EDUSUM

#1 Online Certification Guide

# CAS-003

## CASP

A Success Guide to Prepare-
CompTIA Advanced Security Practitioner

edusum.com

# Table of Contents

# Introduction to CAS-003 Exam on CompTIA Advanced Security Practitioner

Use this quick start guide to collect all the information about CompTIA CASP (CAS-003) Certification exam. This study guide provides a list of objectives and resources that will help you prepare for items on the CAS-003 CompTIA Advanced Security Practitioner exam. The Sample Questions will help you identify the type and difficulty level of the questions and the Practice Exams will make you familiar with the format and environment of an exam. You should refer this guide carefully before attempting your actual CompTIA CASP certification exam.

The CompTIA CASP certification is mainly targeted to those candidates who want to build their career in IT Security domain. The CompTIA Advanced Security Practitioner (CASP) exam verifies that the candidate possesses the fundamental knowledge and proven skills in the area of CompTIA CASP.

## CompTIA CAS-003 Certification Details:

| | |
|---|---|
| Exam Name | CompTIA Advanced Security Practitioner (CASP) |
| Exam Code | CAS-003 |
| Exam Price | $439 (USD) |
| Duration | 165 mins |
| Number of Questions | 90 |
| Passing Score | Pass / Fail |
| Schedule Exam | Pearson VUE |
| Sample Questions | CompTIA CASP Sample Questions |
| Practice Exam | **CompTIA CAS-003 Certification Practice Exam** |

# CompTIA CAS-003 Exam Syllabus:

| Topic | Details |
|---|---|
| **Risk Management 19%** | |
| Summarize business and industry influences and associated security risks. | 1. Risk management of new products, new technologies and user behaviors<br>2. New or changing business models/strategies<br>1. Partnerships<br>2. Outsourcing<br>3. Cloud<br>4. Acquisition/merger – divestiture/demerger<br>Data ownership<br>Data reclassification<br>3. Security concerns of integrating diverse industries<br>1. Rules<br>2. Policies<br>3. Regulations<br>Export controls<br>Legal requirements<br>4. Geography<br>Data sovereignty<br>Jurisdictions<br>4. Internal and external influences<br>1. Competitors<br>2. Auditors/audit findings<br>3. Regulatory entities<br>4. Internal and external client requirements<br>5. Top-level management<br>5. Impact of de-perimeterization (e.g., constantly changing network boundary)<br>1. Telecommuting<br>2. Cloud<br>3. Mobile<br>4. BYOD<br>5. Outsourcing<br>6. Ensuring third-party providers have requisite levels of information security |
| | 1. Policy and process life cycle management<br>1. New business |

| Topic | Details |
|---|---|
| Compare and contrast security, privacy policies and procedures based on organizational requirements. | 2. New technologies<br>3. Environmental changes<br>4. Regulatory requirements<br>5. Emerging risks<br><br>2. Support legal compliance and advocacy by partnering with human resources, legal, management and other entities<br>3. Understand common business documents to support security<br><br>1. Risk assessment (RA)<br>2. Business impact analysis (BIA)<br>3. Interoperability agreement (IA)<br>4. Interconnection security agreement (ISA)<br>5. Memorandum of understanding (MOU)<br>6. Service-level agreement (SLA)<br>7. Operating-level agreement (OLA)<br>8. Non-disclosure agreement (NDA)<br>9. Business partnership agreement (BPA)<br>10. Master service agreement (MSA)<br><br>4. Research security requirements for contracts<br><br>1. Request for proposal (RFP)<br>2. Request for quote (RFQ)<br>3. Request for information (RFI)<br><br>5. Understand general privacy principles for sensitive information<br>6. Support the development of policies containing standard security practices<br><br>1. Separation of duties<br>2. Job rotation<br>3. Mandatory vacation<br>4. Least privilege<br>5. Incident response<br>6. Forensic tasks<br>7. Employment and termination procedures<br>8. Continuous monitoring<br>9. Training and awareness for users<br>10. Auditing requirements and frequency<br>11. Information classification |
|  | 1. Categorize data types by impact levels based on CIA<br>2. Incorporate stakeholder input into CIA impact-level decisions |

