



# CompTIA SecurityX Certification Exam Objectives

**EXAM NUMBER: CAS-005**



# About the Exam

The CompTIA SecurityX certification exam will certify the successful candidate has the knowledge and skills required to:

- Architect, engineer, integrate, and implement secure solutions across complex environments to support a resilient enterprise.
- Use automation, monitoring, detection, and incident response to proactively support ongoing security operations in an enterprise environment.
- Apply security practices to cloud, on-premises, and hybrid environments.
- Consider cryptographic technologies and techniques, as well as the impact of emerging trends (e.g., artificial intelligence) on information security.
- Use the appropriate governance, compliance, risk management, and threat modeling strategies throughout the enterprise.

## **EXAM ACCREDITATION**

The CompTIA SecurityX exam is accredited by ANSI to show compliance with the ISO 17024 standard and, as such, undergoes regular reviews and updates to the exam objectives.

## **EXAM DEVELOPMENT**

CompTIA exams result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an IT professional.

## **CompTIA AUTHORIZED MATERIALS USE POLICY**

CompTIA Certifications, LLC is not affiliated with and does not authorize, endorse, or condone utilizing any content provided by unauthorized third-party training sites (aka “brain dumps”). Individuals who utilize such materials in preparation for any CompTIA examination will have their certifications revoked and be suspended from future testing in accordance with the CompTIA Candidate Agreement. In an effort to more clearly communicate CompTIA’s exam policies on use of unauthorized study materials, CompTIA directs all certification candidates to the [CompTIA Certification Exam Policies](#). Please review all CompTIA policies before beginning the study process for any CompTIA exam. Candidates will be required to abide by the [CompTIA Candidate Agreement](#). If a candidate has a question as to whether study materials are considered unauthorized (aka “brain dumps”), they should contact CompTIA at [examsecurity@comptia.org](mailto:examsecurity@comptia.org) to confirm.

## **PLEASE NOTE**

The lists of examples provided in bulleted format are not exhaustive lists. Other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam, although not listed or covered in this objectives document. CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current, and the security of the questions is protected. When necessary, we will publish updated exams based on existing exam objectives. Please know that all related exam preparation materials will still be valid.

## TEST DETAILS

Required exam	CAS-005
Number of questions	Maximum of 90
Types of questions	Multiple-choice, performance-based
Length of test	
Recommended experience	Minimum of 10 years of general, hands-on IT experience that includes at least 5 years of broad, hands-on IT security experience.
Passing Score	Pass/fail only; no scaled score

## EXAM OBJECTIVES (DOMAINS)

The table below lists the domains measured by this examination and the extent to which they are represented.

DOMAIN		PERCENTAGE OF EXAMINATION
1.0	Governance, Risk, and Compliance	20%
2.0	Security Architecture	27%
3.0	Security Engineering	31%
4.0	Security Operations	22%
<b>Total</b>		<b>100%</b>



# 1.0 Governance, Risk, and Compliance

**1.1** Given a set of organizational security requirements, implement the appropriate governance components.

- **Security program documentation**
  - Policies
  - Procedures
  - Standards
  - Guidelines
- **Security program management**
  - Awareness and training
    - Phishing
    - Security
    - Social engineering
    - Privacy
    - Operational security
    - Situational awareness
  - Communication
  - Reporting
  - Management commitment
  - Responsible, accountable, consulted, and informed (RACI) matrix
- **Governance frameworks**
  - Control Objectives for Information and Related Technologies (COBIT)
  - Information Technology Infrastructure Library (ITIL)
- **Change/configuration management**
  - Asset management life cycle
  - Configuration management database (CMDB)
  - Inventory
- **Governance risk and compliance (GRC) tools**
  - Mapping
  - Automation
  - Compliance tracking
  - Documentation
  - Continuous monitoring
- **Data governance in staging environments**
  - Production
  - Development
  - Testing
  - Quality assurance (QA)
  - Data life cycle management

