TestOut®

TestOut Security Pro – English 7.0.x

Objective Mappings:

TestOut Security Pro
CompTIA Security+ SY0-601

Revised: 2020-11-11

Powered by LABSIM

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 12

Objective Mapping: LabSim Section to CompTIA SY0-601 Objective 15

Objective Mapping: CompTIA SY0-601 Objective to LabSim Section 25

Objective Mapping: LabSim Section to TestOut Security Pro Objective

Section	Title	Objectives
1.0	**Introduction to Security**	
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 3.1.2 Configure Antivirus Protection
2.3	Social Engineering	5.2 Assessment Techniques 5.2.2 Identify Social Engineering
2.4	Vulnerability Concerns	
3.0	**Physical**	
3.1	Physical Threats	2.1 Harden Physical Access 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	3.1 Harden Computer Systems 3.1.1 Configure File System Inheritance 3.1.2 Configure Antivirus Protection 3.1.3 Configure NTFS Permissions 3.1.4 Configure Windows Update
4.3	File Server Security	3.1 Harden Computer Systems 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	2.1 Harden Physical Access 2.1.2 Install and Configure a Security Appliance 2.1.4 Create and Configure a Demilitarized Zone (DMZ)
5.2	Demilitarized Zones	2.1 Harden Physical Access 2.1.4 Create and Configure a Demilitarized Zone (DMZ)
5.3	Firewalls	2.1 Harden Physical Access 2.1.3 Install and Configure a Firewall

5.4	Network Address Translation	2.1 Harden Physical Access 2.1.5 Configure Network Address Translation (NAT)
5.5	Virtual Private Networks	2.2 Harden Network Devices 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 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 2.2.1 Configure and Access a Switch
5.10	Network Applications	
5.11	Switch Security and Attacks	2.1 Harden Physical Access 2.1.1 Implement Physical Security 2.2 Harden Network Devices 2.2.1 Configure and Access a Switch

5.12	Using VLANs	2.2 Harden Network Devices 2.2.7 Create and Connect to a Virtual Local Area Network (VLAN)
5.13	Router Security	2.2 Harden Network Devices 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	1.1 Manage Identity 1.1.1 Manage Windows Local and Domain Users and Groups 1.1.3 Manage Active Directory OUs 1.2 Harden Authentication 1.2.5 Configure and Link Group Policy Objects (GPO)
6.6	Hardening Authentication	1.2 Harden Authentication 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	1.1 Manage Identity 1.1.2 Manage Linux Users and Groups 1.2 Harden Authentication 1.2.2 Manage Account Password
6.8	Linux Groups	1.1 Manage Identity 1.1.2 Manage Linux Users and Groups
6.9	Remote Access	
6.10	Network Authentication	1.2 Harden Authentication 1.2.5 Configure and Link Group Policy Objects (GPO)
7.0	**Cryptography and PKI**	
7.1	Cryptography	4.2 Implement Encryption Technologies 4.2.1 Encrypt Data Communications
7.2	Cryptography Implementations	
7.3	Hashing	4.2 Implement Encryption Technologies 4.2.1 Encrypt Data Communications
7.4	File Encryption	4.2 Implement Encryption Technologies

		4.2.2 Encrypt Files
7.5	Public Key Infrastructure	4.2 Implement Encryption Technologies 4.2.3 Manage Certificates
8.0	**Wireless Threats**	
8.1	Wireless Overview	2.2 Harden Network Devices 2.2.2 Configure and Access a Wireless Network
8.2	Wireless Attacks	2.2 Harden Network Devices 2.2.2 Configure and Access a Wireless Network
8.3	Wireless Defenses	2.2 Harden Network Devices 2.2.4 Harden a Wireless Network
9.0	**Virtualization, Cloud Security, and Securing Mobile Devices**	
9.1	Host Virtualization	3.3 Implement Virtualization 3.3.1 Create Virtual Machines
9.2	Virtual Networking	3.3 Implement Virtualization 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 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 3.2.3 Configure Web Application Security
10.2	Data Loss Prevention	
10.3	Web Application Attacks	3.2 Implement Application Defenses 3.2.3 Configure Web Application Security
10.4	Application Development and Security	3.2 Implement Application Defenses 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 5.2.1 Implement Intrusion Detection
11.4	Security Assessment Techniques	5.2 Assessment Techniques 5.2.3 Scan for Vulnerabilities
11.5	Protocol Analyzers	
11.6	Analyzing Network Attacks	5.2 Assessment Techniques 5.2.4 Analyze Network Attacks
11.7	Password Attacks	5.2 Assessment Techniques 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 4.1.1 Perform Data Backups and Recovery

12.8	Backup and Restore	4.1 Protect and Maintain Data Files 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 3.2.4 Configure Email Filters and Settings
14.0	**Governance and Compliance**	
14.1	Audits	5.1 Implement Logging and Auditing 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+ Question Review (20 Random Questions)	
B.3	CompTIA Security+ Question 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

	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	Harden Computer Systems 3.1.1 Configure File system Inheritance 3.1.2 Configure Antivirus Protection 3.1.3 Configure NTFS Permissions 3.1.4 Configure Windows Update	2.2 4.2, 4.3
3.2	Implement Application Defenses 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	5.6 10.1, 10.3, 10.4 13.3
3.3	Implement Virtualization 3.3.1 Create Virtual Machines 3.3.2 Create Virtual Switches	9.1, 9.2
4.0	**Data Security**	
4.1	Protect and Maintain Data files 4.1.1 Perform Data Backups and Recovery 4.1.2 Implement Redundancy	12.7, 12.8

