EDUSUM
#1 Online Certification Guide

# COMPTIA CAS-004

**CompTIA CASP+ Certification Questions & Answers**

Exam Summary – Syllabus –Questions

**CAS-004**
**CompTIA Advanced Security Practitioner (CASP+)**
**90 Questions Exam – Duration of 165 minutes**

## Table of Contents:

# Know Your CAS-004 Certification Well:

The CAS-004 is best suitable for candidates who want to gain knowledge in the CompTIA Cybersecurity. Before you start your CAS-004 preparation you may struggle to get all the crucial CASP+ materials like CAS-004 syllabus, sample questions, study guide.

But don't worry the CAS-004 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-004 syllabus?
- How many questions are there in the CAS-004 exam?
- Which Practice test would help me to pass the CAS-004 exam at the first attempt?

Passing the CAS-004 exam makes you CompTIA Advanced Security Practitioner. Having the CASP+ 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-004 CASP+ Certification Details:

| | |
|---|---|
| Exam Name | CompTIA Advanced Security Practitioner (CASP+) |
| Exam Code | CAS-004 |
| Exam Price | $466 (USD) |
| Duration | 165 mins |
| Number of Questions | 90 |
| Passing Score | Pass / Fail |
| Books / Training | **CASP+ CAS-004** |
| Schedule Exam | **CompTIA Marketplace**<br>**Pearson VUE** |
| Sample Questions | **CompTIA CASP+ Sample Questions** |
| Practice Exam | **CompTIA CAS-004 Certification Practice Exam** |

# CAS-004 Syllabus:

| Topic | Details |
|---|---|
| Security Architecture 29% | |
| Given a scenario, analyze the security requirements and objectives to ensure an appropriate, secure network architecture for a new or existing network. | - Services<br>• Load balancer<br>• Intrusion detection system (IDS)/network intrusion detection system (NIDS)/wireless intrusion detection system (WIDS)<br>• Intrusion prevention system (IPS)/network intrusion prevention system (NIPS)/wireless intrusion prevention system (WIPS)<br>• Web application firewall (WAF)<br>• Network access control (NAC)<br>• Virtual private network (VPN)<br>• Domain Name System Security Extensions (DNSSEC)<br>• Firewall/unified threat management (UTM)/next-generation firewall (NGFW)<br>• Network address translation (NAT) gateway<br>• Internet gateway<br>• Forward/transparent proxy<br>• Reverse proxy<br>• Distributed denial-of-service (DDoS) protection<br>• Routers<br>• Mail security<br>• Application programming interface (API) gateway/Extensible Markup Language (XML) gateway<br>• Traffic mirroring<br>- Switched port analyzer (SPAN) ports<br>- Port mirroring<br>- Virtual private cloud (VPC)<br>- Network tap<br>• Sensors<br>- Security information and event management (SIEM)<br>- File integrity monitoring (FIM)<br>- Simple Network Management Protocol (SNMP) traps |

| Topic | Details |
|---|---|
| | - NetFlow<br>- Data loss prevention (DLP)<br>- Antivirus<br>- Segmentation<br>• Microsegmentation<br>• Local area network (LAN)/virtual local area network (VLAN)<br>• Jump box<br>• Screened subnet<br>• Data zones<br>• Staging environments<br>• Guest environments<br>• VPC/virtual network (VNET)<br>• Availability zone<br>• NAC lists<br>• Policies/security groups<br>• Regions<br>• Access control lists (ACLs)<br>• Peer-to-peer<br>• Air gap<br>- Deperimeterization/zero trust<br>• Cloud<br>• Remote work<br>• Mobile<br>• Outsourcing and contracting<br>• Wireless/radio frequency (RF) networks<br>- Merging of networks from various organizations<br>• Peering<br>• Cloud to on premises<br>• Data sensitivity levels<br>• Mergers and acquisitions<br>• Cross-domain<br>• Federation<br>• Directory services<br>- Software-defined networking (SDN) |

| Topic | Details |
|---|---|
| | • Open SDN<br>• Hybrid SDN<br>• SDN overlay |
| Given a scenario, analyze the organizational requirements to determine the proper infrastructure security design. | - Scalability<br>• Vertically<br>• Horizontally<br>- Resiliency<br>• High availability<br>• Diversity/heterogeneity<br>• Course of action orchestration<br>• Distributed allocation<br>• Redundancy<br>• Replication<br>• Clustering<br>- Automation<br>• Autoscaling<br>• Security Orchestration, Automation, and Response (SOAR)<br>• Bootstrapping<br>- Performance<br>- Containerization<br>- Virtualization<br>- Content delivery network<br>- Caching |
| Given a scenario, integrate software applications securely into an enterprise architecture. | - Baseline and templates<br>• Secure design patterns/ types of web technologies - Storage design patterns<br>• Container APIs<br>• Secure coding standards<br>• Application vetting processes<br>• API management<br>• Middleware<br>- Software assurance |

