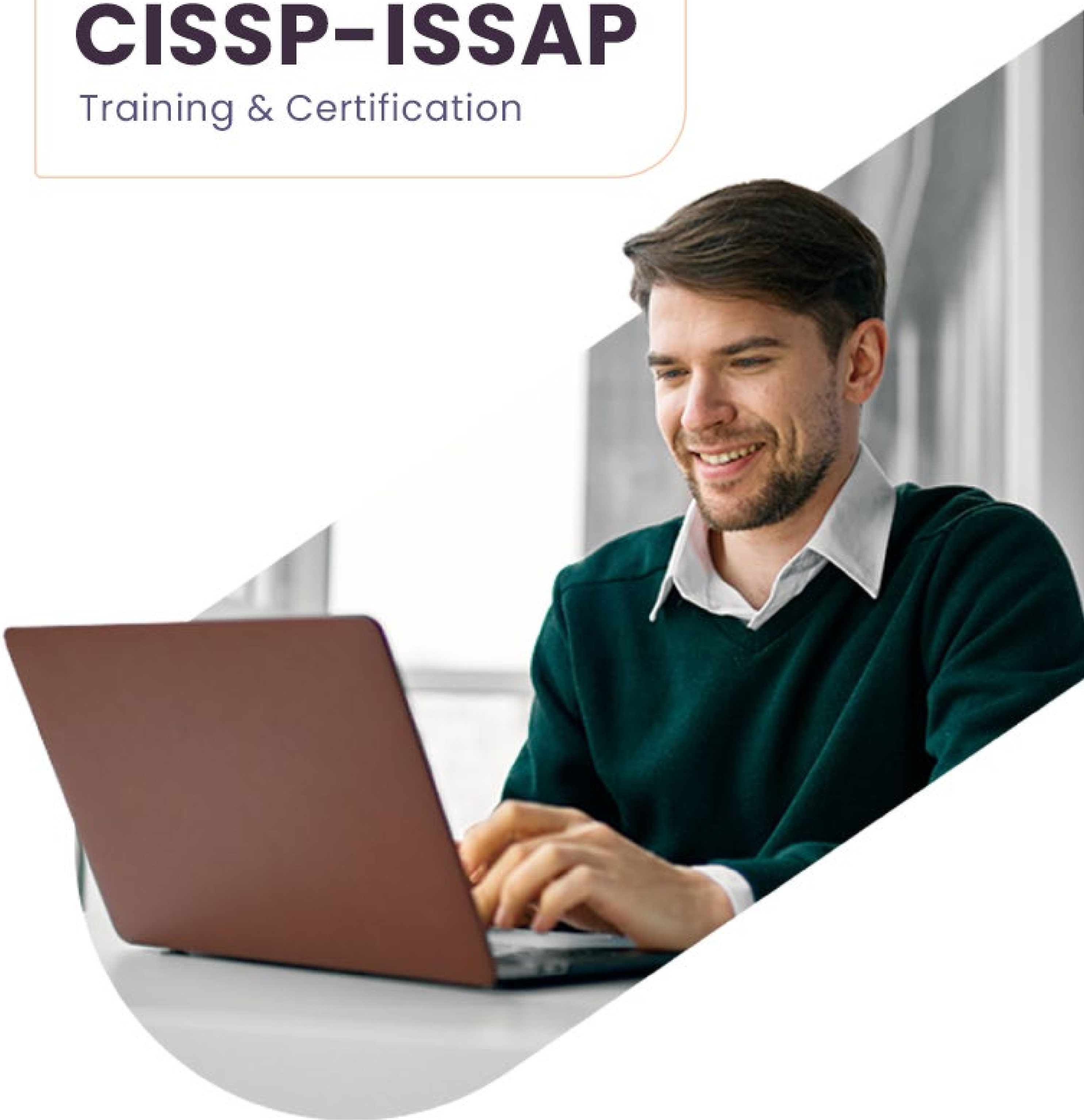