4.2	Implement Encryption Technologies 4.2.1 Encrypt Data Communications 4.2.2 Encrypt Files 4.2.3 Manage Certificates	7.1, 7.3, 7.4, 7.5
5.0	**Audit and Security Assessment**	
5.1	Implement Logging and Auditing 5.1.1 Configure Advanced Audit Policy 5.1.2 Enable Device Logs	14.1
5.2	Assessment Techniques 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	2.3 11.3, 11.4, 11.6, 11.7

Objective Mapping: LabSim Section to CompTIA SY0-601 Objective

TestOut Section	Title	CompTIA Security+ 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 3.1.2 Configure Antivirus Protection
2.3	Social Engineering	5.2 Assessment Techniques Assessment Techniques 5.2.2 Identify Social Engineering
2.4	Vulnerability Concerns	
3.0	**Physical**	
3.1	Physical Threats	2.1 Harden Physical Access 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	3.1 Harden Computer Systems 3.1.1 Configure File System Inheritance 3.1.2 Configure Antivirus Protection 3.1.3 Configure NTFS Permissions 3.1.4 Configure Windows Update
4.3	File Server Security	3.1 Harden Computer Systems 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	2.1 Harden Physical Access 2.1.2 Install and Configure a Security Appliance 2.1.4 Create and Configure a Demilitarized Zone (DMZ)
5.2	Demilitarized Zones	2.1 Harden Physical Access 2.1.4 Create and Configure a Demilitarized Zone (DMZ)
5.3	Firewalls	2.1 Harden Physical Access

		2.1.3 Install and Configure a Firewall
5.4	Network Address Translation	2.1 Harden Physical Access 2.1.5 Configure Network Address Translation (NAT)
5.5	Virtual Private Networks	2.2 Harden Network Devices 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 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 2.2.1 Configure and Access a Switch
5.10	Network Applications	
5.11	Switch Security and Attacks	2.1 Harden Physical Access 2.1.1 Implement Physical Security 2.2 Harden Network Devices

		2.2.1 Configure and Access a Switch
5.12	Using VLANs	2.2 Harden Network Devices 2.2.7 Create and Connect to a Virtual Local Area Network (VLAN)
5.13	Router Security	2.2 Harden Network Devices 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	1.1 Manage Identity 1.1.1 Manage Windows Local and Domain Users and Groups 1.1.3 Manage Active Directory OUs 1.2 Harden Authentication 1.2.5 Configure and Link Group Policy Objects (GPO)
6.6	Hardening Authentication	1.2 Harden Authentication 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	1.1 Manage Identity 1.1.2 Manage Linux Users and Groups 1.2 Harden Authentication 1.2.2 Manage Account Password
6.8	Linux Groups	1.1 Manage Identity 1.1.2 Manage Linux Users and Groups
6.9	Remote Access	
6.10	Network Authentication	1.2 Harden Authentication 1.2.5 Configure and Link Group Policy Objects (GPO)
7.0	**Cryptography and PKI**	
7.1	Cryptography	4.2 Implement Encryption Technologies 4.2.1 Encrypt Data Communications
7.2	Cryptography Implementations	
7.3	Hashing	4.2 Implement Encryption Technologies 4.2.1 Encrypt Data Communications

7.4	File Encryption	4.2 Implement Encryption Technologies 4.2.2 Encrypt Files
7.5	Public Key Infrastructure	4.2 Implement Encryption Technologies 4.2.3 Manage Certificates
8.0	**Wireless Threats**	
8.1	Wireless Overview	2.2 Harden Network Devices 2.2.2 Configure and Access a Wireless Network
8.2	Wireless Attacks	2.2 Harden Network Devices 2.2.2 Configure and Access a Wireless Network
8.3	Wireless Defenses	2.2 Harden Network Devices 2.2.4 Harden a Wireless Network
9.0	**Virtualization, Cloud Security, and Securing Mobile Devices**	
9.1	Host Virtualization	3.3 Implement Virtualization 3.3.1 Create Virtual Machines
9.2	Virtual Networking	3.3 Implement Virtualization

		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 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 3.2.3 Configure Web Application Security
10.2	Data Loss Prevention	
10.3	Web Application Attacks	3.2 Implement Application Defenses 3.2.3 Configure Web Application Security
10.4	Application Development and Security	3.2 Implement Application Defenses 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 5.2.1 Implement Intrusion Detection
11.4	Security Assessment Techniques	5.2 Assessment Techniques Assessment Techniques 5.2.3 Scan for Vulnerabilities
11.5	Protocol Analyzers	
11.6	Analyzing Network Attacks	5.2 Assessment Techniques Assessment Techniques 5.2.4 Analyze Network Attacks
11.7	Password Attacks	5.2 Assessment Techniques Assessment Techniques 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 4.1.1 Perform Data Backups and Recovery
12.8	Backup and Restore	4.1 Protect and Maintain Data Files 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 3.2.4 Configure Email Filters and Settings
14.0	**Governance and Compliance**	
14.1	Audits	5.1 Implement Logging and Auditing Implement Logging and Auditing 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: CompTIA SY0-601 Objective to LabSim Section

