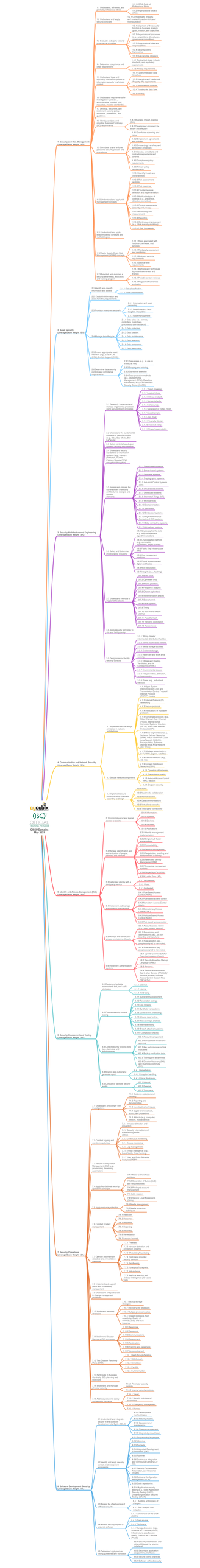
CBK Cubix
(ISC)
OFFICIAL
PRACTICE TESTS
CISSP Domains
May 2021
1. Security and Risk Management (Average Exam Weight 15%)
1.1 Understand, adhere to, and promote professional ethics
1.1.1 (ISC)2 Code of Professional Ethics
1.1.2 Organizational code of ethics
1.2 Understand and apply security concepts
1.2.1 Confidentiality, integrity, and availability, authenticity and nonrepudiation
1.2.2 Alignment of the security function to business strategy, goals, mission, and objectives
1.2.3 Organizational processes (e.g., acquisitions, divestitures, governance committees)
1.2.4 Organizational roles and responsibilities
1.2.5 Security control frameworks
1.2.6 Due care/due diligence
1.2.7 Contractual, legal, industry standards, and regulatory requirements
1.2.8 Privacy requirements
1.3 Evaluate and apply security governance principles
1.3.1 Compliance and risk tolerance
1.3.2 Comprehensive, documented security policy, standards, procedures, and guidelines
1.3.3 Governance and risk management
1.3.4 Licensing and intellectual property (IP) requirements
1.3.5 Intellectual property protects
1.3.6 Transborder data flow
1.3.7 Privacy
1.4 Determine compliance and other requirements
1.5 Understand legal and regulatory issues that pertain to information security in a global context
1.5.1 Cybercrimes and data breaches
1.5.2 Licensing and intellectual property (IP) requirements
1.5.3 Imprisonment protects
1.5.4 Transborder data flow
1.5.5 Privacy
1.6 Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)
1.7 Develop, document, and implement security policy, standards, procedures, and guidelines
1.8 Identify, analyze, and prioritize business continuity (BC) requirements
1.8.1 Business Impact Analysis (BIA)
1.8.2 Develop and document the scope and the plan
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 protection
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 (CAs)
1.10.7 Monitoring and measurement
1.10.8 Reporting
1.10.9 Continuous improvement
1.10.10 Risk frameworks
1.11 Understand and apply threat modeling concepts and methodologies
1.11.1 Risks associated with cloud, virtual, distributed services
1.11.2 Third-party assessment and monitoring
1.11.3 Minimum security requirements
1.12 Apply Supply Chain Risk Management (SCRM) concepts
1.12.1 Service level requirements
1.13 Establish and maintain a security awareness, education, and training program
1.13.1 Security awareness and techniques to prevent social engineering and hacking
1.13.2 Periodic content review
1.13.3 Program effectiveness evaluation
2. Asset Security (Average Exam Weight 10%)
2.1 Identify and classify information and assets
2.1.1 Asset Classification
2.2 Establish information and asset handling requirements
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
2.4 Manage data lifecycle
2.4.1 Acquisition (e.g., purchase, licensing, subscriptions, processors, controllers)
2.4.2 Data collection
2.4.3 Data location
2.4.4 Data maintenance
2.4.5 Data security
2.4.6 Data retention
2.4.7 Data disposition
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))
3. Security Architecture and Engineering (Average Exam Weight 13%)
3.1 Research, implement and manage engineering processes using secure design principles
3.1.1 Threat modeling
3.1.2 Lowest privilege
3.1.3 Defense in depth
3.1.4 Secure defaults
3.1.5 Fail secure
3.1.6 Reassessment of Risks (ROR)
3.1.7 Complexity
3.1.8 Minimization
3.1.9 Layering
3.1.10 Privacy by design
3.1.11 Trust and verify
3.1.12 Shared responsibility
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
3.3.1 Information security capabilities of information system (IS) (e.g., Memory protection, Trusted execution environment (TEE), Hardware root of trust)
3.4 Assess and mitigate the vulnerabilities of security architectures, designs, and solutions elements
3.4.1 Client-based systems
3.4.2 Server based systems
3.4.3 Database systems
3.4.4 Cryptographic systems
3.4.5 Industrial Control Systems (ICS)
3.4.6 Cloud based systems
3.4.7 Distributed systems
3.4.8 Internet of Things (IoT)
3.4.9 Microprocessor
3.4.10 Cryptoprocessor
3.4.11 Biometrics
3.4.12 Embedded systems
3.4.13 High-Performance Computing (HPC) systems