**1.2** Given a set of organizational security requirements, perform risk management activities.

- **Impact analysis**
  - Extreme but plausible scenarios
- **Risk assessment and management**
  - Quantitative vs. qualitative analysis
  - Risk assessment frameworks
  - Appetite/tolerance
  - Risk prioritization
  - Severity impact
  - Remediation
  - Validation
- **Third-party risk management**
  - Supply chain risk
  - Vendor risk
  - Subprocessor risk
- **Availability risk considerations**
  - Business continuity/disaster recovery
    - Testing
  - Backups
    - Connected
    - Disconnected
- **Confidentiality risk considerations**
  - Data leak response
  - Sensitive/privileged data breach
  - Incident response testing
  - Reporting
  - Encryption
- **Integrity risk considerations**
  - Remote journaling
- Hashing
- Interference
- Antitampering
- **Privacy risk considerations**
  - Data subject rights
  - Data sovereignty
  - Biometrics
- **Crisis management**
- **Breach response**



### 1.3 Explain how compliance affects information security strategies.

- **Awareness of industry-specific compliance**
  - Healthcare
  - Financial
  - Government
  - Utilities
- **Industry standards**
  - Payment Card Industry Data Security Standard (PCI DSS)
  - International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27000 series
  - Digital Markets Act (DMA)
- **Security and reporting frameworks**
  - Benchmarks
  - Foundational best practices
  - Security Organization Control Type 2 (SOC 2)
  - National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
  - Center for Internet Security (CIS)
  - Cloud Security Alliance (CSA)
- **Audits vs. assessments vs. certifications**
  - External
  - Internal
- **Privacy regulations**
  - General Data Protection Regulation (GDPR)
  - California Consumer Privacy Act (CCPA)
  - General Data Protection Law (LGPD)
  - Children's Online Privacy Act (COPPA)
- **Awareness of cross-jurisdictional compliance requirements**
  - e-discovery
  - Legal holds
  - Due diligence
  - Due care
  - Export controls
  - Contractual obligations

### 1.4 Given a scenario, perform threat modeling activities.

- **Actor characteristics**
  - Motivation
    - Financial
    - Geopolitical
    - Activism
    - Notoriety
    - Espionage
  - Resources
    - Time
    - Money
  - Capabilities
    - Supply chain access
    - Vulnerability creation
    - Knowledge
    - Exploit creation
- **Attack patterns**
- **Frameworks**
  - MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)
  - Common Attack Pattern Enumeration and Classification (CAPEC)
- Cyber Kill Chain
- Diamond Model of Intrusion Analysis
- Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE)
- Open Web Application Security Project (OWASP)
- **Attack surface determination**
  - Architecture reviews
  - Data flows
  - Trust boundaries
  - Code reviews
  - User factors
  - Organizational change
    - Mergers
    - Acquisitions
    - Divestitures
    - Staffing changes
  - Enumeration/discovery
    - Internally and externally facing assets
    - Third-party connections
    - Unsanctioned assets/accounts
    - Cloud services discovery
    - Public digital presence
- **Methods**
  - Abuse cases
  - Antipatterns
  - Attack trees/graphs
- **Modeling applicability of threats to the organization/environment**
  - With an existing system in place
    - Selection of appropriate controls
  - Without an existing system in place



## 1.5 Summarize the information security challenges associated with artificial intelligence (AI) adoption.

- **Legal and privacy implications**
  - Potential misuse
  - Explainable vs. non-explainable models
  - Organizational policies on the use of AI
  - Ethical governance
- **Threats to the model**
  - Prompt injection
  - Unsecured output handling
  - Training data poisoning
  - Model denial of service (DoS)
  - Supply chain vulnerabilities
  - Model theft
  - Model inversion
- **AI-enabled attacks**
  - Unsecure plugin design
  - Deep fake
    - Digital media
    - Interactivity
  - AI pipeline injections
  - Social engineering
  - Automated exploit generation
- **Risks of AI usage**
  - Overreliance
  - Sensitive information disclosure
    - To the model
    - From the model
  - Excessive agency of the AI
- **AI-enabled assistants/digital workers**
  - Access/permissions
  - Guardrails
  - Data loss prevention (DLP)
  - Disclosure of AI usage