#	CompTIA Security+ (SY0-501) Objective	TestOut Module.Section
1.0	**Attacks, Threats, and Vulnerabilities**	
1.1	Compare and contrast different types of social engineering techniques. Phishing Smishing Vishing Spam Spam over Internet messaging (SPIM) Spear phishing Dumpster diving Shoulder surfing Pharming Tailgating Eliciting information Whaling Prepending Identity fraud Invoice scams Credential harvesting Reconnaissance Hoax Impersonation Watering hole attack Typo squatting Influence campaigns ○ Hybrid warfare ○ Social media Principles (reasons for effectiveness) ○ Authority ○ Intimidation ○ Consensus ○ Scarcity ○ Familiarity	1.2 2.1, 2.3 5.6, 5.10 11.2, 11.7 13.3

	○ Trust ○ Urgency	
1.2	Given a scenario, analyze potential indicators to determine the type of attack. Malware ○ Ransomware ○ Trojans ○ Worms ○ Potentially unwanted programs (PUPs) ○ Fileless virus ○ Command and control ○ Bots ○ Crypto malware ○ Logic bombs ○ Spyware ○ Keyloggers ○ Remote access Trojan (RAT) ○ Rootkit ○ Backdoor Password attacks ○ Spraying ○ Dictionary ○ Brute force ▪ Offline ▪ Online ○ Rainbow tables ○ Plaintext/unencrypted Physical attacks ○ Malicious universal serial bus (USB) cable ○ Malicious flash drive ○ Card cloning ○ Skimming Adversarial artificial intelligence (AI) ○ Tainted training data for machine learning (ML) ○ Security of machine learning algorithms Supply-chain attacks Cloud-based vs. on-premises attacks	2.2 4.2 5.9 7.1, 7.3 11.7

	Cryptographic attacks ○ Birthday ○ Collision ○ Downgrade	
1.3	Given a scenario, analyze potential indicators associated with application attacks. Privilege escalation Cross-site scripting Injections ○ Structured query language (SQL) ○ Dynamic link library (DLL) ○ Lightweight directory access protocol (LDAP) ○ Extensible markup language (XML) Pointer/object dereference Directory traversal Buffer overflows Race conditions ○ Time of check/time of use Error handling Improper input handling Replay attack ○ Session replays Integer overflow Request forgeries ○ Server-side ○ Client-side ○ Cross-site Application programming interface (API) attacks Resource exhaustion Memory leak Secure sockets layer (SSL) stripping Driver manipulation ○ Shimming ○ Refactoring Pass the hash	2.4 5.9 6.1 10.3

1.4	Given a scenario, analyze potential indicators associated with network attacks. Wireless ○ Evil twin ○ Rogue access point ○ Bluesnarfing ○ Bluejacking ○ Disassociation ○ Jamming ○ Radio frequency identifier (RFID) ○ Near field communication (NFC) ○ Initialization vector (IV) Man in the middle Man in the browser Layer 2 attacks ○ Address resolution protocol (ARP) poisoning ○ Media access control (MAC) flooding ○ MAC cloning Domain name system (DNS) ○ Domain hijacking ○ DNS poisoning ○ Universal resource locator (URL) redirection ○ Domain reputation Distributed denial of service (DDoS) ○ Network ○ Application ○ Operational technology (OT) Malicious code or script execution ○ PowerShell ○ Python ○ Bash ○ Macros ○ Virtual Basic for Applications (VBA)	5.8, 5.11 8.2 10.3 11.6 12.6
1.5	Explain different threat actors, vectors, and intelligence sources. Actors and threats ○ Advanced persistent threat (APT)	1.1, 1.2 2.1, 2.3 10.4 11.4

	○ Insider threats ○ State actors ○ Hacktivists ○ Script kiddies ○ Criminal syndicates ○ Hackers ▪ White hat ▪ Black hat ▪ Gray hat ○ Shadow IT ○ Competitors Attributes of actors ○ Internal/external ○ Level of sophistication/capability ○ Resources/funding ○ Intent/motivation Vectors ○ Direct access ○ Wireless ○ Email ○ Supply chain ○ Social media ○ Removable media ○ Cloud Threat intelligence sources ○ Open source intelligence (OSINT) ○ Closed/proprietary ○ Vulnerability databases ○ Public/private information sharing centers ○ Dark web ○ Indicators of compromise ○ Automated indicator sharing (AIS) ▪ Structured threat information exchange (STIX)/Trusted automated exchange of indicator information (TAXII) ○ Predictive analysis ○ Threat maps ○ File/code repositories Research sources ○ Vendor websites	13.3

	○ Vulnerability feeds ○ Conferences ○ Academic journals ○ Request for comments (RFC) ○ Local industry groups ○ Social media ○ Threat feeds ○ Adversary tactics, techniques, and procedures (TTP)	
1.6	Explain the security concerns associated with various types of vulnerabilities. Cloud-based vs. on-premises vulnerabilities Zero-day Weak configurations ○ Open permissions ○ Unsecured root accounts ○ Errors ○ Weak encryption ○ Unsecure protocols ○ Default settings ○ Open ports and services Third-party risks ○ Vendor management ▪ System integration ▪ Lack of vendor support ○ Supply chain ○ Outsourced code development ○ Data storage Improper or weak patch management ○ Firmware ○ Operating system (OS) ○ Applications Legacy platforms Impacts ○ Data loss ○ Data breaches ○ Data exfiltration ○ Identity theft	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

