COMPTIA CAS-003

CompTIA CASP+ Certification Questions & Answers

Exam Summary – Syllabus –Questions

CAS-003
CompTIA Advanced Security Practitioner (CASP+)
90 Questions Exam – Duration of 165 minutes

Table of Contents:

Know Your CAS-003 Certification Well:

The CAS-003 is best suitable for candidates who want to gain knowledge in the CompTIA Cybersecurity. Before you start your CAS-003 preparation you may struggle to get all the crucial CASP+ materials like CAS-003 syllabus, sample questions, study guide.

But don't worry the CAS-003 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-003 syllabus?
- How many questions are there in the CAS-003 exam?
- Which Practice test would help me to pass the CAS-003 exam at the first attempt?

Passing the CAS-003 exam makes you CompTIA Advanced Security Practitioner (CASP+). 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-003 CASP+ Certification Details:

Exam Name	CompTIA Advanced Security Practitioner (CASP+)
Exam Code	CAS-003
Exam Price	$466 (USD)
Duration	165 mins
Number of Questions	90
Passing Score	Pass / Fail
Book / Training	**CASP+ CAS-003**
Schedule Exam	**Pearson VUE**
Sample Questions	**CompTIA CASP+ Sample Questions**
Practice Exam	**CompTIA CAS-003 Certification Practice Exam**

CAS-003 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 2. New or changing business models/strategies 1. Partnerships 2. Outsourcing 3. Cloud 4. Acquisition/merger – divestiture/demerger Data ownership Data reclassification 3. Security concerns of integrating diverse industries 1. Rules 2. Policies 3. Regulations Export controls Legal requirements 4. Geography Data sovereignty Jurisdictions 4. Internal and external influences 1. Competitors 2. Auditors/audit findings 3. Regulatory entities 4. Internal and external client requirements 5. Top-level management 5. Impact of de-perimeterization (e.g., constantly changing network boundary) 1. Telecommuting 2. Cloud 3. Mobile 4. BYOD 5. Outsourcing 6. Ensuring third-party providers have requisite levels of information security

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

Topic	Details
	11. Information classification
Given a scenario, execute risk mitigation strategies and controls.	1. Categorize data types by impact levels based on CIA 2. Incorporate stakeholder input into CIA impact-level decisions 3. Determine minimum-required security controls based on aggregate score 4. Select and implement controls based on CIA requirements and organizational policies 5. Extreme scenario planning/ worst-case scenario 6. Conduct system-specific risk analysis 7. Make risk determination based upon known metrics 1. Magnitude of impact based on ALE and SLE 2. Likelihood of threat Motivation Source ARO Trend analysis 3. Return on investment (ROI) 4. Total cost of ownership 8. Translate technical risks in business terms 9. Recommend which strategy should be applied based on risk appetite 1. Avoid 2. Transfer 3. Mitigate 4. Accept 10. Risk management processes 1. Exemptions 2. Deterrence 3. Inherent 4. Residual 11. Continuous improvement/monitoring 12. Business continuity planning 1. RTO 2. RPO 3. MTTR

Topic	Details
	4. MTBF 13. IT governance 1. Adherence to risk management frameworks 14. Enterprise resilience
Analyze risk metric scenarios to secure the enterprise.	1. Review effectiveness of existing security controls 1. Gap analysis 2. Lessons learned 3. After-action reports 2. Reverse engineer/deconstruct existing solutions 3. Creation, collection and analysis of metrics 1. KPIs 2. KRIs 4. Prototype and test multiple solutions 5. Create benchmarks and compare to baselines 6. Analyze and interpret trend data to anticipate cyber defense needs 7. Analyze security solution metrics and attributes to ensure they meet business needs 1. Performance 2. Latency 3. Scalability 4. Capability 5. Usability 6. Maintainability 7. Availability 8. Recoverability 9. ROI 10. TCO 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,	1. Physical and virtual network and security devices 1. UTM

Topic	Details
concepts and architectures to meet security requirements.	2. IDS/IPS 3. NIDS/NIPS 4. INE 5. NAC 6. SIEM 7. Switch 8. Firewall 9. Wireless controller 10. Router 11. Proxy 12. Load balancer 13. HSM 14. MicroSD HSM 2. Application and protocol-aware technologies 1. WAF 2. Firewall 3. Passive vulnerability scanners 4. DAM 3. Advanced network design (wired/wireless) 1. Remote access VPN IPSec SSL/TLS SSH RDP VNC VDI Reverse proxy 2. IPv4 and IPv6 transitional technologies 3. Network authentication methods 4. 802.1x 5. Mesh networks 6. Placement of fixed/mobile devices 7. Placement of hardware and applications 4. Complex network security solutions for data flow 1. DLP 2. Deep packet inspection 3. Data flow enforcement 4. Network flow (S/flow) 5. Data flow diagram