## 2.0 Security Architecture

### 2.1 Given a scenario, analyze requirements to design resilient systems.

- **Component placement and configuration**
  - Firewall
  - Intrusion prevention system (IPS)
  - Intrusion detection system (IDS)
  - Vulnerability scanner
  - Virtual private network (VPN)
  - Network access control (NAC)
  - Web application firewall (WAF)
  - Proxy
- Reverse proxy
- Application programming interface (API) gateway
- Taps
- Collectors
- Content delivery network (CDN)
- **Availability and integrity design considerations**
  - Load balancing
  - Recoverability
  - Interoperability
  - Geographical considerations
  - Vertical vs. horizontal scaling
  - Persistence vs. non-persistence

### 2.2 Given a scenario, implement security in the early stages of the systems life cycle and throughout subsequent stages.

- **Security requirements definition**
  - Functional requirements
  - Non-functional requirements
  - Security vs. usability trade-off
- **Software assurance**
  - Static application security testing (SAST)
  - Dynamic application security testing (DAST)
  - Interactive application security testing (IAST)
  - Runtime application self-protection (RASP)
- Vulnerability analysis
- Software composition analysis (SCA)
- Software bill of materials (SBOM)
- Formal methods
- **Continuous integration/continuous deployment (CI/CD)**
  - Coding standards and linting
  - Branch protection
  - Continuous improvement
  - Testing activities
    - Canary
    - Regression
    - Integration
- Automated test and retest
- Unit
- **Supply chain risk management**
  - Software
  - Hardware
- **Hardware assurance**
  - Certification and validation process
- **End-of-life (EOL) considerations**

### 2.3 Given a scenario, integrate appropriate controls in the design of a secure architecture.

- **Attack surface management and reduction**
  - Vulnerability management
  - Hardening
  - Defense-in-depth
  - Legacy components within an architecture
- **Detection and threat-hunting enablers**
  - Centralized logging
  - Continuous monitoring
  - Alerting
  - Sensor placement
- **Information and data security design**
  - Classification models
  - Data labeling
  - Tagging strategies
- **DLP**
  - At rest
  - In transit
  - Data discovery
- **Hybrid infrastructures**
- **Third-party integrations**
- **Control effectiveness**
  - Assessments
  - Scanning
  - Metrics



## 2.4 Given a scenario, apply security concepts to the design of access, authentication, and authorization systems.

- Provisioning/deprovisioning
  - Credential issuance
  - Self-provisioning
- Federation
- Single sign-on (SSO)
- Conditional access
- Identity provider
- Service provider
- Attestations
- Policy decision and enforcement points
- Access control models
  - Role-based access control
  - Rule-based access control
  - Attribute-based access control (ABAC)
  - Mandatory access control (MAC)
  - Discretionary access control (DAC)
- Logging and auditing
- Public key infrastructure (PKI) architecture
  - Certificate extensions
- Certificate types
- Online Certificate Status Protocol (OCSP) stapling
- Certificate authority/registration authority (CA/RA)
- Templates
- Deployment/integration approach
- Access control systems
  - Physical
  - Logical

## 2.5 Given a scenario, securely implement cloud capabilities in an enterprise environment.

- Cloud access security broker (CASB)
  - API-based
  - Proxy-based
- Shadow IT detection
- Shared responsibility model
- CI/CD pipeline
- Terraform
- Ansible
- Package monitoring
- Container security
- Container orchestration
- Serverless
- Workloads
- Functions
- Resources
- API security
  - Authorization
  - Logging
  - Rate limiting
- Cloud vs. customer-managed
  - Encryption keys
  - Licenses
- Cloud data security considerations
  - Data exposure
- Data leakage
- Data remanence
- Unsecured storage resources
- Cloud control strategies
  - Proactive
  - Detective
  - Preventative
- Customer-to-cloud connectivity
- Cloud service integration
- Cloud service adoption

## 2.6 Given a scenario, integrate Zero Trust concepts into system architecture design.

- Continuous authorization
- Context-based reauthentication
- Network architecture
  - Segmentation
  - Microsegmentation
  - VPN
  - Always-on VPN
- API integration and validation
- Asset identification, management, and attestation
- Security boundaries
  - Data perimeters
  - Secure zone
  - System components
- Deperimeterization
  - Secure access service edge (SASE)
  - Software-defined wide area network (SD-WAN)
  - Software-defined networking
- Defining subject-object relationships





## 3.0 Security Engineering

**3.1** Given a scenario, troubleshoot common issues with identity and access management (IAM) components in an enterprise environment.