	○ Financial ○ Reputation ○ Availability loss	
1.7	Summarize the techniques used in security assessments. Threat hunting ○ Intelligence fusion ○ Threat feeds ○ Advisories and bulletins ○ Maneuver Vulnerability scans ○ False positives ○ False negatives ○ Log reviews ○ Credentialed vs. non-credentialed ○ Intrusive vs. non-intrusive ○ Application ○ Web application ○ Network ○ Common Vulnerabilities and Exposures (CVE)/Common Vulnerability Scoring System (CVSS) ○ Configuration review Syslog/Security information and event management (SIEM) ○ Review reports ○ Packet capture ○ Data inputs ○ User behavior analysis ○ Sentiment analysis ○ Security monitoring ○ Log aggregation ○ Log collectors Security orchestration, automation, response (SOAR)	5.10 11.3, 11.4 12.3, 12.4, 12.6
1.8	Explain the techniques used in penetration testing. Penetration testing	1.2 5.8 11.1, 11.2

	○ White box ○ Black box ○ Gray box ○ Rules of engagement ○ Lateral movement ○ Privilege escalation ○ Persistence ○ Cleanup ○ Bug bounty ○ Pivoting Passive and active reconnaissance ○ Drones/unmanned aerial vehicle (UAV) ○ War flying ○ War driving ○ Footprinting ○ OSINT Exercise types ○ Red team ○ Blue team ○ White team ○ Purple team	
2.0	**Architecture and Design**	
2.1	Explain the importance of security concepts in an enterprise environment. Configuration management ○ Diagrams ○ Baseline configuration ○ Standard naming conventions ○ Internet protocol (IP) schema Data sovereignty Data protection ○ Data loss prevention (DLP) ○ Masking ○ Encryption ○ At rest ○ In transit/motion	4.1, 4.2 5.1, 5.6 7.2, 7.3, 7.4 9.4, 9.5 10.1, 10.2, 10.4 12.3, 12.5, 12.7 13.1

	○ In processing ○ Tokenization ○ Rights management Hardware security module (HSM) Geographical considerations Cloud access security broker (CASB) Response and recovery controls Secure Sockets Layer (SSL)/Transport Layer Security (TLS) inspection Hashing API considerations Site resiliency ○ Hot site ○ Cold site ○ Warm site Deception and disruption ○ Honeypots ○ Honeyfiles ○ Honeynets ○ Fake telemetry ○ DNS sinkhole	
2.2	Summarize virtualization and cloud computing concepts. Cloud models ○ Infrastructure as a service (IaaS) ○ Platform as a service (PaaS) ○ Software as a service (SaaS) ○ Anything as a service (XaaS) ○ Public ○ Community ○ Private ○ Hybrid Cloud service providers Managed service provider (MSP)/Managed security service provider (MSSP) On-premises vs. off-premises Fog computing Edge computing Thin client	9.1, 9.2, 9.3, 9.4, 9.5

	Containers Micro-services/API Infrastructure as code ○ Software-defined networking (SDN) ○ Software-defined visibility (SDV) Serverless architecture Services integration Resource policies Transit gateway Virtualization ○ Virtual machine (VM) sprawl avoidance ○ VM escape protection	
2.3	Summarize secure application development, deployment, and automation concepts. Environment ○ Development ○ Test ○ Staging ○ Production ○ Quality assurance (QA) Provisioning and deprovisioning Integrity measurement Secure coding techniques ○ Normalization ○ Stored procedures ○ Obfuscation/camouflage ○ Code reuse/dead code ○ Server-side vs. client-side execution and validation ○ Memory management ○ Use of third-party libraries and software development kits (SDKs) ○ Data exposure Open Web Application Security Project (OWASP) Software diversity ○ Compiler ○ Binary Automation/scripting ○ Automated courses of action	10.3, 10.4

	○ Continuous monitoring ○ Continuous validation ○ Continuous integration ○ Continuous delivery ○ Continuous deployment Elasticity Scalability Version control	
2.4	Summarize authentication and authorization design concepts. Authentication methods ○ Directory services ○ Federation ○ Attestation ○ Technologies ▪ Time-based one-time password (TOTP) ▪ HMAC-based one-time password (HOTP) ▪ Short message service (SMS) ▪ Token key ▪ Static codes ▪ Authentication applications ▪ Push notifications ▪ Phone call ○ Smart card authentication Biometrics ○ Fingerprint ○ Retina ○ Iris ○ Facial ○ Voice ○ Vein ○ Gait analysis ○ Efficacy rates ○ False acceptance ○ False rejection ○ Crossover error rate Multifactor authentication (MFA) factors and attributes	4.2 5.7 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.9 7.3

	○ Factors ▪ Something you know ▪ Something you have ▪ Something you are ○ Attributes ▪ Somewhere you are ▪ Something you can do ▪ Something you exhibit ▪ Someone you know ○ Authentication, authorization, and accounting (AAA) ○ Cloud vs. on-premises requirements	
2.5	Given a scenario, implement cybersecurity resilience. Redundancy ○ Geographic dispersal ○ Disk ▪ Redundant array of inexpensive disks (RAID) levels ▪ Multipath ○ Network ▪ Load balancers ▪ Network interface card (NIC) teaming ○ Power ▪ Uninterruptible power supply (UPS) ▪ Generator ▪ Dual supply ▪ Managed power distribution units (PDUs) Replication ○ Storage area network (SAN) ○ VM On-premises vs. cloud Backup types ○ Full ○ Incremental ○ Snapshot ○ Differential ○ Tape ○ Disk	3.3 12.7, 12.8