Topic	Details
	5. Secure configuration and baselining of networking and security components 6. Software-defined networking 7. Network management and monitoring tools 1. Alert definitions and rule writing 2. Tuning alert thresholds 3. Alert fatigue 8. Advanced configuration of routers, switches and other network devices 1. Transport security 2. Trunking security 3. Port security 4. Route protection 5. DDoS protection 6. Remotely triggered black hole 9. Security zones 1. DMZ 2. Separation of critical assets 3. Network segmentation 10. Network access control 1. Quarantine/remediation 2. Persistent/volatile or non-persistent agent 3. Agent vs. agentless 11. Network-enabled devices 1. System on a chip (SoC) 2. Building/home automation systems 3. IP video 4. HVAC controllers 5. Sensors 6. Physical access control systems 7. A/V systems 8. Scientific/industrial equipment 12. Critical infrastructure 1. Supervisory control and data acquisition (SCADA) 2. Industrial control systems (ICS)

Topic	Details
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) 1. SELinux 2. SEAndroid 3. TrustedSolaris 4. Least functionality 2. Endpoint security software 1. Anti-malware 2. Antivirus 3. Anti-spyware 4. Spam filters 5. Patch management 6. HIPS/HIDS 7. Data loss prevention 8. Host-based firewalls 9. Log monitoring 10. Endpoint detection response 3. Host hardening 1. Standard operating environment/ configuration baselining Application whitelisting and blacklisting 2. Security/group policy implementation 3. Command shell restrictions 4. Patch management Manual Automated Scripting and replication 5. Configuring dedicated interfaces Out-of-band management ACLs Management interface Data interface 6. External I/O restrictions USB Wireless Bluetooth NFC IrDA RF 802.11 RFID Drive mounting Drive mapping

Topic	Details
	Webcam Recording mic Audio output SD port HDMI port 7. File and disk encryption 8. Firmware updates 4. Boot loader protections 1. Secure boot 2. Measured launch 3. Integrity measurement architecture 4. BIOS/UEFI 5. Attestation services 6. TPM 5. Vulnerabilities associated with hardware 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 1. Containerization 2. Configuration profiles and payloads 3. Personally owned, corporate-enabled 4. Application wrapping 5. Remote assistance access VNC Screen mirroring 6. Application, content and data management 7. Over-the-air updates (software/firmware) 8. Remote wiping 9. SCEP 10. BYOD 11. COPE 12. VPN 13. Application permissions 14. Side loading 15. Unsigned apps/system apps 16. Context-aware management Geolocation/geofencing User behavior Security restrictions Time-based restrictions 2. Security implications/privacy concerns

Topic	Details
	1. Data storage Non-removable storage Removable storage Cloud storage Transfer/backup data to uncontrolled storage 2. USB OTG 3. Device loss/theft 4. Hardware anti-tamper eFuse 5. TPM 6. Rooting/jailbreaking 7. Push notification services 8. Geotagging 9. Encrypted instant messaging apps 10. Tokenization 11. OEM/carrier Android fragmentation 12. Mobile payment NFC-enabled Inductance-enabled Mobile wallet Peripheral-enabled payments (credit card reader) 13. Tethering USB Spectrum management Bluetooth 3.0 vs. 4.1 14. Authentication Swipe pattern Gesture Pin code Biometric Facial Fingerprint Iris scan 15. Malware 16. Unauthorized domain bridging 17. Baseband radio/SOC 18. Augmented reality 19. SMS/MMS/messaging 3. Wearable technology 1. Devices Cameras Watches Fitness devices Glasses