- **Subject access control**
  - User
  - Process
  - Device
  - Service
- **Biometrics**
- **Secrets management**
  - Tokens
  - Certificates
  - Passwords
  - Keys
  - Rotation
  - Deletion
- **Conditional access**
  - User-to-device binding
  - Geographic location
  - Time-based
  - Configuration
- **Attestation**
- **Cloud IAM access and trust policies**
- **Logging and monitoring**
- **Privilege identity management**
- **Authentication and authorization**
  - Security Assertions Markup Language (SAML)
  - OpenID
- Multifactor authentication (MFA)
- SSO
- Kerberos
- Simultaneous authentication of equals (SAE)
- Privileged access management (PAM)
- Open Authorization (OAuth)
- Extensible Authentication Protocol (EAP)
- Identity proofing
- Institute for Electrical and Electronics Engineers (IEEE) 802.1X
- Federation

**3.2** Given a scenario, analyze requirements to enhance the security of endpoints and servers.

- Application control
- Endpoint detection response (EDR)
- Event logging and monitoring
- Endpoint privilege management
- Attack surface monitoring and reduction
- Host-based intrusion protection system/ host-based detection system (HIPS/ HIDS)
- Anti-malware
- SELinux
- Host-based firewall
- Browser isolation
- Configuration management
- Mobile device management (MDM) technologies
- Threat-actor tactics, techniques, and procedures (TTPs)
  - Injections
  - Privilege escalation
  - Credential dumping
  - Unauthorized execution
  - Lateral movement
  - Defensive evasion



### 3.3 Given a scenario, troubleshoot complex network infrastructure security issues.

- **Network misconfigurations**
  - Configuration drift
  - Routing errors
  - Switching errors
  - Unsecure routing
  - VPN/tunnel errors
- **IPS/IDS issues**
  - Rule misconfigurations
  - Lack of rules
  - False positives/false negatives
  - Placement
- **Observability**
- **Domain Name System (DNS) security**
  - Domain Name System Security Extensions (DNSSEC)
  - DNS poisoning
  - Sinkholing
  - Zone transfers
- **Email security**
  - Domain Keys Identified Mail (DKIM)
  - Sender Policy Framework (SPF)
  - Domain-based Message Authentication Reporting & Conformance (DMARC)
- Secure/Multipurpose Internet Mail Extension (S/MIME)
- **Transport Layer Security (TLS) errors**
- **Cipher mismatch**
- **PKI issues**
- **Issues with cryptographic implementations**
- **DoS/distributed denial of service (DDoS)**
- **Resource exhaustion**
- **Network access control list (ACL) issues**

### 3.4 Given a scenario, implement hardware security technologies and techniques.

- **Roots of trust**
  - Trusted Platform Module (TPM)
  - Hardware Security Module (HSM)
  - Virtual Trusted Platform Module (vTPM)
- **Security coprocessors**
  - Central processing unit (CPU) security extensions
  - Secure enclave
- **Virtual hardware**
- **Host-based encryption**
- **Self-encrypting drive (SED)**
- **Secure boot**
- **Measured boot**
- **Self-healing hardware**
- **Tamper detection and countermeasures**
- **Threat-actor TTPs**
  - Firmware tampering
  - Shimming
  - Universal Serial Bus (USB)-based attacks
- Basic input/output system/Unified Extensible Firmware Interface (BIOS/UEFI)
- Memory
- Electromagnetic interference (EMI)
- Electromagnetic pulse (EMP)