	○ Copy ○ Network attached storage (NAS) ○ SAN ○ Cloud ○ Image ○ Online vs. offline ○ Offsite storage ▪ Distance considerations Non-persistence ○ Revert to known state ○ Last known good configuration ○ Live boot media High availability ○ Scalability Restoration order Diversity ○ Technologies ○ Vendors ○ Crypto ○ Controls	
2.6	Explain the security implications of embedded and specialized systems. Embedded systems ○ Raspberry Pi ○ Field programmable gate array (FPGA) ○ Arduino System control and data acquisition (SCADA)/industrial control system (ICS) ○ Facilities ○ Industrial ○ Manufacturing ○ Energy ○ Logistics Internet of Things (IoT) ○ Sensors ○ Smart devices ○ Wearables ○ Facility automation	5.12 9.9

	○ Weak defaults Specialized ○ Medical systems ○ Vehicles ○ Aircraft ○ Smart meters Voice over IP (VoIP) Heating, ventilation, air conditioning (HVAC) Drones/AVs Multifunction printer (MFP) Real-time operating system (RTOS) Surveillance systems System on chip (SoC) Communication considerations ○ 5G ○ Narrow-band ○ Baseband radio ○ Subscriber identity module (SIM) cards ○ Zigbee Constraints ○ Power ○ Compute ○ Network ○ Crypto ○ Inability to patch ○ Authentication ○ Range ○ Cost ○ Implied trust	
2.7	Explain the importance of physical security controls. Bollards/barricades Mantraps Badges Alarms Signage Cameras	3.1, 3.2, 3.3 5.2, 5.13 14.3

	○ Motion recognition ○ Object detection Closed-circuit television (CCTV) Industrial camouflage Personnel ○ Guards ○ Robot sentries ○ Reception ○ Two-person integrity/control Locks ○ Biometrics ○ Electronic ○ Physical ○ Cable locks USB data blocker Lighting Fencing Fire suppression Sensors ○ Motion detection ○ Noise detection ○ Proximity reader ○ Moisture detection ○ Cards ○ Temperature Drones/UAV Visitor logs Faraday cages Air gap Demilitarized zone (DMZ) Protected cable distribution Secure areas ○ Air gap ○ Vault ○ Safe ○ Hot aisle ○ Cold aisle Secure data destruction ○ Burning	

	○ Shredding ○ Pulping ○ Pulverizing ○ Degaussing ○ Third-party solutions	
2.8	Summarize the basics of cryptographic concepts. Digital signatures Key length Key stretching Salting Hashing Key exchange Elliptical curve cryptography Perfect forward secrecy Quantum ○ Communications ○ Computing Post-quantum Ephemeral Modes of operation ○ Authenticated ○ Unauthenticated ○ Counter Blockchain ○ Public ledgers Cipher suites ○ Stream ○ Block Symmetric vs. asymmetric Lightweight cryptography Steganography ○ Audio ○ Video ○ Image Homomorphic encryption Common use cases	1.1 5.10 7.1, 7.2, 7.3, 7.4 11.7

	○ Low power devices ○ Low latency ○ High resiliency ○ Supporting confidentiality ○ Supporting integrity ○ Supporting obfuscation ○ Supporting authentication ○ Supporting non-repudiation ○ Resource vs. security constraints Limitations ○ Speed ○ Size ○ Weak keys ○ Time ○ Longevity ○ Predictability ○ Reuse ○ Entropy ○ Computational overheads ○ Resource vs. security constraints	
3.0	**Implementation**	
3.1	Given a scenario, implement secure protocols. Protocols ○ Domain Name System Security Extension (DNSSEC) ○ SSH ○ Secure/multipurpose Internet mail exchanger (S/MIME) ○ Secure real-time protocol (SRTP) ○ LDAPS ○ File transfer protocol, secure (FTPS) ○ Secured file transfer protocol (SFTP) ○ Simple Network Management Protocol, version 3 (SNMPv3) ○ Hypertext transfer protocol over SSL/TLS (HTTPS) ○ IPSec ▪ Authentication header (AH)/Encapsulated security payload (ESP)	4.1, 4.3 5.13 6.9, 6.10 7.4 9.7 10.1, 10.3 12.4 13.3

	▪ Tunnel/transport ○ Secure post office protocol (POP)/Internet message access protocol (IMAP) Use cases ○ Voice and video ○ Time synchronization ○ Email and web ○ File transfer ○ Directory services ○ Remote access ○ Domain name resolution ○ Routing and switching ○ Network address allocation ○ Subscription services	
3.2	Given a scenario, implement host or application security solutions. Endpoint protection ○ Antivirus ○ Anti-malware ○ Endpoint detection and response (EDR) ○ DLP ○ Next-generation firewall ○ Host intrusion prevention system (HIPS) ○ Host intrusion detection system (HIDS) ○ Host-based firewall Boot integrity ○ Boot security/Unified Extensible Firmware Interface (UEFI) ○ Measured boot ○ Boot attestation Database ○ Tokenization ○ Salting ○ Hashing Application security ○ Input validations ○ Secure cookies ○ Hypertext Transfer Protocol (HTTP) headers	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

