		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 1: Security and Risk Management			
1.5.1	Cybercrimes and data breaches	3	Cybercrimes and Data Breaches
1.5.2	Licensing and Intellectual Property (IP) requirements	3	Licensing and Intellectual Property Requirements
1.5.3	Import/export controls	3	Import/Export Controls
1.5.4	Transborder data flow	3	Transborder Data Flow
1.5.5	Privacy	3	Privacy
1.6	**Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)**	3	Requirements for Investigations
1.7	**Develop, document, and implement security policy, standards, procedures, and guidelines**	1	Security Policies, Standards, Procedures, and Guidelines
1.8	**Identify, analyze, and prioritize Business Continuity (BC) requirements**	2	Business Continuity
1.8.1	Business Impact Analysis (BIA)	2	Business Impact Analysis
1.8.2	Develop and document the scope and the plan	2	Business Continuity
1.9	**Contribute to and enforce personnel security policies and procedures**	1	Personnel Security
1.9.1	Candidate screening and hiring	1	Candidate Screening and Hiring
1.9.2	Employment agreements and policies	1	Employment Agreements and Policies
1.9.3	Onboarding, transfers, and termination processes	1	Onboarding, Transfers and Termination Processes
1.9.4	Vendor, consultant, and contractor agreements and controls	1	Vendors, Consultants, and Contractors
1.9.5	Compliance policy requirements	1	Compliance Policies
1.9.6	Privacy policy requirements	1	Privacy Policies
1.10	**Understand and apply risk management concepts**	2	Risk Management Concepts
1.10.1	Identify threats and vulnerabilities	2	Identifying Threats and Vulnerabilities
1.10.2	Risk assessment/analysis	2	Assessing Risks
1.10.3	Risk response	2	Responding to Risks
1.10.4	Countermeasure selection and implementation	2	Countermeasure Selection and Implementation

		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 1: Security and Risk Management			
1.10.5	Applicable types of controls (e.g., preventive, detective, corrective)	2	Types of Controls
1.10.6	Control assessments (security and privacy)	2	Control Assessments
1.10.7	Monitoring and measurement	2	Monitoring Risks
1.10.8	Reporting	2	Risk Reporting
1.10.9	Continuous improvement (e.g., Risk maturity modeling)	2	Continuous Improvement
1.10.10	Risk frameworks	4	Risk Frameworks
1.11	**Understand and apply threat modeling concepts and methodologies**	9	Threat Modeling
1.12	**Apply Supply Chain Risk Management (SCRM) concepts**	2	Supply Chain Risk Management
1.12.1	Risks associated with hardware, software, and services	2	Risks Associated with Hardware, Software, and Services
1.12.2	Third-party assessment and monitoring	2	Other Third-Party Risks
1.12.3	Minimum security requirements	2	Minimum Security Requirements
1.12.4	Service level requirements	2	Service Level Agreements
1.13	**Establish and maintain a security awareness, education, and training program**	1	Security Awareness, Education, and Training Programs
1.13.1	Methods and techniques to present awareness and training (e.g., social engineering, phishing, security champions, gamification)	1	Methods and Techniques to Present Awareness and Training
1.13.2	Periodic content reviews	1	Periodic Content Reviews
1.13.3	Program effectiveness evaluation	1	Program Effectiveness Evaluation
Domain 2: Asset Security			
2.1	**Identify and classify information and assets**	5	Information and Assets
2.1.1	Data classification	5	Data Classification
2.1.2	Asset classification	5	Asset Classification
2.2	**Establish information and asset handling requirements**	5	Classification
2.3	**Provision resources securely**	5	Secure Provisioning
2.3.1	Information and asset ownership	5	Ownership

		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 2: Asset Security			
2.3.2	Asset inventory (e.g., tangible, intangible)	5	Inventories
2.3.3	Asset management	5	Managing the Life Cycle of Assets
2.4	**Manage data lifecycle**	5	Data Life Cycle
2.4.1	Data roles (i.e., owners, controllers, custodians, processors, users/subjects)	5	Data Roles
2.4.2	Data collection	5	Data Collection
2.4.3	Data location	5	Where in the World Is My Data?
2.4.4	Data maintenance	5	Data Maintenance
2.4.5	Data retention	5	Data Retention
2.4.6	Data remanence	5	Data Remanence
2.4.7	Data destruction	5	Data Destruction
2.5	**Ensure appropriate asset retention (e.g., End-of-Life (EOL), End-of-Support (EOS))**	5	Asset Retention
2.6	**Determine data security controls and compliance requirements**	6	Data Security Controls
2.6.1	Data states (e.g., in use, in transit, at rest)	6	Data States
2.6.2	Scoping and tailoring	6	Scoping and Tailoring
2.6.3	Standards selection	6	Standards
2.6.4	Data protection methods (e.g., Digital Rights Management (DRM), Data Loss Prevention (DLP), Cloud Access Security Broker (CASB))	6	Data Protection Methods
Domain 3: Security Architecture and Engineering			
3.1	**Research, implement and manage engineering processes using secure design principles**	9	Secure Design Principles
3.1.1	Threat modeling	9	Threat Modeling
3.1.2	Least privilege	9	Least Privilege
3.1.3	Defense in depth	9	Defense in Depth
3.1.4	Secure defaults	9	Secure Defaults
3.1.5	Fail securely	9	Fail Securely
3.1.6	Separation of Duties (SoD)	9	Separation of Duties
3.1.7	Keep it simple	9	Keep It Simple
3.1.8	Zero Trust	9	Zero Trust
3.1.9	Privacy by design	9	Privacy by Design

		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 3: Security Architecture and Engineering			
3.1.10	Trust but verify	9	Trust But Verify
3.1.11	Shared responsibility	9	Shared Responsibility
3.2	**Understand the fundamental concepts of security models (e.g., Biba, Star Model, Bell-LaPadula)**	9	Security Models
3.3	**Select controls based upon systems security requirements**	9	Security Requirements
3.4	**Understand security capabilities of Information Systems (IS) (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)**	9	Security Capabilities of Information Systems
3.5	**Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements**	7	General System Architectures
3.5.1	Client-based systems	7	Client-Based Systems
3.5.2	Server-based systems	7	Server-Based Systems
3.5.3	Database systems	7	Database Systems
3.5.4	Cryptographic systems	8	Cryptosystems
3.5.5	Industrial Control Systems (ICS)	7	Industrial Control Systems
3.5.6	Cloud-based systems (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))	7	Cloud-Based Systems
3.5.7	Distributed systems	7	Distributed Systems
3.5.8	Internet of Things (IoT)	7	Internet of Things
3.5.9	Microservices	7	Microservices
3.5.10	Containerization	7	Containerization
3.5.11	Serverless	7	Serverless
3.5.12	Embedded systems	7	Embedded Systems
3.5.13	High-Performance Computing (HPC) systems	7	High-Performance Computing Systems
3.5.14	Edge computing systems	7	Edge Computing Systems
3.5.15	Virtualized systems	7	Virtualized Systems
3.6	**Select and determine cryptographic solutions**	8	Cryptography Definitions and Concepts
3.6.1	Cryptographic life cycle (e.g., keys, algorithm selection)	8	Cryptographic Life Cycle

		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 3: Security Architecture and Engineering			
3.6.2	Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves, quantum)	8	Cryptographic Methods
3.6.3	Public Key Infrastructure (PKI)	8	Public Key Infrastructure
3.6.4	Key management practices	8	Key Management
3.6.5	Digital signatures and digital certificates	8	Digital Signatures Digital Certificates
3.6.6	Non-repudiation	8	Cryptosystems
3.6.7	Integrity (e.g., hashing)	8	Cryptosystems
3.7	**Understand methods of cryptanalytic attacks**	8	Integrity
3.7.1	Brute force	8	Brute Force
3.7.2	Ciphertext only	8	Ciphertext-Only Attacks
3.7.3	Known plaintext	8	Known-Plaintext Attacks
3.7.4	Frequency analysis	8	Frequency Analysis
3.7.5	Chosen ciphertext	8	Chosen-Ciphertext Attacks
3.7.6	Implementation attacks	8	Implementation Attacks
3.7.7	Side-channel	8	Side-Channel Attacks
3.7.8	Fault injection	8	Fault Injection
3.7.9	Timing	8	Side-Channel Attacks
3.7.10	Man-in-the-Middle (MITM)	8	Man-in-the-Middle
3.7.11	Pass the hash	8	Replay Attacks
3.7.12	Kerberos exploitation	17	Weaknesses of Kerberos
3.7.13	Ransomware	8	Ransomware
3.8	**Apply security principles to site and facility design**	10	Security Principles
3.9	**Design site and facility security controls**	10	Site and Facility Controls
3.9.1	Wiring closets/intermediate distribution facilities	10	Distribution Facilities
3.9.2	Server rooms/data centers	10	Data Processing Facilities
3.9.3	Media storage facilities	10	Media Storage
3.9.4	Evidence storage	10	Evidence Storage
3.9.5	Restricted and work area security	10	Restricted Areas