| Topic | Details |
|---|---|
| Given a scenario, execute risk mitigation strategies and controls. | 3. Determine minimum-required security controls based on aggregate score<br>4. Select and implement controls based on CIA requirements and organizational policies<br>5. Extreme scenario planning/ worst-case scenario<br>6. Conduct system-specific risk analysis<br>7. Make risk determination based upon known metrics<br>1. Magnitude of impact based on ALE and SLE<br>2. Likelihood of threat<br>Motivation<br>Source<br>ARO<br>Trend analysis<br>3. Return on investment (ROI)<br>4. Total cost of ownership<br>8. Translate technical risks in business terms<br>9. Recommend which strategy should be applied based on risk appetite<br>1. Avoid<br>2. Transfer<br>3. Mitigate<br>4. Accept<br>10. Risk management processes<br>1. Exemptions<br>2. Deterrence<br>3. Inherent<br>4. Residual<br>11. Continuous improvement/monitoring<br>12. Business continuity planning<br>1. RTO<br>2. RPO<br>3. MTTR<br>4. MTBF<br>13. IT governance<br>1. Adherence to risk management frameworks<br>14. Enterprise resilience |

| Topic | Details |
|---|---|
| Analyze risk metric scenarios to secure the enterprise. | 1. Review effectiveness of existing security controls<br>1. Gap analysis<br>2. Lessons learned<br>3. After-action reports<br>2. Reverse engineer/deconstruct existing solutions<br>3. Creation, collection and analysis of metrics<br>1. KPIs<br>2. KRIs<br>4. Prototype and test multiple solutions<br>5. Create benchmarks and compare to baselines<br>6. Analyze and interpret trend data to anticipate cyber defense needs<br>7. Analyze security solution metrics and attributes to ensure they meet business needs<br>1. Performance<br>2. Latency<br>3. Scalability<br>4. Capability<br>5. Usability<br>6. Maintainability<br>7. Availability<br>8. Recoverability<br>9. ROI<br>10. TCO<br>8. Use judgment to solve problems where the most secure solution is not feasible |
| **Enterprise Security Architecture 25%** | |
| Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements. | 1. Physical and virtual network and security devices<br>1. UTM<br>2. IDS/IPS<br>3. NIDS/NIPS<br>4. INE<br>5. NAC<br>6. SIEM<br>7. Switch<br>8. Firewall<br>9. Wireless controller<br>10. Router<br>11. Proxy<br>12. Load balancer |

| Topic | Details |
|---|---|
|  | 13. HSM<br>14. MicroSD HSM<br><br>2. Application and protocol-aware technologies<br><br>1. WAF<br>2. Firewall<br>3. Passive vulnerability scanners<br>4. DAM<br><br>3. Advanced network design (wired/wireless)<br><br>1. Remote access<br>VPN<br>IPSec<br>SSL/TLS<br>SSH<br>RDP<br>VNC<br>VDI<br>Reverse proxy<br>2. IPv4 and IPv6 transitional technologies<br>3. Network authentication methods<br>4. 802.1x<br>5. Mesh networks<br>6. Placement of fixed/mobile devices<br>7. Placement of hardware and applications<br><br>4. Complex network security solutions for data flow<br><br>1. DLP<br>2. Deep packet inspection<br>3. Data flow enforcement<br>4. Network flow (S/flow)<br>5. Data flow diagram<br><br>5. Secure configuration and baselining of networking and security components<br>6. Software-defined networking<br>7. Network management and monitoring tools<br><br>1. Alert definitions and rule writing<br>2. Tuning alert thresholds<br>3. Alert fatigue<br><br>8. Advanced configuration of routers, switches and other network devices |

| Topic | Details |
|---|---|
| | 1. Transport security<br>2. Trunking security<br>3. Port security<br>4. Route protection<br>5. DDoS protection<br>6. Remotely triggered black hole<br>9. Security zones<br>1. DMZ<br>2. Separation of critical assets<br>3. Network segmentation<br>10. Network access control<br>1. Quarantine/remediation<br>2. Persistent/volatile or non-persistent agent<br>3. Agent vs. agentless<br>11. Network-enabled devices<br>1. System on a chip (SoC)<br>2. Building/home automation systems<br>3. IP video<br>4. HVAC controllers<br>5. Sensors<br>6. Physical access control systems<br>7. A/V systems<br>8. Scientific/industrial equipment<br>12. Critical infrastructure<br>1. Supervisory control and data acquisition (SCADA)<br>2. Industrial control systems (ICS) |
| Analyze a scenario to integrate security controls for host devices to meet security requirements. | 1. Trusted OS (e.g., how and when to use it)<br>1. SELinux<br>2. SEAndroid<br>3. TrustedSolaris<br>4. Least functionality<br>2. Endpoint security software<br>1. Anti-malware<br>2. Antivirus<br>3. Anti-spyware |