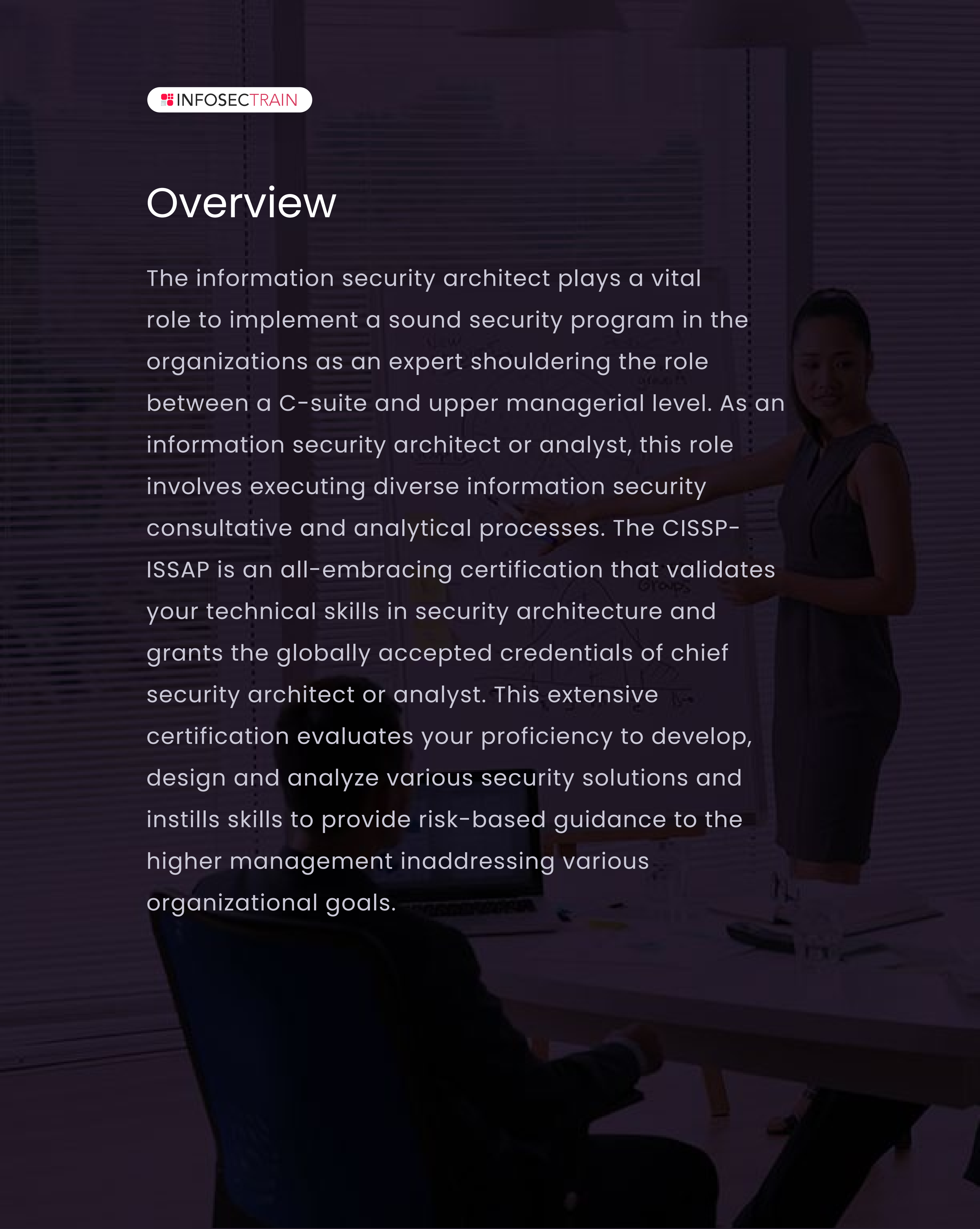
INFOSECTRAIN