		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 3: Security Architecture and Engineering			
3.9.6	Utilities and Heating, Ventilation, and Air Conditioning (HVAC)	10	Utilities
3.9.7	Environmental issues	10	Environmental Issues
3.9.8	Fire prevention, detection, and suppression	10	Fire Safety
3.9.9	Power (e.g., redundant, backup)	10	Electric Power
Domain 4: Communication and Network Security			
4.1	**Assess and implement secure design principles in network architectures**	13	Applying Secure Design Principles to Network Architectures
4.1.1	Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models	11	Network Reference Models
4.1.2	Internet Protocol (IP) networking (e.g., Internet Protocol Security (IPSec), Internet Protocol (IP) v4/6)	11	Internet Protocol Networking
4.1.3	Secure protocols	13	Secure Protocols
4.1.4	Implications of multilayer protocols	13	Multilayer Protocols
4.1.5	Converged protocols (e.g., Fiber Channel Over Ethernet (FCoE), Internet Small Computer Systems Interface (iSCSI), Voice over Internet Protocol (VoIP))	13	Converged Protocols
4.1.6	Micro-segmentation (e.g., Software Defined Networks (SDN), Virtual eXtensible Local Area Network (VXLAN), Encapsulation, Software-Defined Wide Area Network (SD-WAN))	13	Network Segmentation
4.1.7	Wireless networks (e.g., Li-Fi, Wi-Fi, Zigbee, satellite)	12	Wireless Networking Fundamentals
4.1.8	Cellular networks (e.g., 4G, 5G)	12	Mobile Wireless Communication
4.1.9	Content Distribution Networks (CDN)	14	Content Distribution Networks
4.2	**Secure network components**	14	Network Devices
4.2.1	Operation of hardware (e.g., redundant power, warranty, support)	14	Operation of Hardware
4.2.2	Transmission media	14	Transmission Media
4.2.3	Network Access Control (NAC) devices	14	Network Access Control Devices
4.2.4	Endpoint security	14	Endpoint Security

		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 4: Communication and Network Security			
4.3	**Implement secure communication channels according to design**	15	All of Chapter 15
4.3.1	Voice	15	Voice Communications
4.3.2	Multimedia collaboration	15	Multimedia Collaboration
4.3.3	Remote access	15	Remote Access
4.3.4	Data communications	11	Data Communications Foundations
4.3.5	Virtualized networks	15	Virtualized Networks
4.3.6	Third-party connectivity	15	Third-Party Connectivity
Domain 5: Identity and Access Management (IAM)			
5.1	**Control physical and logical access to assets**	17	Controlling Physical and Logical Access
5.1.1	Information	17	Information Access Control
5.1.2	Systems	17	System and Application Access Control
5.1.3	Devices	17	Access Control to Devices
5.1.4	Facilities	17	Facilities Access Control
5.1.5	Applications	17	System and Application Access Control
5.2	**Manage identification and authentication of people, devices, and services**	16	Identification, Authentication, Authorization, and Accountability
5.2.1	Identity Management (IdM) implementation	16	Identity Management
5.2.2	Single/Multi-Factor Authentication (MFA)	16	Identification and Authentication
5.2.3	Accountability	16	Accountability
5.2.4	Session management	16	Session Management
5.2.5	Registration, proofing, and establishment of identity	16	Registration and Proofing of Identity
5.2.6	Federated Identity Management (FIM)	16	Federated Identity Management
5.2.7	Credential management systems	16	Credential Management
5.2.8	Single Sign On (SSO)	16	Single Sign-On
5.2.9	Just-In-Time (JIT)	16	Just-in-Time Access
5.3	**Federated identity with a third-party service**	16	Federated Identity with a Third-Party Service
5.3.1	On-premise	16	On-Premise

		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 5: Identity and Access Management (IAM)			
5.3.2	Cloud	16	Cloud
5.3.3	Hybrid	16	Hybrid
5.4	**Implement and manage authorization mechanisms**	17	Authorization Mechanisms
5.4.1	Role Based Access Control (RBAC)	17	Role-Based Access Control
5.4.2	Rule based access control	17	Rule-Based Access Control
5.4.3	Mandatory Access Control (MAC)	17	Mandatory Access Control
5.4.4	Discretionary Access Control (DAC)	17	Discretionary Access Control
5.4.5	Attribute Based Access Control (ABAC)	17	Attribute-Based Access Control
5.4.6	Risk based access control	17	Risk-Based Access Control
5.5	**Manage the identity and access provisioning lifecycle**	17	Managing the Identity and Access Provisioning Life Cycle
5.5.1	Account access review (e.g., user, system, service)	17	System Account Access Review
5.5.2	Provisioning and deprovisioning (e.g., on /off boarding and transfers)	17	Provisioning Deprovisioning
5.5.3	Role definition (e.g., people assigned to new roles)	17	Role Definitions
5.5.4	Privilege escalation (e.g., managed service accounts, use of sudo, minimizing its use)	17	Privilege Escalation Managed Service Accounts
5.6	**Implement authentication systems**	17	Implementing Authentication and Authorization Systems
5.6.1	OpenID Connect (OIDC)/Open Authorization (Oauth)	17	OpenID Connect Oauth
5.6.2	Security Assertion Markup Language (SAML)	17	Access Control and Markup Languages
5.6.3	Kerberos	17	Kerberos
5.6.4	Remote Authentication Dial-In User Service (RADIUS)/Terminal Access Controller Access Control System Plus (TACACS+)	17	Remote Access Control Technologies

		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 6: Security Assessment and Testing			
6.1	**Design and validate assessment, test, and audit strategies**	18	Test, Assessment, and Audit Strategies
6.1.1	Internal	18	Internal Audits
6.1.2	External	18	External Audits
6.1.3	Third-party	18	Third-Party Audits
6.2	**Conduct security control testing**	18	Testing Technical Controls
6.2.1	Vulnerability assessment	18	Vulnerability Testing
6.2.2	Penetration testing	18	Penetration Testing
6.2.3	Log reviews	18	Log Reviews
6.2.4	Synthetic transactions	18	Synthetic Transactions
6.2.5	Code review and testing	18	Code Reviews
6.2.6	Misuse case testing	18	Misuse Case Testing
6.2.7	Test coverage analysis	18	Test Coverage
6.2.8	Interface testing	18	Interface Testing
6.2.9	Breach attack simulations	18	Breach Attack Simulations
6.2.10	Compliance checks	18	Compliance Checks
6.3	**Collect security process data (e.g., technical and administrative)**	19	Security Process Data
6.3.1	Account management	19	Account Management
6.3.2	Management review and approval	19	Management Review and Approval
6.3.3	Key performance and risk indicators	19	Key Performance and Risk Indicators
6.3.4	Backup verification data	19	Backup Verification
6.3.5	Training and awareness	19	Security Training and Security Awareness Training
6.3.6	Disaster Recovery (DR) and Business Continuity (BC)	19	Disaster Recovery and Business Continuity
6.4	**Analyze test output and generate report**	19	Reporting
6.4.1	Remediation	19	Remediation
6.4.2	Exception handling	19	Exception Handling
6.4.3	Ethical disclosure	19	Ethical Disclosure

		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 6: Security Assessment and Testing			
6.5	**Conduct or facilitate security audits**	18	Conducting Security Audits
6.5.1	Internal	18	Conducting Internal Audits
6.5.2	External	18	Conducting and Facilitating External Audits
6.5.3	Third-party	18	Facilitating Third-Party Audits
Domain 7: Security Operations			
7.1	**Understand and comply with investigations**	22	Investigations
7.1.1	Evidence collection and handling	22	Evidence Collection and Handling
7.1.2	Reporting and documentation	22	Reporting and Documenting
7.1.3	Investigative techniques	22	Other Investigative Techniques
7.1.4	Digital forensics tools, tactics, and procedures	22	Digital Forensics Tools, Tactics, and Procedures
7.1.5	Artifacts (e.g., computer, network, mobile device)	22	Forensic Artifacts
7.2	**Conduct logging and monitoring activities**	21	Logging and Monitoring
7.2.1	Intrusion detection and prevention	21	Intrusion Detection and Prevention Systems
7.2.2	Security Information and Event Management (SIEM)	21	Security Information and Event Management
7.2.3	Continuous monitoring	21	Continuous Monitoring
7.2.4	Egress monitoring	21	Egress Monitoring
7.2.5	Log management	21	Log Management
7.2.6	Threat intelligence (e.g., threat feeds, threat hunting)	21	Threat Intelligence
7.2.7	User and Entity Behavior Analytics (UEBA)	21	User and Entity Behavior Analytics
7.3	**Perform Configuration Management (CM) (e.g., provisioning, baselining, automation)**	20	Configuration Management