Topic	Details
	Medical sensors/devices Headsets 2. Security implications Unauthorized remote activation/ deactivation of devices or features Encrypted and unencrypted communication concerns Physical reconnaissance Personal data theft Health privacy Digital forensics of collected data
Given software vulnerability scenarios, select appropriate security controls.	1. Application security design considerations 1. Secure: by design, by default, by deployment 2. Specific application issues 1. Unsecure direct object references 2. XSS 3. Cross-site request forgery (CSRF) 4. Click-jacking 5. Session management 6. Input validation 7. SQL injection 8. Improper error and exception handling 9. Privilege escalation 10. Improper storage of sensitive data 11. Fuzzing/fault injection 12. Secure cookie storage and transmission 13. Buffer overflow 14. Memory leaks 15. Integer overflows 16. Race conditions Time of check Time of use 17. Resource exhaustion 18. Geotagging 19. Data remnants 20. Use of third-party libraries 21. Code reuse 3. Application sandboxing 4. Secure encrypted enclaves 5. Database activity monitor 6. Web application firewalls 7. Client-side processing vs. server-side processing

Topic	Details
	1. JSON/REST 2. Browser extensions ActiveX Java applets 3. HTML5 4. AJAX 5. SOAP 6. State management 7. JavaScript 8. Operating system vulnerabilities 9. Firmware vulnerabilities
Enterprise Security Operations 20%	
Given a scenario, conduct a security assessment using the appropriate methods.	1. Methods 1. Malware sandboxing 2. Memory dumping, runtime debugging 3. Reconnaissance 4. Fingerprinting 5. Code review 6. Social engineering 7. Pivoting 8. Open source intelligence Social media Whois Routing tables DNS records Search engines 2. Types 1. Penetration testing Black box White box Gray box 2. Vulnerability assessment 3. Self-assessment Tabletop exercises 4. Internal and external audits 5. Color team exercises Red team Blue team White team

Topic	Details
Analyze a scenario or output, and select the appropriate tool for a security assessment.	1. Network tool types 1. Port scanners 2. Vulnerability scanners 3. Protocol analyzer Wired Wireless 4. SCAP scanner 5. Network enumerator 6. Fuzzer 7. HTTP interceptor 8. Exploitation tools/frameworks 9. Visualization tools 10. Log reduction and analysis tools 2. Host tool types 1. Password cracker 2. Vulnerability scanner 3. Command line tools 4. Local exploitation tools/frameworks 5. SCAP tool 6. File integrity monitoring 7. Log analysis tools 8. Antivirus 9. Reverse engineering tools 3. Physical security tools 1. Lock picks 2. RFID tools 3. IR camera
Given a scenario, implement incident response and recovery procedures.	1. E-discovery 1. Electronic inventory and asset control 2. Data retention policies 3. Data recovery and storage 4. Data ownership 5. Data handling 6. Legal holds 2. Data breach 1. Detection and collection Data analytics

Topic	Details
	2. Mitigation Minimize Isolate 3. Recovery/reconstitution 4. Response 5. Disclosure 3. Facilitate incident detection and response 1. Hunt teaming 2. Heuristics/behavioral analytics 3. Establish and review system, audit and security logs 4. Incident and emergency response 1. Chain of custody 2. Forensic analysis of compromised system 3. Continuity of operations 4. Disaster recovery 5. Incident response team 6. Order of volatility 5. Incident response support tools 1. dd 2. tcpdump 3. nbtstat 4. netstat 5. nc (Netcat) 6. memdump 7. tshark 8. foremost 6. Severity of incident or breach 1. Scope 2. Impact 3. Cost 4. Downtime 5. Legal ramifications 7. Post-incident response 1. Root-cause analysis 2. Lessons learned 3. After-action report

Topic	Details
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 2. Standards 1. Open standards 2. Adherence to standards 3. Competing standards 4. Lack of standards 5. De facto standards 3. Interoperability issues 1. Legacy systems and software/current systems 2. Application requirements 3. Software types In-house developed Commercial Tailored commercial Open source 4. Standard data formats 5. Protocols and APIs 4. Resilience issues 1. Use of heterogeneous components 2. Course of action automation/orchestration 3. Distribution of critical assets 4. Persistence and non- persistence of data 5. Redundancy/high availability 6. Assumed likelihood of attack 5. Data security considerations 1. Data remnants 2. Data aggregation 3. Data isolation 4. Data ownership 5. Data sovereignty 6. Data volume 6. Resources provisioning and deprovisioning 1. Users 2. Servers 3. Virtual devices