### 3.5 Given a set of requirements, secure specialized and legacy systems against threats.

- **Operational technology (OT)**
  - Supervisory control and data acquisition (SCADA)
  - Industrial control system (ICS)
  - Heating ventilation and air conditioning (HVAC)/environmental
- **Internet of Things (IoT)**
- **System-on-chip (SoC)**
- **Embedded systems**
- **Wireless technologies/radio frequency (RF)**
- **Security and privacy considerations**
  - Segmentation
  - Monitoring
  - Aggregation
  - Hardening
  - Data analytics
  - Environmental
  - Regulatory
  - Safety
- **Industry-specific challenges**
  - Utilities
- Transportation
- Healthcare
- Manufacturing
- Financial
- Government/defense
- **Characteristics of specialized/legacy systems**
  - Unsecurable
  - Obsolete
  - Unsupported
  - Highly constrained



### 3.6 Given a scenario, use automation to secure the enterprise.

- **Scripting**
  - PowerShell
  - Bash
  - Python
- **Cron/scheduled tasks**
- **Event-based triggers**
- **Infrastructure as code (IaC)**
- **Configuration files**
  - Yet Another Markup Language (YAML)
  - Extensible Markup Language (XML)
  - JavaScript Object Notation (JSON)
  - Tom's Obvious, Minimal Language (TOML)
- **Cloud APIs/software development kits (SDKs)**
  - Web hooks
- **Generative AI**
  - Code assist
  - Documentation
- **Containerization**
- **Automated patching**
- **Auto-containment**
- **Security orchestration, automation, and response (SOAR)**
  - Runbooks
  - Playbooks
- **Vulnerability scanning and reporting**
- **Security Content Automation Protocol (SCAP)**
  - Open Vulnerability Assessment Language (OVAL)
- Extensible Configuration Checklist Description Format (XCCDF)
- Common Platform Enumeration (CPE)
- Common vulnerabilities and exposures (CVE)
- Common Vulnerability Scoring System (CVSS)
- **Workflow automation**

### 3.7 Explain the importance of advanced cryptographic concepts.

- **Post-quantum cryptography (PQC)**
  - Post-quantum vs. Diffie-Hellman and elliptic curve cryptography (ECC)
  - Resistance to quantum computing decryption attack
  - Emerging implementations
- **Key stretching**
- **Key splitting**
- **Homomorphic encryption**
- **Forward secrecy**
- **Hardware acceleration**
- **Envelope encryption**
- **Performance vs. security**
- **Secure multiparty computation**
- **Authenticated encryption with associated data (AEAD)**
- **Mutual authentication**

### 3.8 Given a scenario, apply the appropriate cryptographic use case and/or technique.

- **Use cases**
  - Data at rest
  - Data in transit
    - Encrypted tunnels
  - Data in use/processing
  - Secure email
  - Immutable databases/blockchain
  - Non-repudiation
  - Privacy applications
  - Legal/regulatory considerations
  - Resource considerations
  - Data sanitization
  - Data anonymization
- Certificate-based authentication
- Passwordless authentication
- Software provenance
- Software/code integrity
- Centralized vs. decentralized key management
- **Techniques**
  - Tokenization
  - Code signing
  - Cryptographic erase/obfuscation
  - Digital signatures
  - Obfuscation
  - Serialization
- Hashing
- One-time pad
- Symmetric cryptography
- Asymmetric cryptography
- Lightweight cryptography



## 4.0 Security Operations

### 4.1 Given a scenario, analyze data to enable monitoring and response activities.

- **Security information event management (SIEM)**
  - Event parsing
  - Event duplication
  - Non-reporting devices
  - Retention
  - Event false positives/false negatives
- **Aggregate data analysis**
  - Correlation
  - Audit log reduction
  - Prioritization
  - Trends
- **Behavior baselines and analytics**
  - Network
  - Systems
  - Users
  - Applications/services
- **Incorporating diverse data sources**
  - Third-party reports and logs
  - Threat intelligence feeds
  - Vulnerability scans
  - CVE details
  - Bounty programs
  - DLP data
  - Endpoint logs
  - Infrastructure device logs
  - Application logs
  - Cloud security posture management (CSPM) data
- **Alerting**
  - False positives/false negatives
  - Alert failures
- Prioritization factors
  - Criticality
  - Impact
  - Asset type
  - Residual risk
  - Data classification
- Malware
- Vulnerabilities
- **Reporting and metrics**
  - Visualization
  - Dashboards