		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 7: Security Operations			
7.4	**Apply foundational security operations concepts**	20	Foundational Security Operations Concepts
7.4.1	Need-to-know/least privilege	20	Need-to-Know/Least Privilege
7.4.2	Separation of Duties (SoD) and responsibilities	20	Separation of Duties and Responsibilities
7.4.3	Privileged account management	20	Privileged Account Management
7.4.4	Job rotation	20	Job Rotation
7.4.5	Service Level Agreements (SLAs)	20	Service Level Agreements
7.5	**Apply resource protection**	20	Resource Protection
7.5.1	Media management	20	Hierarchical Storage Management
7.5.2	Media protection techniques	20	Resource Protection
7.6	**Conduct incident management**	22	Overview of Incident Management
7.6.1	Detection	22	Detection
7.6.2	Response	22	Response
7.6.3	Mitigation	22	Mitigation
7.6.4	Reporting	22	Reporting
7.6.5	Recovery	22	Recovery
7.6.6	Remediation	22	Remediation
7.6.7	Lessons learned	22	Lessons Learned
7.7	**Operate and maintain detective and preventative measures**	21	Preventive and Detective Measures
7.7.1	Firewalls (e.g., next generation, web application, network)	21	Firewalls
7.7.2	Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)	21	Intrusion Detection and Prevention Systems
7.7.3	Whitelisting/blacklisting	21	Whitelisting and Blacklisting
7.7.4	Third-party provided security services	21	Outsourced Security Services
7.7.5	Sandboxing	21	Sandboxing
7.7.6	Honeypots/honeynets	21	Honeypots and Honeynets

		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 7: Security Operations			
7.7.7	Anti-malware	21	Antimalware Software
7.7.8	Machine learning and Artificial Intelligence (AI) based tools	21	Artificial Intelligence Tools
7.8	**Implement and support patch and vulnerability management**	20	Vulnerability and Patch Management
7.9	**Understand and participate in change management processes**	20	Change Management
7.10	**Implement recovery strategies**	23	Recovery Strategies
7.10.1	Backup storage strategies	23	Data Backup
7.10.2	Recovery site strategies	23	Recovery Site Strategies
7.10.3	Multiple processing sites	23	Multiple Processing Sites
7.10.4	System resilience, High Availability (HA), Quality of Service (QoS), and fault tolerance	23	Availability
7.11	**Implement Disaster Recovery (DR) processes**	23	Disaster Recovery Processes
7.11.1	Response	23	Response
7.11.2	Personnel	23	Personnel
7.11.3	Communications	23	Communications
7.11.4	Assessment	23	Assessment
7.11.5	Restoration	23	Restoration
7.11.6	Training and awareness	23	Training and Awareness
7.11.7	Lessons learned	23	Lessons Learned
7.12	**Test Disaster Recovery Plans (DRP)**	23	Testing Disaster Recovery Plans
7.12.1	Read-through/tabletop	23	Checklist Test Tabletop Exercises
7.12.2	Walkthrough	23	Structured Walkthrough Test
7.12.3	Simulation	23	Simulation Test
7.12.4	Parallel	23	Parallel Test
7.12.5	Full interruption	23	Full-Interruption Test
7.13	**Participate in Business Continuity (BC) planning and exercises**	23	Business Continuity
7.14	**Implement and manage physical security**	20	Physical Security
7.14.1	Perimeter security controls	20	External Perimeter Security Controls
7.14.2	Internal security controls	20	Internal Security Controls

		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 7: Security Operations			
7.15	**Address personnel safety and security concerns**	20	Personnel Safety and Security
7.15.1	Travel	20	Travel
7.15.2	Security training and awareness	20	Security Training and Awareness
7.15.3	Emergency management	20	Emergency Management
7.15.4	Duress	20	Duress
Domain 8: Software Development Security			
8.1	**Understand and integrate security in the Software Development Life Cycle (SDLC)**	24	Software Development Life Cycle
8.1.1	Development methodologies (e.g., Agile, Waterfall, DevOps, DevSecOps)	24	Development Methodologies
8.1.2	Maturity models (e.g., Capability Maturity Model (CMM), Software Assurance Maturity Model (SAMM))	24	Maturity Models
8.1.3	Operation and maintenance	24	Operations and Maintenance Phase
8.1.4	Change management	24	Change Management
8.1.5	Integrated Product Team (IPT)	24	Integrated Product Team
8.2	**Identify and apply security controls in software development ecosystems**	25	Security Controls for Software Development
8.2.1	Programming languages	25	Programming Languages and Concepts
8.2.2	Libraries	25	Software Libraries
8.2.3	Tool sets	25	Tool Sets
8.2.4	Integrated Development Environment (IDE)	25	Development Platforms
8.2.5	Runtime	25	Runtime Environments
8.2.6	Continuous Integration and Continuous Delivery (CI/CD)	25	Continuous Integration and Delivery
8.2.7	Security Orchestration, Automation, and Response (SOAR)	25	Security Orchestration, Automation, and Response
8.2.8	Software Configuration Management (SCM)	25	Software Configuration Management
8.2.9	Code repositories	25	Code Repositories
8.2.10	Application security testing (e.g., Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST))	25	Application Security Testing

		All-in-One Coverage	
Domain	**Objective**	**Ch #**	**Heading**
Domain 8: Software Development Security			
8.3	**Assess the effectiveness of software security**	25	Software Security Assessments
8.3.1	Auditing and logging of changes	25	Change Management
8.3.2	Risk analysis and mitigation	25	Risk Analysis and Mitigation
8.4	**Assess security impact of acquired software**	25	Assessing the Security of Acquired Software
8.4.1	Commercial-off-the-shelf (COTS)	25	Commercial Software
8.4.2	Open source	25	Open-Source Software
8.4.3	Third-party	25	Third-Party Software
8.4.4	Managed services (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))	25	Managed Services
8.5	**Define and apply secure coding guidelines and standards**	25	Secure Software Development
8.5.1	Security weaknesses and vulnerabilities at the source-code level	25	Source Code Vulnerabilities
8.5.2	Security of Application Programming Interfaces (APIs)	25	Application Programming Interfaces
8.5.3	Secure coding practices	25	Secure Coding Practices
8.5.4	Software-defined security	25	Software-Defined Security

This page intentionally left blank

APPENDIX C

About the Online Content

This book comes complete with TotalTester Online customizable practice exam software with more than 1,400 practice exam questions, separate graphical questions, and access to online CISSP flash cards.

System Requirements

The current and previous major versions of the following desktop browsers are recommended and supported: Chrome, Microsoft Edge, Firefox, and Safari. These browsers update frequently, and sometimes an update may cause compatibility issues with the TotalTester Online or other content hosted on the Training Hub. If you run into a problem using one of these browsers, please try using another until the problem is resolved.

Your Total Seminars Training Hub Account

To get access to the online content you will need to create an account on the Total Seminars Training Hub. Registration is free, and you will be able to track all your online content using your account. You may also opt in if you wish to receive marketing information from McGraw Hill or Total Seminars, but this is not required for you to gain access to the online content.

Privacy Notice

McGraw Hill values your privacy. Please be sure to read the Privacy Notice available during registration to see how the information you have provided will be used. You may view our Corporate Customer Privacy Policy by visiting the McGraw Hill Privacy Center. Visit the **mheducation.com** site and click **Privacy** at the bottom of the page.

Single User License Terms and Conditions

Online access to the digital content included with this book is governed by the McGraw Hill License Agreement outlined next. By using this digital content you agree to the terms of that license.

Access To register and activate your Total Seminars Training Hub account, simply follow these easy steps.

1. Go to this URL: **hub.totalsem.com/mheclaim**
2. To register and create a new Training Hub account, enter your e-mail address, name, and password on the **Register** tab. No further personal information (such as credit card number) is required to create an account.

   If you already have a Total Seminars Training Hub account, enter your e-mail address and password on the **Log in** tab.
3. Enter your Product Key: **`khth-vc35-9bqs`**
4. Click to accept the user license terms.
5. For new users, click the **Register and Claim** button to create your account. For existing users, click the **Log in and Claim** button.

   You will be taken to the Training Hub and have access to the content for this book.

Duration of License Access to your online content through the Total Seminars Training Hub will expire one year from the date the publisher declares the book out of print.

Your purchase of this McGraw Hill product, including its access code, through a retail store is subject to the refund policy of that store.

The Content is a copyrighted work of McGraw Hill, and McGraw Hill reserves all rights in and to the Content. The Work is © 2022 by McGraw Hill.