| Topic | Details |
|---|---|
| | 4. Spam filters<br>5. Patch management<br>6. HIPS/HIDS<br>7. Data loss prevention<br>8. Host-based firewalls<br>9. Log monitoring<br>10. Endpoint detection response<br><br>3. Host hardening<br><br>1. Standard operating environment/ configuration baselining<br>Application whitelisting and blacklisting<br>2. Security/group policy implementation<br>3. Command shell restrictions<br>4. Patch management<br>Manual<br>Automated<br>Scripting and replication<br>5. Configuring dedicated interfaces<br>Out-of-band management<br>ACLs<br>Management interface<br>Data interface<br>6. External I/O restrictions<br>USB<br>Wireless<br>Bluetooth<br>NFC<br>IrDA<br>RF<br>802<br>RFID<br>Drive mounting<br>Drive mapping<br>Webcam<br>Recording mic<br>Audio output<br>SD port<br>HDMI port<br>7. File and disk encryption<br>8. Firmware updates<br><br>4. Boot loader protections<br><br>1. Secure boot<br>2. Measured launch<br>3. Integrity measurement architecture |

| Topic | Details |
|---|---|
|  | 4. BIOS/UEFI<br>5. Attestation services<br>6. TPM<br><br>5. Vulnerabilities associated with hardware<br>6. Terminal services/application delivery services |
| Analyze a scenario to integrate security controls for mobile and small form factor devices to meet security requirements. | 1. Enterprise mobility management<br><br>1. Containerization<br>2. Configuration profiles and payloads<br>3. Personally owned, corporate-enabled<br>4. Application wrapping<br>5. Remote assistance access<br>VNC<br>Screen mirroring<br>6. Application, content and data management<br>7. Over-the-air updates (software/firmware)<br>8. Remote wiping<br>9. SCEP<br>10. BYOD<br>11. COPE<br>12. VPN<br>13. Application permissions<br>14. Side loading<br>15. Unsigned apps/system apps<br>16. Context-aware management<br>Geolocation/geofencing<br>User behavior<br>Security restrictions<br>Time-based restrictions<br><br>2. Security implications/privacy concerns<br><br>1. Data storage<br>Non-removable storage<br>Removable storage<br>Cloud storage<br>Transfer/backup data to uncontrolled storage<br>USB OTG<br>2. Device loss/theft<br>3. Hardware anti-tamper<br>eFuse<br>4. TPM<br>5. Rooting/jailbreaking<br>6. Push notification services<br>7. Geotagging<br>8. Encrypted instant messaging apps |

| Topic | Details |
|---|---|
| | 9. Tokenization<br>10. OEM/carrier Android fragmentation<br>11. Mobile payment<br>NFC-enabled<br>Inductance-enabled<br>Mobile wallet<br>Peripheral-enabled payments (credit card reader)<br>12. Tethering<br>USB<br>Spectrum management<br>Bluetooth 3.0 vs. 4.1<br>13. Authentication<br>Swipe pattern<br>Gesture<br>Pin code<br>Biometric<br>Facial<br>Fingerprint<br>Iris scan<br>14. Malware<br>15. Unauthorized domain bridging<br>16. Baseband radio/SOC<br>17. Augmented reality<br>18. SMS/MMS/messaging<br>3. Wearable technology<br>1. Devices<br>Cameras<br>Watches<br>Fitness devices<br>Glasses<br>Medical sensors/devices<br>Headsets<br>2. Security implications<br>Unauthorized remote activation/ deactivation of devices or features<br>Encrypted and unencrypted communication concerns<br>Physical reconnaissance<br>Personal data theft<br>Health privacy<br>Digital forensics of collected data |
| Given software vulnerability scenarios, select appropriate security controls. | 1. Application security design considerations |

