protection 3.1.3 Configure NTFS Permissions 3.1.4 Configure Windows Update 	<p>2.2 4.2, 4.3</p>
3.2	<p>Implement Application Defenses</p> <ul style="list-style-type: none"> 3.2.1 Implement Application Whitelisting 3.2.2 Implement Data Execution Prevention (DEP) 3.2.3 Configure Web Application Security 3.2.4 Configure Email Filters and Settings 3.2.5 Configure Browser Settings 	<p>5.6 10.1, 10.3, 10.4 13.3</p>
3.3	<p>Implement Virtualization</p> <ul style="list-style-type: none"> 3.3.1 Create Virtual Machines 3.3.2 Create Virtual Switches 	<p>9.1, 9.2</p>
4.0	Data Security	
4.1	<p>Protect and Maintain Data files</p> <ul style="list-style-type: none"> 4.1.1 Perform data backups and recovery 4.1.2 Implement redundancy 	<p>12.7, 12.8</p>

4.2	<p>Implement Encryption Technologies</p> <p>4.2.1 Encrypt Data Communications 4.2.2 Encrypt Files 4.2.3 Manage Certificates</p>	7.1, 7.3, 7.4, 7.5
5.0	Audit and Security Assessment	
5.1	<p>Implement Logging and Auditing</p> <p>5.1.1 Configure Advanced Audit Policy 5.1.2 Enable Device Logs</p>	14.1
5.2 Assessment Techniques	<p>Assessment Techniques</p> <p>5.2.1 Implement Intrusion Detection 5.2.2 Identify Social Engineering 5.2.3 Scan for Vulnerabilities 5.2.4 Analyze Network Attacks 5.2.5 Analyze Password Attacks</p>	2.3 11.3, 11.4, 11.6, 11.7

Objective Mapping: LabSim Section to CompTIA SY0-601 Objective

Section	Title	Objectives
1.0	Introduction	
1.1	Security Overview	<p>1.5 Explain different threat actors, vectors, and intelligence sources.</p> <ul style="list-style-type: none"> • 1.5.1 - Actors and threats <ul style="list-style-type: none"> 1.5.1.2 - Insider threats • 1.5.2 - Attributes of actors <ul style="list-style-type: none"> 1.5.2.1 - Internal/external • 1.5.5 - Research sources <ul style="list-style-type: none"> 1.5.5.8 - Threat feeds <p>1.6 Explain the security concerns associated with various types of vulnerabilities.</p> <ul style="list-style-type: none"> • 1.6.1 - Cloud-based vs. on-premises vulnerabilities <p>2.8 Summarize the basics of cryptographic concepts.</p> <ul style="list-style-type: none"> • 2.8.19 - Common use cases <ul style="list-style-type: none"> 2.8.19.8 - Supporting non-repudiation <p>4.5 Explain the key aspects of digital forensics.</p> <ul style="list-style-type: none"> • 4.5.4 - Integrity

		<p>4.5.4.1 - Hashing</p> <p>5.4 Summarize risk management processes and concepts.</p> <ul style="list-style-type: none"> • 5.4.1 - Risk types <p>5.4.1.2 - Internal</p> <p>5.5 Explain privacy and sensitive data concepts in relation to security.</p> <ul style="list-style-type: none"> • 5.5.3 - Data types <p>5.5.3.1.4 - Classifications - Confidential</p>
1.2	Defense Planning	<p>1.1 Compare and contrast different types of social engineering techniques.</p> <ul style="list-style-type: none"> • 1.1.1 - Phishing <p>1.5 Explain different threat actors, vectors, and intelligence sources.</p> <ul style="list-style-type: none"> • 1.5.1 - Actors and threats <p>1.5.1.2 - Insider threats</p> <p>1.8 Explain the techniques used in penetration testing.</p> <ul style="list-style-type: none"> • 1.8.1 - Penetration testing <p>3.2 Given a scenario, implement host or application security solutions.</p> <ul style="list-style-type: none"> • 3.2.4 - Application security

		<p>3.4 Given a scenario, install and configure wireless security settings.</p> <ul style="list-style-type: none"> • 3.4.1 - Cryptographic protocols <p>4.4 Given an incident, apply mitigation techniques or controls to secure an environment.</p> <ul style="list-style-type: none"> • 4.4.2 - Configuration changes <ul style="list-style-type: none"> 4.4.2.1 - Firewall rules <p>5.3 Explain the importance of policies to organizational security.</p> <ul style="list-style-type: none"> • 5.3.1 - Personnel <ul style="list-style-type: none"> 5.3.1.1 - Acceptable use policy 5.3.1.6 - Clean desk space
1.3	Using the Simulator	
2.0	Threats, Attacks, and Vulnerabilities	
2.1	Understanding Attacks	<p>1.1 Compare and contrast different types of social engineering techniques.</p> <ul style="list-style-type: none"> • 1.1.17 - Reconnaissance <p>1.5 Explain different threat actors, vectors, and intelligence sources.</p> <ul style="list-style-type: none"> • 1.5.1 - Actors and threats <ul style="list-style-type: none"> 1.5.1.1 - Advanced persistent threat (APT) 1.5.1.2 - Insider threats 1.5.1.3 - State actors 1.5.1.4 - Hacktivists 1.5.1.5 - Script kiddies 1.5.1.6 - Criminal syndicates

		<ul style="list-style-type: none"> 1.5.1.7.1 - Hackers - White hat 1.5.1.7.2 - Hackers - Black hat 1.5.1.7.3 - Hackers - Gray hat 1.5.1.8 - Shadow IT 1.5.1.9 - Competitors <ul style="list-style-type: none"> • 1.5.2 - Attributes of actors <ul style="list-style-type: none"> 1.5.2.1 - Internal/external 1.5.2.2 - Level of sophistication/capability 1.5.2.3 - Resources/funding 1.5.2.4 - Intent/motivation <ul style="list-style-type: none"> • 1.5.4 - Threat intelligence sources <ul style="list-style-type: none"> 1.5.4.1 - Open source intelligence (OSINT) <p>5.3 Explain the importance of policies to organizational security.</p> <ul style="list-style-type: none"> • 5.3.1 - Personnel <ul style="list-style-type: none"> 5.3.1.5 - Least privilege
2.2	Malware	<p>1.2 Given a scenario, analyze potential indicators to determine the type of attack.</p> <ul style="list-style-type: none"> • 1.2.1 - Malware <ul style="list-style-type: none"> 1.2.1.1 - Ransomware 1.2.1.2 - Trojans 1.2.1.3 - Worms 1.2.1.4 - Potentially unwanted programs (PUPs) 1.2.1.5 - Fileless virus 1.2.1.6 - Command and control 1.2.1.7 - Bots 1.2.1.8 - Crypto malware 1.2.1.9 - Logic bombs

		<p>1.2.1.10 - Spyware 1.2.1.11 - Keyloggers 1.2.1.12 - Remote access Trojan (RAT) 1.2.1.13 - Rootkit 1.2.1.14 - Backdoor</p>
2.3	Social Engineering	<p>1.1 Compare and contrast different types of social engineering techniques.</p> <ul style="list-style-type: none"> • 1.1.1 - Phishing • 1.1.2 - Smishing • 1.1.3 - Vishing • 1.1.4 - Spam • 1.1.5 - Spam over Internet messaging (SPIM) • 1.1.6 - Spear phishing • 1.1.7 - Dumpster diving • 1.1.8 - Shoulder surfing • 1.1.9 - Pharming • 1.1.10 - Tailgating • 1.1.11 - Eliciting information • 1.1.12 - Whaling • 1.1.13 - Prepending • 1.1.14 - Identity fraud • 1.1.15 - Invoice scams • 1.1.16 - Credential harvesting • 1.1.17 - Reconnaissance • 1.1.18 - Hoax • 1.1.19 - Impersonation • 1.1.20 - Watering hole attack • 1.1.21 - Typo squatting • 1.1.22 - Influence campaigns <p style="margin-left: 40px;">1.1.22.1 - Hybrid warfare 1.1.22.2 - Social media</p> <ul style="list-style-type: none"> • 1.1.23 - Principles (reasons for effectiveness)

		<p>1.1.23.1 - Authority 1.1.23.2 - Intimidation 1.1.23.3 - Consensus 1.1.23.4 - Scarcity 1.1.23.5 - Familiarity 1.1.23.6 - Trust 1.1.23.7 - Urgency</p> <p>1.5 Explain different threat actors, vectors, and intelligence sources.</p> <ul style="list-style-type: none"> 1.5.1 - Actors and threats <p>1.5.1.2 - Insider threats 1.5.1.4 - Hacktivists 1.5.1.5 - Script kiddies</p>
2.4	Vulnerability Concerns	<p>1.2 Given a scenario, analyze potential indicators to determine the type of attack.</p> <ul style="list-style-type: none"> 1.2.5 - Supply-chain attacks <p>1.3 Given a scenario, analyze potential indicators associated with application attacks.</p> <ul style="list-style-type: none"> 1.3.1 - Privilege escalation <p>1.6 Explain the security concerns associated with various types of vulnerabilities.</p> <ul style="list-style-type: none"> 1.6.1 - Cloud-based vs. on-premises vulnerabilities 1.6.2 - Zero-day 1.6.3 - Weak configurations <p>1.6.3.1 - Open permissions 1.6.3.2 - Unsecured root accounts 1.6.3.3 - Errors 1.6.3.4 - Weak encryption 1.6.3.5 - Unsecure protocols</p>

		<p>1.6.3.6 - Default settings 1.6.3.7 - Open ports and services</p> <ul style="list-style-type: none"> • 1.6.4 - Third-party risks <ul style="list-style-type: none"> 1.6.4.1.1 - Vendor management - System integration 1.6.4.1.2 - Vendor management - Lack of vendor support 1.6.4.2 - Supply chain 1.6.4.3 - Outsourced code development 1.6.4.4 - Data storage • 1.6.5 - Improper or weak patch management <ul style="list-style-type: none"> 1.6.5.1 - Firmware 1.6.5.2 - Operating system (OS) 1.6.5.3 - Applications • 1.6.6 - Legacy platforms • 1.6.6 - Impacts <ul style="list-style-type: none"> 1.6.6.1 - Data loss 1.6.6.2 - Data breaches 1.6.6.3 - Data exfiltration 1.6.6.4 - Identity theft 1.6.6.5 - Financial 1.6.6.6 - Reputation 1.6.6.7 - Availability loss <p>5.1 Compare and contrast various types of controls.</p> <ul style="list-style-type: none"> • 5.1.2 - Control type <ul style="list-style-type: none"> 5.1.2.6 - Physical <p>5.4 Summarize risk management processes and concepts.</p>
--	--	---

		<ul style="list-style-type: none"> • 5.4.3 - Risk analysis <p>5.4.3.6 - Inherent risk</p>
3.0	Physical	
3.1	Physical Threats	<p>2.7 Explain the importance of physical security controls.</p> <ul style="list-style-type: none"> • 2.7.1 - Bollards/barricades • 2.7.2 - Mantraps • 2.7.3 - Badges • 2.7.4 - Alarms • 2.7.5 - Signage • 2.7.6 - Cameras <p>2.7.6.1 - Motion recognition 2.7.6.2 - Object detection</p> <ul style="list-style-type: none"> • 2.7.7 - Closed-circuit television (CCTV) • 2.7.8 - Industrial camouflage • 2.7.9 - Personnel <p>2.7.9.1 - Guards 2.7.9.2 - Robot sentries 2.7.9.3 - Reception 2.7.9.4 - Two-person integrity/control</p> <ul style="list-style-type: none"> • 2.7.10 - Locks <p>2.7.10.1 - Biometrics</p> <ul style="list-style-type: none"> • 2.7.11 - USB data blocker • 2.7.12 - Lighting • 2.7.13 - Fencing • 2.7.16 - Drones/UAV • 2.7.17 - Visitor logs

		<ul style="list-style-type: none"> • 2.7.18 - Faraday cages • 2.7.19 - Air gap • 2.7.20 - Demilitarized zone (DMZ) <p>3.7 Given a scenario, implement identity and account management controls.</p> <ul style="list-style-type: none"> • 3.7.1 - Identity <ul style="list-style-type: none"> 3.7.1.6 - Smart cards <p>4.2 Summarize the importance of policies, processes, and procedures for incident response.</p> <ul style="list-style-type: none"> • 4.2.2 - Incident response process <ul style="list-style-type: none"> 4.2.2.5 - Recovery
3.2	Device and Network Protection	<p>1.2 Given a scenario, analyze potential indicators to determine the type of attack.</p> <ul style="list-style-type: none"> • 1.2.3 - Physical attacks <ul style="list-style-type: none"> 1.2.3.1 - Malicious universal serial bus (USB) cable 1.2.3.2 - Malicious flash drive 1.2.3.3 - Card cloning 1.2.3.4 - Skimming <p>2.7 Explain the importance of physical security controls.</p> <ul style="list-style-type: none"> • 2.7.10 - Locks <ul style="list-style-type: none"> 2.7.10.1 - Biometrics 2.7.10.2 - Electronic 2.7.10.3 - Physical 2.7.10.4 - Cable locks

		<ul style="list-style-type: none"> • 2.7.11 - USB data blocker • 2.7.15 - Sensors <ul style="list-style-type: none"> 2.7.15.1 - Motion detection 2.7.15.2 - Noise detection 2.7.15.3 - Proximity reader 2.7.15.4 - Moisture detection 2.7.15.5 - Cards 2.7.15.6 - Temperature • 2.7.18 - Faraday cages • 2.7.19 - Air gap • 2.7.20 - Demilitarized zone (DMZ) • 2.7.21 - Protected cable distribution • 2.7.23 - Secure data destruction
3.3	Environmental Controls	<p>2.5 Given a scenario, implement cybersecurity resilience.</p> <ul style="list-style-type: none"> • 2.5.1 - Redundancy <ul style="list-style-type: none"> 2.5.1.4.1 - Power - Uninterruptible power supply (UPS) <p>2.7 Explain the importance of physical security controls.</p> <ul style="list-style-type: none"> • 2.7.14 - Fire suppression • 2.7.15 - Sensors <ul style="list-style-type: none"> 2.7.15.2 - Noise detection 2.7.15.4 - Moisture detection 2.7.15.6 - Temperature • 2.7.22 - Secure areas <ul style="list-style-type: none"> 2.7.22.1 - Air gap 2.7.22.2 - Vault 2.7.22.3 - Safe 2.7.22.4 - Hot aisle

		2.7.22.5 - Cold aisle
4.0	Networks and Hosts Design and Diagnosis	
4.1	Manageable Network Plan	<p>1.6 Explain the security concerns associated with various types of vulnerabilities.</p> <ul style="list-style-type: none"> • 1.6.5 - Improper or weak patch management <ul style="list-style-type: none"> 1.6.5.1 - Firmware 1.6.5.2 - Operating system (OS) 1.6.5.3 - Applications <p>2.1 Explain the importance of security concepts in an enterprise environment.</p> <ul style="list-style-type: none"> • 2.1.1 - Configuration management <ul style="list-style-type: none"> 2.1.1.1 - Diagrams 2.1.1.2 - Baseline configuration 2.1.1.3 - Standard naming conventions 2.1.1.4 - Internet protocol (IP) schema • 2.1.5 - Geographical considerations <p>3.1 Given a scenario, implement secure protocols.</p> <ul style="list-style-type: none"> • 3.1.1 - Protocols <ul style="list-style-type: none"> 3.1.1.3 - SSH <p>3.2 Given a scenario, implement host or application security solutions.</p> <ul style="list-style-type: none"> • 3.2.5 - Hardening

		<p>3.2.5.5.2 - Patch management - Auto-update</p> <p>3.3 Given a scenario, implement secure network designs.</p> <ul style="list-style-type: none"> • 3.3.2 - Network segmentation <p>3.3.2.1 -Virtual local area network (VLAN)</p> <p>3.7 Given a scenario, implement identity and account management controls.</p> <ul style="list-style-type: none"> • 3.7.3 - Account policies <p>3.7.3.10 - Access policies</p> <p>4.5 Explain the key aspects of digital forensics.</p> <ul style="list-style-type: none"> • 4.5.1 - Documentation/evidence
4.2	Windows System Hardening	<p>1.2 Given a scenario, analyze potential indicators to determine the type of attack.</p> <ul style="list-style-type: none"> • 1.2.1 - Malware <p>1.2.1.1 - Ransomware 1.2.1.2 - Trojans 1.2.1.3 - Worms 1.2.1.4 - Potentially unwanted programs (PUPs) 1.2.1.5 - Fileless virus 1.2.1.6 - Command and control 1.2.1.7 - Bots 1.2.1.8 - Crypto malware 1.2.1.9 - Logic bombs 1.2.1.10 - Spyware 1.2.1.11 - Keyloggers 1.2.1.12 - Remote access Trojan (RAT) 1.2.1.13 - Rootkit</p>

		<p>1.2.1.14 - Backdoor</p> <p>1.6 Explain the security concerns associated with various types of vulnerabilities.</p> <ul style="list-style-type: none"> • 1.6.3 - Weak configurations <ul style="list-style-type: none"> 1.6.3.6 - Default settings <p>2.1 Explain the importance of security concepts in an enterprise environment.</p> <ul style="list-style-type: none"> • 2.1.1 - Configuration management <ul style="list-style-type: none"> 2.1.1.2 - Baseline configuration <p>2.4 Summarize authentication and authorization design concepts.</p> <ul style="list-style-type: none"> • 2.4.3 - Multifactor authentication (MFA) factors and attributes <p>3.2 Given a scenario, implement host or application security solutions.</p> <ul style="list-style-type: none"> • 3.2.1 - Endpoint protection <ul style="list-style-type: none"> 3.2.1.1 - Antivirus 3.2.1.2 - Anti-malware 3.2.1.3 - Endpoint detection and response (EDR) 3.2.1.4 - DLP 3.2.1.5 - Next-generation firewall 3.2.1.6 - Host intrusion prevention system (HIPS) 3.2.1.7 - Host intrusion detection system (HIDS) 3.2.1.9 - Host-based firewall • 3.2.2 - Boot integrity <ul style="list-style-type: none"> 3.2.2.1 - Boot security/Unified Extensible Firmware Interface (UEFI) 3.2.2.2 - Measured boot
--	--	---

		<p>3.2.2.3 - Boot attestation</p> <ul style="list-style-type: none"> 3.2.5 - Hardening <ul style="list-style-type: none"> 3.2.5.1 - Open ports and services 3.2.5.2 - Registry 3.2.5.3 - Disk encryption 3.2.5.4 - OS 3.2.5.5.1 - Patch management - Third-party updates 3.2.5.5.2 - Patch management - Auto-update 3.2.6 - Self-encrypting drive (SED)/full disk encryption (FDE) <ul style="list-style-type: none"> 3.2.6.1 - Opal 3.2.7 - Hardware root of trust 3.2.8 - Trusted Platform Module (TPM) 3.2.9 - Sandboxing <p>3.3 Given a scenario, implement secure network designs.</p> <ul style="list-style-type: none"> 3.3.15 - Monitoring services 3.3.16 - File integrity monitors
4.3	File Server Security	<p>1.6 Explain the security concerns associated with various types of vulnerabilities.</p> <ul style="list-style-type: none"> 1.6.3 - Weak configurations <ul style="list-style-type: none"> 1.6.3.1 - Open permissions <p>3.1 Given a scenario, implement secure protocols.</p> <ul style="list-style-type: none"> 3.1.1 - Protocols <ul style="list-style-type: none"> 3.1.1.3 - SSH 3.1.1.7 - File transfer protocol, secure (FTPS)