### 4.2 Given a scenario, analyze vulnerabilities and attacks, and recommend solutions to reduce the attack surface.

- **Vulnerabilities and attacks**
  - Injection
  - Cross-site scripting (XSS)
  - Unsafe memory utilization
  - Race conditions
  - Cross-site request forgery
  - Server-side request forgery
  - Unsecure configuration
  - Embedded secrets
  - Outdated/unpatched software and libraries
  - End-of-life software
  - Poisoning
  - Directory service misconfiguration
  - Overflows
  - Deprecated functions
  - Vulnerable third parties
- Time of check, time of use (TOCTOU)
- Deserialization
- Weak ciphers
- Confused deputy
- Implants
- **Mitigations**
  - Input validation
  - Output encoding
  - Safe functions
    - Atomic functions
    - Memory-safe functions
    - Thread-safe functions
  - Security design patterns
  - Updating/patching
    - Operating system (OS)
    - Software
    - Hypervisor
- Firmware
- System images
- Least privilege
- Fail secure/fail safe
- Secrets management
  - Key rotation
- Least function/functionality
- Defense-in-depth
- Dependency management
- Code signing
- Encryption
- Indexing
- Allow listing



### 4.3 Given a scenario, apply threat-hunting and threat intelligence concepts.

- **Internal intelligence sources**
  - Adversary emulation engagements
  - Internal reconnaissance
  - Hypothesis-based searches
  - Honeypots
  - Honeynets
  - User behavior analytics (UBA)
- **External intelligence sources**
  - Open-source intelligence (OSINT)
  - Dark web monitoring
- Information sharing and analysis centers (ISACs)
- Reliability factors
- **Counterintelligence and operational security**
- **Threat intelligence platforms (TIPs)**
  - Third-party vendors
- **Indicator of compromise (IoC) sharing**
  - Structured Threat Information eXchange (STIX)
- Trusted automated exchange of indicator information (TAXII)
- **Rule-based languages**
  - Sigma
  - Yet Another Recursive Acronym (YARA)
  - Rita
  - Snort
- **Indicators of attack**
  - TTPs

### 4.4 Given a scenario, analyze data and artifacts in support of incident response activities.

- **Malware analysis**
  - Detonation
  - IoC extractions
  - Sandboxing
  - Code stylometry
    - Variant matching
    - Code similarity
    - Malware attribution
- **Reverse engineering**
  - Disassembly and decompilation
  - Binary
  - Byte code
- **Volatile/non-volatile storage analysis**
- **Network analysis**
- **Host analysis**
- **Metadata analysis**
  - Email header
  - Images
  - Audio/video
  - Files/filesystem
- **Hardware analysis**
  - Joint test action group (JTAG)
- **Data recovery and extraction**
- **Threat response**
- **Preparedness exercises**
- **Timeline reconstruction**
- **Root cause analysis**
- **Cloud workload protection platform (CWPP)**
- **Insider threat**

# CompTIA SecurityX CAS-005 Acronym List

The following is a list of acronyms that appears on the CompTIA SecurityX CAS-005 exam. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as part of a comprehensive exam preparation program.