Restrictions on Transfer The user is receiving only a limited right to use the Content for the user's own internal and personal use, dependent on purchase and continued ownership of this book. The user may not reproduce, forward, modify, create derivative works based upon, transmit, distribute, disseminate, sell, publish, or sublicense the Content or in any way commingle the Content with other third-party content without McGraw Hill's consent.

Limited Warranty The McGraw Hill Content is provided on an "as is" basis. Neither McGraw Hill nor its licensors make any guarantees or warranties of any kind, either express or implied, including, but not limited to, implied warranties of merchantability or fitness for a particular purpose or use as to any McGraw Hill Content or the information therein or any warranties as to the accuracy, completeness, correctness, or results to be obtained from, accessing or using the McGraw Hill Content, or any material referenced in such Content or any information entered into licensee's product by users or other persons and/or any material available on or that can be accessed through the licensee's product (including via any hyperlink or otherwise) or as to non-infringement of third-party rights. Any warranties of any kind, whether express or implied, are disclaimed. Any material or data obtained through use of the McGraw Hill Content is at your own discretion and risk and user understands that it will be solely responsible for any resulting damage to its computer system or loss of data.

Neither McGraw Hill nor its licensors shall be liable to any subscriber or to any user or anyone else for any inaccuracy, delay, interruption in service, error or omission, regardless of cause, or for any damage resulting therefrom.

In no event will McGraw Hill or its licensors be liable for any indirect, special or consequential damages, including but not limited to, lost time, lost money, lost profits or good will, whether in contract, tort, strict liability or otherwise, and whether or not such damages are foreseen or unforeseen with respect to any use of the McGraw Hill Content.

TotalTester Online

TotalTester Online provides you with a simulation of the CISSP exam. Exams can be taken in Practice Mode or Exam Mode. Practice Mode provides an assistance window with hints, references to the book, explanations of the correct and incorrect answers, and the option to check your answer as you take the test. Exam Mode provides a simulation of the actual exam. The number of questions, the types of questions, and the time allowed are intended to be an accurate representation of the exam environment. The option to customize your quiz allows you to create custom exams from selected domains or chapters, and you can further customize the number of questions and time allowed.

To take a test, follow the instructions provided in the previous section to register and activate your Total Seminars Training Hub account. When you register you will be taken to the Total Seminars Training Hub. From the Training Hub Home page, select your certification from the Study drop-down menu at the top of the page to drill down to the TotalTester for your book. You can also scroll to it from the list of Your Topics on the Home page and then click the TotalTester link to launch the TotalTester. Once you've launched your TotalTester, you can select the option to customize your quiz and begin testing yourself in Practice Mode or Exam Mode. All exams provide an overall grade and a grade broken down by domain.

Graphical Questions

In addition to multiple-choice questions, the CISSP exam includes graphical questions. You can access the practice questions included with this book by navigating to the Resources tab and selecting Graphical Questions Quizzes. After you have selected the quizzes, they will appear in your browser, organized by domain.

Hotspot questions are graphical in nature and require the test taker to understand the concepts of the question from a practical and graphical aspect. You will have to point to the correct component within the graphic to properly answer the exam question. For example, you might be required to point to a specific area in a network diagram, point to a location in a network stack graphic, or choose the right location of a component within a graphic illustrating e-commerce–based authentication. It is not as easy to memorize answers for these types of questions, and they in turn make passing the exam more difficult.

The drag-and-drop questions are not as drastically different in format as compared to the hotspot questions. These questions just require the test taker to choose the correct answer or answers and drag them to the right location.

Online Flash Cards

Access to *Shon Harris' Online CISSP Flash Cards* from CISSP learning products company Human Element, LLC is also provided. These flash cards are another great way to study for the CISSP exam.

Privacy Notice Human Element, LLC values your privacy. Please be sure to read the Privacy Notice available during registration to see how the information you have provided will be used. You may view Human Element's Privacy Policy by visiting https://www.humanelementsecurity.com/content/Privacy-Policy.aspx.

To access the flash cards:

1. Go to www.humanelementsecurity.com and navigate to the CISSP Flash Cards page.
2. Choose the desired product and click the Add to Cart button.
3. Enter all required information (name and e-mail address) to set up your free online account.
4. On the payment method page enter the following code: 7YKL3

After following these instructions, you will have access to the CISSP Flash Cards. The Flash Card application is compatible with all Microsoft, Apple, and Android operating systems and browsers.

Single User License Terms and Conditions

Online access to the flash cards included with this book is governed by the McGraw Hill License Agreement outlined next. By using this digital content you agree to the terms of that license.

Duration of License Access to your online content through the Human Element website will expire one year from the date the publisher declares the book out of print.

Your purchase of this McGraw Hill product, including its access code, through a retail store is subject to the refund policy of that store.

Restrictions on Transfer The user is receiving only a limited right to use the Content for user's own internal and personal use, dependent on purchase and continued ownership of this book. The user may not reproduce, forward, modify, create derivative works based upon, transmit, distribute, disseminate, sell, publish, or sublicense the Content or in any way commingle the Content with other third-party content, without Human Element's consent. The Content is a copyrighted work of Human Element, LLC and Human Element reserves all rights in and to the Content.

Limited Warranty The Content is provided on an "as is" basis. Neither McGraw Hill, Human Element nor their licensors make any guarantees or warranties of any kind, either express or implied, including, but not limited to, implied warranties of merchantability or fitness for a particular purpose or use as to any Content or the information therein or any warranties as to the accuracy, completeness, correctness, or results to

be obtained from, accessing or using the Content, or any material referenced in such Content or any information entered into licensee's product by users or other persons and/or any material available on or that can be accessed through the licensee's product (including via any hyperlink or otherwise) or as to non-infringement of thirdparty rights. Any warranties of any kind, whether express or implied, are disclaimed. Any material or data obtained through use of the Content is at your own discretion and risk and user understands that it will be solely responsible for any resulting damage to its computer system or loss of data.

Neither McGraw Hill nor its licensors shall be liable to any subscriber or to any user or anyone else for any inaccuracy, delay, interruption in service, error or omission, regardless of cause, or for any damage resulting therefrom.

In no event will McGraw Hill, Human Element or their licensors be liable for any indirect, special or consequential damages, including but not limited to, lost time, lost money, lost profits or good will, whether in contract, tort, strict liability or otherwise, and whether or not such damages are foreseen or unforeseen with respect to any use of the Content.

Technical Support

- For questions regarding the TotalTester or operation of the Training Hub, visit **www.totalsem.com** or e-mail **support@totalsem.com**.
- For questions regarding the flash cards, e-mail **info@humanelementsecurity.com**.
- For questions regarding book content, visit **www.mheducation.com/customerservice**.

This page intentionally left blank

access A subject's ability to view, modify, or communicate with an object. Access enables the flow of information between the subject and the object.

access control Mechanisms, controls, and methods of limiting access to resources to authorized subjects only.

access control list (ACL) A list of subjects that are authorized to access a particular object. Typically, the types of access are read, write, execute, append, modify, delete, and create.

access control mechanism Administrative, physical, or technical control that is designed to detect and prevent unauthorized access to a resource or environment.

accountability A security principle indicating that individuals must be identifiable and must be held responsible for their actions.

accredited A computer system or network that has received official authorization and approval to process sensitive data in a specific operational environment. There must be a security evaluation of the system's hardware, software, configurations, and controls by technical personnel.

acquisition The act of acquiring an asset. In organizational processes, this can mean either acquiring infrastructure (e.g., hardware, software, services) or another organization.

administrative controls Security mechanisms that are management's responsibility and referred to as "soft" controls. These controls include the development and publication of policies, standards, procedures, and guidelines; the screening of personnel; security-awareness training; the monitoring of system activity; and change control procedures.

aggregation The act of combining information from separate sources of a lower classification level that results in the creation of information of a higher classification level that the subject does not have the necessary rights to access.