	○ Code signing ○ Whitelisting ○ Blacklisting ○ Secure coding practices ○ Static code analysis ▪ Manual code review ○ Dynamic code analysis ○ Fuzzing Hardening ○ Open ports and services ○ Registry ○ Disk encryption ○ OS ○ Patch management ▪ Third-party updates ▪ Auto-update Self-encrypting drive (SED)/full disk encryption (FDE) ○ Opal Hardware root of trust Trusted Platform Module (TPM) Sandboxing	
3.3	Given a scenario, implement secure network designs. Load balancing ○ Active/active ○ Active/passive ○ Scheduling ○ Virtual IP ○ Persistence Network segmentation ○ Virtual local area network (VLAN) ○ DMZ ○ East-west traffic ○ Extranet ○ Intranet ○ Zero trust Virtual private network (VPN)	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

- Always on
- Split tunnel vs. full tunnel
- Remote access vs. site-to-site
- IPSec
- SSL/TLS
- HTML5
- Layer 2 tunneling protocol (L2TP)

DNS

Network access control (NAC)

- Agent and agentless

Out-of-band management

Port security

- Broadcast storm prevention
- Bridge Protocol Data Unit (BPDU) guard
- Loop prevention
- Dynamic Host Configuration Protocol (DHCP) snooping
- Media access control (MAC) filtering

Network appliances

- Jump servers
- Proxy servers
    - Forward
    - Reverse
- Network-based intrusion detection system (NIDS)/network-based intrusion prevention system (NIPS)
    - Signature based
    - Heuristic/behavior
    - Anomaly
    - Inline vs. passive
- HSM
- Sensors
- Collectors
- Aggregators
- Firewalls
    - Web application firewall (WAF)
    - Next-generation firewall
    - Stateful
    - Stateless
    - Unified threat management (UTM)
    - Network address translation (NAT) gateway

	▪ Content/URL filter ▪ Open-source vs. proprietary ▪ Hardware vs. software ▪ Appliance vs. host-based vs. virtual Access control list (ACL) Route security Quality of service (QoS) Implications of IPv6 Port spanning/port mirroring ○ Port taps Monitoring services File integrity monitors	
3.4	Given a scenario, install and configure wireless security settings. Cryptographic protocols ○ WiFi protected access II (WPA2) ○ WiFi protected access III (WPA3) ○ Counter-mode/CBC-MAC protocol (CCMP) ○ Simultaneous Authentication of Equals (SAE) Authentication protocols ○ Extensible Authentication Protocol (EAP) ○ Protected Extensible Application Protocol (PEAP) ○ EAP-FAST ○ EAP-TLS ○ EAP-TTLS ○ IEEE 802.1X ○ Remote Authentication Dial-in User Server (RADIUS) Federation Methods ○ Pre-shared key (PSK) vs. Enterprise vs. Open ○ WiFi Protected Setup (WPS) ○ Captive portals Installation considerations ○ Site surveys ○ Heat maps ○ WiFi analyzers ○ Channel overlays ○ Wireless access point (WAP) placement	1.2 5.9, 5.11, 5.12 8.1, 8.2, 8.3

	○ Controller and access point security	
3.5	Given a scenario, implement secure mobile solutions. Connection methods and receivers ○ Cellular ○ WiFi ○ Bluetooth ○ NFC ○ Infrared ○ USB ○ Point to point ○ Point to multipoint ○ Global Positioning System (GPS) ○ RFID Mobile device management (MDM) ○ Application management ○ Content management ○ Remote wipe ○ Geofencing ○ Geolocation ○ Screen locks ○ Push notifications ○ Passwords and pins ○ Biometrics ○ Context-aware authentication ○ Containerization ○ Storage segmentation ○ Full device encryption Mobile devices ○ MicroSD HSM ○ MDM/Unified endpoint management (UEM) ○ Mobile application management (MAM) ○ SEAndroid Enforcement and monitoring of: ○ Third-party app stores ○ Rooting/jailbreaking ○ Sideloading	8.1 9.4, 9.6, 9.7, 9.8

	○ Custom firmware ○ Carrier unlocking ○ Firmware over-the-air (OTA) updates ○ Camera use ○ SMS/multimedia message service (MMS)/Rich communication services (RCS) ○ External media ○ USB on the go (OTG) ○ Recording microphone ○ GPS tagging ○ WiFi direct/ad hoc ○ Tethering ○ Hotspot ○ Payment methods Deployment models ○ Bring your own device (BYOD) ○ Corporate-owned personally enabled (COPE) ○ Choose your own device (CYOD) ○ Corporate-owned ○ Virtual desktop infrastructure (VDI)	
3.6	Given a scenario, apply cybersecurity solutions to the cloud. Cloud security controls ○ High availability across zones ○ Resource policies ○ Secrets management ○ Integration and auditing ○ Storage ▪ Permissions ▪ Encryption ▪ Replication ▪ High availability ○ Network ▪ Virtual networks ▪ Public and private subnets ▪ Segmentation ▪ API inspection and integration	4.3 5.8 6.3 9.2, 9.4, 9.5, 9.8 14.1