| Topic | Details |
|---|---|
|  | 1. Secure: by design, by default, by deployment<br>2. Specific application issues<br>1. Unsecure direct object references<br>2. XSS<br>3. Cross-site request forgery (CSRF)<br>4. Click-jacking<br>5. Session management<br>6. Input validation<br>7. SQL injection<br>8. Improper error and exception handling<br>9. Privilege escalation<br>10. Improper storage of sensitive data<br>11. Fuzzing/fault injection<br>12. Secure cookie storage and transmission<br>13. Buffer overflow<br>14. Memory leaks<br>15. Integer overflows<br>16. Race conditions<br>Time of check<br>Time of use<br>17. Resource exhaustion<br>18. Geotagging<br>19. Data remnants<br>20. Use of third-party libraries<br>21. Code reuse<br>2. Application sandboxing<br>3. Secure encrypted enclaves<br>4. Database activity monitor<br>5. Web application firewalls<br>6. Client-side processing vs. server-side processing<br>1. JSON/REST<br>2. Browser extensions<br>ActiveX<br>Java applets<br>3. HTML5<br>4. AJAX<br>5. SOAP<br>6. State management<br>7. JavaScript<br>7. Operating system vulnerabilities<br>8. Firmware vulnerabilities |

| Topic | Details |
|---|---|
| **Enterprise Security Operations 20%** | |
| Given a scenario, conduct a security assessment using the appropriate methods. | 1. Methods<br>1. Malware sandboxing<br>2. Memory dumping, runtime debugging<br>3. Reconnaissance<br>4. Fingerprinting<br>5. Code review<br>6. Social engineering<br>7. Pivoting<br>8. Open source intelligence<br>Social media<br>Whois<br>Routing tables<br>DNS records<br>Search engines<br>2. Types<br>1. Penetration testing<br>Black box<br>White box<br>Gray box<br>2. Vulnerability assessment<br>3. Self-assessment<br>Tabletop exercises<br>4. Internal and external audits<br>5. Color team exercises<br>Red team<br>Blue team<br>White team |
| Analyze a scenario or output, and select the appropriate tool for a security assessment. | 1. Network tool types<br>1. Port scanners<br>2. Vulnerability scanners<br>3. Protocol analyzer<br>Wired<br>Wireless<br>4. SCAP scanner<br>5. Network enumerator<br>6. Fuzzer<br>7. HTTP interceptor<br>8. Exploitation tools/frameworks<br>9. Visualization tools<br>10. Log reduction and analysis tools |

| Topic | Details |
|---|---|
|  | 2. Host tool types<br>1. Password cracker<br>2. Vulnerability scanner<br>3. Command line tools<br>4. Local exploitation tools/frameworks<br>5. SCAP tool<br>6. File integrity monitoring<br>7. Log analysis tools<br>8. Antivirus<br>9. Reverse engineering tools<br>3. Physical security tools<br>1. Lock picks<br>2. RFID tools<br>3. IR camera |
| Given a scenario, implement incident response and recovery procedures. | 1. E-discovery<br>1. Electronic inventory and asset control<br>2. Data retention policies<br>3. Data recovery and storage<br>4. Data ownership<br>5. Data handling<br>6. Legal holds<br>2. Data breach<br>1. Detection and collection<br>Data analytics<br>2. Mitigation<br>Minimize<br>Isolate<br>3. Recovery/reconstitution<br>4. Response<br>5. Disclosure<br>3. Facilitate incident detection and response<br>1. Hunt teaming<br>2. Heuristics/behavioral analytics<br>3. Establish and review system, audit and security logs<br>4. Incident and emergency response<br>1. Chain of custody |

