Eric Reed
Email: eric@ericreedlive.com
Phone: 707-722-7333
Mobile: 404-277-0506

ERIC REED
CYBERSECURITY TRAINING

CISSP Course Outline

Chapter 1: Security Governance Through Principles and Policies

Domain 1.0: Security and Risk Management

1.2 Understand and apply security concepts

1.2.1 Confidentiality, integrity, and availability, authenticity and nonrepudiation

1.3 Evaluate and apply security governance principles

1.3.1 Alignment of security function to business strategy, goals, mission, and objectives

1.3.2 Organizational processes (e.g., acquisitions, divestitures, governance committees)

1.3.3 Organizational roles and responsibilities

1.3.4 Security control frameworks

1.3.5 Due care/due diligence

1.7 Develop, document, and implement security policy, standards, procedures, and guidelines

1.11 Understand and apply threat modeling concepts and methodologies

1.12 Apply Supply Chain Risk Management (SCRM) concepts

1.12.1 Risks associated with hardware, software, and services

1.12.2 Third-party assessment and monitoring

1.12.3 Minimum security requirements

1.12.4 Service level requirements

Domain 3: Security Architecture and Engineering

3.1 Research, implement and manage engineering processes using secure design principles

3.1.1 Threat modeling

3.1.3 Defense in depth

Chapter 2: Personnel Security and Risk Management Concepts

Domain 1.0: Security and Risk Management

1.9 Contribute to and enforce personnel security policies and procedures

1.9.1 Candidate screening and hiring

1.9.2 Employment agreements and policies

1.9.3 Onboarding, transfers, and termination processes

1.9.4 Vendor, consultant, and contractor agreements and controls

1.9.5 Compliance policy requirements

1.9.6 Privacy policy requirements

1.10 Understand and apply risk management concepts

1.10.1 Identify threats and vulnerabilities

1.10.2 Risk assessment/analysis

1.10.3 Risk response

1.10.4 Countermeasure selection and implementation

1.10.5 Applicable types of controls (e.g., preventive, detective, corrective)

1.10.6 Control assessments (security and privacy)

1.10.7 Monitoring and measurement

1.10.8 Reporting

1.10.9 Continuous improvement (e.g., Risk maturity modeling)

1.10.10 Risk frameworks

1.13 Establish and maintain a security awareness, education, and training program

1.13.1 Methods and techniques to present awareness and training (e.g., social engineering, phishing, security champions, gamification)

1.13.2 Periodic content reviews

1.13.3 Program effectiveness evaluation

Chapter 3: Business Continuity Planning

Domain 1.0: Security and Risk Management

1.8 Identify, analyze, and prioritize Business Continuity (BC) requirements

1.8.1 Business Impact Analysis (BIA)

1.8.2 Develop and document scope and plan

Domain 7.0: Security Operations

7.13 Participate in Business Continuity (BC) planning and exercises

Chapter 4: Laws, Regulations, and Compliance

Domain 1.0: Security and Risk Management

1.4 Determine compliance and other requirements

1.4.1 Contractual, legal, industry standards, and regulatory requirements

1.4.2 Privacy requirements

1.5 Understand legal and regulatory issues that pertain to information security in a holistic context

1.5.1 Cybercrimes and data breaches

1.5.2 Licensing and Intellectual Property (IP) requirements

1.5.3 Import/export controls

1.5.4 Transborder data flow

1.5.5 Privacy

Chapter 5: Protecting Security of Assets

Domain 2.0: Asset Security

2.1 Identify and classify information and assets

2.1.1 Data classification

2.1.2 Asset classification

2.2 Establish information and asset handling requirements

2.4 Manage data lifecycle

2.4.1 Data roles (i.e., owners, controllers, custodians, processors, users/subjects)

2.4.2 Data collection

2.4.3 Data location

2.4.4 Data maintenance

2.4.5 Data retention

2.4.6 Data remanence

2.4.7 Data destruction

2.5 Ensure appropriate asset retention (e.g., End-of-Life (EOL), End-of-Support (EOS))

2.6 Determine data security controls and compliance requirements

2.6.1 Data states (e.g., in use, in transit, at rest)

2.6.2 Scoping and tailoring

2.6.3 Standards selection

2.6.4 Data protection methods (e.g., Digital Rights Management (DRM), Data Loss Prevention (DLP), Cloud Access Security Broker (CASB))

Chapter 6: Cryptography and Symmetric Key Algorithms

Domain 3.0: Security Architecture and Engineering

3.6 Select and determine cryptographic solutions

3.6.1 Cryptographic life cycle (e.g., keys, algorithm selection)

3.6.2 Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves, quantum)