| Topic | Details |
|---|---|
|  | • Sandboxing/development environment<br>• Validating third-party libraries<br>• Defined DevOps pipeline<br>• Code signing<br>• Interactive application security testing (IAST) vs. dynamic application security testing (DAST) vs. static application security testing (SAST)<br>- Considerations of integrating enterprise applications<br>• Customer relationship management (CRM)<br>• Enterprise resource planning (ERP)<br>• Configuration management database (CMDB)<br>• Content management system (CMS)<br>• Integration enablers<br>- Directory services<br>- Domain name system (DNS)<br>- Service-oriented architecture (SOA)<br>- Enterprise service bus (ESB)<br>- Integrating security into development life cycle<br>• Formal methods<br>• Requirements<br>• Fielding<br>• Insertions and upgrades<br>• Disposal and reuse<br>• Testing<br>- Regression<br>- Unit testing<br>- Integration testing<br>• Development approaches<br>- SecDevOps<br>- Agile<br>- Waterfall<br>- Spiral<br>- Versioning<br>- Continuous integration/continuous delivery (CI/CD) pipelines<br>• Best practices<br>- Open Web Application Security Project (OWASP)<br>- Proper Hypertext Transfer Protocol (HTTP) headers |

| Topic | Details |
|---|---|
| Given a scenario, implement data security techniques for securing enterprise architecture. | - Data loss prevention<br>• Blocking use of external media<br>• Print blocking<br>• Remote Desktop Protocol (RDP) blocking<br>• Clipboard privacy controls<br>• Restricted virtual desktop infrastructure (VDI) implementation<br>• Data classification blocking<br>- Data loss detection<br>• Watermarking<br>• Digital rights management (DRM)<br>• Network traffic decryption/deep packet inspection<br>• Network traffic analysis<br>- Data classification, labeling, and tagging<br>• Metadata/attributes<br>- Obfuscation<br>• Tokenization<br>• Scrubbing<br>• Masking<br>- Anonymization<br>- Encrypted vs. unencrypted<br>- Data life cycle<br>• Create<br>• Use<br>• Share<br>• Store<br>• Archive<br>• Destroy<br>- Data inventory and mapping<br>- Data integrity management<br>- Data storage, backup, and recovery<br>• Redundant array of inexpensive disks (RAID) |

| Topic | Details |
|---|---|
| Given a scenario, analyze the security requirements and objectives to provide the appropriate authentication and authorization controls. | - Credential management<br>• Password repository application<br>- End-user password storage<br>- On premises vs. cloud repository<br>• Hardware key manager<br>• Privileged access management<br>- Password policies<br>• Complexity<br>• Length<br>• Character classes<br>• History<br>• Maximum/minimum age<br>• Auditing<br>• Reversable encryption<br>- Federation<br>• Transitive trust<br>• OpenID<br>• Security Assertion Markup Language (SAML)<br>• Shibboleth<br>- Access control<br>• Mandatory access control (MAC)<br>• Discretionary access control (DAC)<br>• Role-based access control<br>• Rule-based access control<br>• Attribute-based access control<br>- Protocols<br>• Remote Authentication Dial-in User Server (RADIUS)<br>• Terminal Access Controller Access Control System (TACACS)<br>• Diameter<br>• Lightweight Directory Access Protocol (LDAP)<br>• Kerberos<br>• OAuth |

| Topic | Details |
|---|---|
|  | • 802.1X<br>• Extensible Authentication Protocol (EAP)<br>- Multifactor authentication (MFA)<br>• Two-factor authentication (2FA)<br>• 2-Step Verification<br>• In-band<br>• Out-of-band<br>- One-time password (OTP)<br>• HMAC-based one-time password (HOTP)<br>• Time-based one-time password (TOTP)<br>- Hardware root of trust<br>- Single sign-on (SSO)<br>- JavaScript Object Notation (JSON) web token (JWT)<br>- Attestation and identity proofing |
| Given a set of requirements, implement secure cloud and virtualization solutions. | - Virtualization strategies<br>• Type 1 vs. Type 2 hypervisors<br>• Containers<br>• Emulation<br>• Application virtualization<br>• VDI<br>- Provisioning and deprovisioning<br>- Middleware<br>- Metadata and tags<br>- Deployment models and considerations<br>• Business directives<br>- Cost<br>- Scalability<br>- Resources<br>- Location<br>- Data protection<br>• Cloud deployment models<br>- Private<br>- Public<br>- Hybrid<br>- Community<br>- Hosting models |