CISSP-ISSAP

Training & Certification



www.infosectrain.com | sales@infosectrain.com



Overview

The information security architect plays a vital role to implement a sound security program in the organizations as an expert shouldering the role between a C-suite and upper managerial level. As an information security architect or analyst, this role involves executing diverse information security consultative and analytical processes. The CISSP-ISSAP is an all-embracing certification that validates your technical skills in security architecture and grants the globally accepted credentials of chief security architect or analyst. This extensive certification evaluates your proficiency to develop, design and analyze various security solutions and instills skills to provide risk-based guidance to the higher management inaddressing various organizational goals.

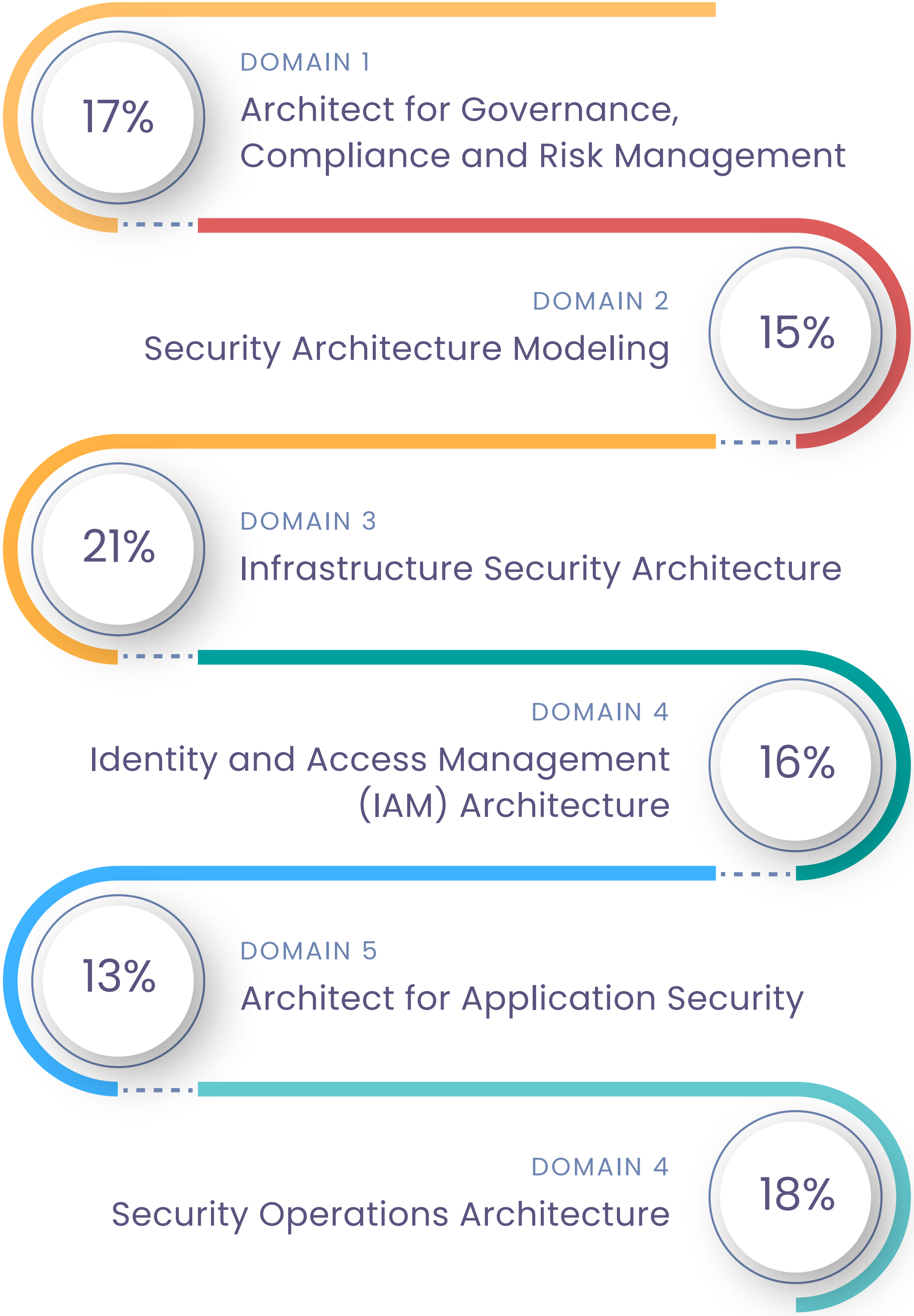
Target Audience

CISSP-ISSAP training helps advancing the technical competencies of:

- System Architects
- Business Analysts
- System and Network Designers
- Chief Security Officers
- Chief Technology Officers

Pre-Requisite

A minimum of 2 years of full-time and cumulative paid work experience in at least one of the six CISSP-ISSAP CBK domains



DOMAIN 1

17%

Architect for Governance, Compliance and Risk Management

DOMAIN 2

15%

Security Architecture Modeling

DOMAIN 3

21%

Infrastructure Security Architecture

DOMAIN 4

16%

Identity and Access Management (IAM) Architecture

DOMAIN 5

13%

Architect for Application Security

DOMAIN 4

18%

Security Operations Architecture

DOMAIN 1

Architect for Governance, Compliance and Risk Management

1.1 Determine legal, regulatory, organizational and industry requirements

- Determine applicable information security standards and guidelines
- Identify third-party and contractual obligations (e.g., supply chain, outsourcing, partners)
- Determine applicable sensitive/personal data standards, guidelines and privacy regulations
- Design for auditability (e.g., determine regulatory, legislative, forensic requirements, segregation, high assurance systems)
- Coordinate with external entities (e.g., law enforcement, public relations, independent assessor)

1.2 Manage Risk

- Identify and classify risks
- Assess risk
- Recommend risk treatment (e.g., mitigate, transfer, accept, avoid)
- Risk monitoring and reporting

DOMAIN 2

Security Architecture Modeling

2.1 Identify security architecture approach

- Types and scope (e.g., enterprise, network, Service-Oriented Architecture (SOA), cloud, Internet of Things (IoT), Industrial Control Systems (ICS)/Supervisory Control and Data Acquisition (SCADA))
- Frameworks (e.g., Sherwood Applied Business Security Architecture (SABSA), Service-Oriented Modeling Framework (SOMF))
- Reference architectures and blueprints
- Security configuration (e.g., baselines, benchmarks, profiles)
- Network configuration (e.g., physical, logical, high availability, segmentation, zones)

2.2 Verify and validate design (e.g., Functional Acceptance Testing (FAT), regression)

- Validate results of threat modeling (e.g., threat vectors, impact, probability)
- Identify gaps and alternative solutions
- Independent Verification and Validation (IV&V) (e.g., tabletop exercises, modeling and simulation, manual review of functions)

DOMAIN 3

Infrastructure Security Architecture

3.1 Develop infrastructure security requirements

- On-premise, cloud-based, hybrid
- Internet of Things (IoT), zero trust

3.2 Design defense-in-depth architecture

- Management networks
- Industrial Control Systems (ICS) security
- Network security
- Operating systems (OS) security
- Database security
- Container security
- Cloud workload security
- Firmware security
- User security awareness considerations

3.3 Secure shared services (e.g., wireless, e-mail, Voice over Internet Protocol (VoIP), Unified Communications (UC), Domain Name System (DNS), Network Time Protocol (NTP))

3.4 Integrate technical security controls

- Design boundary protection (e.g., firewalls, Virtual Private Network (VPN), airgaps, software defined perimeters, wireless, cloud-native)
- Secure device management (e.g., Bring Your Own Device (BYOD), mobile, server, endpoint, cloud instance, storage)

3.5 Design and integrate infrastructure monitoring

- Network visibility (e.g., sensor placement, time reconciliation, span of control, record compatibility)
- Active/Passive collection solutions (e.g., span port, port mirroring, tap, inline, flow logs)
- Security analytics (e.g., Security Information and Event Management (SIEM), log collection, machine learning, User Behavior Analytics (UBA))

3.6 Design infrastructure cryptographic solutions

- Determine cryptographic design considerations and constraints
- Determine cryptographic implementation (e.g., in-transit, in-use, at-rest)
- Plan key management lifecycle (e.g., generation, storage, distribution)

3.7 Design secure network and communication infrastructure (e.g., Virtual Private Network (VPN), Internet Protocol Security (IPsec), Transport Layer Security (TLS))

3.8 Evaluate physical and environmental security requirements

- Map physical security requirements to organizational needs (e.g., perimeter protection and internal zoning, fire suppression)
- Validate physical security controls