3.6.6 Non-repudiation

3.6.7 Integrity (e.g., hashing)

Chapter 7: PKI and Cryptographic Applications

Domain 3:0 Security Architecture and Engineering

3.6 Select and determine cryptographic solutions

3.6.1 Cryptographic life cycle (e.g., keys, algorithm selection)

3.6.2 Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves, quantum)

3.6.3 Public Key Infrastructure (PKI)

3.6.4 Key management practices

3.6.5 Digital signatures and digital certificates

3.6.6 Non-repudiation

3.6.7 Integrity (e.g., hashing)

3.7 Understand methods of cryptanalytic attacks

3.7.1 Brute force

3.7.2 Ciphertext only

3.7.3 Known plaintext

3.7.4 Frequency analysis

3.7.5 Chosen ciphertext

3.7.6 Implementation attacks

3.7.7 Side-channel

3.7.8 Fault injection

3.7.9 Timing

3.7.10 Man-in-the-Middle (MITM)

Chapter 8: Principles of Security Models, Design, and Capabilities

Domain 3.0: Security Architecture and Engineering

3.1 Research, implement and manage engineering processes using secure design principles

3.1.4 Secure defaults

3.1.5 Fail securely

3.1.7 Keep it simple

3.1.8 Zero Trust

3.1.9 Privacy by design

3.1.10 Trust but verify

3.2 Understand the fundamental concepts of security models (e.g. Biba, Star Model, Bell-LaPadula)

3.3 Select controls based upon systems security requirements

3.4 Understand security capabilities of Information Systems (IS) (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Domain 3.0: Security Architecture and Engineering

3.1 Research, implement and manage engineering processes using secure design principles

3.1.11 Shared responsibility

3.5 Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

3.5.1 Client-based systems

3.5.2 Server-based systems

3.5.5 Industrial Control Systems (ICS)

3.5.7 Distributed systems

3.5.8 Internet of Things (IoT)

3.5.9 Microservices

3.5.10 Containerization

3.5.11 Serverless

3.5.12 Embedded systems

3.5.13 High-Performance Computing (HPC) systems

3.5.14 Edge computing systems

3.5.15 Virtualized systems

Chapter 10: Physical Security Requirements

Domain 3.0: Security Architecture and Engineering

3.8 Apply security principles to site and facility design

3.9 Design site and facility security controls

3.9.1 Wiring closets/intermediate distribution facilities

3.9.2 Server rooms/data centers

3.9.3 Media storage facilities

3.9.4 Evidence storage

3.9.5 Restricted and work area security

3.9.6 Utilities and Heating, Ventilation, and Air Conditioning (HVAC)

3.9.7 Environmental issues

3.9.8 Fire prevention, detection, and suppression

3.9.9 Power (e.g., redundant, backup)

Domain 7: Security Operations

7.14 Implement and manage physical security

7.14.1 Perimeter security controls

7.14.2 Internal security controls

Chapter 11: Secure Network Architecture and Securing Network Components

Domain 4.0: Communication and Network Security

4.1 Assess and implement secure design principles in network architectures

4.1.1 Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models

4.1.2 Internet Protocol (IP) networking (e.g., Internet Protocol Security (IPSec), Internet Protocol (IP) v4/6)

4.1.3 Secure protocols

4.1.4 Implications of 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))

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))

4.1.7 Wireless networks (e.g., Li-Fi, Wi-Fi, Zigbee, satellite)

4.1.8 Cellular networks (e.g., 4G, 5G)

4.1.9 Content Distribution Networks (CDN)

4.2 Secure network components

4.2.1 Operation of hardware (e.g., redundant power, warranty, support)

4.2.2 Transmission media

4.2.3 Network Access Control (NAC) devices

4.2.4 Endpoint security

Domain 7: Security Operations

7.7 Operate and maintain detective and preventative measures

7.7.1 Firewalls (e.g., next generation, web application, network)

Chapter 12: Secure Communications and Network Attacks

Domain 4.0: Communication and Network Security

4.1 Assess and implement secure design principles in network architectures

4.1.2 Internet Protocol (IP) networking (e.g., Internet Protocol Security (IPsec), Internet Protocol (IP) v4/6)

4.3 Implement secure communication channels according to design

4.3.1 Voice

4.3.2 Multimedia collaboration

4.3.3 Remote access

4.3.4 Data communications

4.3.5 Virtualized networks

4.3.6 Third-party connectivity

Chapter 13: Managing Identity and Authentication

Domain 5.0: Identity and Access Management (IAM)