| Topic | Details |
|---|---|
| | • Multitenant<br>• Single-tenant<br>- Service models<br>• Software as a service (SaaS)<br>• Platform as a service (PaaS)<br>• Infrastructure as a service (IaaS)<br>- Cloud provider limitations<br>• Internet Protocol (IP) address scheme<br>• VPC peering<br>- Extending appropriate on-premises controls<br>- Storage models<br>• Object storage/file-based storage<br>• Database storage<br>• Block storage<br>• Blob storage<br>• Key-value pairs |
| Explain how cryptography and public key infrastructure (PKI) support security objectives and requirements. | - Privacy and confidentiality requirements<br>- Integrity requirements<br>- Non-repudiation<br>- Compliance and policy requirements<br>- Common cryptography use cases<br>• Data at rest<br>• Data in transit<br>• Data in process/data in use<br>• Protection of web services<br>• Embedded systems<br>• Key escrow/management<br>• Mobile security<br>• Secure authentication<br>• Smart card<br>- Common PKI use cases<br>• Web services<br>• Email |

| Topic | Details |
|---|---|
| | - Code signing<br>- Federation<br>- Trust models<br>- VPN<br>- Enterprise and security automation/orchestration |
| Explain the impact of emerging technologies on enterprise security and privacy. | - Artificial intelligence<br>- Machine learning<br>- Quantum computing<br>- Blockchain<br>- Homomorphic encryption<br>• Private information retrieval<br>• Secure function evaluation<br>• Private function evaluation<br>- Secure multiparty computation<br>- Distributed consensus<br>- Big Data<br>- Virtual/augmented reality<br>- 3-D printing<br>- Passwordless authentication<br>- Nano technology<br>- Deep learning<br>• Natural language processing<br>• Deep fakes<br>- Biometric impersonation |
| Security Operations 30% | |
| Given a scenario, perform threat management activities. | - Intelligence types<br>• Tactical<br>- Commodity malware<br>• Strategic<br>- Targeted attacks<br>• Operational<br>- Threat hunting<br>- Threat emulation<br>- Actor types<br>• Advanced persistent threat (APT)/nation-state |

| Topic | Details |
|---|---|
| | • Insider threat<br>• Competitor<br>• Hacktivist<br>• Script kiddie<br>• Organized crime<br>- Threat actor properties<br>• Resource<br>- Time<br>- Money<br>• Supply chain access<br>• Create vulnerabilities<br>• Capabilities/sophistication<br>• Identifying techniques<br>- Intelligence collection methods<br>• Intelligence feeds<br>• Deep web<br>• Proprietary<br>• Open-source intelligence (OSINT)<br>• Human intelligence (HUMINT)<br>- Frameworks<br>• MITRE Adversarial Tactics, Techniques, & Common knowledge (ATT&CK)<br>- ATT&CK for industrial control system (ICS)<br>• Diamond Model of Intrusion Analysis<br>• Cyber Kill Chain |
| Given a scenario, analyze indicators of compromise and formulate an appropriate response. | - Indicators of compromise<br>• Packet capture (PCAP)<br>• Logs<br>- Network logs<br>- Vulnerability logs<br>- Operating system logs<br>- Access logs<br>- NetFlow logs<br>• Notifications<br>- FIM alerts<br>- SIEM alerts<br>- DLP alerts |