		<p>3.1.1.10 - Hypertext transfer protocol over SSL/TLS (HTTPS)</p> <p>3.3 Given a scenario, implement secure network designs.</p> <ul style="list-style-type: none"> • 3.3.2 - Network segmentation <ul style="list-style-type: none"> 3.3.2.2 -DMZ • 3.3.9 - Access control list (ACL) <p>3.6 Given a scenario, apply cybersecurity solutions to the cloud.</p> <ul style="list-style-type: none"> • 3.6.1 - Cloud security controls <ul style="list-style-type: none"> 3.6.1.5.1 - Storage - Permissions <p>3.8 Given a scenario, implement authentication and authorization solutions.</p> <ul style="list-style-type: none"> • 3.8.3 - Access control schemes <ul style="list-style-type: none"> 3.8.3.8 - Filesystem permissions
4.4	Linux Host Security	<p>1.6 Explain the security concerns associated with various types of vulnerabilities.</p> <ul style="list-style-type: none"> • 1.6.3 - Weak configurations <ul style="list-style-type: none"> 1.6.3.1 - Open permissions 1.6.3.2 - Unsecured root accounts 1.6.3.3 - Errors 1.6.3.4 - Weak encryption 1.6.3.5 - Unsecure protocols 1.6.3.6 - Default settings 1.6.3.7 - Open ports and services

		<p>3.2 Given a scenario, implement host or application security solutions.</p> <ul style="list-style-type: none"> • 3.2.1 - Endpoint protection <ul style="list-style-type: none"> 3.2.1.9 - Host-based firewall • 3.2.5 - Hardening <ul style="list-style-type: none"> 3.2.5.1 - Open ports and services <p>3.3 Given a scenario, implement secure network designs.</p> <ul style="list-style-type: none"> • 3.3.10 - Route security <p>4.1 Given a scenario, use the appropriate tool to assess organizational security.</p> <ul style="list-style-type: none"> • 4.1.1 - Network reconnaissance and discovery <ul style="list-style-type: none"> 4.1.1.4 - nmap 4.1.1.7 - netstat
5.0	Devices and Infrastructure	
5.1	Security Appliances	<p>2.1 Explain the importance of security concepts in an enterprise environment.</p> <ul style="list-style-type: none"> • 2.1.12 - Deception and disruption <ul style="list-style-type: none"> 2.1.12.1 - Honeypots 2.1.12.2 - Honeyfiles 2.1.12.3 - Honeynets <p>3.3 Given a scenario, implement secure network designs.</p> <ul style="list-style-type: none"> • 3.3.2 - Network segmentation

		<p>3.3.2.2 -DMZ 3.3.2.4 -Extranet 3.3.2.5 -Intranet</p> <ul style="list-style-type: none"> • 3.3.5 - Network access control (NAC) • 3.3.8 - Network appliances <p>3.3.8.2.1 - Proxy servers - Forward 3.3.8.2.2 - Proxy servers - Reverse</p> <ul style="list-style-type: none"> • 3.3.11 - Quality of service (QoS) <p>4.4 Given an incident, apply mitigation techniques or controls to secure an environment.</p> <ul style="list-style-type: none"> • 4.4.2 - Configuration changes <p>4.4.2.4 - Content filter/URL filter</p>
5.2	Demilitarized Zones	<p>2.7 Explain the importance of physical security controls.</p> <ul style="list-style-type: none"> • 2.7.20 - Demilitarized zone (DMZ) <p>3.3 Given a scenario, implement secure network designs.</p> <ul style="list-style-type: none"> • 3.3.2 - Network segmentation <p>3.3.2.2 -DMZ</p> <ul style="list-style-type: none"> • 3.3.3 - Virtual private network (VPN)
5.3	Firewalls	<p>3.2 Given a scenario, implement host or application security solutions.</p> <ul style="list-style-type: none"> • 3.2.1 - Endpoint protection

		<p>3.2.1.9 - Host-based firewall</p> <ul style="list-style-type: none"> 3.2.5 - Hardening <ul style="list-style-type: none"> 3.2.5.1 - Open ports and services <p>3.3 Given a scenario, implement secure network designs.</p> <ul style="list-style-type: none"> 3.3.8 - Network appliances <ul style="list-style-type: none"> 3.3.8.7.1 - Firewalls - Web application firewall (WAF) 3.3.8.7.3 - Firewalls - Stateful 3.3.8.7.4 - Firewalls - Stateless 3.3.8.7.7 - Firewalls - Content/URL filter 3.3.8.7.9 - Firewalls - Hardware vs. software 3.3.8.7.10 - Firewalls - Appliance vs. host-based vs. virtual 3.3.9 - Access control list (ACL)
5.4	Network Address Translation	<p>3.3 Given a scenario, implement secure network designs.</p> <ul style="list-style-type: none"> 3.3.8 - Network appliances <ul style="list-style-type: none"> 3.3.8.7.6 - Firewalls - Network address translation (NAT) gateway
5.5	Virtual Private Networks	<p>3.3 Given a scenario, implement secure network designs.</p> <ul style="list-style-type: none"> 3.3.3 - Virtual private network (VPN) <ul style="list-style-type: none"> 3.3.3.1 - Always on 3.3.3.2 - Split tunnel vs. full tunnel 3.3.3.3 - Remote access vs. site-to-site 3.3.3.4 - IPsec 3.3.3.5 - SSL/TLS

		3.3.3.7 - Layer 2 tunneling protocol (L2TP)
5.6	Web Threat Protection	<p>1.1 Compare and contrast different types of social engineering techniques.</p> <ul style="list-style-type: none"> • 1.1.1 - Phishing • 1.1.4 - Spam <p>2.1 Explain the importance of security concepts in an enterprise environment.</p> <ul style="list-style-type: none"> • 2.1.3 - Data protection <ul style="list-style-type: none"> 2.1.3.3 - Encryption <p>3.3 Given a scenario, implement secure network designs.</p> <ul style="list-style-type: none"> • 3.3.8 - Network appliances <ul style="list-style-type: none"> 3.3.8.2.1 - Proxy servers - Forward <p>4.4 Given an incident, apply mitigation techniques or controls to secure an environment.</p> <ul style="list-style-type: none"> • 4.4.2 - Configuration changes <ul style="list-style-type: none"> 4.4.2.1 - Firewall rules 4.4.2.4 - Content filter/URL filter
5.7	Network Access Control	<p>2.4 Summarize authentication and authorization design concepts.</p> <ul style="list-style-type: none"> • 2.4.4 - Authentication, authorization, and accounting (AAA) <p>3.3 Given a scenario, implement secure network designs.</p> <ul style="list-style-type: none"> • 3.3.2 - Network segmentation

		<p>3.3.2.6 -Zero trust</p> <ul style="list-style-type: none"> • 3.3.5 - Network access control (NAC) <p>3.3.5.1 - Agent and agentless</p>
5.8	Network Threats	<p>1.4 Given a scenario, analyze potential indicators associated with network attacks.</p> <ul style="list-style-type: none"> • 1.4.6 - Distributed denial of service (DDoS) <p>1.8 Explain the techniques used in penetration testing.</p> <ul style="list-style-type: none"> • 1.8.2 - Passive and active reconnaissance <p>3.3 Given a scenario, implement secure network designs.</p> <ul style="list-style-type: none"> • 3.3.2 - Network segmentation <p>3.3.2.1 -Virtual local area network (VLAN) 3.3.2.2 -DMZ</p> <p>3.6 Given a scenario, apply cybersecurity solutions to the cloud.</p> <ul style="list-style-type: none"> • 3.6.1 - Cloud security controls <p>3.6.1.6.2 - Network - Public and private subnets</p> <p>4.5 Explain the key aspects of digital forensics.</p> <ul style="list-style-type: none"> • 4.5.1 - Documentation/evidence <p>5.3 Explain the importance of policies to organizational security.</p>

		<ul style="list-style-type: none"> • 5.3.1 - Personnel <ul style="list-style-type: none"> 5.3.1.12.3 - User training - Phishing campaigns <p>5.4 Summarize risk management processes and concepts.</p> <ul style="list-style-type: none"> • 5.4.1 - Risk types
5.9	Network Device Vulnerabilities	<p>1.2 Given a scenario, analyze potential indicators to determine the type of attack.</p> <ul style="list-style-type: none"> • 1.2.1 - Malware <ul style="list-style-type: none"> 1.2.1.14 - Backdoor <p>1.3 Given a scenario, analyze potential indicators associated with application attacks.</p> <ul style="list-style-type: none"> • 1.3.1 - Privilege escalation <p>3.4 Given a scenario, install and configure wireless security settings.</p> <ul style="list-style-type: none"> • 3.4.4 - Installation considerations <ul style="list-style-type: none"> 3.4.4.5 - Wireless access point <p>3.7 Given a scenario, implement identity and account management controls.</p> <ul style="list-style-type: none"> • 3.7.3 - Account policies <ul style="list-style-type: none"> 3.7.3.1 - Password complexity <p>4.1 Given a scenario, use the appropriate tool to assess organizational security.</p> <ul style="list-style-type: none"> • 4.1.7 - Password crackers
5.10	Network Applications	<p>1.1 Compare and contrast different types of social engineering techniques.</p>

		<ul style="list-style-type: none"> • 1.1.5 - Spam over Internet messaging (SPIM) <p>1.7 Summarize the techniques used in security assessments.</p> <ul style="list-style-type: none"> • 1.7.2 - Vulnerability scans <p>2.8 Summarize the basics of cryptographic concepts.</p> <ul style="list-style-type: none"> • 2.8.1 - Digital signatures <p>3.2 Given a scenario, implement host or application security solutions.</p> <ul style="list-style-type: none"> • 3.2.4 - Application security <ul style="list-style-type: none"> 3.2.4.5 - Whitelisting
5.11	Switch Security and Attacks	<p>1.4 Given a scenario, analyze potential indicators associated with network attacks.</p> <ul style="list-style-type: none"> • 1.4.4 - Layer 2 attacks <ul style="list-style-type: none"> 1.4.4.1 - Address resolution protocol (ARP) poisoning 1.4.4.2 - Media access control (MAC) flooding <p>3.3 Given a scenario, implement secure network designs.</p> <ul style="list-style-type: none"> • 3.3.2 - Network segmentation <ul style="list-style-type: none"> 3.3.2.1 -Virtual local area network (VLAN) • 3.3.7 - Port security <p>3.4 Given a scenario, install and configure wireless security settings.</p> <ul style="list-style-type: none"> • 3.4.2 - Authentication protocols

		3.4.2.6 - IEEE 802.1X
5.12	Using VLANs	<p>2.6 Explain the security implications of embedded and specialized systems.</p> <ul style="list-style-type: none"> • 2.3.5 - Voice over IP (VoIP) <p>3.3 Given a scenario, implement secure network designs.</p> <ul style="list-style-type: none"> • 3.3.2 - Network segmentation <ul style="list-style-type: none"> 3.3.2.1 -Virtual local area network (VLAN) <p>3.4 Given a scenario, install and configure wireless security settings.</p> <ul style="list-style-type: none"> • 3.4.2 - Authentication protocols <ul style="list-style-type: none"> 3.4.2.6 - IEEE 802.1X
5.13	Router Security	<p>1.6 Explain the security concerns associated with various types of vulnerabilities.</p> <ul style="list-style-type: none"> • 1.6.5 - Improper or weak patch management <ul style="list-style-type: none"> 1.6.5.1 - Firmware <p>2.7 Explain the importance of physical security controls.</p> <ul style="list-style-type: none"> • 2.7.22 - Secure areas <p>3.1 Given a scenario, implement secure protocols.</p> <ul style="list-style-type: none"> • 3.1.1 - Protocols

		<p>3.1.1.3 - SSH</p> <p>3.3 Given a scenario, implement secure network designs.</p> <ul style="list-style-type: none"> • 3.3.9 - Access control list (ACL) • 3.3.10 - Route security
6.0	Identity, Access, and Account Management	
6.1	Access Control Models	<p>1.3 Given a scenario, analyze potential indicators associated with application attacks.</p> <ul style="list-style-type: none"> • 1.3.1 - Privilege escalation <p>2.4 Summarize authentication and authorization design concepts.</p> <ul style="list-style-type: none"> • 2.4.4 - Authentication, authorization, and accounting (AAA) <p>3.8 Given a scenario, implement authentication and authorization solutions.</p> <ul style="list-style-type: none"> • 3.8.3 - Access control schemes <ul style="list-style-type: none"> 3.8.3.2 - Role-based access control 3.8.3.4 - MAC 3.8.3.5 - Discretionary access control (DAC) <p>5.1 Compare and contrast various types of controls.</p> <ul style="list-style-type: none"> • 5.1.1 - Category <ul style="list-style-type: none"> 5.1.1.3 - Technical • 5.1.2 - Control type <ul style="list-style-type: none"> 5.1.2.2 - Detective

		<p>5.1.2.3 - Corrective</p> <p>5.3 Explain the importance of policies to organizational security.</p> <ul style="list-style-type: none"> • 5.3.1 - Personnel <ul style="list-style-type: none"> 5.3.1.2 - Job rotation 5.3.1.4 - Separation of duties 5.3.1.5 - Least privilege
6.2	Authentication	<p>2.4 Summarize authentication and authorization design concepts.</p> <ul style="list-style-type: none"> • 2.4.1 - Authentication methods <ul style="list-style-type: none"> 2.4.1.5 - Smart card authentication • 2.4.2 - Biometrics <ul style="list-style-type: none"> 2.4.2.10 - False rejection 2.4.2.11 - Crossover error rate • 2.4.3 - Multifactor authentication (MFA) factors and attributes <ul style="list-style-type: none"> 2.4.3.1.1 - Factors - Something you know 2.4.3.1.2 - Factors - Something you have <p>3.7 Given a scenario, implement identity and account management controls.</p> <ul style="list-style-type: none"> • 3.7.1 - Identity
6.3	Authorization	<p>2.4 Summarize authentication and authorization design concepts.</p> <ul style="list-style-type: none"> • 2.4.1 - Authentication methods

		<p>2.4.1.4.4 - Technologies - Token key</p> <ul style="list-style-type: none"> • 2.4.4 - Authentication, authorization, and accounting (AAA) <p>3.3 Given a scenario, implement secure network designs.</p> <ul style="list-style-type: none"> • 3.3.9 - Access control list (ACL) <p>3.6 Given a scenario, apply cybersecurity solutions to the cloud.</p> <ul style="list-style-type: none"> • 3.6.1 - Cloud security controls <ul style="list-style-type: none"> 3.6.1.7.1 - Compute - Security groups <p>3.7 Given a scenario, implement identity and account management controls.</p> <ul style="list-style-type: none"> • 3.7.3 - Account policies <ul style="list-style-type: none"> 3.7.3.11 - Account permissions <p>3.8 Given a scenario, implement authentication and authorization solutions.</p> <ul style="list-style-type: none"> • 3.8.3 - Access control schemes <ul style="list-style-type: none"> 3.8.3.7 - Privilege access management
6.4	Windows User Management	<p>2.4 Summarize authentication and authorization design concepts.</p> <ul style="list-style-type: none"> • 2.4.1 - Authentication methods <ul style="list-style-type: none"> 2.4.1.1 - Directory services

		<p>3.7 Given a scenario, implement identity and account management controls.</p> <ul style="list-style-type: none"> • 3.7.2 - Account types
6.5	Active Directory Overview	<p>2.4 Summarize authentication and authorization design concepts.</p> <ul style="list-style-type: none"> • 2.4.1 - Authentication methods <ul style="list-style-type: none"> 2.4.1.1 - Directory services <p>3.7 Given a scenario, implement identity and account management controls.</p> <ul style="list-style-type: none"> • 3.7.2 - Account types <ul style="list-style-type: none"> 3.7.2.1 - User account • 3.7.3 - Account policies <ul style="list-style-type: none"> 3.7.3.10 - Access policies
6.6	Hardening Authentication	<p>2.4 Summarize authentication and authorization design concepts.</p> <ul style="list-style-type: none"> • 2.4.1 - Authentication methods <ul style="list-style-type: none"> 2.4.1.5 - Smart card authentication <p>3.7 Given a scenario, implement identity and account management controls.</p> <ul style="list-style-type: none"> • 3.7.2 - Account types <ul style="list-style-type: none"> 3.7.2.2 - Shared and generic • 3.7.3 - Account policies <ul style="list-style-type: none"> 3.7.3.1 - Password complexity

		<p>3.7.3.2 - Password history 3.7.3.3 - Password reuse 3.7.3.4 - Time of day 3.7.3.14 - Lockout</p>
6.7	Linux Users	<p>3.7 Given a scenario, implement identity and account management controls.</p> <ul style="list-style-type: none"> 3.7.2 - Account types <ul style="list-style-type: none"> 3.7.2.1 - User account 3.7.3 - Account policies <ul style="list-style-type: none"> 3.7.3.2 - Password history 3.7.3.12 - Account audits 3.7.3.14 - Lockout
6.8	Linux Groups	
6.9	Remote Access	<p>1.6 Explain the security concerns associated with various types of vulnerabilities.</p> <ul style="list-style-type: none"> 1.6.3 - Weak configurations <ul style="list-style-type: none"> 1.6.3.5 - Unsecure protocols <p>2.4 Summarize authentication and authorization design concepts.</p> <ul style="list-style-type: none"> 2.4.4 - Authentication, authorization, and accounting (AAA) <p>3.1 Given a scenario, implement secure protocols.</p> <ul style="list-style-type: none"> 3.1.2 - Use cases <ul style="list-style-type: none"> 3.1.2.6 - Remote access

		<p>3.8 Given a scenario, implement authentication and authorization solutions.</p> <ul style="list-style-type: none"> 3.8.2 - Authentication <ul style="list-style-type: none"> 3.8.2.2 - Challenge Handshake Authentication Protocol (CHAP) 3.8.2.5 - RADIUS 3.8.2.8 - Terminal Access Controller Access Control System Plus (TACACS+)
6.10	Network Authentication	<p>3.1 Given a scenario, implement secure protocols.</p> <ul style="list-style-type: none"> 3.1.1 - Protocols <ul style="list-style-type: none"> 3.1.1.6 - LDAPS <p>3.8 Given a scenario, implement authentication and authorization solutions.</p> <ul style="list-style-type: none"> 3.8.1 - Authentication management <ul style="list-style-type: none"> 3.8.1.2 - Password vaults 3.8.2 - Authentication <ul style="list-style-type: none"> 3.8.2.11 - Kerberos
7.0	Cryptography and PKI	
7.1	Cryptography	<p>1.2 Given a scenario, analyze potential indicators to determine the type of attack.</p> <ul style="list-style-type: none"> 1.2.2 - Password attacks <ul style="list-style-type: none"> 1.2.2.2 - Dictionary

		<p>2.8 Summarize the basics of cryptographic concepts.</p> <ul style="list-style-type: none"> • 2.8.2 - Key length • 2.8.5 - Hashing • 2.8.6 - Key exchange • 2.8.8 - Perfect forward secrecy • 2.8.14 - Cipher suites <ul style="list-style-type: none"> 2.8.14.1 - Stream 2.8.14.2 - Block • 2.8.15 - Symmetric vs. asymmetric • 2.8.17 - Steganography • 2.8.20 - Limitations <ul style="list-style-type: none"> 2.8.20.3 - Weak keys
7.2	Cryptography Implementations	<p>2.1 Explain the importance of security concepts in an enterprise environment.</p> <ul style="list-style-type: none"> • 2.1.3 - Data protection <ul style="list-style-type: none"> 2.1.3.3 - Encryption • 2.1.4 - Hardware security module (HSM) <p>2.8 Summarize the basics of cryptographic concepts.</p> <ul style="list-style-type: none"> • 2.8.1 - Digital signatures • 2.8.2 - Key length • 2.8.5 - Hashing • 2.8.17 - Steganography • 2.8.19 - Common use cases <ul style="list-style-type: none"> 2.8.19.4 - Supporting confidentiality 2.8.19.5 - Supporting integrity

		<p>2.8.19.6 - Supporting obfuscation 2.8.19.7 - Supporting authentication 2.8.19.8 - Supporting non-repudiation 2.8.19.9 - Resource vs. security constraints</p> <ul style="list-style-type: none"> • 2.8.20 - Limitations <ul style="list-style-type: none"> 2.8.20.1 - Speed 2.8.20.2 - Size 2.8.20.3 - Weak keys 2.8.20.4 - Time 2.8.20.5 - Longevity 2.8.20.6 - Predictability 2.8.20.7 - Reuse 2.8.20.8 - Entropy 2.8.20.9 - Computational overheads 2.8.20.10 - Resource vs. security constraints <p>3.2 Given a scenario, implement host or application security solutions.</p> <ul style="list-style-type: none"> • 3.2.8 - Trusted Platform Module (TPM) <p>4.5 Explain the key aspects of digital forensics.</p> <ul style="list-style-type: none"> • 4.5.4 - Integrity
7.3	Hashing	<p>1.2 Given a scenario, analyze potential indicators to determine the type of attack.</p> <ul style="list-style-type: none"> • 1.2.7 - Cryptographic attacks <ul style="list-style-type: none"> 1.2.7.1 - Birthday 1.2.7.2 - Collision <p>1.6 Explain the security concerns associated with various types of vulnerabilities.</p> <ul style="list-style-type: none"> • 1.6.3 - Weak configurations