5.1 Control physical and logical access to assets

5.1.1 Information

5.1.2 Systems

5.1.3 Devices

5.1.4 Facilities

5.1.5 Applications

5.2 Manage identification and authentication of people, devices, and services

5.2.1 Identity management (IdM) implementation

5.2.2 Single/Multi-Factor Authentication (MFA)

5.2.3 Accountability

5.2.4 Session management

5.2.5 Registration, proofing, and establishment of identity

5.2.6 Federated Identity Management (FIM)

5.2.7 Credential management systems

5.2.8 Single Sign On (SSO)

5.2.9 Just-In-Time (JIT)

5.3 Federated identity with a third-party service

5.3.1 On-premise

5.3.2 Cloud

5.3.3 Hybrid

5.5 Manage the identity and access provisioning lifecycle

5.5.1 Account access review (e.g., user, system, service)

5.5.2 Provisioning and deprovisioning (e.g., on/off boarding and transfers)

5.5.3 Role definition (e.g., people assigned to new roles)

Chapter 14: Controlling and Monitoring Access

Domain 3.0: Security Architecture and Engineering

3.7 Understand methods of cryptanalytic attacks

- 3.7.11 Pass the hash
- 3.7.12 Kerberos exploitation

Domain 5.0: Identity and Access Management (IAM)

5.4 Implement and manage authorization mechanisms

5.4.1 Role Based Access Control (RBAC)

5.4.2 Rule based access control

5.4.3 Mandatory Access Control (MAC)

5.4.4 Discretionary Access Control (DAC)

5.4.5 Attribute Based Access Control (ABAC)

5.4.6 Risk based access control

5.5 Manage the identity and access provisioning lifecycle

5.5.4 Privilege escalation (e.g., managed service accounts, use of sudo, minimizing its use)

5.6 Implement authentication systems

5.6.1 OpenID Connect (OIDC)/Open Authorization (Oauth)

5.6.2 Security Assertion Markup Language (SAML)

5.6.3 Kerberos

5.6.4 Remote Authentication Dial-In User Service (RADIUS)/Terminal Access Controller Access Control System Plus (TACACS+)