Agile development An umbrella term for several development methodologies that focus on incremental and iterative development methods and promote cross-functional teamwork and continuous feedback mechanisms.

annualized loss expectancy (ALE) A dollar amount that estimates the loss potential from a risk in a span of a year.

single loss expectancy (SLE) × annualized rate of occurrence (ARO) = ALE

annualized rate of occurrence (ARO) The value that represents the estimated possibility of a specific threat taking place within a one-year timeframe.

antimalware Software whose principal functions include the identification and mitigation of malware; also known as antivirus, although this term could be specific to only one type of malware.

artificial intelligence (AI) A multidisciplinary field concerned with how knowledge is organized, how inference proceeds to support decision-making, and how systems learn.

asset Anything that is useful or valuable to an organization.

assurance A measurement of confidence in the level of protection that a specific security control delivers and the degree to which it enforces the security policy.

asymmetric key cryptography A cryptographic method that uses two different, or asymmetric, keys (also called public and private keys).

attribute-based access control (ABAC) An access control model in which access decisions are based on attributes of any component of or action on the system.

audit A systematic assessment of significant importance to the organization that determines whether the system or process being audited satisfies some external standards.

audit trail A chronological set of logs and records used to provide evidence of a system's performance or activity that took place on the system. These logs and records can be used to attempt to reconstruct past events and track the activities that took place, and possibly detect and identify intruders.

authentication Verification of the identity of a subject requesting the use of a system and/or access to network resources. The steps to giving a subject access to an object should be identification, authentication, and authorization.

authorization Granting a subject access to an object after the subject has been properly identified and authenticated.

availability The reliability and accessibility of data and resources to authorized individuals in a timely manner.

back door An undocumented way of gaining access to a computer system. After a system is compromised, an attacker may load a program that listens on a port (back door) so that the attacker can enter the system at any time. A back door is also referred to as a maintenance hook.

back up Copy and move data to a medium so that it may be restored if the original data is corrupted or destroyed. A full backup copies all the data from the system to the backup medium. An incremental backup copies only the files that have been modified since the previous backup. A differential backup backs up all files since the last full backup.

baseline The minimum level of security necessary to support and enforce a security policy.

Bell-LaPadula model A formal security model for access control that enforces the confidentiality of data (but not its integrity) using three rules: simple security, star property (*-property), and strong star property.

Biba model A formal security model for access control that enforces data integrity (but not confidentiality) using three rules: the *-integrity axiom (referred to as "no write up"), the simple integrity axiom (referred to as "no read down"), and the invocation property.

biometrics When used within computer security, identifies individuals by physiological characteristics, such as a fingerprint, hand geometry, or pattern in the iris.

blacklist (or deny list) A set of known-bad resources such as IP addresses, domain names, or applications.

breach attack simulation An automated system that launches simulated attacks against a target environment and then generates reports on its findings.

brute-force attack An attack that continually tries different inputs to achieve a predefined goal, which can be used to obtain credentials for unauthorized access.

business continuity (BC) Practices intended to keep the organization in business after a major disruption takes place.

business impact analysis (BIA) A functional analysis in which a team collects data through interviews and documentary sources; documents business functions, activities, and transactions; develops a hierarchy of business functions; and applies a classification scheme to indicate each individual function's criticality level.

Capability Maturity Model Integration (CMMI) A process model that captures the organization's maturity and fosters continuous improvement.

certificate authority (CA) A trusted third party that vouches for the identity of a subject, issues a certificate to that subject, and then digitally signs the certificate to assure its integrity.

certification The technical evaluation of the security components and their compliance for the purpose of accreditation. A certification process can use safeguard evaluation, risk analysis, verification, testing, and auditing techniques to assess the appropriateness of a specific system processing a certain level of information within a particular environment. The certification is the testing of the security component or system, and the accreditation is the approval from management of the security component or system.

challenge/response method A method used to verify the identity of a subject by sending the subject an unpredictable or random value. If the subject responds with the expected value in return, the subject is authenticated.

change management A business process aimed at deliberately regulating the changing nature of business activities such as projects.

chosen-ciphertext attack A cryptanalysis technique in which the attacker can choose the ciphertext to be decrypted and has access to the resulting decrypted plaintext, with the goal of determining the key that was used for decryption.

chosen-plaintext attack A cryptanalysis technique in which the attacker has the plaintext and ciphertext, but can choose the plaintext that gets encrypted to see the corresponding ciphertext in an effort to determine the key being used.

CIA triad The three primary security principles: confidentiality, integrity, and availability. Sometimes also presented as AIC: availability, integrity, and confidentiality.

ciphertext Data that has been encrypted and is unreadable until it has been converted into plaintext.

ciphertext-only attack A cryptanalysis technique in which the attacker has the ciphertext of one or more messages, each of which has been encrypted using the same encryption algorithm and key, and attempts to discover the key used in the encryption process.

Clark-Wilson model An integrity model that addresses all three integrity goals: prevent unauthorized users from making modifications, prevent authorized users from making improper modifications, and maintain internal and external consistency through auditing. A distinctive feature of this model is that it focuses on well-formed transactions and separation of duties.

classification A systematic arrangement of objects into groups or categories according to a set of established criteria. Data and resources can be assigned a level of sensitivity as they are being created, amended, enhanced, stored, or transmitted. The classification level then determines the extent to which the resource needs to be controlled and secured and is indicative of its value in terms of information assets.

cleartext In data communications, describes the form of a message or data that is transferred or stored without cryptographic protection.

cloud access security broker (CASB) A system that provides visibility and security controls for cloud services, monitors user activity in the cloud, and enforces policies and controls that are applicable to that activity.

cloud computing The use of shared, remote computing devices for the purpose of providing improved efficiencies, performance, reliability, scalability, and security.

code review A systematic examination of the instructions that comprise a piece of software, performed by someone other than the author of that code.

collusion Two or more people working together to carry out a fraudulent activity. More than one person would need to work together to cause some type of destruction or fraud; this drastically reduces its probability.

compensating controls Alternative controls that provide similar protection as the original controls but have to be used because they are more affordable or allow specifically required business functionality.

compliance Verifiable adherence to applicable laws, regulations, policies, and standards. The term is typically used to refer to compliance with governmental regulations.

compromise A violation of the security policy of a system or an organization such that unauthorized disclosure or modification of sensitive information occurs.

confidentiality A security principle that works to ensure that information is not disclosed to unauthorized subjects.

configuration management An operational process aimed at ensuring that systems and controls are configured correctly and are responsive to the current threat and operational environments.

containerization A type of virtualization in which individual applications run in their own isolated user space (called a container), which allows for more efficient use of computing resources.

content distribution network Multiple servers distributed across a large region, each of which provides content that is optimized for users closest to it. These networks are used not only to improve the user experience but also to mitigate the risk of denial-of-service attacks.

continuous improvement The practice of constantly measuring, analyzing, and improving processes.

continuous integration and continuous delivery (CI/CD) Processes and technologies that allow source code to be integrated, tested, and prepared for delivery to production environments as soon as a change to the code is submitted.

continuous monitoring Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

control A policy, method, technique, or procedure that is put into place to reduce the risk that a threat agent exploits a vulnerability. Also called a countermeasure or safeguard.

control zone The space within a facility that is used to protect sensitive processing equipment. Controls are in place to protect equipment from physical or technical unauthorized entry or compromise. The zone can also be used to prevent electrical waves carrying sensitive data from leaving the area.

converged protocols Protocols that started off independent and distinct from one another but over time converged to become one.

copyright A legal right that protects the expression of ideas.

corrective controls Controls that fix components or systems after an incident has occurred.

cost/benefit analysis An assessment that is performed to ensure that the cost of a safeguard does not outweigh the benefit of the safeguard. Spending more to protect an asset than the asset is actually worth does not make good business sense. All possible safeguards must be evaluated to ensure that the most security-effective and cost-effective choice is made.

countermeasure A policy, method, technique, or procedure that is put into place to reduce the risk that a threat agent exploits a vulnerability. Also called a safeguard or control.

covert channel A communications path that enables a process to transmit information in a way that violates the system's security policy.

covert storage channel A covert channel that involves writing to a storage location by one process and the direct or indirect reading of the storage location by another process. Covert storage channels typically involve a resource (for example, sectors on a disk) that is shared by two subjects at different security levels.

covert timing channel A covert channel in which one process modulates its system resource (for example, CPU cycles), which is interpreted by a second process as some type of communication.

cryptanalysis The practice of breaking cryptosystems and algorithms used in encryption and decryption processes.

cryptography The science of secret writing that enables storage and transmission of data in a form that is available only to the intended individuals.

cryptology The study of cryptography and cryptanalysis.

cryptosystem The hardware or software implementation of cryptography.

data at rest Data that resides in external or auxiliary storage devices such as hard disk drives, solid-state drives, or optical discs.

data classification Assignments to data that indicate the level of availability, integrity, and confidentiality that is required for each type of information.

data controller A senior leader that sets policies with regard to the management of the data life cycle, particularly with regard to sensitive data such as personal data.

data custodian An individual who is responsible for the maintenance and protection of the data. This role is usually filled by the IT department (usually the network administrator). The duties include performing regular backups of the data; implementing and maintaining security controls; periodically validating the integrity of the data; restoring data from backup media; retaining records of activity; and fulfilling the requirements specified in the organization's security policy, standards, and guidelines that pertain to information security and data protection.

data in transit (or data in motion) Data that is moving between computing nodes over a data network such as the Internet.

data in use Data that temporarily resides in primary storage such as registers, caches, or RAM while the CPU is using it.

data loss (or leak) prevention (DLP) The actions that organizations take to prevent unauthorized external parties from gaining access to sensitive data.

data mining The analysis of the data held in data warehouses in order to produce new and useful information.

data owner The person who has final responsibility of data protection and would be the one held liable for any negligence when it comes to protecting the organization's information assets. The person who holds this role—usually a senior executive within the management group—is responsible for assigning a classification to the information and dictating how the information should be protected.

data processor Any person who carries out operations (e.g., querying, modifying, analyzing) on data under the authority of the data controller.

data remanence A measure of the magnetic flux density remaining after removal of the applied magnetic force, which is used to erase data. Refers to any data remaining on magnetic storage media.

data subject The person about whom the data is concerned.

data warehousing The process of combining data from multiple databases or data sources into a large data store for the purpose of providing more extensive information retrieval and data analysis.

declassification An administrative decision or procedure to remove or reduce the security classification of information.

defense in depth A secure design principle that entails the coordinated use of multiple security controls in a layered approach.

degauss Process that demagnetizes magnetic media so that a very low residue of magnetic induction is left on the media. Used to effectively erase data from media.