<b>Acronym</b>	<b>Spelled Out</b>	<b>Acronym</b>	<b>Spelled Out</b>
ABAC	Attribute-based Access Control	D3FEND	Detection, Denial, and Disruption Framework Empowering Network Defense
ACL	Access Control List	DAC	Discretionary Access Control
AEAD	Authenticated Encryption with Associated Data	DAST	Dynamic Application Security Testing
AI	Artificial Intelligence	DDoS	Distributed Denial of Service
API	Application Programming Interface	DHCP	Dynamic Host Configuration Protocol
APT	Advanced Persistent Threat	DKIM	Domain Keys Identified Mail
AQL	Ariel Query Language	DLP	Data Loss Prevention
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge	DMA	Digital Markets Act
BEAST	Browser Exploit against SSL/TLS	DMARC	Domain-based Message Authentication Reporting and Conformance
BIOS	Basic Input/Output System	DNS	Domain Name System
BYOD	Bring Your Own Device	DNSSEC	Domain Name System Security Extensions
C2	Command and Control	DORA	Digital Operational Resilience Act
CAPEC	Common Attack Pattern Enumeration and Classification	DoS	Denial of Service
CA/RA	Certificate Authority/Registration Authority	EAP	Extensible Authentication Protocol
CASB	Cloud Access Security Broker	ECC	Elliptic Curve Cryptography
CBC	Cipher Block Chaining	EDR	Endpoint Detection Response
CCPA	California Consumer Privacy Act	EMI	Electromagnetic Interference
CDN	Content Delivery Network	EMP	Electromagnetic Pulse
CI/CD	Continuous Integration/Continuous Deployment	EOL	End-of-life
CIS	Center for Internet Security	FAST	Flexible Authentication via Secure Tunneling
CMDB	Configuration Database Management	FDE	Full Disk Encryption
CNAME	Canonical Name	FIDO	Fast Identity Online
COBIT	Control Objectives for Information and Related Technologies	GDPR	General Data Protection Regulation
COPPA	Children's Online Privacy Act	GPO	Group Policy Objects
COSO	Committee of Sponsoring Organizations of the Treadway Commission	GRC	Governance, Risk, and Compliance
CPE	Common Platform Enumeration	HIPS/HIDS	Host-based Intrusion Protection System/Host-based Detection System
CPU	Central Processing Unit	HKLM	Hkey_Local_Machine
CRM	Customer Relationship Manager	HSM	Hardware Security Module
CSA	Cloud Security Alliance	HSTS	HTTP Strict Transport Security
CSPM	Cloud Security Posture Management	HVAC	Heating Ventilation and Air Conditioning
CSRF	Cross-site Request Forgery	IaC	Infrastructure as Code
CVE	Common Vulnerabilities and Exposures	IAM	Identity and Access Management
CVSS	Common Vulnerability Scoring System	IAST	Interactive Application Security Testing
CWPP	Cloud Workload Protection Platform	ICS	Industrial Control System
		IDS	Intrusion Detection System