3.4.14 Edge computing systems
3.4.15 Virtualized systems
3.5 Select and determine cryptographic solutions
3.5.1 Cryptographic life cycle (e.g., key management, algorithm selection)
3.5.2 Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves)
3.5.3 Public Key Infrastructure (PKI)
3.5.4 Key management practices
3.5.5 Digital signatures and digital certificates
3.5.6 Non-repudiation
3.5.7 Integrity (e.g., hashing)
3.6 Apply secure principles to site and facility design
3.6.1 Wiring closets
3.6.2 Secure data centers, vaults, telecommunications facilities
3.6.3 Secure server rooms
3.6.4 Restricted and work area security
3.6.5 Utilities and heating, ventilation, and air Conditioning (HVAC)
3.6.6 Environmental issues
3.6.7 Fire prevention, detection, and suppression
3.6.8 Power (e.g., redundant, backup)
3.7 Implement secure design principles in network architectures
3.7.1 Open System Interconnection (OSI) and Transmission Control Protocol/ Internet Protocol (TCP/IP) models
3.7.2 Internet Protocol (IP) (IPv4 / IPv6)
3.7.3 Secure protocols
3.7.4 Implications of multilayer protocols
3.7.5 Converged protocols (e.g., Fibre Channel over Ethernet (FCoE), Internet Small Computer System Interface (iSCSI), Voice over Internet Protocol (VoIP))
3.7.6 Software Defined Networks (SDN), Software Defined Network Security (SDNS), Software Defined Control Area Network (CAN), Encapsulation / Software Defined Security (SDS), Research Only Memory
3.7.7 Wireless networks (e.g., 802.11 series, 802.15 series)
3.7.8 Cellular detection (e.g., 4G, 5G)
3.7.9 Content Distribution Networks (CDN)
3.8 Secure network components
3.8.1 Operation of hardware
3.8.2 Transmission media
3.8.3 Network Access Control (NAC) devices
3.8.4 Endpoint security
3.9.1 Data
3.9.2 Multimedia collaboration
3.9.3 Storage area networks
3.9.4 Data communication
3.9.5 Virtualized networks
3.9.6 Third-party connectivity
4. Communication and Network Security (Average Exam Weight 13%)
4.1 Implement secure design principles in network architectures
4.1.1 Information
4.1.2 Systems
4.1.3 Devices
4.1.4 Facilities
4.1.5 Applications
4.2 Secure network components
4.2.1 Identity management
4.2.2 Multi-factor authentication
4.2.3 Accountability
4.2.4 Session management
4.2.5 Registration, proofing, and establishment of identity
4.2.6 Federated identity management (FIM)
4.2.7 Credential management
4.2.8 Single Sign On (SSO)
4.2.9 Lost and Found (LF)
4.2.10 Organizational
4.2.11 Physical
4.3 Implement communication channels according to design
4.3.1 Voice Access Score (VAS)
4.3.2 Multimedia Access Control (MAC)
4.3.3 Multiplexing Access Control (MAC)
4.3.4 Time Division Access Control (TDAC)
4.3.5 Code Division Access Control (CDAC)
4.3.6 Frequency Division Access Control (FDAC)
4.3.7 Open Systems Interconnection (OSI) Data Authentication Charts
4.3.8 Security Assertion Markup Language (SAML)
4.3.9 Kerberos
4.3.10 Remote Authentication Dial-In User Service (RADIUS) / Terminal Access Controller Access Control System Plus (TACACS+)
5. Identity and Access Management (IAM) (Average Exam Weight 13%)
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
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
5.2.8 Single Sign On (SSO)
5.2.9 Lost and Found (LF)
5.2.10 Organizational
5.2.11 Physical
5.3 Federated identity with a third-party service
5.3.1 Open Access Score (OAS)
5.3.2 Transmission media
5.3.3 Network Access Control (NAC) devices
5.3.4 Endpoint security
5.3.5 Data
5.3.6 Multimedia collaboration
5.3.7 Storage area networks
5.3.8 Data communication
5.3.9 Virtualized networks
5.3.10 Third-party connectivity
5.4 Implement and manage authorization mechanisms
5.4.1 Information
5.4.2 Systems
5.4.3 Devices
5.4.4 Facilities
5.4.5 Applications
5.4.6 Identity management
5.4.7 Single/Multi-factor authentication
5.4.8 Accountability
5.4.9 Session management
5.4.10 Registration, proofing, and establishment of identity
5.4.11 Federated identity management (FIM)
5.4.12 Credential management
5.4.13 Single Sign On (SSO)
5.4.14 Lost and Found (LF)
5.4.15 Organizational
5.4.16 Physical
5.5 Manage the identity and access provisioning lifecycle
5.5.1 Time Access Score (TAS)
5.5.2 Role access control (RAC)
5.5.3 Attribution Access Control (AAC)