Topic	Details
	4. Applications 5. Data remnants 7. Design considerations during mergers, acquisitions and demergers/divestitures 8. Network secure segmentation and delegation 9. Logical deployment diagram and corresponding physical deployment diagram of all relevant devices 10. Security and privacy considerations of storage integration 11. Security implications of integrating enterprise applications 1. CRM 2. ERP 3. CMDB 4. CMS 5. Integration enablers Directory services DNS SOA ESB
Given a scenario, integrate cloud and virtualization technologies into a secure enterprise architecture.	1. Technical deployment models (outsourcing/insourcing/ managed services/partnership) 1. Cloud and virtualization considerations and hosting options Public Private Hybrid Community Multi-tenancy Single tenancy 2. On-premise vs. hosted 3. Cloud service models SaaS IaaS PaaS 2. Security advantages and disadvantages of virtualization 1. Type 1 vs. Type 2 hypervisors 2. Container-based 3. vTPM 4. Hyperconverged infrastructure 5. Virtual desktop infrastructure

Topic	Details
	6. Secure enclaves and volumes 3. Cloud augmented security services 1. Anti-malware 2. Vulnerability scanning 3. Sandboxing 4. Content filtering 5. Cloud security broker 6. Security as a service 7. Managed security service providers 4. Vulnerabilities associated with comingling of hosts with different security requirements 1. VMEscape 2. Privilege elevation 3. Live VM migration 4. Data remnants 5. Data security considerations 1. Vulnerabilities associated with a single server hosting multiple data types 2. Vulnerabilities associated with a single platform hosting multiple data types/owners on multiple virtual machines 6. Resources provisioning and deprovisioning 1. Virtual devices 2. Data remnants
Given a scenario, integrate and troubleshoot advanced authentication and authorization technologies to support enterprise security objectives.	1. Authentication 1. Certificate-based authentication 2. Single sign-on 3. 802.1x 4. Context-aware authentication 5. Push-based authentication 2. Authorization 1. OAuth 2. XACML

Topic	Details
	3. SPML 3. Attestation 4. Identity proofing 5. Identity propagation 6. Federation 1. SAML 2. OpenID 3. Shibboleth 4. WAYF 7. Trust models 1. RADIUS configurations 2. LDAP 3. AD
Given a scenario, implement cryptographic techniques.	1. Techniques 1. Key stretching 2. Hashing 3. Digital signature 4. Message authentication 5. Code signing 6. Pseudo-random number generation 7. Perfect forward secrecy 8. Data-in-transit encryption 9. Data-in-memory/processing 10. Data-at-rest encryption Disk Block File Record 11. Steganography 2. Implementations 1. Crypto modules 2. Crypto processors 3. Cryptographic service providers 4. DRM 5. Watermarking 6. GPG 7. SSL/TLS 8. SSH 9. S/MIME

Topic	Details
	10. Cryptographic applications and proper/improper implementations Strength Performance Feasibility to implement Interoperability 11. Stream vs. block 12. PKI Wild card OCSP vs. CRL Issuance to entities Key escrow Certificate Tokens Stapling Pinning 13. Cryptocurrency/blockchain 14. Mobile device encryption considerations 15. Elliptic curve cryptography 16. P-256 vs. P-384 vs. P521
Given a scenario, select the appropriate control to secure communications and collaboration solutions.	1. Remote access 1. Resource and services 2. Desktop and application sharing 3. Remote assistance 2. Unified collaboration tools 1. Conferencing Web Video Audio 2. Storage and document collaboration tools 3. Unified communication 4. Instant messaging 5. Presence 6. Email 7. Telephony and VoIP integration 8. Collaboration sites Social media Cloud-based

Topic	Details
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 1. Best practices 2. New technologies, security systems and services 3. Technology evolution (e.g., RFCs, ISO) 2. Threat intelligence 1. Latest attacks 2. Knowledge of current vulnerabilities and threats 3. Zero-day mitigation controls and remediation 4. Threat model 3. Research security implications of emerging business tools 1. Evolving social media platforms 2. Integration within the business 3. Big Data 4. AI/machine learning 4. Global IA industry/community 1. Computer emergency response team (CERT) 2. Conventions/conferences 3. Research consultants/vendors 4. Threat actor activities 5. Emerging threat sources
Given a scenario, implement security activities across the technology life cycle.	1. Systems development life cycle 1. Requirements 2. Acquisition 3. Test and evaluation 4. Commissioning/decommissioning 5. Operational activities Monitoring Maintenance Configuration and change management 6. Asset disposal 7. Asset/object reuse 2. Software development life cycle