		<p>1.6.3.4 - Weak encryption</p> <p>2.1 Explain the importance of security concepts in an enterprise environment.</p> <ul style="list-style-type: none"> • 2.1.9 - Hashing <p>2.4 Summarize authentication and authorization design concepts.</p> <ul style="list-style-type: none"> • 2.4.1 - Authentication methods <ul style="list-style-type: none"> 2.4.1.4.2 - Technologies - HMAC-based one-time password (HOTP) <p>2.8 Summarize the basics of cryptographic concepts.</p> <ul style="list-style-type: none"> • 2.8.4 - Salting • 2.8.5 - Hashing
7.4	File Encryption	<p>1.6 Explain the security concerns associated with various types of vulnerabilities.</p> <ul style="list-style-type: none"> • 1.6.3 - Weak configurations <ul style="list-style-type: none"> 1.6.3.4 - Weak encryption <p>2.1 Explain the importance of security concepts in an enterprise environment.</p> <ul style="list-style-type: none"> • 2.1.3 - Data protection <ul style="list-style-type: none"> 2.1.3.3 - Encryption <p>2.8 Summarize the basics of cryptographic concepts.</p> <ul style="list-style-type: none"> • 2.8.19 - Common use cases

		<p>2.8.19.4 - Supporting confidentiality</p> <p>3.1 Given a scenario, implement secure protocols.</p> <ul style="list-style-type: none"> • 3.1.1 - Protocols <ul style="list-style-type: none"> 3.1.1.11.1 - IPSec - Authentication header (AH)/Encapsulated security payload (ESP) <p>3.2 Given a scenario, implement host or application security solutions.</p> <ul style="list-style-type: none"> • 3.2.5 - Hardening <ul style="list-style-type: none"> 3.2.5.3 - Disk encryption • 3.2.8 - Trusted Platform Module (TPM)
7.5	Public Key Infrastructure	<p>3.9 Given a scenario, implement public key infrastructure.</p> <ul style="list-style-type: none"> • 3.9.1 - Public key infrastructure (PKI) <ul style="list-style-type: none"> 3.9.1.1 - Key management 3.9.1.2 - Certificate authority (CA) 3.9.1.3 - Intermediate CA 3.9.1.4 - Registration authority (RA) 3.9.1.5 - Certificate revocation list (CRL) 3.9.1.6 - Certificate attributes 3.9.1.7 - Online Certificate Status Protocol (OCSP) 3.9.1.8 - Certificate signing request (CSR) 3.9.1.9 - CN 3.9.1.10 - SAN 3.9.1.11 - Expiration • 3.9.2 - Types of certificates

		<ul style="list-style-type: none"> 3.9.2.1 - Wildcard 3.9.2.2 - SAN 3.9.2.3 - Code signing 3.9.2.4 - Self-signed 3.9.2.5 - Machine/computer 3.9.2.6 - Email 3.9.2.7 - User 3.9.2.8 - Root 3.9.2.9 - Domain validation <ul style="list-style-type: none"> • 3.9.3 - Extended validation <ul style="list-style-type: none"> 3.9.3.1 - Certificate formats 3.9.3.2 - Distinguished encoding rules (DER) 3.9.3.4 - Privacy enhanced mail (PEM) 3.9.3.5 - Personal information exchange (PFX) 3.9.3.6 - .cer 3.9.3.7 - P12 3.9.3.8 - P7B • 3.9.4 - Concepts <ul style="list-style-type: none"> 3.9.4.1 - Online vs. offline CA 3.9.4.2 - Stapling 3.9.4.3 - Pinning 3.9.4.4 - Trust model 3.9.4.5 - Key escrow 3.9.4.6 - Certificate chaining
8.0	Wireless Threats	
8.1	Wireless Overview	<p>3.4 Given a scenario, install and configure wireless security settings.</p> <ul style="list-style-type: none"> • 3.4.4 - Installation considerations <ul style="list-style-type: none"> 3.4.4.1 - Site surveys

		<p>3.4.4.2 - Heat maps 3.4.4.3 - WiFi analyzers 3.4.4.4 - Channel overlays 3.4.4.5 - Wireless access point 3.4.4.6 - (WAP) placement 3.4.4.7 - Controller and access point security</p> <p>3.5 Given a scenario, implement secure mobile solutions.</p> <ul style="list-style-type: none"> • 3.5.1 - Connection methods and receivers <ul style="list-style-type: none"> 3.5.1.2 - WiFi • 3.5.4 - Enforcement and monitoring of: <ul style="list-style-type: none"> 3.5.4.13 - WiFi direct/ad hoc
8.2	Wireless Attacks	<p>1.4 Given a scenario, analyze potential indicators associated with network attacks.</p> <ul style="list-style-type: none"> • 1.4.1 - Wireless <ul style="list-style-type: none"> 1.4.1.1 - Evil twin 1.4.1.2 - Rogue access point 1.4.1.3 - Bluesnarfing 1.4.1.4 - Bluejacking 1.4.1.5 - Disassociation 1.4.1.6 - Jamming 1.4.1.7 - Radio frequency identifier (RFID) 1.4.1.8 - Near field communication (NFC) 1.4.1.9 - Initialization vector (IV) <p>3.4 Given a scenario, install and configure wireless security settings.</p> <ul style="list-style-type: none"> • 3.4.4 - Installation considerations

		<p>3.4.4.1 - Site surveys</p> <p>4.1 Given a scenario, use the appropriate tool to assess organizational security.</p> <ul style="list-style-type: none"> 4.1.4 - Packet capture and replay <p>4.1.4.3 - Wireshark</p>
8.3	Wireless Defenses	<p>1.6 Explain the security concerns associated with various types of vulnerabilities.</p> <ul style="list-style-type: none"> 1.6.3 - Weak configurations <p>1.6.3.4 - Weak encryption 1.6.3.6 - Default settings</p> <p>3.2 Given a scenario, implement host or application security solutions.</p> <ul style="list-style-type: none"> 3.2.5 - Hardening <p>3.2.5.5.1 - Patch management - Third-party updates 3.2.5.5.2 - Patch management - Auto-update</p> <p>3.3 Given a scenario, implement secure network designs.</p> <ul style="list-style-type: none"> 3.3.7 - Port security <p>3.3.7.5 - Media access control (MAC) filtering</p> <p>3.4 Given a scenario, install and configure wireless security settings.</p> <ul style="list-style-type: none"> 3.4.1 - Cryptographic protocols <p>3.4.1.1 - WiFi protected access II (WPA2)</p>

		<p>3.4.1.2 - WiFi protected access III (WPA3)</p> <ul style="list-style-type: none"> • 3.4.2 - Authentication protocols <ul style="list-style-type: none"> 3.4.2.1 - Extensible Authentication Protocol (EAP) 3.4.2.2 - Protected Extensible Application Protocol (PEAP) 3.4.2.3 - EAP-FAST 3.4.2.4 - EAP-TLS 3.4.2.5 - EAP-TTLS 3.4.2.6 - IEEE 802.1X 3.4.2.5 - Remote Authentication Dial-in 3.4.2.6 - User Server (RADIUS) Federation • 3.4.3 - Methods <ul style="list-style-type: none"> 3.4.3.1 - Pre-shared key (PSK) vs. Enterprise vs. Open 3.4.3.2 - WiFi Protected Setup (WPS) 3.4.3.3 - Captive portals • 3.4.4 - Installation considerations <ul style="list-style-type: none"> 3.4.4.5 - Wireless access point 3.4.4.6 - (WAP) placement 3.4.4.7 - Controller and access point security <p>3.8 Given a scenario, implement authentication and authorization solutions.</p> <ul style="list-style-type: none"> • 3.8.2 - Authentication <ul style="list-style-type: none"> 3.8.2.1 - EAP 3.8.2.5 - RADIUS
9.0	Virtualization, Cloud Security, and Securing Mobile Devices	

9.1	Host Virtualization	<p>2.2 Summarize virtualization and cloud computing concepts.</p> <ul style="list-style-type: none"> • 2.2.15 - Virtualization <ul style="list-style-type: none"> 2.2.15.1 - Virtual machine (VM) 2.2.15.3 - VM escape protection <p>3.2 Given a scenario, implement host or application security solutions.</p> <ul style="list-style-type: none"> • 3.2.9 - Sandboxing <p>3.3 Given a scenario, implement secure network designs.</p> <ul style="list-style-type: none"> • 3.3.1 - Load balancing
9.2	Virtual Networking	<p>2.2 Summarize virtualization and cloud computing concepts.</p> <ul style="list-style-type: none"> • 2.2.15 - Virtualization <ul style="list-style-type: none"> 2.2.15.1 - Virtual machine (VM) <p>3.3 Given a scenario, implement secure network designs.</p> <ul style="list-style-type: none"> • 3.3.2 - Network segmentation <ul style="list-style-type: none"> 3.3.2.1 -Virtual local area network (VLAN) • 3.3.3 - Virtual private network (VPN) <p>3.6 Given a scenario, apply cybersecurity solutions to the cloud.</p> <ul style="list-style-type: none"> • 3.6.1 - Cloud security controls <ul style="list-style-type: none"> 3.6.1.6.1 - Network - Virtual networks

9.3	Software-Defined Networking	<p>2.2 Summarize virtualization and cloud computing concepts.</p> <ul style="list-style-type: none"> • 2.2.10 - Infrastructure as code <ul style="list-style-type: none"> 2.2.10.1 - Software-defined networking (SDN)
9.4	Cloud Services	<p>2.1 Explain the importance of security concepts in an enterprise environment.</p> <ul style="list-style-type: none"> • 2.1.6 - Cloud access security broker (CASB) <p>2.2 Summarize virtualization and cloud computing concepts.</p> <ul style="list-style-type: none"> • 2.2.1 - Cloud models <ul style="list-style-type: none"> 2.2.1.2 - Platform as a service (PaaS) 2.2.1.3 - Software as a service (SaaS) 2.2.1.4 - Anything as a service (XaaS) 2.2.1.6 - Community • 2.2.2 - Cloud service providers • 2.2.5 - Fog computing • 2.2.6 - Edge computing • 2.2.7 - Thin client • 2.2.11 - Serverless architecture • 2.2.12 - Services integration • 2.2.13 - Resource policies <p>3.5 Given a scenario, implement secure mobile solutions.</p> <ul style="list-style-type: none"> • 3.5.4 - Deployment models <ul style="list-style-type: none"> 3.5.4.5 - Virtual desktop infrastructure (VDI) <p>3.6 Given a scenario, apply cybersecurity solutions to the cloud.</p>

		<ul style="list-style-type: none"> • 3.6.1 - Cloud security controls <ul style="list-style-type: none"> 3.6.1.5.1 - Storage - Permissions 3.6.1.5.2 - Storage - Encryption 3.6.1.5.3 - Storage - Replication 3.6.1.5.4 - Storage - High availability
9.5	Cloud Security	<p>1.6 Explain the security concerns associated with various types of vulnerabilities.</p> <ul style="list-style-type: none"> • 1.6.6 - Impacts <ul style="list-style-type: none"> 1.6.6.7 - Availability loss <p>2.1 Explain the importance of security concepts in an enterprise environment.</p> <ul style="list-style-type: none"> • 2.1.6 - Cloud access security broker (CASB) <p>2.2 Summarize virtualization and cloud computing concepts.</p> <ul style="list-style-type: none"> • 2.2.12 - Services integration <p>3.6 Given a scenario, apply cybersecurity solutions to the cloud.</p> <ul style="list-style-type: none"> • 3.6.1 - Cloud security controls <ul style="list-style-type: none"> 3.6.1.5.3 - Storage - Replication 3.6.1.7.3 - Compute - Instance awareness • 3.6.2 - Solutions <ul style="list-style-type: none"> 3.6.2.3 - Next-generation secure web gateway (SWG) 3.6.2.4.2 - Firewall considerations in a cloud environment - Need for segmentation

		3.6.2.4.3 - Firewall considerations in a cloud environment - Open Systems Interconnection (OSI) layers
9.6	Mobile Devices	<p>3.5 Given a scenario, implement secure mobile solutions.</p> <ul style="list-style-type: none"> • 3.5.1 - Connection methods and receivers <ul style="list-style-type: none"> 3.5.1.1 - Cellular 3.5.1.2 - WiFi 3.5.1.3 - Bluetooth 3.5.1.4 - NFC 3.5.1.5 - Infrared 3.5.1.6 - USB 3.5.1.7 - Point to point 3.5.1.8 - Point to multipoint 3.5.1.9 - Global Positioning System (GPS) 3.5.1.10 - RFID • 3.5.2 - Mobile device management (MDM) <ul style="list-style-type: none"> 3.5.2.3 - Remote wipe 3.5.2.6 - Screen locks • 3.5.4 - Enforcement and monitoring of: <ul style="list-style-type: none"> 3.5.4.3 - Sideloaded <p>3.7 Given a scenario, implement identity and account management controls.</p> <ul style="list-style-type: none"> • 3.7.3 - Account policies <ul style="list-style-type: none"> 3.7.3.7 - Geotagging <p>4.4 Given an incident, apply mitigation techniques or controls to secure an environment.</p>

		<ul style="list-style-type: none"> • 4.4.1 - Reconfigure endpoint security solutions <ul style="list-style-type: none"> 4.4.1.1 - Application whitelisting
9.7	Mobile Device Management	<p>3.1 Given a scenario, implement secure protocols.</p> <ul style="list-style-type: none"> • 3.1.2 - Use cases <ul style="list-style-type: none"> 3.1.2.6 - Remote access <p>3.5 Given a scenario, implement secure mobile solutions.</p> <ul style="list-style-type: none"> • 3.5.2 - Mobile device management (MDM) <ul style="list-style-type: none"> 3.5.2.2 - Content management 3.5.2.3 - Remote wipe • 3.5.3 - Mobile devices <ul style="list-style-type: none"> 3.5.3.2 - MDM/Unified endpoint management (UEM) 3.5.3.3 - Mobile application management (MAM) • 3.5.4 - Enforcement and monitoring of:
9.8	BYOD Security	<p>3.3 Given a scenario, implement secure network designs.</p> <ul style="list-style-type: none"> • 3.3.5 - Network access control (NAC) <p>3.5 Given a scenario, implement secure mobile solutions.</p> <ul style="list-style-type: none"> • 3.5.4 - Enforcement and monitoring of: • 3.5.4 - Deployment models <ul style="list-style-type: none"> 3.5.4.1 - Bring your own device (BYOD) 3.5.4.2 - Corporate-owned personally enabled (COPE)

		<p>3.5.4.3 - Choose your own device (CYOD) 3.5.4.5 - Virtual desktop infrastructure (VDI)</p> <p>3.6 Given a scenario, apply cybersecurity solutions to the cloud.</p> <ul style="list-style-type: none"> • 3.6.1 - Cloud security controls <ul style="list-style-type: none"> 3.6.1.6.2 - Network - Public and private subnets <p>5.3 Explain the importance of policies to organizational security.</p> <ul style="list-style-type: none"> • 5.3.1 - Personnel <ul style="list-style-type: none"> 5.3.1.1 - Acceptable use policy
9.9	Embedded and Specialized Systems	<p>2.6 Explain the security implications of embedded and specialized systems.</p> <ul style="list-style-type: none"> • 2.3.1 - Embedded systems <ul style="list-style-type: none"> 2.3.1.1 - Raspberry Pi 2.3.1.2 - Field programmable gate array (FPGA) 2.3.1.3 - Arduino • 2.3.2 - System control and data acquisition (SCADA)/industrial control system (ICS) <ul style="list-style-type: none"> 2.3.2.1 - Facilities 2.3.2.3 - Manufacturing • 2.3.3 - Internet of Things (IoT) <ul style="list-style-type: none"> 2.3.3.2 - Smart devices 2.3.3.5 - Weak defaults • 2.3.4 - Specialized

		<p>2.3.4.1 - Medical systems 2.3.4.2 - Vehicles 2.3.4.3 - Aircraft 2.3.4.4 - Smart meters</p> <ul style="list-style-type: none"> • 2.3.5 - Voice over IP (VoIP) • 2.3.9 - Real-time operating system (RTOS) • 2.3.11 - System on chip (SoC) • 2.3.12 - Communication considerations <p>2.3.12.1 - 5G 2.3.12.2 - Narrow-band 2.3.12.3 - Baseband radio 2.3.12.4 - Subscriber identity module (SIM) cards 2.3.12.5 - Zigbee</p> <ul style="list-style-type: none"> • 2.3.13 - Constraints <p>2.3.13.1 - Power 2.3.13.2 - Compute 2.3.13.3 - Network 2.3.13.4 - Crypto 2.3.13.5 - Inability to patch 2.3.13.6 - Authentication 2.3.13.7 - Range 2.3.13.8 - Cost 2.3.13.9 - Implied trust</p>
10.0	Securing Data and Applications	
10.1	Data Transmission Security	<p>2.1 Explain the importance of security concepts in an enterprise environment.</p> <ul style="list-style-type: none"> • 2.1.8 - Secure Sockets Layer (SSL)/Transport Layer Security (TLS) inspection

		<p>3.1 Given a scenario, implement secure protocols.</p> <ul style="list-style-type: none"> • 3.1.1 - Protocols <ul style="list-style-type: none"> 3.1.1.3 - SSH 3.1.1.7 - File transfer protocol, secure (FTPS) 3.1.1.10 - Hypertext transfer protocol over SSL/TLS (HTTPS) 3.1.1.11.1 - IPSec - Authentication header (AH)/Encapsulated security payload (ESP) 3.1.1.11.2 - IPSec - Tunnel/transport
10.2	Data Loss Prevention	<p>2.1 Explain the importance of security concepts in an enterprise environment.</p> <ul style="list-style-type: none"> • 2.1.3 - Data protection <ul style="list-style-type: none"> 2.1.3.1 - Data loss prevention (DLP) <p>3.2 Given a scenario, implement host or application security solutions.</p> <ul style="list-style-type: none"> • 3.2.1 - Endpoint protection <ul style="list-style-type: none"> 3.2.1.4 - DLP <p>5.5 Explain privacy and sensitive data concepts in relation to security.</p> <ul style="list-style-type: none"> • 5.5.4 - Privacy enhancing technologies <ul style="list-style-type: none"> 5.5.4.2 - Data masking 5.5.4.3 - Tokenization
10.3	Web Application Attacks	<p>1.3 Given a scenario, analyze potential indicators associated with application attacks.</p> <ul style="list-style-type: none"> • 1.3.2 - Cross-site scripting

		<ul style="list-style-type: none"> • 1.3.3 - Injections <ul style="list-style-type: none"> 1.3.3.1 - Structured query language (SQL) • 1.3.6 - Buffer overflows • 1.3.18 - Pass the hash <p>1.4 Given a scenario, analyze potential indicators associated with network attacks.</p> <ul style="list-style-type: none"> • 1.4.3 - Man in the browser <p>1.6 Explain the security concerns associated with various types of vulnerabilities.</p> <ul style="list-style-type: none"> • 1.6.2 - Zero-day <p>2.3 Summarize secure application development, deployment, and automation concepts.</p> <ul style="list-style-type: none"> • 2.3.4 - Secure coding techniques <ul style="list-style-type: none"> 2.3.4.5 - Server-side vs. client-side execution and validation <p>3.1 Given a scenario, implement secure protocols.</p> <ul style="list-style-type: none"> • 3.1.2 - Use cases <ul style="list-style-type: none"> 3.1.2.3 - Email and web <p>3.2 Given a scenario, implement host or application security solutions.</p> <ul style="list-style-type: none"> • 3.2.4 - Application security <ul style="list-style-type: none"> 3.2.4.1 - Input validations <p>4.1 Given a scenario, use the appropriate tool to assess organizational security.</p>
--	--	--