<b>Acronym</b>	<b>Spelled Out</b>	<b>Acronym</b>	<b>Spelled Out</b>
IDE	Integrated Development Environment	SASE	Secure Access Service Edge
IEEE	Institute for Electrical and Electronics Engineers	SAST	Static Application Security Testing
IIS	Internet Information Services	SBoM	Software Bill of Materials
IKE	Internet Key Exchange	SCA	Software Composition Analysis
IoC	Indicator of Compromise	SCADA	Supervisory Control and Data Acquisition
IoT	Internet of Things	SCAP	Security Content Automation Protocol
IPS	Intrusion Prevention System	SCCM	System Center Configuration Management
ISAC	Information Sharing and Analysis Centers	SCHANNEL	Secure Channel
ISO/IEC	International Organization for Standardization/ International Electrotechnical Commission	SDK	Software Development Kit
ISP	Internet Service Provider	SDLC	Software Development Life Cycle
ITIL	Information Technology Infrastructure Library	SDN	Software-defined Network
JSON	JavaScript Object Notation	SDR	Software-defined Radio
JTAG	Joint Test Action Group	SD-WAN	Software-defined Wide Area Network
LDAP	Lightweight Directory Access Protocol	SED	Self-encrypting Drive
LGPD	General Data Protection Law	SIEM	Security Information Event Management
MAC	Mandatory Access Control	S/MIME	Secure/Multipurpose Internet Mail Extensions
MDM	Mobile Device Management	SOA	Service-oriented Architecture
MFA	Multifactor Authentication	SOAR	Security Orchestration, Automation, and Response
MIME	Multipurpose Internet Mail Extensions	SoC	System-on-Chip
MX	Mail Exchange	SPF	Sender Policy Framework
NAC	Network Access Control	SSD	Solid-state Drive
NIDS	Network-based Intrusion Detection System	SSH	Secure Shell
NIPS	Network-based Intrusion Prevention System	SSL	Secure Sockets Layer
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework	SSO	Single Sign-on
OAuth	Open Authorization	STIX	Structured Threat Information eXchange
OCSP	Online Certificate Status Protocol	STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege
OEM	Original Equipment Manufacturer	TAXII	Trusted Automated Exchange of Indicator Information
OS	Operating System	TIP	Threat Intelligence Platforms
OSINT	Open-source Intelligence	TLS	Transport Layer Security
OT	Operational Technology	TOCTOU	Time of Check, Time of Use
OTP	One-time Password	TOML	Tom's Obvious, Minimal Language
OVAL	Open Vulnerability Assessment Language	TPM	Trusted Platform Module
OWASP	Open Web Application Security Project	TTPs	Tactics, Techniques, and Procedures
PaaS	Platform as a Service	VPN	Virtual Private Network
PAM	Privileged Access Management	vTPM	Virtual Trusted Platform Module
PCI DSS	Payment Card Industry Data Security Standard	UBA	User Behavior Analytics
PEAP	Protected Extensible Authentication Protocol	UDP	User Datagram Protocol
PII	Personally Identifiable Information	UEBA	User & Entity Behavior Analytics
PKI	Public Key Infrastructure	UEFI	Unified Extensible Firmware Interface
PQC	Post-quantum Cryptography	USB	Universal Serial Bus
PTR	Pointer Record	VLAN	Virtual Local Area Network
QA	Quality Assurance	VPN	Virtual Private Network
RACI	Responsible, Accountable, Consulted, and Informed	WAF	Web Application Firewall
RADIUS	Remote Authentication Dial-in User Service	WIPS	Wireless Intrusion Prevention System
RASP	Runtime Application Self-protection	WLAN	Wireless Local Area Network
RAT	Remote Access Trojan	XCCDF	Extensible Configuration Checklist Description Format
RCE	Remote Code Execution	XDR	Extended Detection and Response
RDP	Remote Desktop Protocol	XML	Extensible Markup Language
RF	Radio Frequency	XSS	Cross-site Scripting
RSA	Rivest-Shamir-Aldeman Encryption Algorithm	YAML	Yet Another Markup Language
SAE	Simultaneous Authentication of Equals	YARA	Yet Another Recursive Acronym
SAML	Security Assertions Markup Language		
SAN	Storage Area Network		

# CompTIA SecurityX Proposed Hardware and Software List

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the SecurityX CAS-005 certification exam. This list may also be helpful for training companies that wish to create a lab component for their training offering. The bulleted lists below each topic are sample lists and are not exhaustive.

## Equipment

- Computers with a TPM
- Basic server hardware (email server/Active Directory server, trusted OS)
- Tokens
- Mobile devices (Android and iOS)
- Switches (managed switch)
- Gateway/router (wired/wireless)
- Firewall
- Proxy server
- Load balancer
- Access points
- Biometric devices
- Arduino/Raspberry Pi
- Software-defined radio (SDR)

## Other

- Sample logs
- Sample network traffic (packet capture)
- Sample organizational structure
- Sample network documentation
- Internet connection
- Cloud services
- Online productivity suite
- Diagramming software

## Software

- Virtualized appliances (firewall, IPS, SIEM solution)
- Windows
- Linux distributions
- VMware Workstation Player
- Vulnerability assessment tools
- Secure Shell (SSH) and Telnet utilities
- Threat modeling tool
- IPS/IDS
- HIPS
- Wireless intrusion prevention system (WIPS)
- Forensic tools
- Certificate authority
- Kali and all Kali toolsets
- GNS and associated firmware
- Log analysis tools
- API SDKs
- Python 3+
- Security Onion tools
- Metasploitable
- Large language model platform
- IDE
- Cryptographic library
- Code versioning, integration, and deployment platform