5.5.4 Discretionary Access Control (DAC)
5.5.5 Mandatory Access Control (MAC)
5.5.6 Rule based access control
5.5.7 Account access review (e.g., role, entitlement, authentication)
5.5.8 Time-based access control (e.g., dayconstraining, e.g., not after 5 PM, not before 8 AM)
5.5.9 Location-based access control (e.g., access granted to one room, not another)
5.5.10 Role definition (e.g., nurse, doctor, receptionist, peer)
5.5.11 OpenID Connect (OIDC) / Open Authorization (Oauth)
5.5.12 Security Assertion Markup Language (SAML)
5.5.13 Kerberos
5.5.14 Remote Authentication Dial-In User Service (RADIUS) / Terminal Access Controller Access Control System Plus (TACACS+)
6. Security Assessment and Testing (Average Exam Weight 12%)
6.1 Design and validate assessment, test, and audit strategies
6.1.1 Internal
6.1.2 External
6.1.3 Third-party
6.1.4 Vulnerability assessments
6.1.5 Penetration testing
6.1.6 Code review
6.1.7 Synthetic transactions
6.1.8 Code review and testing
6.1.9 Misuse case testing
6.1.10 Test coverage analysis
6.1.11 Interface testing
6.1.12 Breach attack simulations
6.1.13 Compliance checks
6.2 Conduct security control testing
6.2.1 Assessment and test strategies
6.2.2 Management review and approval
6.2.3 Key performance and risk indicators
6.2.4 Backup verification data
6.2.5 Training and awareness
6.2.6 Disaster recovery (DR) and business continuity (BC)
6.2.7 Technical
6.2.8 Administrative
6.2.9 Management
6.2.10 Physical
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)
6.3.7 Technical
6.3.8 Administrative
6.3.9 Management
6.3.10 Physical
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 comply with 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
7.1.5 Artifacts (e.g., computer, network, mobile device)
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., Indicators of Compromise)
7.2.7 User and Entity Behavior Analytics (UEBA)
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 Hardware protections
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
7.7.1 Firewalls
7.7.2 Intrusion detection and prevention systems
7.7.3 Whitelisting/blacklisting
7.7.4 Third-party provisioning
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
7.8 Implement and support patch and vulnerability management
7.9 Understand and participate in change management processes
7.10 Implement recovery strategies
7.10.1 Backup storage strategies
7.10.2 Recovery site strategies
7.10.3 Multi-site solutions (i.e., High availability, Quality of service (QoS), Multi-homed)
7.10.4 Repository
7.10.5 Personnel
7.10.6 Communications
7.10.7 Assessment
7.10.8 Restoration
7.10.9 Training and awareness
7.10.10 Lessons learned
7.11 Implement disaster recovery (DR) processes
7.11.1 Response
7.11.2 Mitigation
7.11.3 Reporting
7.11.4 Communications
7.11.5 Assessment
7.11.6 Restoration
7.11.7 Training and awareness
7.11.8 Lessons learned
7.12 Test Disaster Recovery Plans (DRP)
7.12.1 Walkthroughs
7.12.2 Simulations
7.12.3 Parallel
7.12.4 Interruption
7.13 Participate in Business Continuity (BC) planning and exercises
7.14 Implement and manage physical security
7.14.1 Perimeter security controls
7.14.2 Internal security controls
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
8. Software Development Security (Average Exam Weight 11%)
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 Operational and maintenance
8.1.4 Change management
8.1.5 Integrated product team
8.2 Identify and apply security controls in 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)
8.2.7 Security Orchestration, Automation, and Response (SOAR)
8.2.8 Software Configuration Management (SCM)
8.2.9 Code repositories
8.2.10 Application Security Testing (e.g., Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST))
8.3 Assess the effectiveness of software security
8.3.1 Auditing and logging of changes
8.3.2 Risk analysis and mitigation
8.4.1 Commercial-off-the-shelf (COTS)
8.4.2 Open source
8.4.3 Third-party
8.4.4 Managed services (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))
8.5.1 Security awareness and vulnerabilities at the source-code level
8.5.2 Security of application programming interfaces
8.5.3 Secure coding practices
8.5.4 Software-defined security