| Topic | Details |
|---|---|
| | - IDS/IPS alerts<br>- Antivirus alerts<br>• Notification severity/priorities<br>• Unusual process activity<br>- Response<br>• Firewall rules<br>• IPS/IDS rules<br>• ACL rules<br>• Signature rules<br>• Behavior rules<br>• DLP rules<br>• Scripts/regular expressions |
| Given a scenario, perform vulnerability management activities. | - Vulnerability scans<br>• Credentialed vs. non-credentialed<br>• Agent-based/server-based<br>• Criticality ranking<br>• Active vs. passive<br>- Security Content Automation Protocol (SCAP)<br>• Extensible Configuration Checklist Description Format (XCCDF)<br>• Open Vulnerability and Assessment Language (OVAL)<br>• Common Platform Enumeration (CPE)<br>• Common Vulnerabilities and Exposures (CVE)<br>• Common Vulnerability Scoring System (CVSS)<br>• Common Configuration Enumeration (CCE)<br>• Asset Reporting Format (ARF)<br>- Self-assessment vs. third-party vendor assessment<br>- Patch management<br>- Information sources<br>• Advisories<br>• Bulletins<br>• Vendor websites<br>• Information Sharing and Analysis Centers (ISACs)<br>• News reports |

| Topic | Details |
|---|---|
| Given a scenario, use the appropriate vulnerability assessment and penetration testing methods and tools. | - Methods<br>• Static analysis<br>• Dynamic analysis<br>• Side-channel analysis<br>• Reverse engineering<br>- Software<br>- Hardware<br>• Wireless vulnerability scan<br>• Software composition analysis<br>• Fuzz testing<br>• ivoting<br>• Post-exploitation<br>• Persistence<br>- Tools<br>• SCAP scanner<br>• Network traffic analyzer<br>• Vulnerability scanner<br>• Protocol analyzer<br>• Port scanner<br>• HTTP interceptor<br>• Exploit framework<br>• Password cracker<br>- Dependency management<br>- Requirements<br>• Scope of work<br>• Rules of engagement<br>• Invasive vs. non-invasive<br>• Asset inventory<br>• Permissions and access<br>• Corporate policy considerations<br>• Facility considerations<br>• Physical security considerations<br>• Rescan for corrections/changes |

| Topic | Details |
|---|---|
| Given a scenario, analyze vulnerabilities and recommend risk mitigations. | - Vulnerabilities<br>• Race conditions<br>• Overflows<br>- Buffer<br>- Integer<br>• Broken authentication<br>• Unsecure references<br>• Poor exception handling<br>• Security misconfiguration<br>• Improper headers<br>• Information disclosure<br>• Certificate errors<br>• Weak cryptography implementations<br>• Weak ciphers<br>• Weak cipher suite implementations<br>• Software composition analysis<br>• Use of vulnerable frameworks and software modules<br>• Use of unsafe functions<br>• Third-party libraries<br>- Dependencies<br>- Code injections/malicious changes<br>- End of support/end of life<br>- Regression issues<br>- Inherently vulnerable system/application<br>• Client-side processing vs. server-side processing<br>• JSON/representational state transfer (REST)<br>• Browser extensions<br>- Flash<br>- ActiveX<br>• Hypertext Markup Language 5 (HTML5)<br>• Asynchronous JavaScript and XML (AJAX)<br>• Simple Object Access Protocol (SOAP)<br>• Machine code vs. bytecode or interpreted vs. emulated<br>- Attacks<br>• Directory traversal |

| Topic | Details |
|---|---|
|  | • Cross-site scripting (XSS)<br>• Cross-site request forgery (CSRF)<br>• Injection<br>- XML<br>- LDAP<br>- Structured Query Language (SQL)<br>- Command<br>- Process<br>• Sandbox escape<br>• Virtual machine (VM) hopping<br>• VM escape<br>• Border Gateway Protocol (BGP)/route hijacking<br>• Interception attacks<br>• Denial-of-service (DoS)/DDoS<br>• Authentication bypass<br>• Social engineering<br>• VLAN hopping |
| Given a scenario, use processes to reduce risk. | - Proactive and detection<br>• Hunts<br>• Developing countermeasures<br>• Deceptive technologies<br>- Honeynet<br>- Honeypot<br>- Decoy files<br>- Simulators<br>- Dynamic network configurations<br>- Security data analytics<br>• Processing pipelines<br>- Data<br>- Stream<br>• Indexing and search<br>• Log collection and curation<br>• Database activity monitoring<br>- Preventive<br>• Antivirus<br>• Immutable systems<br>• Hardening |

| Topic | Details |
|---|---|
|  | • Sandbox detonation<br>- Application control<br>• License technologies<br>• Allow list vs. block list<br>• Time of check vs. time of use<br>• Atomic execution<br>- Security automation<br>• Cron/scheduled tasks<br>• Bash<br>• PowerShell<br>• Python<br>- Physical security<br>• Review of lighting<br>• Review of visitor logs<br>• Camera reviews<br>• Open spaces vs. confined spaces |
| Given an incident, implement the appropriate response. | - Event classifications<br>• False positive<br>• False negative<br>• True positive<br>• True negative<br>- Triage event<br>- Preescalation tasks<br>- Incident response process<br>• Preparation<br>• Detection<br>• Analysis<br>• Containment<br>• Recovery<br>• Lessons learned<br>- Specific response playbooks/processes<br>• Scenarios<br>- Ransomware |