Chapter 15: Security Assessment and Testing

Domain 6: Security Assessment and Testing

6.1 Design and validate assessment, test, and audit strategies

6.1.1 Internal

6.1.2 External

6.1.3 Third-party

6.2. Conduct security control testing

6.2.1 Vulnerability assessment

6.2.2 Penetration testing

6.2.3 Log reviews

6.2.4 Synthetic transactions

6.2.5 Code review and testing

6.2.6 Misuse case testing

6.2.7 Test coverage analysis

6.2.8 Interface testing

6.2.9 Breach attack simulations

6.2.10 Compliance checks

6.3 Collect security process data

6.3.1 Account management

6.3.2 Management review and approval

6.3.3 Key performance and risk indicators

6.3.4 Backup verification data

6.3.5 Training and awareness

6.4 Analyze test output and generate report

6.4.1 Remediation

6.4.2 Exception handling

6.4.3 Ethical disclosure

6.5 Conduct or facilitate security audits

6.5.1 Internal

6.5.2 External

6.5.3 Third Party

8.2 Identify and apply security controls in software development ecosystems

8.2.10 Application security testing (e.g., Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST))

Chapter 16: Managing Security Operations

Domain 2: Asset Security

2.3 Provision resources securely

2.3.1 Information and asset ownership

2.3.2 Asset inventory (e.g., tangible, intangible)

2.3.3 Asset management

Domain 3: Security Architecture and Engineering

3.1 Research, implement and manage engineering processes using secure design principles

3.1.2 Least privilege

3.1.6 Separation of Duties (SoD)

3.5 Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

3.5.6 Cloud-based systems (e.g. Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))

Domain 7: Security Operations

7.3 Perform Configuration Management (CM) (e.g., provisioning, baselining, automation)

7.4 Apply foundational security operations concepts

7.4.1 Need-to-know/least privilege

7.4.2 Separation of Duties (SoD) and responsibilities

7.4.3 Privileged account management

7.4.4 Job rotation

7.4.5 Service Level Agreements (SLAs)

7.5 Apply resource protection

7.5.1 Media management

7.5.2 Media protection techniques

7.8 Implement and support patch and vulnerability management

7.9 Understand and participate in change management processes

7.15 Address personnel safety and security concerns

7.15.1 Travel

7.15.2 Security training and awareness

7.15.3 Emergency management

7.15.4 Duress

Domain 8: Software Development Security

8.4 Assess security impact of acquired software

8.4.4 Managed services (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))

Chapter 17: Preventing and Responding to Incidents

Domain 7: Security Operations

7.2 Conduct logging and monitoring activities

7.2.1 Intrusion detection and prevention

7.2.2 Security Information and Event Management (SIEM)

7.2.3 Continuous monitoring

7.2.4 Egress monitoring

7.2.5 Log management

7.2.6 Threat intelligence (e.g., threat feeds, threat hunting)

7.6 Conduct incident management

7.6.1 Detection

7.6.2 Response

7.6.3 Mitigation

7.6.4 Reporting

7.6.5 Recovery

7.6.6 Remediation

7.6.7 Lessons learned

7.7 Operate and maintain detective and preventative measures

7.7.2 Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

7.7.3 Whitelisting/blacklisting

7.7.4 Third-party provided security services

7.7.5 Sandboxing

7.7.6 Honeypots/honeynets

7.7.7 Anti-malware

7.7.8 Machine learning and Artificial intelligence (AI) based tools

Domain 8: Software Development Security

8.2 Identify and apply security controls in software development ecosystems

8.2.7 Security Orchestration, Automation, and Response (SOAR)

Chapter 18: Disaster Recovery Planning

Domain 6: Security Assessment and Testing

6.3 Collect security process data

6.3.5 Training and awareness

6.3.6 Disaster Recovery (DR) and Business Continuity (BC)

Domain 7: Security Operations

7.10 Implement recovery strategies

7.10.1 Backup storage strategies

7.10.2 Recovery site strategies

7.10.3 Multiple processing sites

7.10.4 System resilience, High Availability (HA), Quality of Service (QoS), and fault tolerance

7.11 Implement Disaster Recovery (DR) processes

7.11.1 Response

7.11.2 Personnel

7.11.3 Communications

7.11.4 Assessment

7.11.5 Restoration

7.11.6 Training and awareness

7.11.7 Lessons learned

7.12 Test Disaster Recovery Plans (DRP)

7.12.1 Read-through /tabletop

7.12.2 Walkthrough

7.12.3 Simulation

7.12.4 Parallel

7.12.5 Full interruption

Chapter 19: Incidents and Ethics

Domain 1: Security and Risk Management

Understand, adhere to, and promote professional ethics

$(ISC)^2$ Code of Professional Ethics

Organizational code of ethics

1.6 Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)

Domain 7: Security Operations

7.1 Understand and comply with investigations

7.1.1 Evidence collection and handling

7.1.2 Reporting and documenting

7.1.3 Investigative techniques

7.1.4 Digital forensics tools, tactics, and procedures

7.1.5 Artifacts (e.g. computer, network, mobile device)

Chapter 20: Software Development Security

Domain 3: Security Architecture and Engineering

3.5 Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

3.5.3 Database systems

Domain 8: Software Development Security

8.1 Understand and integrate security in the software development lifecycle (SDLC)

8.1.1 Development methodologies (e.g. Agile, Waterfall, DevOps, DevSecOps)

8.1.2 Maturity models (e.g. Capability Maturity Model (CMM), Software Assurance Maturity Model (SAMM))

8.1.3 Operation and maintenance

8.1.4 Change management

8.1.5 Integrated product team

8.2 Identify and apply security controls in software development ecosystems

8.2.1 Programming languages

8.2.2 Libraries

8.2.3 Tool sets

8.2.4 Integrated Development Environment (IDE)

8.2.5 Runtime

8.2.6 Continuous Integration and Continuous Delivery (CI/CD)

8.2.8 Software Configuration Management (SCM)

8.2.9 Code repositories

8.3 Assess the effectiveness of software security

8.3.1 Auditing and logging of changes

8.3.2 Risk analysis and mitigation

8.4 Assess security impact of acquired software

8.4.1 Commercial-off-the-shelf (COTS)

8.4.2 Open source

8.4.3 Third-party

8.5 Define and apply secure coding guidelines and standards

8.5.2 Security of application programming interfaces

8.5.3 Secure coding practices

8.5.4 Software-defined security

Chapter 21: Malicious Code and Application Attacks

Domain 3: Security Architecture and Engineering

3.7 Understand methods of cryptanalytic attacks

3.7.13 Ransomware

Domain 7: Security Operations

7.2 Conduct logging and monitoring activities

7.2.7 User and Entity Behavior Analytics (UEBA)

7.7 Operate and maintain detective and preventative measures

7.7.7 Anti-malware

Domain 8: Software Development Security

8.2 Identify and apply security controls in software development ecosystems

8.5 Define and apply secure coding guidelines and standards

8.5.1 Security weaknesses and vulnerabilities at the source-code level