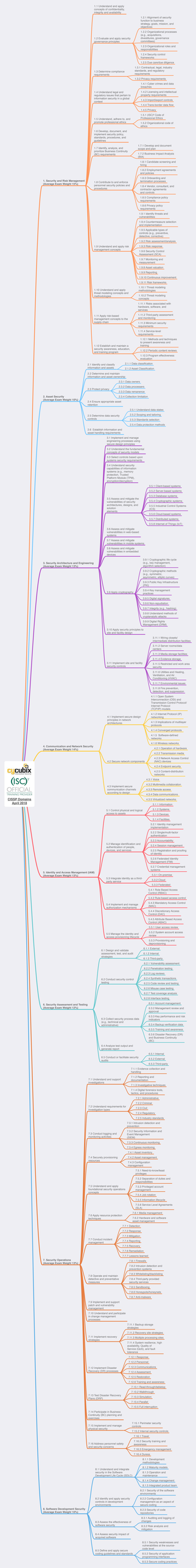
cybrid
(ISC)²
OFFICIAL TRAINING PROVIDER
CISSP Domains April 2018
1. Security and Risk Management (Average Exam Weight 10%)
1.1 Understand and apply concepts of confidentiality, integrity and availability
1.2 Evaluate and apply security governance principles
1.2.1 Alignment of security function to business strategy, goals, mission, and objectives
1.2.2 Organizational processes (e.g., acquisitions, divestitures, governance committees)
1.2.3 Organizational roles and responsibilities
1.2.4 Security control frameworks
1.2.5 Due care/due diligence
1.3 Determine compliance requirements
1.3.1 Contractual, legal, industry standards, and regulatory requirements
1.3.2 Privacy requirements
1.4 Understand legal and regulatory issues that pertain to information security in a global context
1.4.1 Cyber crimes and data breaches
1.4.2 Licensing and intellectual property requirements
1.4.3 Import/export controls
1.4.4 Trans-border data flow
1.4.5 Privacy
1.5 Understand, adhere to, and promote professional ethics
1.5.1 (ISC)² Code of Professional Ethics
1.5.2 Organizational code of ethics
1.6 Develop, document, and implement security policy, standards, procedures, and guidelines
1.7 Identify, analyze, and prioritize Business Continuity (BC) requirements
1.7.1 Develop and document scope and plan
1.7.2 Business Impact Analysis (BIA)
1.8 Contribute to and enforce personnel security policies and procedures
1.8.1 Candidate screening and hiring
1.8.2 Employment agreements and policies
1.8.3 Onboarding and termination processes
1.8.4 Vendor, consultant, and contractor agreements and controls
1.8.5 Compliance policy requirements
1.8.6 Privacy policy requirements
1.9 Understand and apply risk management concepts
1.9.1 Identify threats and vulnerabilities
1.9.2 Qualitative and quantitative impact assessments
1.9.3 Asset valuation
1.9.4 Reassessment of risk
1.9.5 Assign roles and responsibilities
1.9.6 Risk frameworks
1.10 Understand and apply threat modeling concepts and methodologies
1.10.1 Threat modeling methodologies
1.10.2 Threat modeling concepts
1.11 Apply risk-based management concepts to the supply chain
1.11.1 Risks associated with hardware, software, and services
1.11.2 Third-party assessment and monitoring
1.11.3 Minimum security requirements
1.11.4 Service level requirements
1.12 Establish and maintain a security awareness, education, and training program
1.12.1 Methods and techniques to present awareness and training
1.12.2 Periodic content reviews
1.12.3 Program effectiveness evaluation
2. Asset Security (Average Exam Weight 10%)
2.1 Identify and classify information and assets
2.1.1 Data classification
2.1.2 Asset Classification
2.2 Determine and maintain information and asset ownership
2.3 Protect privacy
2.3.1 Data owners
2.3.2 Data processers
2.3.3 Data remanence
2.3.4 Collection limitation
2.4 Ensure appropriate asset retention
2.5 Determine data security controls
2.5.1 Understand data states
2.5.2 Scoping and tailoring
2.5.3 Standards selection
2.5.4 Data protection methods
2.6 Establish information and asset handling requirements
3. Security Architecture and Engineering (Average Exam Weight 12%)
3.1 Implement and manage engineering processes using secure design principles
3.2 Understand the fundamental concepts of security models
3.3 Select controls based upon systems security requirements
3.4 Understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)
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
3.5.3 Database systems
3.5.4 Cryptographic systems
3.5.5 Industrial Control Systems
3.5.6 Cloud-based systems
3.5.7 Distributed systems
3.5.8 Internet of Things (IoT)
3.6 Assess and mitigate vulnerabilities in web-based systems
3.7 Assess and mitigate vulnerabilities in mobile systems
3.8 Assess and mitigate vulnerabilities in embedded devices
3.9 Apply cryptography
3.9.1 Cryptographic life cycle (e.g., key management, algorithm selection)
3.9.2 Cryptographic methods (e.g., symmetric, asymmetric, elliptic)
3.9.3 Public Key Infrastructure (PKI)
3.9.4 Key management practices
3.9.5 Digital signatures
3.9.6 Non-repudiation
3.9.7 Integrity (e.g., hashing)
3.9.8 Understand methods of cryptanalytic attacks
3.9.9 Digital Rights Management (DRM)
3.10 Apply security principles to site and facility design
3.11 Implement site and facility security controls
3.11.1 Wiring closets/ intermediate distribution facilities
3.11.2 Server rooms/data centers
3.11.3 Media storage facilities
3.11.4 Evidence storage
3.11.5 Restricted and work area security
3.11.6 Utilities and Heating, Ventilation, and Air Conditioning (HVAC)
3.11.7 Environmental issues
3.11.8 Fire prevention, detection, and suppression
4. Communication and Network Security (Average Exam Weight 14%)
4.1 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