| Topic | Details |
|---|---|
|  | - Data exfiltration<br>- Social engineering<br>• Non-automated response methods<br>• Automated response methods<br>- Runbooks<br>- SOAR<br>- Communication plan<br>- Stakeholder management |
| Explain the importance of forensic concepts. | - Legal vs. internal corporate purposes<br>- Forensic process<br>• Identification<br>• Evidence collection<br>- Chain of custody<br>- Order of volatility<br>1. Memory snapshots<br>2. Images<br>- Cloning<br>• Evidence preservation<br>- Secure storage<br>- Backups<br>• Analysis<br>- Forensics tools<br>• Verification<br>• Presentation<br>- Integrity preservation<br>• Hashing<br>- Cryptanalysis<br>- Steganalysis |
| Given a scenario, use forensic analysis tools. | - File carving tools<br>• Foremost<br>• Strings<br>- Binary analysis tools<br>• Hex dump<br>• Binwalk<br>• Ghidra<br>• GNU Project debugger (GDB) |

| Topic | Details |
|---|---|
| | • OllyDbg<br>• readelf<br>• objdump<br>• strace<br>• ldd<br>• file<br>- Analysis tools<br>• ExifTool<br>• Nmap<br>• Aircrack-ng<br>• Volatility<br>• The Sleuth Kit<br>• Dynamically vs. statically linked<br>- Imaging tools<br>• Forensic Toolkit (FTK) Imager<br>• dd<br>- Hashing utilities<br>• sha256sum<br>• ssdeep<br>- Live collection vs. post-mortem tools<br>• netstat<br>• ps<br>• vmstat<br>• ldd<br>• lsof<br>• netcat<br>• tcpdump<br>• conntrack<br>• Wireshark |
| Security Engineering and Cryptography 26% | |
| Given a scenario, apply secure configurations to enterprise mobility | - Managed configurations<br>• Application control |

| Topic | Details |
|---|---|
| | • Password<br>• MFA requirements<br>• Token-based access<br>• Patch repository<br>• Firmware Over-the-Air<br>• Remote wipe<br>• WiFi<br>- WiFi Protected Access (WPA2/3)<br>- Device certificates<br>• Profiles<br>• Bluetooth<br>• Near-field communication (NFC)<br>• Peripherals<br>• Geofencing<br>• VPN settings<br>• Geotagging<br>• Certificate management<br>• Full device encryption<br>• Tethering<br>• Airplane mode<br>• Location services<br>• DNS over HTTPS (DoH)<br>• Custom DNS<br>- Deployment scenarios<br>• Bring your own device (BYOD)<br>• Corporate-owned<br>• Corporate owned, personally enabled (COPE)<br>• Choose your own device (CYOD)<br>- Security considerations<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 |

| Topic | Details |
|---|---|
| | • Implications of wearable devices<br>• Digital forensics of collected data<br>• Unauthorized application stores<br>• Jailbreaking/rooting<br>• Side loading<br>• Containerization<br>• Original equipment manufacturer (OEM) and carrier differences<br>• Supply chain issues<br>• eFuse |
| Given a scenario, configure and implement endpoint security controls. | - Hardening techniques<br>• Removing unneeded services<br>• Disabling unused accounts<br>• Images/templates<br>• Remove end-of-life devices<br>• Remove end-of-support devices<br>• Local drive encryption<br>• Enable no execute (NX)/execute never (XN) bit<br>• Disabling central processing unit (CPU) virtualization support<br>• Secure encrypted enclaves/memory encryption<br>• Shell restrictions<br>• Address space layout randomization (ASLR)<br>- Processes<br>• Patching<br>• Firmware<br>• Application<br>• Logging<br>• Monitoring<br>- Mandatory access control<br>• Security-Enhanced Linux (SELinux)/Security-Enhanced Android (SEAndroid)<br>• Kernel vs. middleware<br>- Trustworthy computing |