| Topic | Details |
|---|---|
|  | 2. Forensic analysis of compromised system<br>3. Continuity of operations<br>4. Disaster recovery<br>5. Incident response team<br>6. Order of volatility<br>5. Incident response support tools<br>1. dd<br>2. tcpdump<br>3. nbtstat<br>4. netstat<br>5. nc (Netcat)<br>6. memdump<br>7. tshark<br>8. foremost<br>6. Severity of incident or breach<br>1. Scope<br>2. Impact<br>3. Cost<br>4. Downtime<br>5. Legal ramifications<br>7. Post-incident response<br>1. Root-cause analysis<br>2. Lessons learned<br>3. After-action report |
| **Technical Integration of Enterprise Security 23%** |  |
| Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture. | 1. Adapt data flow security to meet changing business needs<br>2. Standards<br>1. Open standards<br>2. Adherence to standards<br>3. Competing standards<br>4. Lack of standards<br>5. De facto standards<br>3. Interoperability issues<br>1. Legacy systems and software/current systems<br>2. Application requirements |

| Topic | Details |
|---|---|
| | 3. Software types<br>In-house developed<br>Commercial<br>Tailored commercial<br>Open source<br>4. Standard data formats<br>5. Protocols and APIs<br><br>4. Resilience issues<br><br>1. Use of heterogeneous components<br>2. Course of action automation/orchestration<br>3. Distribution of critical assets<br>4. Persistence and non- persistence of data<br>5. Redundancy/high availability<br>6. Assumed likelihood of attack<br><br>5. Data security considerations<br><br>1. Data remnants<br>2. Data aggregation<br>3. Data isolation<br>4. Data ownership<br>5. Data sovereignty<br>6. Data volume<br><br>6. Resources provisioning and deprovisioning<br><br>1. Users<br>2. Servers<br>3. Virtual devices<br>4. Applications<br>5. Data remnants<br><br>7. Design considerations during mergers, acquisitions and demergers/divestitures<br>8. Network secure segmentation and delegation<br>9. Logical deployment diagram and corresponding physical deployment diagram of all relevant devices<br>10. Security and privacy considerations of storage integration<br>11. Security implications of integrating enterprise applications<br><br>1. CRM<br>2. ERP<br>3. CMDB<br>4. CMS |

| Topic | Details |
|---|---|
| | 5. Integration enablers<br>Directory services<br>DNS<br>SOA<br>ESB |
| Given a scenario, integrate cloud and virtualization technologies into a secure enterprise architecture. | 1. Technical deployment models (outsourcing/insourcing/ managed services/partnership)<br>1. Cloud and virtualization considerations and hosting options<br>Public<br>Private<br>Hybrid<br>Community<br>Multi-tenancy<br>Single tenancy<br>2. On-premise vs. hosted<br>3. Cloud service models<br>SaaS<br>IaaS<br>PaaS<br>2. Security advantages and disadvantages of virtualization<br>1. Type 1 vs. Type 2 hypervisors<br>2. Container-based<br>3. vTPM<br>4. Hyperconverged infrastructure<br>5. Virtual desktop infrastructure<br>6. Secure enclaves and volumes<br>3. Cloud augmented security services<br>1. Anti-malware<br>2. Vulnerability scanning<br>3. Sandboxing<br>4. Content filtering<br>5. Cloud security broker<br>6. Security as a service<br>7. Managed security service providers<br>4. Vulnerabilities associated with comingling of hosts with different security requirements<br>1. VMEscape<br>2. Privilege elevation<br>3. Live VM migration |

| Topic | Details |
|---|---|
|  | 4. Data remnants<br>5. Data security considerations<br>1. Vulnerabilities associated with a single server hosting multiple data types<br>2. Vulnerabilities associated with a single platform hosting multiple data types/owners on multiple virtual machines<br>6. Resources provisioning and deprovisioning<br>1. Virtual devices<br>2. Data remnants |
| Given a scenario, integrate and troubleshoot advanced authentication and authorization technologies to support enterprise security objectives. | 1. Authentication<br>1. Certificate-based authentication<br>2. Single sign-on<br>3. 802.1x<br>4. Context-aware authentication<br>5. Push-based authentication<br>2. Authorization<br>1. OAuth<br>2. XACML<br>3. SPML<br>3. Attestation<br>4. Identity proofing<br>5. Identity propagation<br>6. Federation<br>1. SAML<br>2. OpenID<br>3. Shibboleth<br>4. WAYF<br>7. Trust models<br>1. RADIUS configurations<br>2. LDAP<br>3. AD |

