EDUSUM

#1 Online Certification Guide

COMPTIA CAS-005

CompTIA SecurityX Certification Questions & Answers

Exam Summary – Syllabus –Questions

CAS-005

CompTIA SecurityX

90 Questions Exam – Pass/ Fail Cut Score – Duration of 165 minutes

Table of Contents:

Know Your CAS-005 Certification Well:

The CAS-005 is best suitable for candidates who want to gain knowledge in the CompTIA Cybersecurity. Before you start your CAS-005 preparation you may struggle to get all the crucial SecurityX materials like CAS-005 syllabus, sample questions, study guide.

But don't worry the CAS-005 PDF is here to help you prepare in a stress-free manner.
The PDF is a combination of all your queries like-

- What is in the CAS-005 syllabus?
- How many questions are there in the CAS-005 exam?
- Which Practice test would help me to pass the CAS-005 exam at the first attempt?

Passing the CAS-005 exam makes you CompTIA SecurityX. Having the SecurityX certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

CompTIA CAS-005 SecurityX Certification Details:

Exam Name	CompTIA SecurityX
Exam Code	CAS-005
Exam Price	$509 (USD)
Duration	165 mins
Number of Questions	90
Passing Score	Pass/Fail
Schedule Exam	Pearson VUE
Sample Questions	CompTIA SecurityX Sample Questions
Practice Exam	**CompTIA CAS-005 Certification Practice Exam**

CAS-005 Syllabus:

Topic	**Details**
Governance, Risk, and Compliance - 20%	
Given a set of organizational security requirements, implement the appropriate governance components.	- Security program documentation • Policies • Procedures • Standards • Guidelines

Topic	Details
	- 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
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

Topic	Details
	• 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
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 • System and Organization Controls 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

Topic	Details
	• e-discovery • Legal holds • Due diligence • Due care • Export controls • Contractual obligations
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

Topic	Details
	- 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
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 • Insecure output handling • Training data poisoning • Model denial of service (DoS) • Supply chain vulnerabilities • Model theft • Model inversion - AI-enabled attacks • Insecure plug-in 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
Security Architecture - 27%	
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)

Topic	Details
	• 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
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
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

Topic	Details
	• 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
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
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

Topic	Details
	- 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 • Insecure storage resources - Cloud control strategies • Proactive • Detective • Preventative - Customer-to-cloud connectivity - Cloud service integration - Cloud service adoption
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
Security Engineering - 31%	

Topic	Details
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
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

Topic	Details
	- Mobile device management (MDM) technologies - Threat-actor tactics, techniques, and procedures (TTPs) • Injections • Privilege escalation • Credential dumping • Unauthorized execution • Lateral movement • Defensive evasion
Given a scenario, troubleshoot complex network infrastructure security issues.	- Network misconfigurations • Configuration drift • Routing errors • Switching errors • Insecure 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
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

Topic	Details
	- 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)
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 • Unable to secure • Obsolete • Unsupported • Highly constrained
Given a scenario, use automation to secure the enterprise.	- Scripting • PowerShell • Bash • Python - Cron/scheduled tasks - Event-based triggers

Topic	Details
	- 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
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
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

Topic	Details
	• 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
Security Operations - 22%	
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

Topic	Details
	• 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
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 • Insecure 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

Topic	Details
	- 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
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
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

Topic	Details
	• 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 CAS-005 Sample Questions:

Question: 1

After an increase in adversarial activity, a company wants to implement security measures to mitigate the risk of a threat actor using compromised accounts to mask unauthorized activity. Which of the following is the best way to mitigate the issue?

a) Web application firewall
b) Threat intelligence platforms
c) Reverse engineering
d) User and entity behavior analytics

Answer: d

Question: 2

Which of the following AI concerns is most adequately addressed by input sanitation?

a) Model inversion
b) Prompt Injection
c) Data poisoning
d) Non-explainable model

Answer: b

Question: 3

A company runs a DAST scan on a web application. The tool outputs the following recommendations:

• Use Cookie prefixes.

• Content Security Policy - SameSite=strict is not set.

Which of the following vulnerabilities has the tool identified?

a) RCE
b) XSS
c) CSRF
d) TOCTOU

Answer: c

Question: 4

Which of the following best explains the importance of determining organization risk appetite when operating with a constrained budget?

a) Risk appetite directly impacts acceptance of high-impact low-likelihood events.
b) Organizational risk appetite varies from organization to organization
c) Budgetary pressure drives risk mitigation planning in all companies
d) Risk appetite directly influences which breaches are disclosed publicly

Answer: a

Question: 5

An organization receives OSINT reports about an increase in ransomware targeting fileshares at peer companies. The organization wants to deploy hardening policies to its servers and workstations in order to contain potential ransomware. Which of the following should an engineer do to best achieve this goal?

a) Enable biometric authentication mechanisms on user workstations and block port 53 traffic.
b) Allow only interactive log-in for users on workstations and restrict port 445 traffic to fileshares.
c) Instruct users to use a password manager when generating new credentials and secure port 443 traffic.
d) Give users permission to rotate administrator passwords and deny port 80 traffic.

Answer: b

Question: 6

Which of the following best describes the challenges associated with widespread adoption of homomorphic encryption techniques?

a) Incomplete mathematical primitives
b) No use cases to drive adoption
c) Quantum computers not yet capable
d) insufficient coprocessor support

Answer: d

Question: 7

A compliance officer is reviewing the data sovereignty laws in several countries where the organization has no presence. Which of the following is the most likely reason for reviewing these laws?

a) The organization is performing due diligence of potential tax issues.
b) The organization has been subject to legal proceedings in countries where it has a presence.
c) The organization is concerned with new regulatory enforcement in other countries.
d) The organization has suffered brand reputation damage from incorrect media coverage.

Answer: c

Question: 8

An organization's load balancers have reached EOL and are scheduled to be replaced. The organization identified a new, critical vulnerability that affects an unused function of the load balancers. Which of the following are the best ways to address the risk to the organization? (Choose two.)

a) Disable the vulnerable service.
b) Request a risk acceptance for the vulnerability indefinitely.
c) Exclude the devices from vulnerability scans.
d) Immediately decommission the hardware.
e) Do not allow any network traffic to or from the hardware.
f) Request a risk acceptance for the vulnerability for 90 days.

Answer: a, f

Question: 9

A company detects suspicious activity associated with external connections. Security detection tools are unable to categorize this activity. Which of the following is the best solution to help the company overcome this challenge?

a) Implement an Interactive honeypot
b) Map network traffic to known loCs.
c) Monitor the dark web
d) implement UEBA

Answer: d

Question: 10

Which of the following best describes the advantage of homomorphic encryption when compared to other encryption methodologies?

a) The need for a pre-shared key is removed.
b) Resource utilization is lower.
c) Support for field-specific tokenization is added.
d) Data integrity is protected by advanced hashing routines.

Answer: a

Study Guide to Crack CompTIA SecurityX CAS-005 Exam:

- Getting details of the CAS-005 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the CAS-005 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the CompTIA provided training for CAS-005 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the CAS-005 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.

- Practicing on CAS-005 practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for CAS-005 Certification

Make EduSum.com your best friend during your CompTIA SecurityX exam preparation. We provide authentic practice tests for the CAS-005 exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual CAS-005 exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the CAS-005 exam.

Start Online practice of CAS-005 Exam by visiting URL
https://www.edusum.com/comptia/cas-005-comptia-securityx