| Topic | Details |
|---|---|
| | • Trusted Platform Module (TPM)<br>• Secure Boot<br>• Unified Extensible Firmware Interface (UEFI)/basic input/output system (BIOS) protection<br>• Attestation services<br>• Hardware security module (HSM)<br>• Measured boot<br>• Self-encrypting drives (SEDs)<br>- Compensating controls<br>• Antivirus<br>• Application controls<br>• Host-based intrusion detection system (HIDS)/Host-based intrusion prevention system (HIPS)<br>• Host-based firewall<br>• Endpoint detection and response (EDR)<br>• Redundant hardware<br>• Self-healing hardware<br>• User and entity behavior analytics (UEBA) |
| Explain security considerations impacting specific sectors and operational technologies. | - Embedded<br>• Internet of Things (IoT)<br>• System on a chip (SoC)<br>• Application-specific integrated circuit (ASIC)<br>• Field-programmable gate array (FPGA)<br>- ICS/supervisory control and data acquisition (SCADA)<br>• Programmable logic controller (PLC)<br>• Historian<br>• Ladder logic<br>• Safety instrumented system<br>• Heating, ventilation, and air conditioning (HVAC)<br>- Protocols<br>• Controller Area Network (CAN) bus<br>• Modbus<br>• Distributed Network Protocol 3 (DNP3) |

| Topic | Details |
|---|---|
|  | • Zigbee<br>• Common Industrial Protocol (CIP)<br>• Data distribution service<br>- Sectors<br>• Energy<br>• Manufacturing<br>• Healthcare<br>• Public utilities<br>• Public services<br>• Facility services |
| Explain how cloud technology adoption impacts organizational security. | - Automation and orchestration<br>- Encryption configuration<br>- Logs<br>• Availability<br>• Collection<br>• Monitoring<br>• Configuration<br>• Alerting<br>- Monitoring configurations<br>- Key ownership and location<br>- Key life-cycle management<br>- Backup and recovery methods<br>• Cloud as business continuity and disaster recovery (BCDR)<br>• Primary provider BCDR<br>• Alternative provider BCDR<br>- Infrastructure vs. serverless computing<br>- Application virtualization<br>- Software-defined networking<br>- Misconfigurations<br>- Collaboration tools<br>- Storage configurations<br>• Bit splitting<br>• Data dispersion<br>- Cloud access security broker (CASB) |

| Topic | Details |
|---|---|
| Given a business requirement, implement the appropriate PKI solution. | - PKI hierarchy<br>• Certificate authority (CA)<br>• Subordinate/intermediate CA<br>• Registration authority (RA)<br>- Certificate types<br>• Wildcard certificate<br>• Extended validation<br>• Multidomain<br>• General purpose<br>- Certificate usages/profiles/templates<br>• Client authentication<br>• Server authentication<br>• Digital signatures<br>• Code signing<br>- Extensions<br>• Common name (CN)<br>• Subject alternate name (SAN)<br>- Trusted providers<br>- Trust model<br>- Cross-certification<br>- Configure profiles<br>- Life-cycle management<br>- Public and private keys<br>- Digital signature<br>- Certificate pinning<br>- Certificate stapling<br>- Certificate signing requests (CSRs)<br>- Online Certificate Status Protocol (OCSP) vs. certificate revocation list (CRL)<br>- HTTP Strict Transport Security (HSTS) |
| Given a business requirement, implement the appropriate cryptographic protocols and algorithms. | - Hashing<br>• Secure Hashing Algorithm (SHA)<br>• Hash-based message authentication code (HMAC)<br>• Message digest (MD) |

| Topic | Details |
|---|---|
| | • RACE integrity primitives evaluation message digest (RIPEMD)<br>• Poly1305<br>- Symmetric algorithms<br>• Modes of operation<br>- Galois/Counter Mode (GCM)<br>- Electronic codebook (ECB)<br>- Cipher block chaining (CBC)<br>- Counter (CTR)<br>- Output feedback (OFB)<br>• Stream and block<br>- Advanced Encryption Standard (AES)<br>- Triple digital encryption standard (3DES)<br>- ChaCha<br>- Salsa20<br>- Asymmetric algorithms<br>• Key agreement<br>- Diffie-Hellman<br>- Elliptic-curve Diffie-Hellman (ECDH)<br>• Signing<br>- Digital signature algorithm (DSA)<br>- Rivest, Shamir, and Adleman (RSA)<br>- Elliptic-curve digital signature algorithm (ECDSA)<br>- Protocols<br>• Secure Sockets Layer (SSL)/Transport Layer Security (TLS)<br>• Secure/Multipurpose Internet Mail Extensions (S/MIME)<br>• Internet Protocol Security (IPSec)<br>• Secure Shell (SSH)<br>• EAP<br>- Elliptic curve cryptography<br>• P256<br>• P384<br>- Forward secrecy<br>- Authenticated encryption with associated data<br>- Key stretching |