		<ul style="list-style-type: none"> • 4.1.2 - File manipulation <ul style="list-style-type: none"> 4.1.2.1 - head
10.4	Application Development and Security	<p>1.5 Explain different threat actors, vectors, and intelligence sources.</p> <ul style="list-style-type: none"> • 1.5.4 - Threat intelligence sources <ul style="list-style-type: none"> 1.5.4.10 - File/code repositories <p>2.1 Explain the importance of security concepts in an enterprise environment.</p> <ul style="list-style-type: none"> • 2.1.3 - Data protection <p>2.3 Summarize secure application development, deployment, and automation concepts.</p> <ul style="list-style-type: none"> • 2.3.1 - Environment <ul style="list-style-type: none"> 2.3.1.1 - Development 2.3.1.2 - Test 2.3.1.3 - Staging 2.3.1.4 - Production 2.3.1.5 - Quality assurance (QA) • 2.3.4 - Secure coding techniques <ul style="list-style-type: none"> 2.3.4.1 - Normalization 2.3.4.2 - Stored procedures 2.3.4.3 - Obfuscation/camouflage 2.3.4.4 - Code reuse/dead code 2.3.4.5 - Server-side vs. client-side execution and validation 2.3.4.6 - Memory management 2.3.4.7 - Use of third-party libraries and software development kits (SDKs)

		<p>2.3.4.8 - Data exposure</p> <ul style="list-style-type: none"> • 2.3.10 - Version control <p>3.2 Given a scenario, implement host or application security solutions.</p> <ul style="list-style-type: none"> • 3.2.4 - Application security <ul style="list-style-type: none"> 3.2.4.5 - Whitelisting 3.2.4.10 - Fuzzing • 3.2.5 - Hardening <ul style="list-style-type: none"> 3.2.5.4 - OS <p>3.9 Given a scenario, implement public key infrastructure.</p> <ul style="list-style-type: none"> • 3.9.2 - Types of certificates <ul style="list-style-type: none"> 3.9.2.3 - Code signing
11.0	Security Assessments	
11.1	Penetration Testing	<p>1.8 Explain the techniques used in penetration testing.</p> <ul style="list-style-type: none"> • 1.8.1 - Penetration testing <ul style="list-style-type: none"> 1.8.1.1 - White box 1.8.1.2 - Black box 1.8.1.3 - Gray box 1.8.1.4 - Rules of engagement 1.8.1.5 - Lateral movement 1.8.1.6 - Privilege escalation 1.8.1.7 - Persistence 1.8.1.8 - Cleanup 1.8.1.9 - Bug bounty

		<p>1.8.1.10 - Pivoting</p> <ul style="list-style-type: none"> • 1.8.3 - Exercise types <ul style="list-style-type: none"> 1.8.3.1 - Red team 1.8.3.2 - Blue team 1.8.3.3 - White team 1.8.3.4 - Purple team
11.2	Monitoring and Reconnaissance	<p>1.1 Compare and contrast different types of social engineering techniques.</p> <ul style="list-style-type: none"> • 1.1.17 - Reconnaissance <p>1.8 Explain the techniques used in penetration testing.</p> <ul style="list-style-type: none"> • 1.8.2 - Passive and active reconnaissance <ul style="list-style-type: none"> 1.8.2.3 - War driving 1.8.2.5 - OSINT <p>4.1 Given a scenario, use the appropriate tool to assess organizational security.</p> <ul style="list-style-type: none"> • 4.1.1 - Network reconnaissance and discovery <ul style="list-style-type: none"> 4.1.1.2 - nslookup/dig 4.1.1.4 - nmap 4.1.1.5 - ping/pathping 4.1.1.13 - the harvester 4.1.1.17 - Nessus
11.3	Intrusion Detection	<p>1.7 Summarize the techniques used in security assessments.</p> <ul style="list-style-type: none"> • 1.7.2 - Vulnerability scans

		<p>1.7.2.1 - False positives 1.7.2.2 - False negatives</p> <p>3.2 Given a scenario, implement host or application security solutions.</p> <ul style="list-style-type: none"> 3.2.1 - Endpoint protection <ul style="list-style-type: none"> 3.2.1.7 - Host intrusion detection system (HIDS) <p>3.3 Given a scenario, implement secure network designs.</p> <ul style="list-style-type: none"> 3.3.8 - Network appliances <ul style="list-style-type: none"> 3.3.8.3 - Network-based intrusion detection system (NIDS)/network-based intrusion prevention system (NIPS) <ul style="list-style-type: none"> 3.3.8.3.1 - NDIS/NIPS - Signature based 3.3.8.3.2 - NDIS/NIPS - Heuristic/behavior 3.3.8.3.3 - NDIS/NIPS - Anomaly 3.3.8.3.4 - NDIS/NIPS - Inline vs. passive
11.4	Security Assessment Techniques	<p>1.5 Explain different threat actors, vectors, and intelligence sources.</p> <ul style="list-style-type: none"> 1.5.5 - Research sources <ul style="list-style-type: none"> 1.5.5.8 - Threat feeds <p>1.6 Explain the security concerns associated with various types of vulnerabilities.</p> <ul style="list-style-type: none"> 1.6.3 - Weak configurations <ul style="list-style-type: none"> 1.6.3.7 - Open ports and services <p>1.7 Summarize the techniques used in security assessments.</p>

		<ul style="list-style-type: none"> • 1.7.2 - Vulnerability scans <ul style="list-style-type: none"> 1.7.2.1 - False positives 1.7.2.4 - Credentialed vs. non-credentialed • 1.7.3 - Syslog/Security information and event management (SIEM) <ul style="list-style-type: none"> 1.7.3.1 - Review reports 1.7.3.2 - Packet capture 1.7.3.3 - Data inputs 1.7.3.4 - User behavior analysis 1.7.3.5 - Sentiment analysis 1.7.3.6 - Security monitoring 1.7.3.7 - Log aggregation 1.7.3.8 - Log collectors • 1.7.4 - Security orchestration, automation, response (SOAR) <p>4.4 Given an incident, apply mitigation techniques or controls to secure an environment.</p> <ul style="list-style-type: none"> • 4.4.6 - Secure Orchestration, Automation, and Response (SOAR) <ul style="list-style-type: none"> 4.4.6.2 - Playbooks
11.5	Protocol Analyzers	<p>3.3 Given a scenario, implement secure network designs.</p> <ul style="list-style-type: none"> • 3.3.13 - Port spanning/port mirroring <p>4.1 Given a scenario, use the appropriate tool to assess organizational security.</p> <ul style="list-style-type: none"> • 4.1.4 - Packet capture and replay <p>4.3 Given an incident, utilize appropriate data sources to support an investigation.</p> <ul style="list-style-type: none"> • 4.3.11 - Protocol analyzer output

		<p>4.4 Given an incident, apply mitigation techniques or controls to secure an environment.</p> <ul style="list-style-type: none"> 4.4.6 - Secure Orchestration, Automation, and Response (SOAR)
11.6	Analyzing Network Attacks	<p>1.4 Given a scenario, analyze potential indicators associated with network attacks.</p> <ul style="list-style-type: none"> 1.4.4 - Layer 2 attacks <ul style="list-style-type: none"> 1.4.4.1 - Address resolution protocol (ARP) poisoning 1.4.5 - Domain name system (DNS) <ul style="list-style-type: none"> 1.4.5.2 - DNS poisoning 1.4.6 - Distributed denial of service (DDoS) 1.4.7 - Malicious code or script execution <ul style="list-style-type: none"> 1.4.7.1 - PowerShell 1.4.7.2 - Python 1.4.7.3 - Bash 1.4.7.4 - Macros 1.4.7.5 - Virtual Basic for Applications (VBA) <p>4.1 Given a scenario, use the appropriate tool to assess organizational security.</p> <ul style="list-style-type: none"> 4.1.4 - Packet capture and replay <ul style="list-style-type: none"> 4.1.4.2 - Tcpdump
11.7	Password Attacks	<p>1.1 Compare and contrast different types of social engineering techniques.</p> <ul style="list-style-type: none"> 1.1.7 - Dumpster diving 1.1.8 - Shoulder surfing 1.1.19 - Impersonation

		<p>1.2 Given a scenario, analyze potential indicators to determine the type of attack.</p> <ul style="list-style-type: none"> • 1.2.2 - Password attacks <ul style="list-style-type: none"> 1.2.2.1 - Spraying 1.2.2.2 - Dictionary 1.2.2.3.1 - Brute force - Offline 1.2.2.3.2 - Brute force - Online 1.2.2.4 - Rainbow tables 1.2.2.5 - Plaintext/unencrypted <p>2.8 Summarize the basics of cryptographic concepts.</p> <ul style="list-style-type: none"> • 2.8.4 - Salting <p>3.7 Given a scenario, implement identity and account management controls.</p> <ul style="list-style-type: none"> • 3.7.3 - Account policies <ul style="list-style-type: none"> 3.7.3.1 - Password complexity <p>4.1 Given a scenario, use the appropriate tool to assess organizational security.</p> <ul style="list-style-type: none"> • 4.1.7 - Password crackers
12.0	Incident Response, Forensics, and Recovery	
12.1	Incident Response	<p>4.2 Summarize the importance of policies, processes, and procedures for incident response.</p> <ul style="list-style-type: none"> • 4.2.1 - Incident response plans • 4.2.2 - Incident response process <ul style="list-style-type: none"> 4.2.2.1 - Preparation 4.2.2.2 - Identification

		<ul style="list-style-type: none"> 4.2.2.3 - Containment 4.2.2.4 - Eradication 4.2.2.5 - Recovery 4.2.2.6 - Lessons learned <ul style="list-style-type: none"> • 4.2.4 - Attack frameworks <ul style="list-style-type: none"> 4.2.4.1 - MITRE ATT&CK 4.2.4.2 - The Diamond Model of Intrusion Analysis 4.2.4.3 - Cyber Kill Chain • 4.2.8 - Business continuity plan <p>4.3 Given an incident, utilize appropriate data sources to support an investigation.</p> <ul style="list-style-type: none"> • 4.3.3 - Log files <p>4.5 Explain the key aspects of digital forensics.</p> <ul style="list-style-type: none"> • 4.5.1 - Documentation/evidence
12.2	Mitigation of an Incident	<p>3.2 Given a scenario, implement host or application security solutions.</p> <ul style="list-style-type: none"> • 3.2.4 - Application security <ul style="list-style-type: none"> 3.2.4.5 - Whitelisting <p>3.3 Given a scenario, implement secure network designs.</p> <ul style="list-style-type: none"> • 3.3.8 - Network appliances <ul style="list-style-type: none"> 3.3.8.7.7 - Firewalls - Content/URL filter <p>3.7 Given a scenario, implement identity and account management controls.</p> <ul style="list-style-type: none"> • 3.7.1 - Identity

		<p>3.7.1.3 - Certificates</p> <p>4.2 Summarize the importance of policies, processes, and procedures for incident response.</p> <ul style="list-style-type: none"> 4.2.2 - Incident response process <p>4.2.2.3 - Containment</p> <p>4.4 Given an incident, apply mitigation techniques or controls to secure an environment.</p> <ul style="list-style-type: none"> 4.4.1 - Reconfigure endpoint security solutions <ul style="list-style-type: none"> 4.4.1.1 - Application whitelisting 4.4.1.2 - Application blacklisting 4.4.1.3 - Quarantine 4.4.2 - Configuration changes <ul style="list-style-type: none"> 4.4.2.1 - Firewall rules 4.4.2.2 - MDM 4.4.3 - Isolation 4.4.4 - Containment 4.4.5 - Segmentation 4.4.6 - Secure Orchestration, Automation, and Response (SOAR) <ul style="list-style-type: none"> 4.4.6.1 - Runbooks 4.4.6.2 - Playbooks
12.3	Log Management	<p>1.7 Summarize the techniques used in security assessments.</p> <ul style="list-style-type: none"> 1.7.3 - Syslog/Security information and event management (SIEM)

		<p>2.1 Explain the importance of security concepts in an enterprise environment.</p> <ul style="list-style-type: none"> • 2.1.1 - Configuration management <ul style="list-style-type: none"> 2.1.1.2 - Baseline configuration <p>4.3 Given an incident, utilize appropriate data sources to support an investigation.</p> <ul style="list-style-type: none"> • 4.3.2 - SIEM dashboards <ul style="list-style-type: none"> 4.3.2.4 - Alerts • 4.3.3 - Log files <ul style="list-style-type: none"> 4.3.3.2 - System 4.3.3.3 - Application 4.3.3.5 - Web 4.3.3.6 - DNS 4.3.3.8 - Dump files • 4.3.4 - syslog/rsyslog/syslog-ng • 4.3.9 - Metadata <ul style="list-style-type: none"> 4.3.9.1 - Email 4.3.9.2 - Mobile 4.3.9.3 - Web 4.3.9.4 - File
12.4	Windows Logging	<p>1.7 Summarize the techniques used in security assessments.</p> <ul style="list-style-type: none"> • 1.7.3 - Syslog/Security information and event management (SIEM) <ul style="list-style-type: none"> 1.7.3.8 - Log collectors

		<p>3.1 Given a scenario, implement secure protocols.</p> <ul style="list-style-type: none"> • 3.1.2 - Use cases <ul style="list-style-type: none"> 3.1.2.10 - Subscription services <p>3.3 Given a scenario, implement secure network designs.</p> <ul style="list-style-type: none"> • 3.3.8 - Network appliances <ul style="list-style-type: none"> 3.3.8.6 - Collectors <p>4.5 Explain the key aspects of digital forensics.</p> <ul style="list-style-type: none"> • 4.5.1 - Documentation/evidence <ul style="list-style-type: none"> 4.5.1.8 - Event logs
12.5	Digital Forensics	<p>2.1 Explain the importance of security concepts in an enterprise environment.</p> <ul style="list-style-type: none"> • 2.1.9 - Hashing <p>4.1 Given a scenario, use the appropriate tool to assess organizational security.</p> <ul style="list-style-type: none"> • 4.1.5 - Forensics <ul style="list-style-type: none"> 4.1.5.1 - dd 4.1.5.2 - Memdump 4.1.5.3 - WinHex 4.1.5.4 - FTK imager 4.1.5.5 - Autopsy <p>4.5 Explain the key aspects of digital forensics.</p> <ul style="list-style-type: none"> • 4.5.1 - Documentation/evidence

		<ul style="list-style-type: none">4.5.1.1 - Legal hold4.5.1.2 - Video4.5.1.3 - Admissibility4.5.1.4 - Chain of custody4.5.1.5.1 - Timelines of sequence of events - Time stamps4.5.1.5.2 - Timelines of sequence of events - Time offset4.5.1.6 - Tags4.5.1.7 - Reports4.5.1.8 - Event logs4.5.1.9 - Interviews <ul style="list-style-type: none">• 4.5.2 - Acquisition<ul style="list-style-type: none">4.5.2.1 - Order of volatility4.5.2.2 - Disk4.5.2.3 - Random-access memory (RAM)4.5.2.4 - Swap/pagefile4.5.2.5 - OS4.5.2.6 - Device4.5.2.7 - Firmware4.5.2.8 - Snapshot4.5.2.9 - Cache4.5.2.10 - Network4.5.2.11 - Artifacts• 4.5.3 - On-premises vs. cloud• 4.5.4 - Integrity<ul style="list-style-type: none">4.5.4.1 - Hashing4.5.4.2 - Checksums4.5.4.3 - Provenance• 4.5.5 - Preservation• 4.5.6 - E-discovery• 4.5.7 - Data recovery• 4.5.8 - Non-repudiation
--	--	--

		<ul style="list-style-type: none"> • 4.5.9 - Strategic intelligence/counterintelligence
12.6	File and Packet Manipulation	<p>1.4 Given a scenario, analyze potential indicators associated with network attacks.</p> <ul style="list-style-type: none"> • 1.4.4 - Layer 2 attacks <p>1.7 Summarize the techniques used in security assessments.</p> <ul style="list-style-type: none"> • 1.7.3 - Syslog/Security information and event management (SIEM) <ul style="list-style-type: none"> 1.7.3.2 - Packet capture <p>4.1 Given a scenario, use the appropriate tool to assess organizational security.</p> <ul style="list-style-type: none"> • 4.1.2 - File manipulation <ul style="list-style-type: none"> 4.1.2.1 - head 4.1.2.2 - tail 4.1.2.3 - cat 4.1.2.4 - grep 4.1.2.5 - chmod 4.1.2.6 - logger • 4.1.3 - Shell and script environments <ul style="list-style-type: none"> 4.1.3.1 - SSH 4.1.3.2 - PowerShell 4.1.3.3 - Python 4.1.3.4 - OpenSSL • 4.1.4 - Packet capture and replay <ul style="list-style-type: none"> 4.1.4.1 - Tcpreplay 4.1.4.2 - Tcpdump 4.1.4.3 - Wireshark

		<p>4.3 Given an incident, utilize appropriate data sources to support an investigation.</p> <ul style="list-style-type: none"> • 4.3.3 - Log files <ul style="list-style-type: none"> 4.3.3.2 - System
12.7	Redundancy	<p>2.1 Explain the importance of security concepts in an enterprise environment.</p> <ul style="list-style-type: none"> • 2.1.11 - Site resiliency <ul style="list-style-type: none"> 2.1.11.1 - Hot site 2.1.11.2 - Cold site 2.1.11.3 - Warm site <p>2.5 Given a scenario, implement cybersecurity resilience.</p> <ul style="list-style-type: none"> • 2.5.1 - Redundancy <ul style="list-style-type: none"> 2.5.1.1 - Geographic dispersal 2.5.1.2.1 - Disk - Redundant array of inexpensive disks (RAID) levels 2.5.1.2.2 - Disk - Multipath 2.5.1.3.1 - Network - Load balancers 2.5.1.3.2 - Network - Network interface card (NIC) teaming 2.5.1.4.1 - Power - Uninterruptible power supply (UPS) 2.5.1.4.2 - Power - Generator 2.5.1.4.3 - Power - Dual supply 2.5.1.4.4 - Power - Managed power distribution units (PDUs) • 2.5.2 - Replication <ul style="list-style-type: none"> 2.5.2.1 - Storage area network (SAN) • 2.5.4 - Backup types • 2.5.6 - High availability

12.8	Backup and Restore	<p>2.5 Given a scenario, implement cybersecurity resilience.</p> <ul style="list-style-type: none"> • 2.5.4 - Backup types <ul style="list-style-type: none"> 2.5.4.1 - Full 2.5.4.2 - Incremental 2.5.4.3 - Snapshot 2.5.4.4 - Differential 2.5.4.5 - Tape 2.5.4.6 - Disk 2.5.4.7 - Copy 2.5.4.8 - Network attached storage (NAS) 2.5.4.9 - SAN 2.5.4.10 - Cloud 2.5.4.11 - Image 2.5.4.12 - Online vs. offline 2.5.4.13.1 - Offsite storage - Distance considerations <p>4.5 Explain the key aspects of digital forensics.</p> <ul style="list-style-type: none"> • 4.5.7 - Data recovery
13.0	Risk Management	
13.1	Organizational Security Policies	<p>2.1 Explain the importance of security concepts in an enterprise environment.</p> <ul style="list-style-type: none"> • 2.1.3 - Data protection <ul style="list-style-type: none"> 2.1.3.1 - Data loss prevention (DLP) 2.1.3.2 - Masking 2.1.3.3 - Encryption 2.1.3.4 - At rest 2.1.3.5 - In transit/motion 2.1.3.6 - In processing 2.1.3.7 - Tokenization 2.1.3.8 - Rights management