	○ Compute ▪ Security groups ▪ Dynamic resource allocation ▪ Instance awareness ▪ Virtual private cloud (VPC) endpoint ▪ Container security Solutions ○ CASB ○ Application security ○ Next-generation secure web gateway (SWG) ○ Firewall considerations in a cloud environment ▪ Cost ▪ Need for segmentation ▪ Open Systems Interconnection (OSI) layers ○ Cloud native controls vs. third-party solutions	
3.7	Given a scenario, implement identity and account management controls. Identity ○ Identity provider (IdP) ○ Attributes ○ Certificates ○ Tokens ○ SSH keys ○ Smart cards Account types ○ User account ○ Shared and generic accounts/credentials ○ Guest accounts ○ Service accounts Account policies ○ Password complexity ○ Password history ○ Password reuse ○ Time of day ○ Network location ○ Geofencing ○ Geotagging	3.1 4.1 5.9 6.2, 6.3, 6.5, 6.6, 6.7 9.6 11.7 12.2 14.1

	○ Geolocation ○ Time-based logins ○ Access policies ○ Account permissions ○ Account audits ○ Impossible travel time/risky login ○ Lockout ○ Disablement	
3.8	Given a scenario, implement authentication and authorization solutions. Authentication management ○ Password keys ○ Password vaults ○ TPM ○ HSM ○ Knowledge-based authentication Authentication ○ EAP ○ Challenge Handshake Authentication Protocol (CHAP) ○ Password Authentication Protocol (PAP) ○ 802.1X ○ RADIUS ○ Single sign-on (SSO) ○ Security Assertions Markup Language (SAML) ○ Terminal Access Controller Access Control System Plus (TACACS+) ○ OAuth ○ OpenID ○ Kerberos Access control schemes ○ Attribute-based access control (ABAC) ○ Role-based access control ○ Rule-based access control ○ MAC ○ Discretionary access control (DAC) ○ Conditional access ○ Privilege access management	4.3 6.1, 6.3, 6.9, 6.10 8.3

	○ Filesystem permissions	
3.9	Given a scenario, implement public key infrastructure. Public key infrastructure (PKI) ○ Key management ○ Certificate authority (CA) ○ Intermediate CA ○ Registration authority (RA) ○ Certificate revocation list (CRL) ○ Certificate attributes ○ Online Certificate Status Protocol (OCSP) ○ Certificate signing request (CSR) ○ CN ○ SAN ○ Expiration Types of certificates ○ Wildcard ○ SAN ○ Code signing ○ Self-signed ○ Machine/computer ○ Email ○ User ○ Root ○ Domain validation ○ Extended validation Certificate formats ○ Distinguished encoding rules (DER) ○ Privacy enhanced mail (PEM) ○ Personal information exchange (PFX) ○ .cer ○ P12 ○ P7B Concepts ○ Online vs. offline CA ○ Stapling ○ Pinning	7.5 10.4

	○ Trust model ○ Key escrow ○ Certificate chaining	
4.0	**Operations and Incident Response**	
4.1	Given a scenario, use the appropriate tool to assess organizational security. Network reconnaissance and discovery ○ tracert/traceroute ○ nslookup/dig ○ ipconfig/ifconfig ○ nmap ○ ping/pathping ○ hping ○ netstat ○ netcat ○ IP scanners ○ arp ○ route ○ curl ○ the harvester ○ sn1per ○ scanless ○ dnsenum ○ Nessus ○ Cuckoo File manipulation ○ head ○ tail ○ cat ○ grep ○ chmod ○ logger Shell and script environments ○ SSH ○ PowerShell ○ Python	4.4 5.9 8.2 10.3 11.2, 11.5, 11.6, 11.7 12.5, 12.6

	○ OpenSSL Packet capture and replay ○ Tcpreplay ○ Tcpdump ○ Wireshark Forensics ○ dd ○ Memdump ○ WinHex ○ FTK imager ○ Autopsy Exploitation frameworks Password crackers Data sanitization	
4.2	Summarize the importance of policies, processes, and procedures for incident response. Incident response plans Incident response process ○ Preparation ○ Identification ○ Containment ○ Eradication ○ Recovery ○ Lessons learned Exercises ○ Tabletop ○ Walkthroughs ○ Simulations Attack frameworks ○ MITRE ATT&CK ○ The Diamond Model of Intrusion Analysis ○ Cyber Kill Chain Stakeholder management Communication plan Disaster recovery plan Business continuity plan Continuity of operation planning (COOP)	3.1 12.1, 12.2 13.2

	Incident response team Retention policies	
4.3	Given an incident, utilize appropriate data sources to support an investigation. Vulnerability scan output SIEM dashboards ○ Sensor ○ Sensitivity ○ Trends ○ Alerts ○ Correlation Log files ○ Network ○ System ○ Application ○ Security ○ Web ○ DNS ○ Authentication ○ Dump files ○ VoIP and call managers ○ Session Initiation Protocol (SIP) traffic syslog/rsyslog/syslog-ng journalctl nxlog Retention Bandwidth monitors Metadata ○ Email ○ Mobile ○ Web ○ File Netflow/sflow ○ Echo ○ IPfix Protocol analyzer output	11.5 12.1, 12.3, 12.6