| Topic | Details |
|---|---|
| | • Password-based key derivation function 2 (PBKDF2)<br>• Bcrypt |
| Given a scenario, troubleshoot issues with cryptographic implementations. | - Implementation and configuration issues<br>• Validity dates<br>• Wrong certificate type<br>• Revoked certificates<br>• Incorrect name<br>• Chain issues<br>- Invalid root or intermediate CAs<br>- Self-signed<br>• Weak signing algorithm<br>• Weak cipher suite<br>• Incorrect permissions<br>• Cipher mismatches<br>• Downgrade<br>- Keys<br>• Mismatched<br>• Improper key handling<br>• Embedded keys<br>• Rekeying<br>• Exposed private keys<br>• Crypto shredding<br>• Cryptographic obfuscation<br>• Key rotation<br>• Compromised keys |
| **Governance, Risk, and Compliance 15%** | |
| Given a set of requirements, apply the appropriate risk strategies. | - Risk assessment<br>• Likelihood<br>• Impact<br>• Qualitative vs. quantitative<br>• Exposure factor<br>• Asset value |

| Topic | Details |
|---|---|
|  | • Total cost of ownership (TCO)<br>• Return on investment (ROI)<br>• Mean time to recovery (MTTR)<br>• Mean time between failure (MTBF)<br>• Annualized loss expectancy (ALE)<br>• Annualized rate of occurrence (ARO)<br>• Single loss expectancy (SLE)<br>• Gap analysis<br>- Risk handling techniques<br>• Transfer<br>• Accept<br>• Avoid<br>• Mitigate<br>- Risk types<br>• Inherent<br>• Residual<br>• Exceptions<br>- Risk management life cycle<br>• Identify<br>• Assess<br>• Control<br>- People<br>- Process<br>- Technology<br>- Protect<br>- Detect<br>- Respond<br>- Restore<br>• Review<br>• Frameworks<br>- Risk tracking<br>• Risk register<br>• Key performance indicators<br>- Scalability<br>Reliability<br>- Availability |

| Topic | Details |
|---|---|
| | • Key risk indicators<br>- Risk appetite vs. risk tolerance<br>• Tradeoff analysis<br>• Usability vs. security requirements<br>- Policies and security practices<br>• Separation of duties<br>• Job rotation<br>• Mandatory vacation<br>• Least privilege<br>• Employment and termination procedures<br>• Training and awareness for users<br>• Auditing requirements and frequency |
| Explain the importance of managing and mitigating vendor risk. | - Shared responsibility model (roles/responsibilities)<br>• Cloud service provider (CSP)<br>- Geographic location<br>- Infrastructure<br>- Compute<br>- Storage<br>- Networking<br>- Services<br>• Client<br>- Encryption<br>- Operating systems<br>- Applications<br>- Data<br>- Vendor lock-in and vendor lockout<br>- Vendor viability<br>• Financial risk<br>• Merger or acquisition risk<br>- Meeting client requirements<br>• Legal<br>• Change management<br>• Staff turnover<br>• Device and technical configurations<br>- Support availability<br>- Geographical considerations |

| Topic | Details |
|---|---|
|  | - Supply chain visibility<br>- Incident reporting requirements<br>- Source code escrows<br>- Ongoing vendor assessment tools<br>- Third-party dependencies<br>• Code<br>• Hardware<br>• Modules<br>- Technical considerations<br>• Technical testing<br>• Network segmentation<br>• Transmission control<br>• Shared credentials |
| Explain compliance frameworks and legal considerations, and their organizational impact. | - Security concerns of integrating diverse industries<br>- Data considerations<br>• Data sovereignty<br>• Data ownership<br>• Data classifications<br>• Data retention<br>• Data types<br>- Health<br>- Financial<br>- Intellectual property<br>• Personally identifiable information (PII)<br>• Data removal, destruction, and sanitization<br>- Geographic considerations<br>• Location of data<br>• Location of data subject<br>• Location of cloud provider<br>- Third-party attestation of compliance<br>- Regulations, accreditations, and standards<br>• Payment Card Industry Data Security Standard (PCI DSS)<br>• General Data Protection Regulation (GDPR) |