		<p>5.3 Explain the importance of policies to organizational security.</p> <ul style="list-style-type: none">• 5.3.1 - Personnel<ul style="list-style-type: none">5.3.1.1 - Acceptable use policy5.3.1.2 - Job rotation5.3.1.3 - Mandatory vacation5.3.1.4 - Separation of duties5.3.1.5 - Least privilege5.3.1.6 - Clean desk space5.3.1.7 - Background checks5.3.1.8 - Non-disclosure agreement (NDA)5.3.1.9 - Social media analysis5.3.1.10 - Onboarding5.3.1.11 - Offboarding5.3.1.12.1 - User training - Gamification5.3.1.12.2 - User training - Capture the flag5.3.1.12.3 - User training - Phishing campaigns5.3.1.12.4 - User training - Computer-based training (CBT)5.3.1.12.5 - User training - Role-based training• 5.3.3 - Third-party risk management<ul style="list-style-type: none">5.3.3.1 - Vendors5.3.3.2 - Supply chain5.3.3.3 - Business partners5.3.3.4 - Service level agreement (SLA)5.3.3.5 - Memorandum of understanding (MOU)5.3.3.6 - Measurement systems analysis (MSA)5.3.3.7 - Business partnership agreement (BPA)5.3.3.8 - End of life (EOL)5.3.3.9 - End of service (EOS)5.3.3.10 - NDA• 5.3.4 - Data
--	--	---

		<p>5.3.4.3 - Retention</p> <ul style="list-style-type: none"> • 5.3.5 - Credential policies <ul style="list-style-type: none"> 5.3.5.1 - Personnel 5.3.5.2 - Third party 5.3.5.3 - Devices 5.3.5.4 - Service accounts 5.3.5.5 - Administrator/root accounts • 5.3.6 - Organizational policies <ul style="list-style-type: none"> 5.3.6.1 - Change management 5.3.6.2 - Change control 5.3.6.3 - Asset management
<p>13.2</p>	<p>Risk Management</p>	<p>4.2 Summarize the importance of policies, processes, and procedures for incident response.</p> <ul style="list-style-type: none"> • 4.2.8 - Business continuity plan <p>5.3 Explain the importance of policies to organizational security.</p> <ul style="list-style-type: none"> • 5.3.6 - Organizational policies <ul style="list-style-type: none"> 5.3.6.3 - Asset management <p>5.4 Summarize risk management processes and concepts.</p> <ul style="list-style-type: none"> • 5.4.1 - Risk types <ul style="list-style-type: none"> 5.4.1.1 - External 5.4.1.2 - Internal 5.4.1.3 - Legacy systems

		<ul style="list-style-type: none"> 5.4.1.4 - Multiparty 5.4.1.5 - IP theft 5.4.1.6 - Software compliance/licensing <ul style="list-style-type: none"> • 5.4.3 - Risk analysis <ul style="list-style-type: none"> 5.4.3.1 - Risk register 5.4.3.2 - Risk matrix/heat map 5.4.3.3 - Risk control assessment 5.4.3.4 - Risk control self-assessment 5.4.3.5 - Risk awareness 5.4.3.6 - Inherent risk 5.4.3.7 - Residual risk 5.4.3.8 - Control risk 5.4.3.9 - Risk appetite 5.4.3.10 - Regulations that affect risk posture 5.4.3.11.1 - Risk assessment - Qualitative 5.4.3.11.2 - Risk assessment - Quantitative 5.4.3.12 - Likelihood of occurrence 5.4.3.13 - Impact 5.4.3.14 - Asset value 5.4.3.15 - Single loss expectancy (SLE) 5.4.3.16 - Annualized loss expectancy (ALE) 5.4.3.17 - Annualized rate of occurrence (ARO) <ul style="list-style-type: none"> • 5.4.4 - Disasters <ul style="list-style-type: none"> 5.4.4.1 - Environmental <ul style="list-style-type: none"> • 5.4.5 - Business impact analysis <ul style="list-style-type: none"> 5.4.5.1 - Recovery time objective (RTO) 5.4.5.2 - Recovery point objective (RPO) 5.4.5.3 - Mean time to repair (MTTR) 5.4.5.4 - Mean time between failures (MTBF) 5.4.5.5 - Functional recovery plans 5.4.5.6 - Single point of failure 5.4.5.7 - Disaster recovery plan (DRP)
--	--	--

		<p>5.4.5.8 - Mission essential functions 5.4.5.9 - Identification of critical systems 5.4.5.10 - Site risk assessment</p>
13.3	Email	<p>1.1 Compare and contrast different types of social engineering techniques.</p> <ul style="list-style-type: none"> • 1.1.1 - Phishing • 1.1.4 - Spam <p>1.5 Explain different threat actors, vectors, and intelligence sources.</p> <ul style="list-style-type: none"> • 1.5.3 - Vectors <ul style="list-style-type: none"> 1.5.3.3 - Email <p>3.1 Given a scenario, implement secure protocols.</p> <ul style="list-style-type: none"> • 3.1.1 - Protocols <ul style="list-style-type: none"> 3.1.1.4 - Secure/multipurpose internet mail exchanger (S/MIME) • 3.1.2 - Use cases <ul style="list-style-type: none"> 3.1.2.3 - Email and web <p>3.2 Given a scenario, implement host or application security solutions.</p> <ul style="list-style-type: none"> • 3.2.4 - Application security <ul style="list-style-type: none"> 3.2.4.6 - Blacklisting <p>5.3 Explain the importance of policies to organizational security.</p> <ul style="list-style-type: none"> • 5.3.1 - Personnel

		5.3.1.12.3 - User training - Phishing campaigns
14.0	Governance and Compliance	
14.1	Audits	<p>3.6 Given a scenario, apply cybersecurity solutions to the cloud.</p> <ul style="list-style-type: none"> 3.6.1 - Cloud security controls <ul style="list-style-type: none"> 3.6.1.4 - Integration and auditing <p>3.7 Given a scenario, implement identity and account management controls.</p> <ul style="list-style-type: none"> 3.7.3 - Account policies <ul style="list-style-type: none"> 3.7.3.12 - Account audits <p>5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.</p> <ul style="list-style-type: none"> 5.2.1 - Regulations, standards, and legislation <ul style="list-style-type: none"> 5.2.1.3 - Payment Card Industry Data Security Standard (PCI DSS) <p>5.3 Explain the importance of policies to organizational security.</p> <ul style="list-style-type: none"> 5.3.1 - Personnel <ul style="list-style-type: none"> 5.3.1.5 - Least privilege 5.3.6 - Organizational policies
14.2	Controls and Frameworks	<p>5.1 Compare and contrast various types of controls.</p> <ul style="list-style-type: none"> 5.1.1 - Category

		<p>5.1.1.1 - Managerial 5.1.1.2 - Operational 5.1.1.3 - Technical</p> <ul style="list-style-type: none"> • 5.1.2 - Control type <p>5.1.2.1 - Preventative 5.1.2.2 - Detective 5.1.2.3 - Corrective 5.1.2.4 - Deterrent 5.1.2.5 - Compensating 5.1.2.6 - Physical</p> <p>5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.</p> <ul style="list-style-type: none"> • 5.2.2 - Key frameworks <p>5.2.2.1 - Center for Internet Security (CIS) 5.2.2.2 - National Institute of Standards and Technology (NIST) RMF/CSF 5.2.2.3 - International Organization for Standardization (ISO) 27001/27002/27701/31000 5.2.2.4 - SSAE SOC 2 Type II/III 5.2.2.5.1 - Cloud security alliance - Cloud control matrix 5.2.2.5.2 - Cloud security alliance - Reference architecture</p>
14.3	Sensitive Data and Privacy	<p>2.7 Explain the importance of physical security controls.</p> <ul style="list-style-type: none"> • 2.7.23 - Secure data destruction <p>2.7.23.1 - Burning 2.7.23.2 - Shredding 2.7.23.3 - Pulping 2.7.23.4 - Pulverizing</p>

		<p>2.7.23.5 - Degaussing 2.7.23.6 - Third-party solutions</p> <p>5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.</p> <ul style="list-style-type: none"> • 5.2.1 - Regulations, standards, and legislation <p>5.5 Explain privacy and sensitive data concepts in relation to security.</p> <ul style="list-style-type: none"> • 5.5.1 - Organizational consequences of privacy breaches <ul style="list-style-type: none"> 5.5.1.1 - Reputation damage 5.5.1.2 - Identity theft 5.5.1.3 - Fines 5.5.1.4 - IP theft • 5.5.3 - Data types <ul style="list-style-type: none"> 5.5.3.1.1 - Classifications - Public 5.5.3.1.2 - Classifications - Private 5.5.3.1.3 - Classifications - Sensitive 5.5.3.1.4 - Classifications - Confidential 5.5.3.1.5 - Classifications - Critical 5.5.3.1.6 - Classifications - Proprietary 5.5.3.2 - Personally identifiable information (PII) • 5.5.4 - Privacy enhancing technologies <ul style="list-style-type: none"> 5.5.4.1 - Data minimization 5.5.4.2 - Data masking 5.5.4.3 - Tokenization 5.5.4.4 - Anonymization 5.5.4.5 - Pseudo-anonymization • 5.5.5 - Roles and responsibilities
--	--	--

		5.5.5.1 - Data owners 5.5.5.2 - Data controller 5.5.5.3 - Data processor 5.5.5.4 - Data custodian/steward 5.5.5.5 - Data privacy officer (DPO)
A.0	TestOut Security Pro - Practice Exams	
A.1	Prepare for TestOut Security Pro Certification	
A.2	TestOut Security Pro Domain Review	
B.0	CompTIA Security+ SY0-601 - Practice Exams	
B.1	Prepare for CompTIA Security+ SY0-601 Certification	
B.2	CompTIA Security+ Domain Review (20 Questions)	
B.3	CompTIA Security+ Domain Review (All Questions)	

Objective Mapping: CompTIA SY0-601 Objective to LabSim Section

#	Domain	TestOut Module.Section
1.0	Attacks, Threats, and Vulnerabilities	
1.1	<p>Compare and contrast different types of social engineering techniques.</p> <ul style="list-style-type: none"> 1.1.1 - Phishing 1.1.2 - Smishing 1.1.3 - Vishing 1.1.4 - Spam 1.1.5 - Spam over Internet messaging (SPIM) 1.1.6 - Spear phishing 1.1.7 - Dumpster diving 1.1.8 - Shoulder surfing 1.1.9 - Pharming 1.1.10 - Tailgating 1.1.11 - Eliciting information 1.1.12 - Whaling 1.1.13 - Prepending 1.1.14 - Identity fraud 1.1.15 - Invoice scams 1.1.16 - Credential harvesting 1.1.17 - Reconnaissance 1.1.18 - Hoax 1.1.19 - Impersonation 1.1.20 - Watering hole attack 1.1.21 - Typo squatting 1.1.22 - Influence campaigns <ul style="list-style-type: none"> ○ 1.1.22.1 - Hybrid warfare ○ 1.1.22.2 - Social media 1.1.23 - Principles (reasons for effectiveness) <ul style="list-style-type: none"> ○ 1.1.23.1 - Authority ○ 1.1.23.2 - Intimidation ○ 1.1.23.3 - Consensus ○ 1.1.23.4 - Scarcity ○ 1.1.23.5 - Familiarity 	<p>1.2 2.1, 2.3 5.6, 5.10 11.2, 11.7 13.3</p>

	<ul style="list-style-type: none"> ○ 1.1.23.6 - Trust ○ 1.1.23.7 - Urgency 	
1.2	<p>Given a scenario, analyze potential indicators to determine the type of attack.</p> <p>1.2.1 - Malware</p> <ul style="list-style-type: none"> ○ 1.2.1.1 - Ransomware ○ 1.2.1.2 - Trojans ○ 1.2.1.3 - Worms ○ 1.2.1.4 - Potentially unwanted programs (PUPs) ○ 1.2.1.5 - Fileless virus ○ 1.2.1.6 - Command and control ○ 1.2.1.7 - Bots ○ 1.2.1.8 - Crypto malware ○ 1.2.1.9 - Logic bombs ○ 1.2.1.10 - Spyware ○ 1.2.1.11 - Keyloggers ○ 1.2.1.12 - Remote access Trojan (RAT) ○ 1.2.1.13 - Rootkit ○ 1.2.1.14 - Backdoor <p>1.2.2 - Password attacks</p> <ul style="list-style-type: none"> ○ 1.2.2.1 - Spraying ○ 1.2.2.2 - Dictionary ○ 1.2.2.3 - Brute force ○ 1.2.2.3.1 - Brute force - Offline ○ 1.2.2.3.2 - Brute force - Online ○ 1.2.2.4 - Rainbow tables ○ 1.2.2.5 - Plaintext/unencrypted <p>1.2.3 - Physical attacks</p> <ul style="list-style-type: none"> ○ 1.2.3.1 - Malicious universal serial bus (USB) cable ○ 1.2.3.2 - Malicious flash drive ○ 1.2.3.3 - Card cloning ○ 1.2.3.4 - Skimming <p>1.2.4 - Adversarial artificial intelligence (AI)</p> <ul style="list-style-type: none"> ○ 1.2.4.1 - Tainted training data for machine learning (ML) ○ 1.2.4.2 - Security of machine learning algorithms <p>1.2.5 - Supply-chain attacks</p> <p>1.2.6 - Cloud-based vs. on-premises attacks</p>	<p>2.2, 2.4</p> <p>3.2</p> <p>4.2</p> <p>5.9</p> <p>7.1, 7.3</p> <p>11.7</p>

	<p>1.2.7 - Cryptographic attacks</p> <ul style="list-style-type: none"> ○ 1.2.7.1 - Birthday ○ 1.2.7.2 - Collision ○ 1.2.7.3 - Downgrade 	
1.3	<p>Given a scenario, analyze potential indicators associated with application attacks.</p> <p>1.3.1 - Privilege escalation</p> <p>1.3.2 - Cross-site scripting</p> <p>1.3.3 - Injections</p> <ul style="list-style-type: none"> ○ 1.3.3.1 - Structured query language (SQL) ○ 1.3.3.2 - Dynamic link library (DLL) ○ 1.3.3.3 - Lightweight directory access protocol (LDAP) ○ 1.3.3.4 - Extensible markup language (XML) <p>1.3.4 - Pointer/object dereference</p> <p>1.3.5 - Directory traversal</p> <p>1.3.6 - Buffer overflows</p> <p>1.3.7 - Race conditions</p> <ul style="list-style-type: none"> ○ 1.3.7.1 - Time of check/time of use <p>1.3.8 - Error handling</p> <p>1.3.9 - Improper input handling</p> <p>1.3.10 - Replay attack</p> <ul style="list-style-type: none"> ○ 1.3.10.1 - Session replays <p>1.3.11 - Integer overflow</p> <p>1.3.12 - Request forgeries</p> <ul style="list-style-type: none"> ○ 1.3.12.1 - Server-side ○ 1.3.12.2 - Client-side ○ 1.3.12.3 - Cross-site <p>1.3.13 - Application programming interface (API) attacks</p> <p>1.3.14 - Resource exhaustion</p> <p>1.3.15 - Memory leak</p> <p>1.3.16 - Secure sockets layer (SSL) stripping</p> <p>1.3.17 - Driver manipulation</p> <ul style="list-style-type: none"> ○ 1.3.17.1 - Shimming ○ 1.3.17.2 - Refactoring <p>1.3.18 - Pass the hash</p>	<p>2.4</p> <p>5.9</p> <p>6.1</p> <p>10.3</p>

1.4	<p>Given a scenario, analyze potential indicators associated with network attacks.</p> <ul style="list-style-type: none"> 1.4.1 - Wireless <ul style="list-style-type: none"> ○ 1.4.1.1 - Evil twin ○ 1.4.1.2 - Rogue access point ○ 1.4.1.3 - Bluesnarfing ○ 1.4.1.4 - Bluejacking ○ 1.4.1.5 - Disassociation ○ 1.4.1.6 - Jamming ○ 1.4.1.7 - Radio frequency identifier (RFID) ○ 1.4.1.8 - Near field communication (NFC) ○ 1.4.1.9 - Initialization vector (IV) 1.4.2 - Man in the middle 1.4.3 - Man in the browser 1.4.4 - Layer 2 attacks <ul style="list-style-type: none"> ○ 1.4.4.1 - Address resolution protocol (ARP) poisoning ○ 1.4.4.2 - Media access control (MAC) flooding ○ 1.4.4.3 - MAC cloning 1.4.5 - Domain name system (DNS) <ul style="list-style-type: none"> ○ 1.4.5.1 - Domain hijacking ○ 1.4.5.2 - DNS poisoning ○ 1.4.5.3 - Universal resource locator (URL) redirection ○ 1.4.5.4 - Domain reputation 1.4.6 - Distributed denial of service (DDoS) <ul style="list-style-type: none"> ○ 1.4.6.1 - Network ○ 1.4.6.2 - Application ○ 1.4.6.3 - Operational technology (OT) 1.4.7 - Malicious code or script execution <ul style="list-style-type: none"> ○ 1.4.7.1 - PowerShell ○ 1.4.7.2 - Python ○ 1.4.7.3 - Bash ○ 1.4.7.4 - Macros ○ 1.4.7.5 - Virtual Basic for Applications (VBA) 	5.8, 5.11 8.2 10.3 11.6 12.6
1.5	<p>Explain different threat actors, vectors, and intelligence sources.</p> <ul style="list-style-type: none"> 1.5.1 - Actors and threats <ul style="list-style-type: none"> ○ 1.5.1.1 - Advanced persistent threat (APT) 	1.1, 1.2 2.1, 2.3 10.4 11.4

	<ul style="list-style-type: none"> ○ 1.5.1.2 - Insider threats ○ 1.5.1.3 - State actors ○ 1.5.1.4 - Hacktivists ○ 1.5.1.5 - Script kiddies ○ 1.5.1.6 - Criminal syndicates ○ 1.5.1.7 - Hackers ○ 1.5.1.7.1 - Hackers - White hat ○ 1.5.1.7.2 - Hackers - Black hat ○ 1.5.1.7.3 - Hackers - Gray hat ○ 1.5.1.8 - Shadow IT ○ 1.5.1.9 - Competitors 1.5.2 - Attributes of actors <ul style="list-style-type: none"> ○ 1.5.2.1 - Internal/external ○ 1.5.2.2 - Level of sophistication/capability ○ 1.5.2.3 - Resources/funding ○ 1.5.2.4 - Intent/motivation 1.5.3 - Vectors <ul style="list-style-type: none"> ○ 1.5.3.1 - Direct access ○ 1.5.3.2 - Wireless ○ 1.5.3.3 - Email ○ 1.5.3.4 - Supply chain ○ 1.5.3.5 - Social media ○ 1.5.3.6 - Removable media ○ 1.5.3.7 - Cloud 1.5.4 - Threat intelligence sources <ul style="list-style-type: none"> ○ 1.5.4.1 - Open source intelligence (OSINT) ○ 1.5.4.2 - Closed/proprietary ○ 1.5.4.3 - Vulnerability databases ○ 1.5.4.4 - Public/private information sharing centers ○ 1.5.4.5 - Dark web ○ 1.5.4.6 - Indicators of compromise ○ 1.5.4.7 - Automated indicator sharing (AIS) ○ 1.5.4.7.1 - AIS - Structured threat information exchange (STIX)/Trusted automated exchange of indicator information (TAXII) ○ 1.5.4.8 - Predictive analysis ○ 1.5.4.9 - Threat maps ○ 1.5.4.10 - File/code repositories 1.5.5 - Research sources <ul style="list-style-type: none"> ○ 1.5.5.1 - Vendor websites 	13.3
--	--	------

	<ul style="list-style-type: none"> ○ 1.5.5.2 - Vulnerability feeds ○ 1.5.5.3 - Conferences ○ 1.5.5.4 - Academic journals ○ 1.5.5.5 - Request for comments (RFC) ○ 1.5.5.6 - Local industry groups ○ 1.5.5.7 - Social media ○ 1.5.5.8 - Threat feeds ○ 1.5.5.9 - Adversary tactics, techniques, and procedures (TTP) 	
1.6	<p>Explain the security concerns associated with various types of vulnerabilities.</p> <ul style="list-style-type: none"> 1.6.1 - Cloud-based vs. on-premises vulnerabilities 1.6.2 - Zero-day 1.6.3 - Weak configurations <ul style="list-style-type: none"> ○ 1.6.3.1 - Open permissions ○ 1.6.3.2 - Unsecured root accounts ○ 1.6.3.3 - Errors ○ 1.6.3.4 - Weak encryption ○ 1.6.3.5 - Unsecure protocols ○ 1.6.3.6 - Default settings ○ 1.6.3.7 - Open ports and services 1.6.4 - Third-party risks <ul style="list-style-type: none"> ○ 1.6.4.1 - Vendor management <ul style="list-style-type: none"> ○ 1.6.4.1.1 - Vendor management - System integration ○ 1.6.4.1.2 - Vendor management - Lack of vendor support ○ 1.6.4.2 - Supply chain ○ 1.6.4.3 - Outsourced code development ○ 1.6.4.4 - Data storage 1.6.5 - Improper or weak patch management <ul style="list-style-type: none"> ○ 1.6.5.1 - Firmware ○ 1.6.5.2 - Operating system (OS) ○ 1.6.5.3 - Applications 1.6.6 - Legacy platforms 1.6.6 - Impacts <ul style="list-style-type: none"> ○ 1.6.6.1 - Data loss ○ 1.6.6.2 - Data breaches ○ 1.6.6.3 - Data exfiltration ○ 1.6.6.4 - Identity theft 	<p>1.1 2.4 4.1, 4.2, 4.3, 4.4 5.13 6.9 7.3, 7.4 8.3 9.5 10.3 11.4</p>

