Back to SecurityX

SecurityX Study Notes

Expert-level study guide for CompTIA SecurityX CAS-005

Domain 1: Governance, Risk & Compliance (20%)

Key Topics:

- Security governance frameworks (NIST CSF, ISO 27001/27002, COBIT)
- Enterprise risk management (ERM) and risk tolerance
- Regulatory compliance requirements (GDPR, HIPAA, PCI-DSS, SOX)
- Privacy regulations and data protection frameworks
- Third-party risk management and vendor assessment
- Security policy development and program management
- Legal considerations in cybersecurity
- Business continuity and disaster recovery planning

Risk Management Concepts:

Risk Appetite vs. Risk Tolerance: Risk appetite is the amount of risk an organization is willing to accept. Risk tolerance is the acceptable variance from stated risk appetite. SecurityX candidates must understand how to align security programs with enterprise risk posture.

Qualitative vs. Quantitative Risk: Qualitative risk uses descriptive scales (high/medium/low), while quantitative approaches use ALE (Annual Loss Expectancy) = SLE × ARO. ALE helps justify security investment.

Third-Party Risk: Vendor risk assessments, supply chain security, right-to-audit clauses, and SLA security requirements are all exam-relevant topics at the SecurityX level.

Domain 2: Security Architecture (27%)

Key Topics:

Analytics (

- Enterprise security architecture frameworks (SABSA, TOGAF, Zachman)
- Zero Trust architecture principles and implementation
- Cloud security architecture (multi-cloud, hybrid, SaaS/PaaS/IaaS)
- Identity and access management (IAM) at scale
- Network segmentation, microsegmentation, and SD-WAN
- Secure remote access (SASE, VPN, ZTNA)
- Data security architecture and classification
- Security for IoT, OT/SCADA, and embedded systems

Zero Trust Architecture:

Core Principles: Never trust, always verify. Assume breach. Least privilege access. All resources treated as external. Strong identity verification for every user, device, and workload.

NIST SP 800-207: NIST's Zero Trust Architecture publication defines three approaches: identity-based, network-based, and device-agent/gateway. The logical components include a Policy Engine, Policy Administrator, and Policy Enforcement Point.

SASE (Secure Access Service Edge): Combines SD-WAN capabilities with security services (CASB, SWG, ZTNA, FWaaS) delivered from the cloud. Key for securing distributed workforce environments.

🕮 Domain 3: Security Engineering (31%)

Key Topics:

- Advanced cryptography (ECC, post-quantum, homomorphic encryption)
- PKI design, certificate lifecycle management, and HSMs
- Application security, SSDLC, and secure coding practices
- Infrastructure hardening and configuration management
- Vulnerability management frameworks and remediation
- Supply chain security and software composition analysis
- API security and microservices hardening
- Container and serverless security

Cryptography at Expert Level:

Post-Quantum Cryptography: NIST has standardized PQC algorithms including CRYSTALS-Kyber (key encapsulation) and CRYSTALS-Dilithium (digital signatures). Organizations must plan "crypto-agility" to migrate before quantum computing threatens current algorithms.

HSM (Hardware Security Module): Physical or cloud-based devices that manage cryptographic keys securely. FIPS 140-2/140-3 Level 3+ validation required for high-assurance environments. Key ceremonies are formal processes for root CA key generation.

Supply Chain Security: Software Bill of Materials (SBOM), SLSA framework (Supply chain Levels for Software Artifacts), and dependency scanning are critical engineering controls evaluated in SecurityX.

Domain 4: Security Operations (22%)

Key Topics:

- Threat intelligence platforms and STIX/TAXII
- Advanced incident response and DFIR methodologies
- Threat hunting techniques and hypotheses
- SOAR (Security Orchestration, Automation, and Response)
- Security monitoring and SIEM at enterprise scale
- Digital forensics and chain of custody
- Deception technologies (honeypots, honeynets)
- Vulnerability disclosure and CVE programs

Advanced Security Operations Concepts:

Threat Intelligence Sharing: STIX (Structured Threat Information eXpression) is the language format and TAXII (Trusted Automated eXchange of Intelligence Information) is the transport protocol for sharing threat intelligence. ISACs facilitate sector-specific sharing.

Threat Hunting: Proactive, hypothesis-driven search for advanced threats not detected by automated tools. Uses TTPs from frameworks like MITRE ATT&CK. Hunt teams pivot on indicators, behaviors, and anomalies.

SOAR: Combines security orchestration (playbooks and automation), incident response case management, and threat intelligence feeds. Reduces MTTD (Mean Time to Detect) and MTTR (Mean Time to Respond) through automation.

Exam Simulator
Roadmaps
Study Guides
Blog
AI Corner
Newsletter

Company
About
Contact
FAQ

Legal
Privacy Policy
Terms of Service

Our Products
CollegeDecider
College comparison tool
BoostLogik
SEO & AEO solutions
WanderingHermit
Brakto