Delphi technique A group decision method used to ensure that each member of a group gives an honest and anonymous opinion pertaining to what the result of a particular threat will be.

denial of service (DoS) Any action, or series of actions, that prevents a system, or its resources, from functioning in accordance with its intended purpose.

detective controls Controls that help identify an incident's activities and potentially an intruder.

DevOps The practice of incorporating development, IT, and quality assurance (QA) staff into software development projects to align their incentives and enable frequent, efficient, and reliable releases of software products.

DevSecOps The integration of development, security, and operations professionals into a software development team. It's DevOps with the security team added in.

dial-up The service whereby a computer terminal can use telephone lines, usually via a modem, to initiate and continue communication with another computer system.

dictionary attack A form of attack in which an attacker uses a large set of likely combinations to guess a secret, usually a password.

digital certificate A mechanism used to associate a public key with a collection of components in a manner that is sufficient to uniquely identify the claimed owner. The most commonly used standard for digital certificates is the International Telecommunications Union's X.509.

Digital Rights Management (DRM) A set of technologies that is applied to controlling access to copyrighted data.

digital signature A hash value that has been encrypted with the sender's private key.

disaster recovery (DR) The set of practices that enables an organization to minimize loss of, and restore, mission-critical technology infrastructure after a catastrophic incident.

disaster recovery plan (DRP) A plan developed to help an organization recover from a disaster. It provides procedures for emergency response, extended backup operations, and post-disaster recovery when an organization suffers a loss of computer processing capability or resources and physical facilities.

discretionary access control (DAC) An access control model and policy that restricts access to objects based on the identity of the subjects and the groups to which those subjects belong. The data owner has the discretion of allowing or denying others access to the resources it owns.

Distributed Network Protocol 3 (DNP3) A communications protocol designed for use in SCADA systems, particularly those within the power sector, that does not include routing functionality.

domain The set of objects that a subject is allowed to access. Within this domain, all subjects and objects share a common security policy, procedures, and rules, and they are managed by the same management system.

due care The precautions that a reasonable and competent person would take in a given situation.

due diligence The process of systematically evaluating information to identify vulnerabilities, threats, and issues relating to an organization's overall risk.

duress The use of threats or violence against someone in order to force them to do something they don't want to do.

dynamic application security testing (DAST) Also known as dynamic analysis, the evaluation of a program in real time, while it is running.

edge computing A distributed system in which some computational and data storage assets are deployed close to where they are needed in order to reduce latency and network traffic.

egress monitoring Maintaining awareness of the information that is flowing out of a network, whether it appears to be malicious or not.

electronic discovery (e-discovery) The process of producing for a court or external attorney all electronically stored information pertinent to a legal proceeding.

electronic vaulting The transfer of backup data to an offsite location. This process is primarily a batch process of transmitting data through communications lines to a server at an alternative location.

elliptic curve cryptography A cryptographic method that uses complex mathematical equations (plotted as elliptic curves) that are more efficient than traditional asymmetric key cryptography but also much more difficult to cryptanalyze.

emanations Electrical and electromagnetic signals emitted from electrical equipment that can transmit through the airwaves. These signals carry information that can be captured and deciphered, which can cause a security breach. These are also called *emissions*.

embedded system A self-contained, typically ruggedized, computer system with its own processor, memory, and input/output devices that is designed for a very specific purpose.

encryption The transformation of plaintext into unreadable ciphertext.

end-of-life (EOL) The point in time when a manufacturer ceases to manufacture or sustain a product.

end-of-support (EOS) The point in time when a manufacturer is no longer patching bugs or vulnerabilities on a product, which is typically a few years after EOL.

endpoint A networked computing device that initiates or responds to network communications.

endpoint detection and response (EDR) An integrated security system that continuously monitors endpoints for security violations and uses rules-based automated response and analysis capabilities.

end-to-end encryption A technology that encrypts the data payload of a packet.

ethical disclosure The practice of informing anyone who might be affected by a discovered vulnerability as soon as feasible, so a patch can be developed before any threat actors become aware of the vulnerability.

exposure An instance of being exposed to losses from a threat. A weakness or vulnerability can cause an organization to be exposed to possible damages.

exposure factor The percentage of loss a realized threat could have on a certain asset.

failover A backup operation that automatically switches to a standby system if the primary system fails or is taken offline. It is an important fault-tolerant function that provides system availability.

fail-safe A functionality that ensures that when software or a system fails for any reason, it does not compromise anyone's safety. After a failure, a fail-safe electronic lock might default to an unlocked state, which would prevent it from interfering with anyone trying to escape in an emergency.

fail-secure A functionality that ensures that when software or a system fails for any reason, it does not end up in a vulnerable state. After a failure, a fail-secure lock might default to a locked state, which would ensure the security of whatever it is protecting.

federated identity management (FIM) The management of portable identities, and their associated entitlements, that can be used across business boundaries.

Fibre Channel over Ethernet (FCoE) A converged protocol that allows Fibre Channel frames to ride over Ethernet networks.

firmware Software instructions that have been written into read-only memory (ROM) or a programmable ROM (PROM) chip.

forensic artifact Anything that has evidentiary value.

formal verification Validating and testing of highly trusted systems. The tests are designed to show design verification, consistency between the formal specifications and the formal security policy model, implementation verification, consistency between the formal specifications, and the actual implementation of the product.

full-interruption test A type of security test in which a live system or facility is shut down, forcing the recovery team to switch processing to an alternate system or facility.

gamification The application of elements of game play to other activities such as security awareness training.

gateway A system or device that connects two unlike environments or systems. The gateway is usually required to translate between different types of applications or protocols.

guidelines Recommended actions and operational guides for users, IT staff, operations staff, and others when a specific standard does not apply.

handshaking procedure A dialog between two entities for the purpose of identifying and authenticating the entities to one another. The dialog can take place between two computers or two applications residing on different computers. It is an activity that usually takes place within a protocol.

high-performance computing (HPC) The aggregation of computing power in ways that exceed the capabilities of general-purpose computers for the specific purpose of solving large problems.

honeynet A network of honeypots designed to keep adversaries engaged (and thus under observation) for longer than would be possible with a single honeypot.

honeypot A network device that is intended to be exploited by attackers, with the administrator's goal being to gain information on the attackers' tactics, techniques, and procedures (TTPs).

identification A subject provides some type of data to an authentication service. Identification is the first step in the authentication process.

Identity as a Service (IDaaS) A type of Software as a Service (SaaS) offering that normally provides single sign-on (SSO), federated identity management (IdM), and password management services.

identity management (IdM) A broad term that encompasses the use of different products to identify, authenticate, and authorize users through automated means. It usually includes user account management, access control, credential management, single sign-on (SSO) functionality, managing rights and permissions for user accounts, and auditing and monitoring all of these items.

industrial control system (ICS) Information technology that is specifically designed to control physical devices in industrial processes. The two main types of ICS are distributed control systems (DCSs) and supervisory control and data acquisition (SCADA) systems. The main difference between them is that a DCS controls local processes while SCADA is used to control things remotely.

inference The ability to derive information not explicitly available.

Infrastructure as a Service (IaaS) A cloud computing model that provides users unfettered access to a cloud device, such as an instance of a server, which includes both the operating system and the virtual machine on which it runs.

Integrated Product Team (IPT) A multidisciplinary software development team with representatives from many or all the stakeholder populations.

integrity A security principle that makes sure that information and systems are not modified maliciously or accidentally.

Internet of Things (IoT) The global network of connected, uniquely addressable, embedded systems.