	<ul style="list-style-type: none"> ○ 1.6.6.5 - Financial ○ 1.6.6.6 - Reputation ○ 1.6.6.7 - Availability loss 	
1.7	<p>Summarize the techniques used in security assessments.</p> <p>1.7.1 - Threat hunting</p> <ul style="list-style-type: none"> ○ 1.7.1.1 - Intelligence fusion ○ 1.7.1.2 - Threat feeds ○ 1.7.1.3 - Advisories and bulletins ○ 1.7.1.4 - Maneuver <p>1.7.2 - Vulnerability scans</p> <ul style="list-style-type: none"> ○ 1.7.2.1 - False positives ○ 1.7.2.2 - False negatives ○ 1.7.2.3 - Log reviews ○ 1.7.2.4 - Credentialed vs. non-credentialed ○ 1.7.2.5 - Intrusive vs. non-intrusive ○ 1.7.2.6 - Application ○ 1.7.2.7 - Web application ○ 1.7.2.8 - Network ○ 1.7.2.9 - Common Vulnerabilities and Exposures (CVE)/Common Vulnerability Scoring System (CVSS) ○ 1.7.2.10 - Configuration review <p>1.7.3 - Syslog/Security information and event management (SIEM)</p> <ul style="list-style-type: none"> ○ 1.7.3.1 - Review reports ○ 1.7.3.2 - Packet capture ○ 1.7.3.3 - Data inputs ○ 1.7.3.4 - User behavior analysis ○ 1.7.3.5 - Sentiment analysis ○ 1.7.3.6 - Security monitoring ○ 1.7.3.7 - Log aggregation ○ 1.7.3.8 - Log collectors <p>1.7.4 - Security orchestration, automation, response (SOAR)</p>	<p>5.10</p> <p>11.3, 11.4</p> <p>12.3, 12.4, 12.6</p>
1.8	<p>Explain the techniques used in penetration testing.</p> <p>1.8.1 - Penetration testing</p>	<p>1.2</p> <p>5.8</p> <p>11.1, 11.2</p>

	<ul style="list-style-type: none"> ○ 1.8.1.1 - White box ○ 1.8.1.2 - Black box ○ 1.8.1.3 - Gray box ○ 1.8.1.4 - Rules of engagement ○ 1.8.1.5 - Lateral movement ○ 1.8.1.6 - Privilege escalation ○ 1.8.1.7 - Persistence ○ 1.8.1.8 - Cleanup ○ 1.8.1.9 - Bug bounty ○ 1.8.1.10 - Pivoting <p>1.8.2 - Passive and active reconnaissance</p> <ul style="list-style-type: none"> ○ 1.8.2.1 - Drones/unmanned aerial vehicle (UAV) ○ 1.8.2.2 - War flying ○ 1.8.2.3 - War driving ○ 1.8.2.4 - Footprinting ○ 1.8.2.5 - OSINT <p>1.8.3 - Exercise types</p> <ul style="list-style-type: none"> ○ 1.8.3.1 - Red team ○ 1.8.3.2 - Blue team ○ 1.8.3.3 - White team ○ 1.8.3.4 - Purple team 	
2.0	Architecture and Design	
2.1	<p>Explain the importance of security concepts in an enterprise environment.</p> <p>2.1.1 - Configuration management</p> <ul style="list-style-type: none"> ○ 2.1.1.1 - Diagrams ○ 2.1.1.2 - Baseline configuration ○ 2.1.1.3 - Standard naming conventions ○ 2.1.1.4 - Internet protocol (IP) schema <p>2.1.2 - Data sovereignty</p> <p>2.1.3 - Data protection</p> <ul style="list-style-type: none"> ○ 2.1.3.1 - Data loss prevention (DLP) ○ 2.1.3.2 - Masking ○ 2.1.3.3 - Encryption ○ 2.1.3.4 - At rest ○ 2.1.3.5 - In transit/motion 	<p>4.1, 4.2</p> <p>5.1, 5.6</p> <p>7.2, 7.3, 7.4</p> <p>9.4, 9.5</p> <p>10.1, 10.2, 10.4</p> <p>12.3, 12.5, 12.7</p> <p>13.1</p>

	<ul style="list-style-type: none"> ○ 2.1.3.6 - In processing ○ 2.1.3.7 - Tokenization ○ 2.1.3.8 - Rights management <p>2.1.4 - Hardware security module (HSM)</p> <p>2.1.5 - Geographical considerations</p> <p>2.1.6 - Cloud access security broker (CASB)</p> <p>2.1.7 - Response and recovery controls</p> <p>2.1.8 - Secure Sockets Layer (SSL)/Transport Layer Security (TLS) inspection</p> <p>2.1.9 - Hashing</p> <p>2.1.10 - API considerations</p> <p>2.1.11 - Site resiliency</p> <ul style="list-style-type: none"> ○ 2.1.11.1 - Hot site ○ 2.1.11.2 - Cold site ○ 2.1.11.3 - Warm site <p>2.1.12 - Deception and disruption</p> <ul style="list-style-type: none"> ○ 2.1.12.1 - Honeypots ○ 2.1.12.2 - Honeyfiles ○ 2.1.12.3 - Honeynets ○ 2.1.12.4 - Fake telemetry ○ 2.1.12.5 - DNS sinkhole 	
2.2	<p>Summarize virtualization and cloud computing concepts.</p> <p>2.2.1 - Cloud models</p> <ul style="list-style-type: none"> ○ 2.2.1.1 - Infrastructure as a service (IaaS) ○ 2.2.1.2 - Platform as a service (PaaS) ○ 2.2.1.3 - Software as a service (SaaS) ○ 2.2.1.4 - Anything as a service (XaaS) ○ 2.2.1.5 - Public ○ 2.2.1.6 - Community ○ 2.2.1.7 - Private ○ 2.2.1.8 - Hybrid <p>2.2.2 - Cloud service providers</p> <p>2.2.3 - Managed service provider (MSP)/Managed security service provider (MSSP)</p> <p>2.2.4 - On-premises vs. off-premises</p> <p>2.2.5 - Fog computing</p> <p>2.2.6 - Edge computing</p> <p>2.2.7 - Thin client</p>	9.1, 9.2, 9.3, 9.4, 9.5

	<ul style="list-style-type: none"> 2.2.8 - Containers 2.2.9 - Micro-services/API 2.2.10 - Infrastructure as code <ul style="list-style-type: none"> ○ 2.2.10.1 - Software-defined networking (SDN) ○ 2.2.10.2 - Software-defined visibility (SDV) 2.2.11 - Serverless architecture 2.2.12 - Services integration 2.2.13 - Resource policies 2.2.14 - Transit gateway 2.2.15 - Virtualization <ul style="list-style-type: none"> ○ 2.2.15.1 - Virtual machine (VM) ○ 2.2.15.2 - sprawl avoidance ○ 2.2.15.3 - VM escape protection 	
2.3	<p>Summarize secure application development, deployment, and automation concepts.</p> <ul style="list-style-type: none"> 2.3.1 - Environment <ul style="list-style-type: none"> ○ 2.3.1.1 - Development ○ 2.3.1.2 - Test ○ 2.3.1.3 - Staging ○ 2.3.1.4 - Production ○ 2.3.1.5 - Quality assurance (QA) 2.3.2 - Provisioning and deprovisioning 2.3.3 - Integrity measurement 2.3.4 - Secure coding techniques <ul style="list-style-type: none"> ○ 2.3.4.1 - Normalization ○ 2.3.4.2 - Stored procedures ○ 2.3.4.3 - Obfuscation/camouflage ○ 2.3.4.4 - Code reuse/dead code ○ 2.3.4.5 - Server-side vs. client-side execution and validation ○ 2.3.4.6 - Memory management ○ 2.3.4.7 - Use of third-party libraries and software development kits (SDKs) ○ 2.3.4.8 - Data exposure 2.3.5 - Open Web Application Security Project (OWASP) 2.3.6 - Software diversity <ul style="list-style-type: none"> ○ 2.3.6.1 - Compiler ○ 2.3.6.2 - Binary 	10.3, 10.4

	<p>2.3.7 - Automation/scripting</p> <ul style="list-style-type: none"> ○ 2.3.7.1 - Automated courses of action ○ 2.3.7.2 - Continuous monitoring ○ 2.3.7.3 - Continuous validation ○ 2.3.7.4 - Continuous integration ○ 2.3.7.5 - Continuous delivery ○ 2.3.7.6 - Continuous deployment <p>2.3.8 - Elasticity 2.3.9 - Scalability 2.3.10 - Version control</p>	
2.4	<p>Summarize authentication and authorization design concepts.</p> <p>2.4.1 - Authentication methods</p> <ul style="list-style-type: none"> ○ 2.4.1.1 - Directory services ○ 2.4.1.2 - Federation ○ 2.4.1.3 - Attestation ○ 2.4.1.4 - Technologies <ul style="list-style-type: none"> ○ 2.4.1.4.1 - Technologies - Time-based one-time password (TOTP) ○ 2.4.1.4.2 - Technologies - HMAC-based one-time password (HOTP) ○ 2.4.1.4.3 - Technologies - Short message service (SMS) ○ 2.4.1.4.4 - Technologies - Token key ○ 2.4.1.4.5 - Technologies - Static codes ○ 2.4.1.4.6 - Technologies - Authentication applications ○ 2.4.1.4.7 - Technologies - Push notifications ○ 2.4.1.4.8 - Technologies - Phone call ○ 2.4.1.5 - Smart card authentication <p>2.4.2 - Biometrics</p> <ul style="list-style-type: none"> ○ 2.4.2.1 - Fingerprint ○ 2.4.2.2 - Retina ○ 2.4.2.3 - Iris ○ 2.4.2.4 - Facial ○ 2.4.2.5 - Voice ○ 2.4.2.6 - Vein ○ 2.4.2.7 - Gait analysis ○ 2.4.2.8 - Efficacy rates ○ 2.4.2.9 - False acceptance ○ 2.4.2.10 - False rejection 	<p>4.2 5.7 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.9 7.3</p>

	<ul style="list-style-type: none"> ○ 2.4.2.11 - Crossover error rate <p>2.4.3 - Multifactor authentication (MFA) factors and attributes</p> <ul style="list-style-type: none"> ○ 2.4.3.1 - Factors ○ 2.4.3.1.1 - Factors - Something you know ○ 2.4.3.1.2 - Factors - Something you have ○ 2.4.3.1.3 - Factors - Something you are ○ 2.4.3.2 - Attributes ○ 2.4.3.2.1 - Attributes - Somewhere you are ○ 2.4.3.2.2 - Attributes - Something you can do ○ 2.4.3.2.3 - Attributes - Something you exhibit ○ 2.4.3.2.4 - Attributes - Someone you know <p>2.4.4 - Authentication, authorization, and accounting (AAA)</p> <p>2.4.5 - Cloud vs. on-premises requirements</p>	
2.5	<p>Given a scenario, implement cybersecurity resilience.</p> <p>2.5.1 - Redundancy</p> <ul style="list-style-type: none"> ○ 2.5.1.1 - Geographic dispersal ○ 2.5.1.2 - Disk ○ 2.5.1.2.1 - Disk - Redundant array of inexpensive disks (RAID) levels ○ 2.5.1.2.2 - Disk - Multipath ○ 2.5.1.3 - Network ○ 2.5.1.3.1 - Network - Load balancers ○ 2.5.1.3.2 - Network - Network interface card (NIC) teaming ○ 2.5.1.4 - Power ○ 2.5.1.4.1 - Power - Uninterruptible power supply (UPS) ○ 2.5.1.4.2 - Power - Generator ○ 2.5.1.4.3 - Power - Dual supply ○ 2.5.1.4.4 - Power - Managed power distribution units (PDUs) <p>2.5.2 - Replication</p> <ul style="list-style-type: none"> ○ 2.5.2.1 - Storage area network (SAN) ○ 2.5.2.2 - VM <p>2.5.3 - On-premises vs. cloud</p> <p>2.5.4 - Backup types</p> <ul style="list-style-type: none"> ○ 2.5.4.1 - Full ○ 2.5.4.2 - Incremental ○ 2.5.4.3 - Snapshot ○ 2.5.4.4 - Differential 	<p>3.3 12.7, 12.8</p>

	<ul style="list-style-type: none"> ○ 2.5.4.5 - Tape ○ 2.5.4.6 - Disk ○ 2.5.4.7 - Copy ○ 2.5.4.8 - Network attached storage (NAS) ○ 2.5.4.9 - SAN ○ 2.5.4.10 - Cloud ○ 2.5.4.11 - Image ○ 2.5.4.12 - Online vs. offline ○ 2.5.4.13 - Offsite storage ○ 2.5.4.13.1 - Offsite storage - Distance considerations <p>2.5.5 - Non-persistence</p> <ul style="list-style-type: none"> ○ 2.5.5.1 - Revert to known state ○ 2.5.5.2 - Last known good configuration ○ 2.5.5.3 - Live boot media <p>2.5.6 - High availability</p> <ul style="list-style-type: none"> ○ 2.5.6.1 - Scalability <p>2.5.7 - Restoration order</p> <p>2.5.8 - Diversity</p> <ul style="list-style-type: none"> ○ 2.5.8.1 - Technologies ○ 2.5.8.2 - Vendors ○ 2.5.8.3 - Crypto ○ 2.5.8.4 - Controls 	
2.6	<p>Explain the security implications of embedded and specialized systems.</p> <p>2.3.1 - Embedded systems</p> <ul style="list-style-type: none"> ○ 2.3.1.1 - Raspberry Pi ○ 2.3.1.2 - Field programmable gate array (FPGA) ○ 2.3.1.3 - Arduino <p>2.3.2 - System control and data acquisition (SCADA)/industrial control system (ICS)</p> <ul style="list-style-type: none"> ○ 2.3.2.1 - Facilities ○ 2.3.2.2 - Industrial ○ 2.3.2.3 - Manufacturing ○ 2.3.2.4 - Energy ○ 2.3.2.5 - Logistics <p>2.3.3 - Internet of Things (IoT)</p> <ul style="list-style-type: none"> ○ 2.3.3.1 - Sensors ○ 2.3.3.2 - Smart devices 	<p>5.12</p> <p>9.9</p>

	<ul style="list-style-type: none"> ○ 2.3.3.3 - Wearables ○ 2.3.3.4 - Facility automation ○ 2.3.3.5 - Weak defaults <p>2.3.4 - Specialized</p> <ul style="list-style-type: none"> ○ 2.3.4.1 - Medical systems ○ 2.3.4.2 - Vehicles ○ 2.3.4.3 - Aircraft ○ 2.3.4.4 - Smart meters <p>2.3.5 - Voice over IP (VoIP)</p> <p>2.3.6 - Heating, ventilation, air conditioning (HVAC)</p> <p>2.3.7 - Drones/AVs</p> <p>2.3.8 - Multifunction printer (MFP)</p> <p>2.3.9 - Real-time operating system (RTOS)</p> <p>2.3.10 - Surveillance systems</p> <p>2.3.11 - System on chip (SoC)</p> <p>2.3.12 - Communication considerations</p> <ul style="list-style-type: none"> ○ 2.3.12.1 - 5G ○ 2.3.12.2 - Narrow-band ○ 2.3.12.3 - Baseband radio ○ 2.3.12.4 - Subscriber identity module (SIM) cards ○ 2.3.12.5 - Zigbee <p>2.3.13 - Constraints</p> <ul style="list-style-type: none"> ○ 2.3.13.1 - Power ○ 2.3.13.2 - Compute ○ 2.3.13.3 - Network ○ 2.3.13.4 - Crypto ○ 2.3.13.5 - Inability to patch ○ 2.3.13.6 - Authentication ○ 2.3.13.7 - Range ○ 2.3.13.8 - Cost ○ 2.3.13.9 - Implied trust 	
2.7	<p>Explain the importance of physical security controls.</p> <ul style="list-style-type: none"> 2.7.1 - Bollards/barricades 2.7.2 - Mantraps 2.7.3 - Badges 2.7.4 - Alarms 	<p>3.1, 3.2, 3.3 5.2, 5.13 14.3</p>

	<ul style="list-style-type: none">2.7.5 - Signage2.7.6 - Cameras<ul style="list-style-type: none">○ 2.7.6.1 - Motion recognition○ 2.7.6.2 - Object detection2.7.7 - Closed-circuit television (CCTV)2.7.8 - Industrial camouflage2.7.9 - Personnel<ul style="list-style-type: none">○ 2.7.9.1 - Guards○ 2.7.9.2 - Robot sentries○ 2.7.9.3 - Reception○ 2.7.9.4 - Two-person integrity/control2.7.10 - Locks<ul style="list-style-type: none">○ 2.7.10.1 - Biometrics○ 2.7.10.2 - Electronic○ 2.7.10.3 - Physical○ 2.7.10.4 - Cable locks2.7.11 - USB data blocker2.7.12 - Lighting2.7.13 - Fencing2.7.14 - Fire suppression2.7.15 - Sensors<ul style="list-style-type: none">○ 2.7.15.1 - Motion detection○ 2.7.15.2 - Noise detection○ 2.7.15.3 - Proximity reader○ 2.7.15.4 - Moisture detection○ 2.7.15.5 - Cards○ 2.7.15.6 - Temperature2.7.16 - Drones/UAV2.7.17 - Visitor logs2.7.18 - Faraday cages2.7.19 - Air gap2.7.20 - Demilitarized zone (DMZ)2.7.21 - Protected cable distribution2.7.22 - Secure areas<ul style="list-style-type: none">○ 2.7.22.1 - Air gap○ 2.7.22.2 - Vault○ 2.7.22.3 - Safe○ 2.7.22.4 - Hot aisle○ 2.7.22.5 - Cold aisle	
--	--	--

	<p>2.7.23 - Secure data destruction</p> <ul style="list-style-type: none"> ○ 2.7.23.1 - Burning ○ 2.7.23.2 - Shredding ○ 2.7.23.3 - Pulping ○ 2.7.23.4 - Pulverizing ○ 2.7.23.5 - Degaussing ○ 2.7.23.6 - Third-party solutions 	
2.8	<p>Summarize the basics of cryptographic concepts.</p> <p>2.8.1 - Digital signatures</p> <p>2.8.2 - Key length</p> <p>2.8.3 - Key stretching</p> <p>2.8.4 - Salting</p> <p>2.8.5 - Hashing</p> <p>2.8.6 - Key exchange</p> <p>2.8.7 - Elliptical curve cryptography</p> <p>2.8.8 - Perfect forward secrecy</p> <p>2.8.9 - Quantum</p> <ul style="list-style-type: none"> ○ 2.8.9.1 - Communications ○ 2.8.9.2 - Computing <p>2.8.10 - Post-quantum</p> <p>2.8.11 - Ephemeral</p> <p>2.8.12 - Modes of operation</p> <ul style="list-style-type: none"> ○ 2.8.12.1 - Authenticated ○ 2.8.12.2 - Unauthenticated ○ 2.8.12.3 - Counter <p>2.8.13 - Blockchain</p> <ul style="list-style-type: none"> ○ 2.8.13.1 - Public ledgers <p>2.8.14 - Cipher suites</p> <ul style="list-style-type: none"> ○ 2.8.14.1 - Stream ○ 2.8.14.2 - Block <p>2.8.15 - Symmetric vs. asymmetric</p> <p>2.8.16 - Lightweight cryptography</p> <p>2.8.17 - Steganography</p> <ul style="list-style-type: none"> ○ 2.8.17.1 - Audio ○ 2.8.17.2 - Video ○ 2.8.17.3 - Image 	<p>1.1</p> <p>5.10</p> <p>7.1, 7.2, 7.3, 7.4</p> <p>11.7</p>