| Topic | Details |
|---|---|
| Given a scenario, implement cryptographic techniques. | 1. Techniques<br>1. Key stretching<br>2. Hashing<br>3. Digital signature<br>4. Message authentication<br>5. Code signing<br>6. Pseudo-random number generation<br>7. Perfect forward secrecy<br>8. Data-in-transit encryption<br>9. Data-in-memory/processing<br>10. Data-at-rest encryption<br>Disk<br>Block<br>File<br>Record<br>11. Steganography<br>2. Implementations<br>1. Crypto modules<br>2. Crypto processors<br>3. Cryptographic service providers<br>4. DRM<br>5. Watermarking<br>6. GPG<br>7. SSL/TLS<br>8. SSH<br>9. S/MIME<br>10. Cryptographic applications and proper/improper implementations<br>Strength<br>Performance<br>Feasibility to implement<br>Interoperability<br>11. Stream vs. block<br>12. PKI<br>Wild card<br>OCSP vs. CRL<br>Issuance to entities<br>Key escrow<br>Certificate<br>Tokens<br>Stapling<br>Pinning<br>13. Cryptocurrency/blockchain<br>14. Mobile device encryption considerations |

| Topic | Details |
|---|---|
| | 15. Elliptic curve cryptography<br>P-256 vs. P-384 vs. P521 |
| Given a scenario, select the appropriate control to secure communications and collaboration solutions. | 1. Remote access<br>1. Resource and services<br>2. Desktop and application sharing<br>3. Remote assistance<br>2. Unified collaboration tools<br>1. Conferencing<br>Web<br>Video<br>Audio<br>2. Storage and document collaboration tools<br>3. Unified communication<br>4. Instant messaging<br>5. Presence<br>6. Email<br>7. Telephony and VoIP integration<br>8. Collaboration sites<br>Social media<br>Cloud-based |
| **Research, Development and Collaboration 13%** | |
| Given a scenario, apply research methods to determine industry trends and their impact to the enterprise. | 1. Perform ongoing research<br>1. Best practices<br>2. New technologies, security systems and services<br>3. Technology evolution (e.g., RFCs, ISO)<br>2. Threat intelligence<br>1. Latest attacks<br>2. Knowledge of current vulnerabilities and threats<br>3. Zero-day mitigation controls and remediation<br>4. Threat model<br>3. Research security implications of emerging business tools<br>1. Evolving social media platforms<br>2. Integration within the business<br>3. Big Data<br>4. AI/machine learning |

| Topic | Details |
|---|---|
|  | 4. Global IA industry/community<br>1. Computer emergency response team (CERT)<br>2. Conventions/conferences<br>3. Research consultants/vendors<br>4. Threat actor activities<br>5. Emerging threat sources |
| Given a scenario, implement security activities across the technology life cycle. | 1. Systems development life cycle<br>1. Requirements<br>2. Acquisition<br>3. Test and evaluation<br>4. Commissioning/decommissioning<br>5. Operational activities<br>Monitoring<br>Maintenance<br>Configuration and change management<br>6. Asset disposal<br>7. Asset/object reuse<br>2. Software development life cycle<br>1. Application security frameworks<br>2. Software assurance<br>Standard libraries<br>Industry-accepted approaches<br>Web services security (WS-security)<br>3. Forbidden coding techniques<br>4. NX/XN bit use<br>5. ASLR use<br>6. Code quality<br>7. Code analyzers<br>Fuzzer<br>Static<br>Dynamic<br>8. Development approaches<br>DevOps<br>Security implications of agile, waterfall and spiral software development methodologies<br>Continuous integration<br>Versioning<br>9. Secure coding standards<br>10. Documentation<br>Security requirements traceability matrix (SRTM)<br>Requirements definition<br>System design document<br>Testing plans |

| Topic | Details |
|---|---|
| | 11. Validation and acceptance testing<br>Regression<br>User acceptance testing<br>Unit testing<br>Integration testing<br>Peer review<br>3. Adapt solutions to address:<br>1. Emerging threats<br>2. Disruptive technologies<br>3. Security trends<br>4. Asset management (inventory control) |
| Explain the importance of interaction across diverse business units to achieve security goals. | 1. Interpreting security requirements and goals to communicate with stakeholders from other disciplines<br>1. Sales staff<br>2. Programmer<br>3. Database administrator<br>4. Network administrator<br>5. Management/executive management<br>6. Financial<br>7. Human resources<br>8. Emergency response team<br>9. Facilities manager<br>10. Physical security manager<br>11. Legal counsel<br>2. Provide objective guidance and impartial recommendations to staff and senior management on security processes and controls<br>3. Establish effective collaboration within teams to implement secure solutions<br>4. Governance, risk and compliance committee |