| Topic | Details |
|---|---|
| | • International Organization for Standardization (ISO)<br>• Capability Maturity Model Integration (CMMI)<br>• National Institute of Standards and Technology (NIST)<br>• Children’s Online Privacy Protection Act (COPPA)<br>• Common Criteria<br>• Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR)<br>- Legal considerations<br>• Due diligence<br>• Due care<br>• Export controls<br>• Legal holds<br>• E-discovery<br>- Contract and agreement types<br>• Service-level agreement (SLA)<br>• Master service agreement (MSA)<br>• Non-disclosure agreement (NDA)<br>• Memorandum of understanding (MOU)<br>• Interconnection security agreement (ISA)<br>• Operational-level agreement<br>• Privacy-level agreement |
| Explain the importance of business continuity and disaster recovery concepts. | - Business impact analysis<br>• Recovery point objective<br>• Recovery time objective<br>• Recovery service level<br>• Mission essential functions<br>- Privacy impact assessment<br>- Disaster recovery plan (DRP)/business continuity plan (BCP)<br>• Cold site<br>• Warm site<br>• Hot site |

| Topic | Details |
|---|---|
| | • Mobile site<br>- Incident response plan<br>• Roles/responsibilities<br>• After-action reports<br>- Testing plans<br>• Checklist<br>• Walk-through<br>• Tabletop exercises<br>• Full interruption test<br>• Parallel test/simulation test |

# CompTIA CAS-004 Sample Questions:

## Question: 1

In a large enterprise, e-discovery is best handled via which of the following?(c)

a) A separate department
b) Outsourcing
c) Specialty appliances
d) Large in-house legal staff

**Answer: c**

## Question: 2

Geolocation data would most likely be found in which of the following?

a) Word documents
b) Photographs
c) PDFsSpreadsheets
d) Spreadsheets

**Answer: b**

## Question: 3

A junior administrator at a sister company called to report a possible exposed private key that is used for PKI transactions. The administrator would like to know the easiest way to check whether the lost key has been flagged by the system.

What are you going to recommend to the administrator?

a) Hashing
b) Issuance to entities
c) Online Certificate Status Protocol
d) Wildcard verification

**Answer: c**

## Question: 4

Which of the following best describes augmented reality?

a) Users' perception of their real-world environment is completely replaced by a digital reality.
b) Users' perception of their real-world environment is enhanced by digital elements.
c) Users' devices and appliances are all networked together, forming a smart home.
d) Users' devices and appliances are all networked together, forming a smart business.

**Answer: b**

## Question: 5

When reviewing a cloud services contract, which provisions should you consider regarding the storage and handling of sensitive data?

a) Encryption of data at rest
b) Separation of data from other organizations
c) Encryption of data in transit
d) All of the above

**Answer: d**

## Question: 6

A common multitier network architecture might consist of which of the following layers?

a) DMZ, SAN, and VLAN tier
b) DMZ, application tier, and data tier
c) NAS, DMZ, and data tier
d) Public tier, private tier, and FMZ

**Answer: b**

## Question: 7

You have just run a tool that has identified the targeted operating system as Microsoft Windows 10. What step has occurred?

a) Port scanning
b) OS fingerprinting
c) Footprinting
d) Vulnerability scanning

**Answer: b**

## Question: 8

You are testing an application for arithmetic errors. What is your best tool?

a) Fault injection
b) A fuzzing framework
c) Code walkthroughs
d) Use of specific library calls for math functions

**Answer: b**

## Question: 9

A hacker gains unauthorized access to your system and deletes data. This is an example of what type of failure?

a) Confidentiality
b) Availability
c) Authorization
d) Integrity

**Answer: d**

Question: 10

______________ are tactical documents that specify steps or processes required to meet a certain requirement.

a) Procedures
b) Guidelines
c) Baselines
d) Standards

**Answer: d**

# Study Guide to Crack CompTIA CASP+ CAS-004 Exam:

- Getting details of the CAS-004 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-004 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-004 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-004 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-004 practice tests is must. Continuous practice will make you an expert in all syllabus areas.

## Reliable Online Practice Test for CAS-004 Certification

Make EduSum.com your best friend during your CompTIA Advanced Security Practitioner exam preparation. We provide authentic practice tests for the CAS-004 exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual CAS-004 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-004 exam.

**Start Online practice of CAS-004 Exam by visiting URL**
**https://www.edusum.com/comptia/cas-004-comptia-advanced-security-practitioner**