4.4	Given an incident, apply mitigation techniques or controls to secure an environment. Reconfigure endpoint security solutions ○ Application whitelisting ○ Application blacklisting ○ Quarantine Configuration changes ○ Firewall rules ○ MDM ○ DLP ○ Content filter/URL filter ○ Update or revoke certificates Isolation Containment Segmentation Secure Orchestration, Automation, and Response (SOAR) ○ Runbooks ○ Playbooks	1.2 5.1, 5.6 9.6 11.4, 11.5 12.2
4.5	Explain the key aspects of digital forensics. Documentation/evidence ○ Legal hold ○ Video ○ Admissibility ○ Chain of custody ○ Timelines of sequence of events ▪ Time stamps ▪ Time offset ○ Tags ○ Reports ○ Event logs ○ Interviews Acquisition ○ Order of volatility ○ Disk ○ Random-access memory (RAM) ○ Swap/pagefile	1.1 4.1 5.8 7.2 12.4, 12.5, 12.8 14.1

	○ OS ○ Device ○ Firmware ○ Snapshot ○ Cache ○ Network ○ Artifacts On-premises vs. cloud ○ Right to audit clauses ○ Regulatory/jurisdiction ○ Data breach notification laws Integrity ○ Hashing ○ Checksums ○ Provenance Preservation E-discovery Data recovery Non-repudiation Strategic intelligence/counterintelligence	
5.0	**Governance, Risk, and Compliance**	
5.1	Compare and contrast various types of controls. Category ○ Managerial ○ Operational ○ Technical Control type ○ Preventative ○ Detective ○ Corrective ○ Deterrent ○ Compensating ○ Physical	2.4 6.1 14.2

5.2	Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture. Regulations, standards, and legislation ○ General Data Protection Regulation (GDPR) ○ National, territory, or state laws ○ Payment Card Industry Data Security Standard (PCI DSS) Key frameworks ○ Center for Internet Security (CIS) ○ National Institute of Standards and Technology (NIST) RMF/CSF ○ International Organization for Standardization (ISO) 27001/27002/27701/31000 ○ SSAE SOC 2 Type II/III ○ Cloud security alliance ▪ Cloud control matrix ▪ Reference architecture Benchmarks /secure configuration guides ○ Platform/vendor-specific guides ▪ Web server ▪ OS ▪ Application server ▪ Network infrastructure devices	14.1, 14.2, 14.3
5.3	Explain the importance of policies to organizational security. Personnel ○ Acceptable use policy ○ Job rotation ○ Mandatory vacation ○ Separation of duties ○ Least privilege ○ Clean desk space ○ Background checks ○ Non-disclosure agreement (NDA) ○ Social media analysis ○ Onboarding ○ Offboarding ○ User training	1.2 2.1 5.8 6.1 9.8 13.1, 13.2, 13.3 14.1

	▪ Gamification ▪ Capture the flag ▪ Phishing campaigns - phishing simulations ▪ Computer-based training (CBT) ▪ Role-based training Diversity of training techniques Third-party risk management ○ Vendors ○ Supply chain ○ Business partners ○ Service level agreement (SLA) ○ Memorandum of understanding (MOU) ○ Measurement systems analysis (MSA) ○ Business partnership agreement (BPA) ○ End of life (EOL) ○ End of service (EOS) ○ NDA Data ○ Classification ○ Governance ○ Retention Credential policies ○ Personnel ○ Third party ○ Devices ○ Service accounts ○ Administrator/root accounts Organizational policies ○ Change management ○ Change control ○ Asset management	
5.4	Summarize risk management processes and concepts. Risk types ○ External ○ Internal ○ Legacy systems	1.1 2.4 5.8 13.2

	○ Multiparty ○ IP theft ○ Software compliance/licensing Risk management strategies ○ Acceptance ○ Avoidance ○ Transference ▪ Cybersecurity insurance ○ Mitigation Risk analysis ○ Risk register ○ Risk matrix/heat map ○ Risk control assessment ○ Risk control self-assessment ○ Risk awareness ○ Inherent risk ○ Residual risk ○ Control risk ○ Risk appetite ○ Regulations that affect risk posture ○ Risk assessment types ▪ Qualitative ▪ Quantitative ○ Likelihood of occurrence ○ Impact ○ Asset value ○ Single loss expectancy (SLE) ○ Annualized loss expectancy (ALE) ○ Annualized rate of occurrence (ARO) Disasters ○ Environmental ○ Man-made ○ Internal vs. external Business impact analysis ○ Recovery time objective (RTO) ○ Recovery point objective (RPO) ○ Mean time to repair (MTTR) ○ Mean time between failures (MTBF) ○ Functional recovery plans	

	○ Single point of failure ○ Disaster recovery plan (DRP) ○ Mission essential functions ○ Identification of critical systems ○ Site risk assessment	
5.5	Explain privacy and sensitive data concepts in relation to security. Organizational consequences of privacy breaches ○ Reputation damage ○ Identity theft ○ Fines ○ IP theft Notifications of breaches ○ Escalation ○ Public notifications and disclosures Data types ○ Classifications ▪ Public ▪ Private ▪ Sensitive ▪ Confidential ▪ Critical ▪ Proprietary ○ Personally identifiable information (PII) ○ Health information ○ Financial information ○ Government data ○ Customer data Privacy enhancing technologies ○ Data minimization ○ Data masking ○ Tokenization ○ Anonymization ○ Pseudo-anonymization Roles and responsibilities ○ Data owners ○ Data controller	1.1 10.2 14.3

	○ Data processor ○ Data custodian/steward ○ Data privacy officer (DPO) Information life cycle Impact assessment Terms of agreement Privacy notice	