4.1.3 Implications of multilayer protocols
4.1.4 Converged protocols
4.1.5 Software-defined networks
4.1.6 Wireless networks
4.2 Secure network components
4.2.1 Operation of hardware
4.2.2 Transmission media
4.2.3 Network Access Control (NAC) devices
4.2.4 Endpoint security
4.2.5 Content-distribution networks
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
5. Identity and Access Management (IAM) (Average Exam Weight 12%)
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
5.2 Manage identification and authentication of people, devices, and services
5.2.1 Identity management implementation
5.2.2 Single/multi-factor authentication
5.2.3 Accountability
5.2.4 Session management
5.2.5 Registration, proofing and provisioning of identity
5.2.6 Federated identity Management (FIM)
5.2.7 Credential management systems
5.3 Integrate identity as a third-party service
5.3.1 On-premise
5.3.2 Cloud
5.3.3 Federated
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)
5.5 Manage the identity and access provisioning lifecycle
5.5.1 User access review
5.5.2 System account access review
5.5.3 Provisioning and deprovisioning
6. Security Assessment and Testing (Average Exam Weight 12%)
6.1 Design and validate assessment, test, and audit strategies
6.1.1 External
6.1.2 Internal
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
6.3 Collect security process data (e.g., technical and administrative)
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
6.3.6 Disaster Recovery (DR) and Business Continuity (BC)
6.4 Analyze test output and generate report
6.5 Conduct or facilitate security audits
6.5.1 Internal
6.5.2 External
6.5.3 Third-party
7. Security Operations (Average Exam Weight 13%)
7.1 Understand and support investigations
7.1.1 Evidence collection and handling
7.1.2 Reporting and documentation
7.1.3 Investigative techniques
7.1.4 Digital forensics tools, tactics, and procedures
7.2 Understand requirements for investigation types
7.2.1 Administrative
7.2.2 Criminal
7.2.3 Civil
7.2.4 Regulatory
7.2.5 Industry standards
7.3 Conduct logging and monitoring activities
7.3.1 Intrusion detection and prevention
7.3.2 Security information and Event Management (SIEM)
7.3.3 Continuous monitoring
7.3.4 Egress monitoring
7.4 Secure provisioning resources
7.4.1 Asset inventory
7.4.2 Asset management
7.4.3 Configuration management
7.5 Understand and apply foundational security operations concepts
7.5.1 Need-to-know/least privilege
7.5.2 Separation of duties and responsibilities
7.5.3 Privileged account management
7.5.4 Job rotation
7.5.5 Information lifecycle
7.6 Apply resource protection techniques
7.6.1 Media management
7.6.2 Hardware and software asset management
7.7 Conduct incident management
7.7.1 Detection
7.7.2 Response
7.7.3 Mitigation
7.7.4 Reporting
7.7.5 Recovery
7.7.6 Remediation
7.7.7 Lessons learned
7.8 Operate and maintain detective and preventative measures
7.8.1 Firewalls
7.8.2 Intrusion detection and prevention systems
7.8.3 Whitelisting/blacklisting
7.8.4 Third-party provided security services
7.8.5 Sandboxing
7.8.6 Honeypots/honeynets
7.8.7 Anti-malware
7.9 Implement and support patch and vulnerability management
7.10 Understand and participate in change management processes
7.11 Implement recovery strategies
7.11.1 Backup storage strategies
7.11.2 Recovery site strategies
7.11.3 Multi-site processing sites
7.12 Implement Disaster Recovery (DR) processes
7.12.1 Response
7.12.2 Personnel
7.12.3 Communications
7.12.4 Assessment
7.12.5 Restoration
7.12.6 Training and awareness
7.13 Test Disaster Recovery Plans (DRP)
7.13.1 Read-through/walkthrough
7.13.2 Walkthrough
7.13.3 Simulation
7.13.4 Parallel
7.13.5 Full interruption
7.14 Participate in Business Continuity (BC) planning and exercises
7.15 Implement and manage physical security
7.15.1 Perimeter security controls
7.15.2 Internal security controls
7.16 Address personnel safety and security concerns
7.16.1 Travel
7.16.2 Security training and awareness
7.16.3 Emergency management
7.16.4 Duress
8. Software Development Security (Average Exam Weight 10%)
8.1 Understand and integrate security in the Software Development Life Cycle (SDLC)
8.1.1 Development methodologies
8.1.2 Maturity models
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 development environments
8.2.1 Security of the software environments
8.2.2 Configuration management as an aspect of secure coding
8.2.3 Security of code repositories
8.2.4 Security of application programming interfaces
8.2.5 Secure coding practices
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 software
8.5 Define and apply secure coding guidelines and standards
8.5.1 Security weaknesses and vulnerabilities at the source-code level
8.5.2 Security of application programming interfaces
8.5.3 Secure coding practices