# CAS-003 Sample Questions:

**01. As a condition of being awarded a new contract, an organization must increase the security of its VPN ensuring that one compromised SA session key cannot be used to compromise any other sessions.**
**Which of the following could be configured to meet this requirement?**
**a)** Opportunistic encryption
**b)** Pseudo-random number generator
**c)** Dual-factor authentication
**d)** Perfect forward secrecy

**02. An IT Manager has requested that specific files stored on the company SAN containing data which is not protected by patent law, but is classified as trade secret encrypted with a block cipher which is both secure and fast.**
**Which of the following BEST satisfies the request?**
**a)** Blowfish
**b)** MD5
**c)** Triple-DES
**d)** RC4

**03. During a routine security assessment of a network, the security administrator discovers a user workstation with multiple SSH connections to servers outside the corporate network.**
**Using a protocol analyzer, the administrator identifies hundreds of gigabytes of information being transferred to an external server via SCP. After identifying the user, the administrator discovers that today is the user's last day of employment, and that the employee is going to work for a competitor. Which of the following tactics is being used to steal company secrets?**
**a)** Logic bomb
**b)** SSH worm
**c)** Data exfiltration
**d)** Privilege escalation
**e)** SAML exploit

**04. A new system has recently been built using the SSDLC process and is in the validation process to ensure the system is behaving correctly.**
**During this process, the development team notices that the system is behaving as it should, except for a few minor internal application bugs. Which of the following validation types would be a result of this issue?**
**a)** Application interface validation
**b)** Code validation
**c)** Functional validation
**d)** Requirements validation

**05. When considering security requirements which require third party vendor requests, which of the following is a correctly ordered set of events from start to finish?**
**a)** RFP, RFQ, RFC
**b)** RFI, RFQ, RFP
**c)** RFP, RFQ, RFI
**d)** RFC, RFT

**06. An administrator uses an iSCSI unencrypted connection over the corporate network. Which of the following vulnerabilities would be present in regards to iSCSI authentication?**
**a)** Authentication uses the older TACACS protocol and is vulnerable to a botnet attack.
**b)** Authentication is vulnerable to a dictionary attack.
**c)** iSCSI uses LDAP authentication in plain text, which can be easily compromised.
**d)** Kerberos authentication would not be supported on Linux hosts.

**07. A security administrator notices a network intrusion and quickly solves the problem by closing an unused port. Which of the following should be completed?**
**a)** After action report
**b)** ELA
**c)** MOA
**d)** Reverse engineering incident report

**08. Which of the following practices is MOST likely employed during e-discovery?**
**a)** Legal hold and chain of custody
**b)** Risk mitigation and policy generation
**c)** Network enumeration and fingerprinting
**d)** Data deduplication and hashing

**09. A new Chief Information Officer's (CIO's) primary initiative is to reduce risk and the number of vulnerabilities affecting an organization. Which of the following reduces the number of locations to patch internal applications?**
**a)** Provide application access through a VDI
**b)** Host applications using terminal services
**c)** Implement an enterprise patch management solution
**d)** Convert applications to leverage hosted cloud computing

**10. A server administrator needs to find a web service that will allow most systems to communicate over HTTP using an XML based protocol. Which of the following communication methods will allow this?**
**a)** SOAP
**b)** XACML
**c)** SSO
**d)** SAML

# Answers to CAS-003 Exam Questions:

| | | | | |
|---|---|---|---|---|
| Question: 01<br>Answer: d | Question: 02<br>Answer: a | Question: 03<br>Answer: c | Question: 04<br>Answer: b | Question: 05<br>Answer: b |
| Question: 06<br>Answer: b | Question: 07<br>Answer: a | Question: 08<br>Answer: a | Question: 09<br>Answer: b | Question: 10<br>Answer: a |

Note: If you find any typo or data entry error in these sample questions, we request you to update us by commenting on this page or write an email on feedback@edusum.com