	<ul style="list-style-type: none"> 2.8.18 - Homomorphic encryption 2.8.19 - Common use cases <ul style="list-style-type: none"> ○ 2.8.19.1 - Low power devices ○ 2.8.19.2 - Low latency ○ 2.8.19.3 - High resiliency ○ 2.8.19.4 - Supporting confidentiality ○ 2.8.19.5 - Supporting integrity ○ 2.8.19.6 - Supporting obfuscation ○ 2.8.19.7 - Supporting authentication ○ 2.8.19.8 - Supporting non-repudiation ○ 2.8.19.9 - Resource vs. security constraints 2.8.20 - Limitations <ul style="list-style-type: none"> ○ 2.8.20.1 - Speed ○ 2.8.20.2 - Size ○ 2.8.20.3 - Weak keys ○ 2.8.20.4 - Time ○ 2.8.20.5 - Longevity ○ 2.8.20.6 - Predictability ○ 2.8.20.7 - Reuse ○ 2.8.20.8 - Entropy ○ 2.8.20.9 - Computational overheads ○ 2.8.20.10 - Resource vs. security constraints 	
3.0	Implementation	
3.1	<p>Given a scenario, implement secure protocols.</p> <ul style="list-style-type: none"> 3.1.1 - Protocols <ul style="list-style-type: none"> ○ 3.1.1.1 - Domain Name System ○ 3.1.1.2 - Security Extension (DNSSEC) ○ 3.1.1.3 - SSH ○ 3.1.1.4 - Secure/multipurpose internet mail exchanger (S/MIME) ○ 3.1.1.5 - Secure real-time protocol (SRTP) ○ 3.1.1.6 - LDAPS ○ 3.1.1.7 - File transfer protocol, secure (FTPS) ○ 3.1.1.8 - Secured file transfer protocol (SFTP) ○ 3.1.1.9 - Simple Network Management Protocol, version 3 (SNMPv3) ○ 3.1.1.10 - Hypertext transfer protocol over SSL/TLS (HTTPS) 	<p>4.1, 4.3 5.13 6.9, 6.10 7.4 9.7 10.1, 10.3 12.4 13.3</p>

	<ul style="list-style-type: none"> ○ 3.1.1.11 - IPsec ○ 3.1.1.11.1 - IPsec - Authentication header (AH)/Encapsulated security payload (ESP) ○ 3.1.1.11.2 - IPsec - Tunnel/transport ○ 3.1.1.12 - Secure post office protocol (POP)/Internet message access protocol (IMAP) <p>3.1.2 - Use cases</p> <ul style="list-style-type: none"> ○ 3.1.2.1 - Voice and video ○ 3.1.2.2 - Time synchronization ○ 3.1.2.3 - Email and web ○ 3.1.2.4 - File transfer ○ 3.1.2.5 - Directory services ○ 3.1.2.6 - Remote access ○ 3.1.2.7 - Domain name resolution ○ 3.1.2.8 - Routing and switching ○ 3.1.2.9 - Network address allocation ○ 3.1.2.10 - Subscription services 	
3.2	<p>Given a scenario, implement host or application security solutions.</p> <p>3.2.1 - Endpoint protection</p> <ul style="list-style-type: none"> ○ 3.2.1.1 - Antivirus ○ 3.2.1.2 - Anti-malware ○ 3.2.1.3 - Endpoint detection and response (EDR) ○ 3.2.1.4 - DLP ○ 3.2.1.5 - Next-generation firewall ○ 3.2.1.6 - Host intrusion prevention system (HIPS) ○ 3.2.1.7 - Host intrusion detection system (HIDS) ○ 3.2.1.9 - Host-based firewall <p>3.2.2 - Boot integrity</p> <ul style="list-style-type: none"> ○ 3.2.2.1 - Boot security/Unified Extensible Firmware Interface (UEFI) ○ 3.2.2.2 - Measured boot ○ 3.2.2.3 - Boot attestation <p>3.2.3 - Database</p> <ul style="list-style-type: none"> ○ 3.2.3.1 - Tokenization ○ 3.2.3.2 - Salting ○ 3.2.3.3 - Hashing <p>3.2.4 - Application security</p>	<p>1.2 4.1, 4.2, 4.4 5.3, 5.10 7.2, 7.4 8.3 9.1 10.2, 10.3, 10.4 11.3 12.2 13.3</p>

	<ul style="list-style-type: none"> ○ 3.2.4.1 - Input validations ○ 3.2.4.2 - Secure cookies ○ 3.2.4.3 - Hypertext Transfer Protocol (HTTP) headers ○ 3.2.4.4 - Code signing ○ 3.2.4.5 - Whitelisting ○ 3.2.4.6 - Blacklisting ○ 3.2.4.7 - Secure coding practices ○ 3.2.4.8 - Static code analysis ○ 3.2.4.8.1 - Static code analysis - Manual code review ○ 3.2.4.9 - Dynamic code analysis ○ 3.2.4.10 - Fuzzing <p>3.2.5 - Hardening</p> <ul style="list-style-type: none"> ○ 3.2.5.1 - Open ports and services ○ 3.2.5.2 - Registry ○ 3.2.5.3 - Disk encryption ○ 3.2.5.4 - OS ○ 3.2.5.5- Patch management ○ 3.2.5.5.1 - Patch management - Third-party updates ○ 3.2.5.5.2 - Patch management - Auto-update <p>3.2.6 - Self-encrypting drive (SED)/full disk encryption (FDE)</p> <ul style="list-style-type: none"> ○ 3.2.6.1 - Opal <p>3.2.7 - Hardware root of trust</p> <p>3.2.8 - Trusted Platform Module (TPM)</p> <p>3.2.9 - Sandboxing</p>	
3.3	<p>Given a scenario, implement secure network designs.</p> <p>3.3.1 - Load balancing</p> <ul style="list-style-type: none"> ○ 3.3.1.1 - Active/active ○ 3.3.1.2 - Active/passive ○ 3.3.1.3 - Scheduling ○ 3.3.1.4 - Virtual IP ○ 3.3.1.5 - Persistence <p>3.3.2 - Network segmentation</p> <ul style="list-style-type: none"> ○ 3.3.2.1 -Virtual local area network (VLAN) ○ 3.3.2.2 -DMZ ○ 3.3.2.3 -East-west traffic ○ 3.3.2.4 -Extranet 	<p>4.1, 4.2, 4.3, 4.4 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.11, 5.12, 5.13 6.3 8.3 9.1, 9.2, 9.8 11.3, 11.5 12.2, 12.4</p>

	<ul style="list-style-type: none"> ○ 3.3.2.5 -Intranet ○ 3.3.2.6 -Zero trust 3.3.3 - Virtual private network (VPN) <ul style="list-style-type: none"> ○ 3.3.3.1 - Always on ○ 3.3.3.2 - Split tunnel vs. full tunnel ○ 3.3.3.3 - Remote access vs. site-to-site ○ 3.3.3.4 - IPSec ○ 3.3.3.5 - SSL/TLS ○ 3.3.3.6 - HTML5 ○ 3.3.3.7 - Layer 2 tunneling protocol (L2TP) 3.3.4 - DNS 3.3.5 - Network access control (NAC) <ul style="list-style-type: none"> ○ 3.3.5.1 - Agent and agentless 3.3.6 - Out-of-band management 3.3.7 - Port security <ul style="list-style-type: none"> ○ 3.3.7.1 - Broadcast storm prevention ○ 3.3.7.2 - Bridge Protocol Data Unit (BPDU) guard ○ 3.3.7.3 - Loop prevention ○ 3.3.7.4 - Dynamic Host Configuration Protocol (DHCP) snooping ○ 3.3.7.5 - Media access control (MAC) filtering 3.3.8 - Network appliances <ul style="list-style-type: none"> ○ 3.3.8.1 - Jump servers ○ 3.3.8.2 - Proxy servers <ul style="list-style-type: none"> ○ 3.3.8.2.1 - Proxy servers - Forward ○ 3.3.8.2.2 - Proxy servers - Reverse ○ 3.3.8.3 - Network-based intrusion detection system (NIDS)/network-based intrusion prevention system (NIPS) <ul style="list-style-type: none"> ○ 3.3.8.3.1 - NDIS/NIPS - Signature based ○ 3.3.8.3.2 - NDIS/NIPS - Heuristic/behavior ○ 3.3.8.3.3 - NDIS/NIPS - Anomaly ○ 3.3.8.3.4 - NDIS/NIPS - Inline vs. passive ○ 3.3.8.4 - HSM ○ 3.3.8.5 - Sensors ○ 3.3.8.6 - Collectors ○ 3.3.8.7 - Aggregators <ul style="list-style-type: none"> ○ 3.3.8.7.1 - Firewalls - Web application firewall (WAF) ○ 3.3.8.7.2 - Firewalls - Next-generation firewall ○ 3.3.8.7.3 - Firewalls - Stateful ○ 3.3.8.7.4 - Firewalls - Stateless 	
--	--	--

	<ul style="list-style-type: none"> ○ 3.3.8.7.5 - Firewalls - Unified threat management (UTM) ○ 3.3.8.7.6 - Firewalls - Network address translation (NAT) gateway ○ 3.3.8.7.7 - Firewalls - Content/URL filter ○ 3.3.8.7.8 - Firewalls - Open-source vs. proprietary ○ 3.3.8.7.9 - Firewalls - Hardware vs. software ○ 3.3.8.7.10 - Firewalls - Appliance vs. host-based vs. virtual <p>3.3.9 - Access control list (ACL) 3.3.10 - Route security 3.3.11 - Quality of service (QoS) 3.3.12 - Implications of IPv6 3.3.13 - Port spanning/port mirroring <ul style="list-style-type: none"> ○ 3.3.13.1 - Port taps 3.3.15 - Monitoring services 3.3.16 - File integrity monitors</p>	
3.4	<p>Given a scenario, install and configure wireless security settings.</p> <p>3.4.1 - Cryptographic protocols</p> <ul style="list-style-type: none"> ○ 3.4.1.1 - WiFi protected access II (WPA2) ○ 3.4.1.2 - WiFi protected access III (WPA3) ○ 3.4.1.3 - Counter-mode/CBC-MAC protocol (CCMP) ○ 3.4.1.4 - Simultaneous Authentication of Equals (SAE) <p>3.4.2 - Authentication protocols</p> <ul style="list-style-type: none"> ○ 3.4.2.1 - Extensible Authentication Protocol (EAP) ○ 3.4.2.2 - Protected Extensible Application Protocol (PEAP) ○ 3.4.2.3 - EAP-FAST ○ 3.4.2.4 - EAP-TLS ○ 3.4.2.5 - EAP-TTLS ○ 3.4.2.6 - IEEE 802.1X ○ 3.4.2.5 - Remote Authentication Dial-in ○ 3.4.2.6 - User Server (RADIUS) Federation <p>3.4.3 - Methods</p> <ul style="list-style-type: none"> ○ 3.4.3.1 - Pre-shared key (PSK) vs. Enterprise vs. Open ○ 3.4.3.2 - WiFi Protected Setup (WPS) ○ 3.4.3.3 - Captive portals <p>3.4.4 - Installation considerations</p> <ul style="list-style-type: none"> ○ 3.4.4.1 - Site surveys ○ 3.4.4.2 - Heat maps 	<p>1.2 5.9, 5.11, 5.12 8.1, 8.2, 8.3</p>

	<ul style="list-style-type: none"> ○ 3.4.4.3 - WiFi analyzers ○ 3.4.4.4 - Channel overlays ○ 3.4.4.5 - Wireless access point ○ 3.4.4.6 - (WAP) placement ○ 3.4.4.7 - Controller and access point security 	
3.5	<p>Given a scenario, implement secure mobile solutions.</p> <p>3.5.1 - Connection methods and receivers</p> <ul style="list-style-type: none"> ○ 3.5.1.1 - Cellular ○ 3.5.1.2 - WiFi ○ 3.5.1.3 - Bluetooth ○ 3.5.1.4 - NFC ○ 3.5.1.5 - Infrared ○ 3.5.1.6 - USB ○ 3.5.1.7 - Point to point ○ 3.5.1.8 - Point to multipoint ○ 3.5.1.9 - Global Positioning System (GPS) ○ 3.5.1.10 - RFID <p>3.5.2 - Mobile device management (MDM)</p> <ul style="list-style-type: none"> ○ 3.5.2.1 - Application management ○ 3.5.2.2 - Content management ○ 3.5.2.3 - Remote wipe ○ 3.5.2.4 - Geofencing ○ 3.5.2.5 - Geolocation ○ 3.5.2.6 - Screen locks ○ 3.5.2.7 - Push notifications ○ 3.5.2.8 - Passwords and pins ○ 3.5.2.9 - Biometrics ○ 3.5.2.10 - Context-aware authentication ○ 3.5.2.11 - Containerization ○ 3.5.2.12 - Storage segmentation ○ 3.5.2.13 - Full device encryption <p>3.5.3 - Mobile devices</p> <ul style="list-style-type: none"> ○ 3.5.3.1 - MicroSD HSM ○ 3.5.3.2 - MDM/Unified endpoint management (UEM) ○ 3.5.3.3 - Mobile application management (MAM) ○ 3.5.3.4 - SEAndroid 	<p>8.1 9.4, 9.6, 9.7, 9.8</p>

	<p>3.5.4 - Enforcement and monitoring of:</p> <ul style="list-style-type: none"> ○ 3.5.4.1 - Third-party app stores ○ 3.5.4.2 - Rooting/jailbreaking ○ 3.5.4.3 - Sideloads ○ 3.5.4.4 - Custom firmware ○ 3.5.4.5 - Carrier unlocking ○ 3.5.4.6 - Firmware over-the-air (OTA) updates ○ 3.5.4.7 - Camera use ○ 3.5.4.8 - SMS/multimedia message service (MMS)/Rich communication services (RCS) ○ 3.5.4.9 - External media ○ 3.5.4.10 - USB on the go (OTG) ○ 3.5.4.11 - Recording microphone ○ 3.5.4.12 - GPS tagging ○ 3.5.4.13 - WiFi direct/ad hoc ○ 3.5.4.14 - Tethering ○ 3.5.4.15 - Hotspot ○ 3.5.4.16 - Payment methods <p>3.5.4 - Deployment models</p> <ul style="list-style-type: none"> ○ 3.5.4.1 - Bring your own device (BYOD) ○ 3.5.4.2 - Corporate-owned personally enabled (COPE) ○ 3.5.4.3 - Choose your own device (CYOD) ○ 3.5.4.4 - Corporate-owned ○ 3.5.4.5 - Virtual desktop infrastructure (VDI) 	
3.6	<p>Given a scenario, apply cybersecurity solutions to the cloud.</p> <p>3.6.1 - Cloud security controls</p> <ul style="list-style-type: none"> ○ 3.6.1.1 - High availability across zones ○ 3.6.1.2 - Resource policies ○ 3.6.1.3 - Secrets management ○ 3.6.1.4 - Integration and auditing ○ 3.6.1.5 - Storage ○ 3.6.1.5.1 - Storage - Permissions ○ 3.6.1.5.2 - Storage - Encryption ○ 3.6.1.5.3 - Storage - Replication ○ 3.6.1.5.4 - Storage - High availability ○ 3.6.1.6 - Network 	<p>4.3 5.8 6.3 9.2, 9.4, 9.5, 9.8 14.1</p>

	<ul style="list-style-type: none"> ○ 3.6.1.6.1 - Network - Virtual networks ○ 3.6.1.6.2 - Network - Public and private subnets ○ 3.6.1.6.3 - Network - Segmentation ○ 3.6.1.6.4 - Network - API inspection and integration ○ 3.6.1.7 - Compute ○ 3.6.1.7.1 - Compute - Security groups ○ 3.6.1.7.2 - Compute - Dynamic resource allocation ○ 3.6.1.7.3 - Compute - Instance awareness ○ 3.6.1.7.4 - Compute - Virtual private cloud (VPC) endpoint ○ 3.6.1.7.5 - Compute - Container security <p>3.6.2 - Solutions</p> <ul style="list-style-type: none"> ○ 3.6.2.1 - CASB ○ 3.6.2.2 - Application security ○ 3.6.2.3 - Next-generation secure web gateway (SWG) ○ 3.6.2.4 - Firewall considerations in a cloud environment ○ 3.6.2.4.1 - Firewall considerations in a cloud environment - Cost ○ 3.6.2.4.2 - Firewall considerations in a cloud environment - Need for segmentation ○ 3.6.2.4.3 - Firewall considerations in a cloud environment - Open Systems Interconnection (OSI) layers <p>3.6.3 - Cloud native controls vs. third-party solutions</p>	
<p>3.7</p>	<p>Given a scenario, implement identity and account management controls.</p> <p>3.7.1 - Identity</p> <ul style="list-style-type: none"> ○ 3.7.1.1 - Identity provider (IdP) ○ 3.7.1.2 - Attributes ○ 3.7.1.3 - Certificates ○ 3.7.1.4 - Tokens ○ 3.7.1.5 - SSH keys ○ 3.7.1.6 - Smart cards <p>3.7.2 - Account types</p> <ul style="list-style-type: none"> ○ 3.7.2.1 - User account ○ 3.7.2.2 - Shared and generic ○ 3.7.2.3 - accounts/credentials ○ 3.7.2.4 - Guest accounts ○ 3.7.2.5 - Service accounts <p>3.7.3 - Account policies</p>	<p>3.1 4.1 5.9 6.2, 6.3, 6.4, 6.5, 6.6, 6.7 9.6 11.7 12.2 14.1</p>

	<ul style="list-style-type: none"> ○ 3.7.3.1 - Password complexity ○ 3.7.3.2 - Password history ○ 3.7.3.3 - Password reuse ○ 3.7.3.4 - Time of day ○ 3.7.3.5 - Network location ○ 3.7.3.6 - Geofencing ○ 3.7.3.7 - Geotagging ○ 3.7.3.8 - Geolocation ○ 3.7.3.9 - Time-based logins ○ 3.7.3.10 - Access policies ○ 3.7.3.11 - Account permissions ○ 3.7.3.12 - Account audits ○ 3.7.3.13 - Impossible travel time/risky login ○ 3.7.3.14 - Lockout ○ 3.7.3.15 - Disablement 	
3.8	<p>Given a scenario, implement authentication and authorization solutions.</p> <ul style="list-style-type: none"> 3.8.1 - Authentication management <ul style="list-style-type: none"> ○ 3.8.1.1 - Password keys ○ 3.8.1.2 - Password vaults ○ 3.8.1.3 - TPM ○ 3.8.1.4 - HSM ○ 3.8.1.5 - Knowledge-based authentication 3.8.2 - Authentication <ul style="list-style-type: none"> ○ 3.8.2.1 - EAP ○ 3.8.2.2 - Challenge Handshake Authentication Protocol (CHAP) ○ 3.8.2.3 - Password Authentication Protocol (PAP) ○ 3.8.2.4 - 802.1X ○ 3.8.2.5 - RADIUS ○ 3.8.2.6 - Single sign-on (SSO) ○ 3.8.2.7 - Security Assertions Markup Language (SAML) ○ 3.8.2.8 - Terminal Access Controller Access Control System Plus (TACACS+) ○ 3.8.2.9 - OAuth ○ 3.8.2.10 - OpenID ○ 3.8.2.11 - Kerberos 3.8.3 - Access control schemes 	<p>4.3 6.1, 6.3, 6.9, 6.10 8.3</p>