Internet Small Computer System Interface (iSCSI) A converged protocol that encapsulates SCSI data in TCP segments in order to allow peripherals to be connected to computers across networks.

intrusion detection system (IDS) Software employed to monitor and detect possible attacks and behaviors that vary from the normal and expected activity. The IDS can be network based, which monitors network traffic, or host based, which monitors activities of a specific system and protects system files and control mechanisms.

intrusion prevention system (IPS) An intrusion detection system (IDS) that is also able to take actions to stop a detected intrusion.

IP Security (IPSec) A suite of protocols that was developed to specifically protect IP traffic. It includes the Authentication Header (AH), Encapsulating Security Payload (ESP), Internet Security Association and Key Management Protocol (ISAKMP), and Internet Key Exchange (IKE) protocols.

isolation The containment of processes in a system in such a way that they are separated from one another to ensure integrity and confidentiality.

job rotation The practice of ensuring that, over time, more than one person fulfills the tasks of one position within the organization. This enables the organization to have staff backup and redundancy, and helps detect fraudulent activities.

just in time (JIT) access A provisioning methodology that elevates users to the necessary privileged access to perform a specific task.

Kerberos A client/server authentication protocol based on symmetric key cryptography that is the default authentication mechanism in Microsoft Active Directory environments.

kernel The core of an operating system, manages the machine's hardware resources (including the processor and the memory) and provides and controls the way any other software component accesses these resources.

key A discrete data set that controls the operation of a cryptography algorithm. In encryption, a key specifies the particular transformation of plaintext into ciphertext, or vice versa, during decryption. Keys are also used in other cryptographic algorithms, such as digital signature schemes and keyed-hash functions (also known as HMACs), which are often used for authentication and integrity.

keystroke monitoring A type of auditing that can review or record keystrokes entered by a user during an active session.

known-plaintext attack A cryptanalysis technique in which the attacker has the plaintext and corresponding ciphertext of one or more messages and wants to discover the key used to encrypt the message(s).

least privilege The secure design principle that requires each subject to be granted the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

Li-Fi A wireless networking technology that uses light rather than radio waves to transmit and receive data.

Lightweight Directory Access Protocol (LDAP) A directory service based on a subset of the X.500 standard that allows users and applications to interact with a directory.

link encryption A type of encryption technology that encrypts packets' headers, trailers, and the data payload. Each network communications node, or hop, must decrypt the packets to read their addresses and routing information and then re-encrypt the packets. This is different from end-to-end encryption.

machine learning (ML) Systems that acquire their knowledge, in the form of numeric parameters (i.e., weights), through training with data sets consisting of millions of examples. In supervised learning, ML systems are told whether or not they made the right decision. In unsupervised training they learn by observing an environment. Finally, in reinforcement learning they get feedback on their decisions from the environment.

maintenance hook Instructions within a program's code that enable the developer or maintainer to enter the program without having to go through the usual access control and authentication processes. Maintenance hooks should be removed from the code before it is released to production; otherwise, they can cause serious security risks. Also called a back door.

malware Malicious software. Code written to perform activities that circumvent the security policy of a system. Examples are viruses, malicious applets, Trojan horses, logic bombs, and worms.

mandatory access control (MAC) An access policy that restricts subjects' access to objects based on the security clearance of the subject and the classification of the object. The system enforces the security policy, and users cannot share their files with other users.

message authentication code (MAC) In cryptography, a generated value used to authenticate a message. A MAC can be generated by HMAC or CBC-MAC methods. The MAC protects both a message's integrity (by ensuring that a different MAC will be produced if the message has changed) and its authenticity, because only someone who knows the secret key could have modified the message.

microsegmentation The practice of isolating individual assets (e.g., data servers) in their own protected network environment.

microservice An architectural style that consists of small, decentralized, loosely coupled, individually deployable services built around business capabilities.

multifactor authentication (MFA) Authentication mechanisms that employ more than one factor. Factors are something a person knows (e.g., password), something a person has (e.g., a hardware token), and something a person is (e.g., biometrics).

multilayer protocol A protocol that works across multiple layers of the OSI model.

multilevel security A class of systems containing information with different classifications. Access decisions are based on the subject's security clearances, need to know, and formal approval.

Multiprotocol Label Switching (MPLS) A converged data communications protocol designed to improve the routing speed of high-performance networks.

need to know A security principle stating that users should have access only to the information and resources necessary to complete their tasks that fulfill their roles within an organization. Need to know is commonly used in access control criteria by operating systems and applications.

network detection and response (NDR) Systems that monitor network traffic for malicious actors and suspicious behavior, and react and respond to the detection of cyberthreats to the network.

nonrepudiation A service that ensures the sender cannot later falsely deny sending a message or taking an action.

OAuth An open standard for authorization (not authentication) to third parties that lets users authorize a web system to use something that they control at a different website.

object A passive entity that contains or receives information. Access to an object potentially implies access to the information that it contains. Examples of objects include records, pages, memory segments, files, directories, directory trees, and programs.

onboarding The process of turning a candidate into a trusted employee who is able to perform all assigned duties.

one-time pad A method of encryption in which the plaintext is combined with a random "pad," which should be the same length as the plaintext. This encryption process uses a nonrepeating set of random bits that are combined bitwise (XOR) with the message to produce ciphertext. A one-time pad is a perfect encryption scheme because it is unbreakable and each pad is used exactly once, but it is impractical because of all of the required overhead.

Open System Interconnection (OSI) model A conceptual framework used to describe the functions of a networking system along seven layers in which each layer relies on services provided by the layer below it and provides services to the layer above it.

OpenID Connect A simple authentication layer built on top of the OAuth 2.0 protocol that allows transparent authentication and authorization of client resource requests.

password A sequence of characters used to prove one's identity. It is used during a logon process and should be highly protected.

patent A grant of legal ownership given to an individual or organization to exclude others from using or copying the invention covered by the patent.

Payment Card Industry Data Security Standard (PCI DSS) An information security standard for organizations that are involved in payment card transactions.

penetration testing A method of evaluating the security of a computer system or network by simulating an attack that a malicious hacker would carry out. Pen testing is performed to uncover vulnerabilities and weaknesses.

personnel security The procedures that are established to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearances. Procedures confirm a person's background and provide assurance of necessary trustworthiness.

physical controls Controls that pertain to controlling individual access into the facility and different departments, locking systems and removing unnecessary USB and optical drives, protecting the perimeter of the facility, monitoring for intrusion, and checking environmental controls.

physical security Controls and procedures put into place to prevent intruders from physically accessing a system or facility. The controls enforce access control and authorized access.

piggyback Unauthorized access to a facility or area by using another user's legitimate credentials or access rights.

plaintext In cryptography, the original readable text before it is encrypted.

Platform as a Service (PaaS) A cloud computing model that provides users access to a computing platform but not to the operating system or to the virtual machine on which it runs.

preventive controls Controls that are intended to keep an incident from occurring.

privacy A security principle that protects an individual's information and employs controls to ensure that this information is not disseminated or accessed in an unauthorized manner.

privacy by design A secure design principle that ensures privacy of user data is an integral part of the design of an information system, not an afterthought or later-stage feature.

procedure Detailed step-by-step instructions to achieve a certain task, which are used by users, IT staff, operations staff, security members, and others.

protocol A set of rules and formats that enables the standardized exchange of information between different systems.

public key encryption A type of encryption that uses two mathematically related keys to encrypt and decrypt messages. The private key is known only to the owner, and the public key is available to anyone.

public key infrastructure (PKI) A framework of programs, procedures, communication protocols, and public key cryptography that enables a diverse group of individuals to communicate securely.

qualitative risk analysis A risk analysis method that uses opinion and experience to judge an organization's exposure to risks. It uses scenarios and ratings systems. Compare to quantitative risk analysis.

quantitative risk analysis A risk analysis method that attempts to use percentages in damage estimations and assigns real numbers to the costs of countermeasures for particular risks and the amount of damage that could result from the risk. Compare to qualitative risk analysis.

quantum key distribution (QKD) A system that generates and securely distributes encryption keys of any length between two parties.