DOMAIN 4

Identity and Access Management (IAM) Architecture

4.1 Design identity management and lifecycle

- Establish and verify identity
- Assign identifiers (e.g., to users, services, processes, devices)
- Identity provisioning and de-provisioning
- Define trust relationships (e.g., federated, standalone)
- Define authentication methods (e.g., Multi-Factor Authentication (MFA), risk-based, location-based, knowledge-based, object-based, characteristicsbased)
- Authentication protocols and technologies (e.g., Security Assertion Markup Language (SAML), Remote Authentication Dial-In User Service (RADIUS), Kerberos)

4.2 Design access control management and lifecycle

- Access control concepts and principles (e.g., discretionary/mandatory, segregation/Separation of Duties (SoD), least privilege)
- Access control configurations (e.g., physical, logical, administrative)
- Authorization process and workflow (e.g., governance, issuance, periodic review, revocation)
- Roles, rights, and responsibilities related to system, application, and data access control (e.g., groups, Digital Rights Management (DRM), trust relationships)
- Management of privileged accounts
- Authorization (e.g., Single Sign-On (SSO), rulebased, role-based, attribute- based)

4.3 Design identity and access solutions

- Access control protocols and technologies (e.g., eXtensible Access Control Markup Language (XACML), Lightweight Directory Access Protocol (LDAP))
- Credential management technologies (e.g., password management, certificates, smart cards)
- Centralized Identity and Access Management (IAM) architecture (e.g., cloud-based, on-premise, hybrid)
- Decentralized Identity and Access Management (IAM) architecture (e.g., cloud-based, on-premise, hybrid)
- Privileged Access Management (PAM) implementation (for users with elevated privileges)
- Accounting (e.g., logging, tracking, auditing)

DOMAIN 5

Architect for Application Security

5.1 Integrate Software Development Life Cycle (SDLC) with application security architecture (e.g., Requirements Traceability Matrix (RTM), security architecture documentation, secure coding)

- Assess code review methodology (e.g., dynamic, manual, static)
- Assess the need for application protection (e.g., Web Application Firewall (WAF), anti-malware, secure Application Programming Interface (API), secure Security Assertion Markup Language (SAML))
- Determine encryption requirements (e.g., at-rest, in-transit, in-use)
- Assess the need for secure communications between applications and databases or other endpoints
- Leverage secure code repository

5.2 Determine application security capability requirements and strategy (e.g., open source, Cloud Service Providers (CSP), Software as a Service (SaaS)/Infrastructure as a Service (IaaS)/ Platform as a Service (PaaS) environments)

- Review security of applications (e.g., custom, Commercial Off-the-Shelf (COTS), in-house, cloud)
- Determine application cryptographic solutions (e.g., cryptographic Application Programming Interface (API), Pseudo Random Number Generator (PRNG), key management)
- Evaluate applicability of security controls for system components (e.g., mobile and web client applications; proxy, application, and database services)

5.3 Identify common proactive controls for applications (e.g., Open Web Application Security Project (OWASP))

DOMAIN 6

Security Operations Architecture

6.1 Gather security operations requirements (e.g., legal, compliance, organizational, and business requirements)

6.2 Design information security monitoring (e.g., Security Information and Event Management (SIEM), insider threat, threat intelligence, user behavior analytics, Incident Response (IR) procedures)

- Detection and analysis
- Proactive and automated security monitoring and remediation (e.g., vulnerability management, compliance audit, penetration testing)

6.3 Design Business Continuity (BC) and resiliency solutions

- Incorporate Business Impact Analysis (BIA)
- Determine recovery and survivability strategy
- Identify continuity and availability solutions (e.g., cold, warm, hot, cloud backup)
- Define processing agreement requirements (e.g., provider, reciprocal, mutual, cloud, virtualization)
- Establish Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)
- Design secure contingency communication for operations (e.g., backup communication channels, Out-of-Band (OOB))

6.4 Validate Business Continuity Plan (BCP)/Disaster Recovery Plan (DRP) architecture

6.5 Design Incident Response (IR) management

- Preparation (e.g., communication plan, Incident Response Plan (IRP), training)
- Identification
- Containment
- Eradication
- Recovery
- Review lessons learned