	<ul style="list-style-type: none"> ○ 3.8.3.1 - Attribute-based access control (ABAC) ○ 3.8.3.2 - Role-based access control ○ 3.8.3.3 - Rule-based access control ○ 3.8.3.4 - MAC ○ 3.8.3.5 - Discretionary access control (DAC) ○ 3.8.3.6 - Conditional access ○ 3.8.3.7 - Privilege access management ○ 3.8.3.8 - Filesystem permissions 	
3.9	<p>Given a scenario, implement public key infrastructure.</p> <p>3.9.1 - Public key infrastructure (PKI)</p> <ul style="list-style-type: none"> ○ 3.9.1.1 - Key management ○ 3.9.1.2 - Certificate authority (CA) ○ 3.9.1.3 - Intermediate CA ○ 3.9.1.4 - Registration authority (RA) ○ 3.9.1.5 - Certificate revocation list (CRL) ○ 3.9.1.6 - Certificate attributes ○ 3.9.1.7 - Online Certificate Status Protocol (OCSP) ○ 3.9.1.8 - Certificate signing request (CSR) ○ 3.9.1.9 - CN ○ 3.9.1.10 - SAN ○ 3.9.1.11 - Expiration <p>3.9.2 - Types of certificates</p> <ul style="list-style-type: none"> ○ 3.9.2.1 - Wildcard ○ 3.9.2.2 - SAN ○ 3.9.2.3 - Code signing ○ 3.9.2.4 - Self-signed ○ 3.9.2.5 - Machine/computer ○ 3.9.2.6 - Email ○ 3.9.2.7 - User ○ 3.9.2.8 - Root ○ 3.9.2.9 - Domain validation <p>3.9.3 - Extended validation</p> <ul style="list-style-type: none"> ○ 3.9.3.1 - Certificate formats ○ 3.9.3.2 - Distinguished encoding rules (DER) ○ 3.9.3.4 - Privacy enhanced mail (PEM) ○ 3.9.3.5 - Personal information exchange (PEM) 	<p>7.5</p> <p>10.4</p>

	<ul style="list-style-type: none"> ○ 3.9.3.6 - .cer ○ 3.9.3.7 - P12 ○ 3.9.3.8 - P7B <p>3.9.4 - Concepts</p> <ul style="list-style-type: none"> ○ 3.9.4.1 - Online vs. offline CA ○ 3.9.4.2 - Stapling ○ 3.9.4.3 - Pinning ○ 3.9.4.4 - Trust model ○ 3.9.4.5 - Key escrow ○ 3.9.4.6 - Certificate chaining 	
4.0	Operations and Incident Response	
4.1	<p>Given a scenario, use the appropriate tool to assess organizational security.</p> <p>4.1.1 - Network reconnaissance and discovery</p> <ul style="list-style-type: none"> ○ 4.1.1.1 - tracert/traceroute ○ 4.1.1.2 - nslookup/dig ○ 4.1.1.3 - ipconfig/ifconfig ○ 4.1.1.4 - nmap ○ 4.1.1.5 - ping/pathping ○ 4.1.1.6 - hping ○ 4.1.1.7 - netstat ○ 4.1.1.8 - netcat ○ 4.1.1.9 - IP scanners ○ 4.1.1.10 - arp ○ 4.1.1.11 - route ○ 4.1.1.12 - curl ○ 4.1.1.13 - the harvester ○ 4.1.1.14 - sn1per ○ 4.1.1.15 - scanless ○ 4.1.1.16 - dnsenum ○ 4.1.1.17 - Nessus ○ 4.1.1.18 - Cuckoo <p>4.1.2 - File manipulation</p> <ul style="list-style-type: none"> ○ 4.1.2.1 - head ○ 4.1.2.2 - tail ○ 4.1.2.3 - cat 	<p>4.4</p> <p>5.9</p> <p>8.2</p> <p>10.3</p> <p>11.2, 11.5, 11.6, 11.7</p> <p>12.5, 12.6</p>

	<ul style="list-style-type: none"> ○ 4.1.2.4 - grep ○ 4.1.2.5 - chmod ○ 4.1.2.6 - logger 4.1.3 - Shell and script environments <ul style="list-style-type: none"> ○ 4.1.3.1 - SSH ○ 4.1.3.2 - PowerShell ○ 4.1.3.3 - Python ○ 4.1.3.4 - OpenSSL 4.1.4 - Packet capture and replay <ul style="list-style-type: none"> ○ 4.1.4.1 - Tcpreplay ○ 4.1.4.2 - Tcpdump ○ 4.1.4.3 - Wireshark 4.1.5 - Forensics <ul style="list-style-type: none"> ○ 4.1.5.1 - dd ○ 4.1.5.2 - Memdump ○ 4.1.5.3 - WinHex ○ 4.1.5.4 - FTK imager ○ 4.1.5.5 - Autopsy 4.1.6 - Exploitation frameworks 4.1.7 - Password crackers 4.1.8 - Data sanitization 	
4.2	<p>Summarize the importance of policies, processes, and procedures for incident response.</p> <ul style="list-style-type: none"> 4.2.1 - Incident response plans 4.2.2 - Incident response process <ul style="list-style-type: none"> ○ 4.2.2.1 - Preparation ○ 4.2.2.2 - Identification ○ 4.2.2.3 - Containment ○ 4.2.2.4 - Eradication ○ 4.2.2.5 - Recovery ○ 4.2.2.6 - Lessons learned 4.2.3 - Exercises <ul style="list-style-type: none"> ○ 4.2.3.1 - Tabletop ○ 4.2.3.2 - Walkthroughs ○ 4.2.3.3 - Simulations 4.2.4 - Attack frameworks <ul style="list-style-type: none"> ○ 4.2.4.1 - MITRE ATT&CK 	<p>3.1 12.1, 12.2 13.2</p>

	<ul style="list-style-type: none"> ○ 4.2.4.2 - The Diamond Model of Intrusion Analysis ○ 4.2.4.3 - Cyber Kill Chain <p>4.2.5 - Stakeholder management 4.2.6 - Communication plan 4.2.7 - Disaster recovery plan 4.2.8 - Business continuity plan 4.2.9 - Continuity of operation planning (COOP) 4.2.10 - Incident response team 4.2.11 - Retention policies</p>	
4.3	<p>Given an incident, utilize appropriate data sources to support an investigation.</p> <p>4.3.1 - Vulnerability scan output 4.3.2 - SIEM dashboards</p> <ul style="list-style-type: none"> ○ 4.3.2.1 - Sensor ○ 4.3.2.2 - Sensitivity ○ 4.3.2.3 - Trends ○ 4.3.2.4 - Alerts ○ 4.3.2.5 - Correlation <p>4.3.3 - Log files</p> <ul style="list-style-type: none"> ○ 4.3.3.1 - Network ○ 4.3.3.2 - System ○ 4.3.3.3 - Application ○ 4.3.3.4 - Security ○ 4.3.3.5 - Web ○ 4.3.3.6 - DNS ○ 4.3.3.7 - Authentication ○ 4.3.3.8 - Dump files ○ 4.3.3.9 - VoIP and call managers ○ 4.3.3.10 - Session Initiation Protocol (SIP) traffic <p>4.3.4 - syslog/rsyslog/syslog-ng 4.3.5 - journalctl 4.3.6 - nxlog 4.3.7 - Retention 4.3.8 - Bandwidth monitors 4.3.9 - Metadata</p> <ul style="list-style-type: none"> ○ 4.3.9.1 - Email ○ 4.3.9.2 - Mobile 	<p>11.5 12.1, 12.3, 12.6</p>

	<ul style="list-style-type: none"> ○ 4.3.9.3 - Web ○ 4.3.9.4 - File <p>4.3.10 - Netflow/sflow</p> <ul style="list-style-type: none"> ○ 4.3.10.1 - Echo ○ 4.3.10.2 - IPfix <p>4.3.11 - Protocol analyzer output</p>	
4.4	<p>Given an incident, apply mitigation techniques or controls to secure an environment.</p> <p>4.4.1 - Reconfigure endpoint security solutions</p> <ul style="list-style-type: none"> ○ 4.4.1.1 - Application whitelisting ○ 4.4.1.2 - Application blacklisting ○ 4.4.1.3 - Quarantine <p>4.4.2 - Configuration changes</p> <ul style="list-style-type: none"> ○ 4.4.2.1 - Firewall rules ○ 4.4.2.2 - MDM ○ 4.4.2.3 - DLP ○ 4.4.2.4 - Content filter/URL filter ○ 4.4.2.5 - Update or revoke certificates <p>4.4.3 - Isolation</p> <p>4.4.4 - Containment</p> <p>4.4.5 - Segmentation</p> <p>4.4.6 - Secure Orchestration, Automation, and Response (SOAR)</p> <ul style="list-style-type: none"> ○ 4.4.6.1 - Runbooks ○ 4.4.6.2 - Playbooks 	<p>1.2</p> <p>5.1, 5.6</p> <p>9.6</p> <p>11.4, 11.5</p> <p>12.2</p>
4.5	<p>Explain the key aspects of digital forensics.</p> <p>4.5.1 - Documentation/evidence</p> <ul style="list-style-type: none"> ○ 4.5.1.1 - Legal hold ○ 4.5.1.2 - Video ○ 4.5.1.3 - Admissibility ○ 4.5.1.4 - Chain of custody ○ 4.5.1.5 - Timelines of sequence of events ○ 4.5.1.5.1 - Timelines of sequence of events - Time stamps ○ 4.5.1.5.2 - Timelines of sequence of events - Time offset ○ 4.5.1.6 - Tags 	<p>1.1</p> <p>4.1</p> <p>5.8</p> <p>7.2</p> <p>12.1, 12.4, 12.5, 12.8</p>

	<ul style="list-style-type: none"> ○ 4.5.1.7 - Reports ○ 4.5.1.8 - Event logs ○ 4.5.1.9 - Interviews <p>4.5.2 - Acquisition</p> <ul style="list-style-type: none"> ○ 4.5.2.1 - Order of volatility ○ 4.5.2.2 - Disk ○ 4.5.2.3 - Random-access memory (RAM) ○ 4.5.2.4 - Swap/pagefile ○ 4.5.2.5 - OS ○ 4.5.2.6 - Device ○ 4.5.2.7 - Firmware ○ 4.5.2.8 - Snapshot ○ 4.5.2.9 - Cache ○ 4.5.2.10 - Network ○ 4.5.2.11 - Artifacts <p>4.5.3 - On-premises vs. cloud</p> <ul style="list-style-type: none"> ○ 4.5.3.1 - Right to audit clauses ○ 4.5.3.2 - Regulatory/jurisdiction ○ 4.5.3.3 - Data breach notification laws <p>4.5.4 - Integrity</p> <ul style="list-style-type: none"> ○ 4.5.4.1 - Hashing ○ 4.5.4.2 - Checksums ○ 4.5.4.3 - Provenance <p>4.5.5 - Preservation</p> <p>4.5.6 - E-discovery</p> <p>4.5.7 - Data recovery</p> <p>4.5.8 - Non-repudiation</p> <p>4.5.9 - Strategic intelligence/counterintelligence</p>	
5.0	Governance, Risk, and Compliance	
5.1	<p>Compare and contrast various types of controls.</p> <p>5.1.1 - Category</p> <ul style="list-style-type: none"> ○ 5.1.1.1 - Managerial ○ 5.1.1.2 - Operational ○ 5.1.1.3 - Technical <p>5.1.2 - Control type</p>	<p>2.4</p> <p>6.1</p> <p>14.2</p>

	<ul style="list-style-type: none"> ○ 5.1.2.1 - Preventative ○ 5.1.2.2 - Detective ○ 5.1.2.3 - Corrective ○ 5.1.2.4 - Deterrent ○ 5.1.2.5 - Compensating ○ 5.1.2.6 - Physical 	
5.2	<p>Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.</p> <p>5.2.1 - Regulations, standards, and legislation</p> <ul style="list-style-type: none"> ○ 5.2.1.1 - General Data Protection Regulation (GDPR) ○ 5.2.1.2 - National, territory, or state laws ○ 5.2.1.3 - Payment Card Industry Data Security Standard (PCI DSS) <p>5.2.2 - Key frameworks</p> <ul style="list-style-type: none"> ○ 5.2.2.1 - Center for Internet Security (CIS) ○ 5.2.2.2 - National Institute of Standards and Technology (NIST) RMF/CSF ○ 5.2.2.3 - International Organization for Standardization (ISO) 27001/27002/27701/31000 ○ 5.2.2.4 - SSAE SOC 2 Type II/III ○ 5.2.2.5 - Cloud security alliance ○ 5.2.2.5.1 - Cloud security alliance - Cloud control matrix ○ 5.2.2.5.2 - Cloud security alliance - Reference architecture <p>5.2.3 - Benchmarks /secure configuration guides</p> <ul style="list-style-type: none"> ○ 5.2.3.1 - Platform/vendor-specific guides - ○ 5.2.3.1.1 - Platform/vendor-specific guides - Web server ○ 5.2.3.1.2 - Platform/vendor-specific guides - OS ○ 5.2.3.1.3 - Platform/vendor-specific guides - Application server ○ 5.2.3.1.4 - Platform/vendor-specific guides - Network infrastructure devices 	14.1, 14.2, 14.3
5.3	<p>Explain the importance of policies to organizational security.</p> <p>5.3.1 - Personnel</p> <ul style="list-style-type: none"> ○ 5.3.1.1 - Acceptable use policy ○ 5.3.1.2 - Job rotation 	1.2 2.1 5.8 6.1 9.8

	<ul style="list-style-type: none"> ○ 5.3.1.3 - Mandatory vacation ○ 5.3.1.4 - Separation of duties ○ 5.3.1.5 - Least privilege ○ 5.3.1.6 - Clean desk space ○ 5.3.1.7 - Background checks ○ 5.3.1.8 - Non-disclosure agreement (NDA) ○ 5.3.1.9 - Social media analysis ○ 5.3.1.10 - Onboarding ○ 5.3.1.11 - Offboarding ○ 5.3.1.12 - User training <ul style="list-style-type: none"> ○ 5.3.1.12.1 - User training - Gamification ○ 5.3.1.12.2 - User training - Capture the flag ○ 5.3.1.12.3 - User training - Phishing campaigns ○ 5.3.1.12.31 - User training - Phishing campaigns - Phishing simulations ○ 5.3.1.12.4 - User training - Computer-based training (CBT) ○ 5.3.1.12.5 - User training - Role-based training 5.3.2 - Diversity of training techniques 5.3.3 - Third-party risk management <ul style="list-style-type: none"> ○ 5.3.3.1 - Vendors ○ 5.3.3.2 - Supply chain ○ 5.3.3.3 - Business partners ○ 5.3.3.4 - Service level agreement (SLA) ○ 5.3.3.5 - Memorandum of understanding (MOU) ○ 5.3.3.6 - Measurement systems analysis (MSA) ○ 5.3.3.7 - Business partnership agreement (BPA) ○ 5.3.3.8 - End of life (EOL) ○ 5.3.3.9 - End of service (EOS) ○ 5.3.3.10 - NDA 5.3.4 - Data <ul style="list-style-type: none"> ○ 5.3.4.1 - Classification ○ 5.3.4.2 - Governance ○ 5.3.4.3 - Retention 5.3.5 - Credential policies <ul style="list-style-type: none"> ○ 5.3.5.1 - Personnel ○ 5.3.5.2 - Third party ○ 5.3.5.3 - Devices ○ 5.3.5.4 - Service accounts ○ 5.3.5.5 - Administrator/root accounts 5.3.6 - Organizational policies 	<p>13.1, 13.2, 13.3 14.1</p>
--	---	----------------------------------

	<ul style="list-style-type: none"> ○ 5.3.6.1 - Change management ○ 5.3.6.2 - Change control ○ 5.3.6.3 - Asset management 	
5.4	<p>Summarize risk management processes and concepts.</p> <p>5.4.1 - Risk types</p> <ul style="list-style-type: none"> ○ 5.4.1.1 - External ○ 5.4.1.2 - Internal ○ 5.4.1.3 - Legacy systems ○ 5.4.1.4 - Multiparty ○ 5.4.1.5 - IP theft ○ 5.4.1.6 - Software compliance/licensing <p>5.4.2 - Risk management strategies</p> <ul style="list-style-type: none"> ○ 5.4.2.1 - Acceptance ○ 5.4.2.2 - Avoidance ○ 5.4.2.3 - Transference ○ 5.4.2.3.1 - Transference - Cybersecurity insurance ○ 5.4.2.4 - Mitigation <p>5.4.3 - Risk analysis</p> <ul style="list-style-type: none"> ○ 5.4.3.1 - Risk register ○ 5.4.3.2 - Risk matrix/heat map ○ 5.4.3.3 - Risk control assessment ○ 5.4.3.4 - Risk control self-assessment ○ 5.4.3.5 - Risk awareness ○ 5.4.3.6 - Inherent risk ○ 5.4.3.7 - Residual risk ○ 5.4.3.8 - Control risk ○ 5.4.3.9 - Risk appetite ○ 5.4.3.10 - Regulations that affect risk posture ○ 5.4.3.11 - Risk assessment ○ 5.4.3.11.1 - Risk assessment - Qualitative ○ 5.4.3.11.2 - Risk assessment - Quantitative ○ 5.4.3.12 - Likelihood of occurrence ○ 5.4.3.13 - Impact ○ 5.4.3.14 - Asset value ○ 5.4.3.15 - Single loss expectancy (SLE) ○ 5.4.3.16 - Annualized loss expectancy (ALE) 	<p>1.1</p> <p>2.4</p> <p>5.8</p> <p>13.2</p>

	<ul style="list-style-type: none"> ○ 5.4.3.17 - Annualized rate of occurrence (ARO) <p>5.4.4 - Disasters</p> <ul style="list-style-type: none"> ○ 5.4.4.1 - Environmental ○ 5.4.4.2 - Man-made ○ 5.4.4.3 - Internal vs. external <p>5.4.5 - Business impact analysis</p> <ul style="list-style-type: none"> ○ 5.4.5.1 - Recovery time objective (RTO) ○ 5.4.5.2 - Recovery point objective (RPO) ○ 5.4.5.3 - Mean time to repair (MTTR) ○ 5.4.5.4 - Mean time between failures (MTBF) ○ 5.4.5.5 - Functional recovery plans ○ 5.4.5.6 - Single point of failure ○ 5.4.5.7 - Disaster recovery plan (DRP) ○ 5.4.5.8 - Mission essential functions ○ 5.4.5.9 - Identification of critical systems ○ 5.4.5.10 - Site risk assessment 	
5.5	<p>Explain privacy and sensitive data concepts in relation to security.</p> <p>5.5.1 - Organizational consequences of privacy breaches</p> <ul style="list-style-type: none"> ○ 5.5.1.1 - Reputation damage ○ 5.5.1.2 - Identity theft ○ 5.5.1.3 - Fines ○ 5.5.1.4 - IP theft <p>5.5.2 - Notifications of breaches</p> <ul style="list-style-type: none"> ○ 5.5.2.1 - Escalation ○ 5.5.2.2 - Public notifications and disclosures <p>5.5.3 - Data types</p> <ul style="list-style-type: none"> ○ 5.5.3.1 - Classifications <ul style="list-style-type: none"> ○ 5.5.3.1.1 - Classifications - Public ○ 5.5.3.1.2 - Classifications - Private ○ 5.5.3.1.3 - Classifications - Sensitive ○ 5.5.3.1.4 - Classifications - Confidential ○ 5.5.3.1.5 - Classifications - Critical ○ 5.5.3.1.6 - Classifications - Proprietary ○ 5.5.3.2 - Personally identifiable information (PII) ○ 5.5.3.3 - Health information ○ 5.5.3.4 - Financial information 	<p>1.1</p> <p>10.2</p> <p>14.3</p>

	<ul style="list-style-type: none">○ 5.5.3.5 - Government data○ 5.5.3.6 - Customer data5.5.4 - Privacy enhancing technologies<ul style="list-style-type: none">○ 5.5.4.1 - Data minimization○ 5.5.4.2 - Data masking○ 5.5.4.3 - Tokenization○ 5.5.4.4 - Anonymization○ 5.5.4.5 - Pseudo-anonymization5.5.5 - Roles and responsibilities<ul style="list-style-type: none">○ 5.5.5.1 - Data owners○ 5.5.5.2 - Data controller○ 5.5.5.3 - Data processor○ 5.5.5.4 - Data custodian/steward○ 5.5.5.5 - Data privacy officer (DPO)5.5.6 - Information life cycle5.5.7 - Impact assessment5.5.8 - Terms of agreement5.5.9 - Privacy notice	
--	--	--