RADIUS (Remote Authentication Dial-In User Service) A security service that authenticates and authorizes dial-up users and is a centralized access control mechanism.

recovery point objective (RPO) The acceptable amount of data loss measured in time.

recovery time objective (RTO) The maximum time period within which a mission-critical system must be restored to a designated service level after a disaster to avoid unacceptable consequences associated with a break in business continuity.

reference monitor concept An abstract machine that mediates all access subjects have to objects, both to ensure that the subjects have the necessary access rights and to protect the objects from unauthorized access and destructive modification.

registration authority (RA) A trusted entity that establishes and confirms the identity of an individual, initiates the certification process with a CA on behalf of an end user, and performs certificate life-cycle management functions.

reliability The assurance of a given system, or individual component, performing its mission adequately for a specified period of time under the expected operating conditions.

remote journaling A method of transmitting changes to data to an offsite facility. This takes place as parallel processing of transactions, meaning that changes to the data are saved locally and to an offsite facility. These activities take place in real time and provide redundancy and fault tolerance.

repudiation When the sender of a message denies sending the message. The countermeasure to this is to implement digital signatures.

residual risk The remaining risk after the security controls have been applied. The conceptual formulas that explain the difference between total risk and residual risk are

threats × vulnerability × asset value = total risk

(threats × vulnerability × asset value) × controls gap = residual risk

risk The likelihood of a threat agent taking advantage of a vulnerability and the resulting business impact. A risk is the loss potential, or probability, that a threat will exploit a vulnerability.

risk analysis A detailed examination of the components of risk that is used to ensure that security is cost-effective, relevant, timely, and responsive to threats.

risk assessment A method of identifying vulnerabilities and threats and assessing the possible impacts to determine where to implement security controls.

risk management The process of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level of risk.

risk-based access control An authorization mechanism that estimates the risk associated with a particular request in real time and, if it doesn't exceed a given threshold, grants the subject access to the requested resource.

role-based access control (RBAC) Type of access control model that provides access to resources based on the role the user holds within the organization or the tasks that the user has been assigned.

rule-based access control (RB-RBAC) Type of access control model that uses specific rules that indicate what can and cannot happen between a subject and an object; built on top of traditional RBAC and is thus commonly called RB-RBAC to disambiguate the otherwise overloaded RBAC acronym.

safeguard A policy, method, technique, or procedure that is put into place to reduce the risk that a threat agent exploits a vulnerability. Also called a countermeasure or control.

sandboxing A type of control that isolates processes from the operating system to prevent security violations.

scoping The process of taking a broader standard and trimming out the irrelevant or otherwise unwanted parts.

secure defaults A secure design principle that entails having every system start off in a state where security trumps user friendliness and functionality, and then has controls deliberately relaxed to enable additional features and generally make the system more user friendly.

Security Assertion Markup Language (SAML) An XML standard that allows the exchange of authentication and authorization data to be shared between security domains.

security awareness The knowledge and attitude of an individual concerning likely threats.

security control Any measure taken by an organization to mitigate information security risks.

security evaluation Assesses the degree of trust and assurance that can be placed in systems for the secure handling of sensitive information.

security information and event management (SIEM) A software platform that aggregates security information and security events and presents them in a single, consistent, and cohesive manner.

security label An identifier that represents the security level of an object.

security orchestration, automation, and response (SOAR) Integrated systems that enable more efficient security operations through automation of various workflows.

security testing Testing all security mechanisms and features within a system to determine the level of protection they provide. Security testing can include penetration testing, formal design and implementation verification, and functional testing.

sensitive information Information that would cause a negative effect on the organization if it were lost or compromised.

sensitivity label A piece of information that represents the security level of an object. Sensitivity labels are used as the basis for mandatory access control (MAC) decisions.

separation of duties A secure design principle that splits up a critical task among two or more individuals to ensure that one person cannot complete a risky task by himself.

serverless architecture A computing architecture in which the services offered to end users, such as compute, storage, or messaging, along with their required configuration and management, can be performed without a requirement from the user to set up any server infrastructure.

service level agreement (SLA) A contract between a service provider and a service user that specifies the minimum acceptable parameters of the services being provided.

shared responsibility A secure design principle that addresses situations in which a service provider is responsible for certain security controls, while the customer is responsible for others.

shoulder surfing When a person looks over another person's shoulder and watches keystrokes or watches data as it appears on the screen in order to uncover information in an unauthorized manner.

simple security property A Bell-LaPadula security model rule that stipulates that a subject cannot read data at a higher security level.

single loss expectancy (SLE) A monetary value that is assigned to a single event that represents the organization's potential loss amount if a specific threat were to take place.

asset value × exposure factor = SLE

single sign-on (SSO) A technology that allows a user to authenticate one time and then access resources in the environment without needing to reauthenticate.

social engineering The act of tricking another person into providing confidential information by posing as an individual who is authorized to receive that information.

Software as a Service (SaaS) A cloud computing model that provides users access to a specific application that executes in the service provider's environment.

Software Assurance Maturity Model (SAMM) A maturity model that is specifically focused on secure software development and allows organizations of any size to decide their target maturity levels within each of five critical business functions.

software-defined networking (SDN) An approach to networking that relies on distributed software to provide improved agility and efficiency by centralizing the configuration and control of networking devices.

software-defined security (SDS or SDsec) A security model in which security functions such as firewalling, IDS/IPS, and network segmentation are implemented in software within an SDN environment.

spoofing Presenting false information, usually within packets, to trick other systems and hide the origin of the message. This is usually done by hackers so that their identity cannot be successfully uncovered.

standards Rules indicating how hardware and software should be implemented, used, and maintained. Standards provide a means to ensure that specific technologies, applications, parameters, and procedures are carried out in a uniform way across the organization. They are compulsory.

star property (*-property) A Bell-LaPadula security model rule that stipulates that a subject cannot write data to an object at a lower security level.

static application security testing (SAST) A technique, also called static analysis, that identifies certain software defects or security policy violations by examining the source code without executing the program.

subject An active entity, generally in the form of a person, process, or device, that causes information to flow among objects or that changes the system state.

supervisory control and data acquisition (SCADA) A system for remotely monitoring and controlling physical systems such as power and manufacturing plants.

supply chain An interconnected network of interdependent suppliers and consumers involved in delivering some product or service.

symmetric key cryptography A cryptographic method that uses instances of the same key (called the secret key) for encryption and decryption.

synthetic transaction A transaction that is executed in real time by a software agent to test or monitor the performance of a distributed system.

tabletop exercise (TTX) A type of exercise in which participants respond to notional events to test out procedures and ensure they actually do what they're intended to and that everyone knows their role in responding to the events.

TACACS (Terminal Access Controller Access Control System) A client/server authentication protocol that provides the same type of functionality as RADIUS and is used as a central access control mechanism mainly for remote users.

tailoring The practice of making changes to specific provisions of a standard so they better address organizational requirements.

technical controls Controls that work in software to provide availability, integrity, or confidentiality protection; also called logical access control mechanisms. Some examples are passwords, identification and authentication methods, security devices, auditing, and the configuration of the network.

test coverage A measure of how much of a system is examined by a specific test (or group of tests), which is typically expressed as a percentage.

threat A potential cause of an unwanted incident, which can result in harm to a system or organization.

threat intelligence Evidence-based knowledge about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding responses to that menace or hazard.

threat modeling The process of describing probable adverse effects on an organization's assets caused by specific threat sources.

top-down approach An approach in which the initiation, support, and direction for a project come from top management and work their way down through middle management and then to staff members.

topology The physical construction of how nodes are connected to form a network.

total risk The risk an organization faces if it chooses not to implement any type of safeguard.

trade secret Something that is proprietary to a company and important for its survival and profitability.

trademark A legal right that protects a word, name, product shape, symbol, color, or a combination of these used to identify a product or an organization.

transborder data flow (TDF) The movement of machine-readable data across a political boundary such as a country's border.

Trojan horse A computer program that has an apparently or actually useful function, but that also contains hidden malicious capabilities to exploit a vulnerability and/or provide unauthorized access into a system.

trust but verify A secure design principle that requires that even when an entity and its behaviors are trusted, they should be monitored and verified.

user A person or process that is accessing a computer system.

user and entity behavior analytics (UEBA) Processes that determine normal patterns of behavior so that abnormalities can be detected and investigated.

user ID A unique set of characters or code that is used to identify a specific user to a system.

validation The act of performing tests and evaluations to test a system's security level to see if it complies with security specifications and requirements.

Virtual eXtensible Local Area Network (VxLAN) A network virtualization technology that encapsulates layer 2 frames onto UDP (layer 4) datagrams for distribution anywhere in the world.

virtualization The practice of running a virtual computing system in an environment that is abstracted from the actual hardware.

virus A small application, or string of code, that infects applications. The main function of a virus is to reproduce, and it requires a host application to do this. It can damage data directly or degrade system performance.

vulnerability A weakness in a system that allows a threat source to compromise its security. It can be a software, hardware, procedural, or human weakness that can be exploited.

Waterfall methodology A software development methodology that uses a strictly linear, sequential life-cycle approach in which each phase must be completed in its entirety before the next phase can begin.

whitelist (or allow list) A set of known-good resources such as IP addresses, domain names, or applications.

work factor The estimated time and effort required for an attacker to overcome a security control.

worm An independent program that can reproduce by copying itself from one system to another. It may damage data directly or degrade system performance by tying up resources.

zero trust A secure design principle that assumes that every entity is hostile until proven otherwise.

This page intentionally left blank

INDEX

B