Topic	Details
	1. Application security frameworks 2. Software assurance Standard libraries Industry-accepted approaches Web services security (WS-security) Forbidden coding techniques NX/XN bit use ASLR use Code quality Code analyzers Fuzzer Static Dynamic 3. Development approaches DevOps Security implications of agile, waterfall and spiral software development methodologies Continuous integration Versioning 4. Secure coding standards 5. Documentation Security requirements traceability matrix (SRTM) Requirements definition System design document Testing plans 6. Validation and acceptance testing Regression User acceptance testing Unit testing Integration testing Peer review 3. Adapt solutions to address: 1. Emerging threats 2. Disruptive technologies 3. Security trends 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 1. Sales staff 2. Programmer 3. Database administrator 4. Network administrator

Topic	Details
	5. Management/executive management 6. Financial 7. Human resources 8. Emergency response team 9. Facilities manager 10. Physical security manager 11. Legal counsel 2. Provide objective guidance and impartial recommendations to staff and senior management on security processes and controls 3. Establish effective collaboration within teams to implement secure solutions 4. Governance, risk and compliance committee

CompTIA CAS-003 Sample Questions:

Question: 1

A power outage is caused by a severe thunderstorm and a facility is on generator power. The CISO decides to activate a plan and shut down non-critical systems to reduce power consumption.

Which of the following is the CISO activating to identify critical systems and the required steps?

a) BIA
b) CERT
c) IRP
d) COOP

Answer: c

Question: 2

Which of the following describes a contract that is used to define the various levels of maintenance to be provided by an external business vendor in a secure environment?

a) NDA
b) MOU
c) BIA
d) SLA

Answer: d

Question: 3

During the decommissioning phase of a hardware project, a security administrator is tasked with ensuring no sensitive data is released inadvertently.

All paper records are scheduled to be shredded in a crosscut shredder, and the waste will be burned. The system drives and removable media have been removed prior to e-cycling the hardware.

Which of the following would ensure no data is recovered from the system drives once they are disposed of?

a) Overwriting all HDD blocks with an alternating series of data
b) Physically disabling the HDDs by removing the drive head
c) Demagnetizing the hard drive using a degausser
d) Deleting the UEFI boot loaders from each HDD

Answer: c

Question: 4

The Chief Information Security Officer (CISO) is concerned that certain systems administrators with privileged access may be reading other users' emails. Review of a tool's output shows the administrators have used web mail to log into other users' inboxes.

Which of the following tools would show this type of output?

a) Log analysis tool
b) Password cracker
c) Command-line tool
d) File integrity monitoring tool

Answer: a

Question: 5

Which of the following is the GREATEST security concern with respect to BYOD?

a) The filtering of sensitive data out of data flows at geographic boundaries.
b) Removing potential bottlenecks in data transmission paths.
c) The transfer of corporate data onto mobile corporate devices.
d) The migration of data into and out of the network in an uncontrolled manner.

Answer: d

Question: 6

A pharmaceutical company is considering moving its technology operations from on-premises to externally-hosted to reduce costs while improving security and resiliency.

These operations contain data that includes the prescription records, medical doctors' notes about treatment options, and the success rates of prescribed drugs.

The company wants to maintain control over its operations because many custom applications are in use.

Which of the following options represent the MOST secure technical deployment options?

(Select THREE).

a) Single tenancy
b) Multi-tenancy
c) Community
d) Public
e) Private
f) Hybrid
g) Saas
h) Iaas
i) Paas

Answer: a, e, h

Question: 7

A Chief Information Security Officer (CISO) is reviewing the controls in place to support the organization’s vulnerability management program. The CISO finds patching and vulnerability scanning policies and procedures are in place.
However, the CISO is concerned the organization is siloed and is not maintaining awareness of new risks to the organization. The CISO determines systems administrators need to participate in industry security events.

Which of the following is the CISO looking to improve?

a) Vendor diversification
b) System hardening standards
c) Bounty programs
d) Threat awareness
e) Vulnerability signatures

Answer: d

Question: 8

During a security assessment, activities were divided into two phases: internal and external exploitation. The security assessment team set a hard time limit on external activities before moving to a compromised box within the enterprise perimeter.

Which of the following methods is the assessment team most likely to employ NEXT?

a) Pivoting from the compromised, moving laterally through the enterprise, and trying to exfiltrate data and compromise devices.
b) Conducting a social engineering attack attempt with the goal of accessing the compromised box physically.
c) Exfiltrating network scans from the compromised box as a precursor to social media reconnaissance
d) Open-source intelligence gathering to identify the network perimeter and scope to enable further system compromises.

Answer: a

Question: 9

While attending a meeting with the human resources department, an organization's information security officer sees an employee using a username and password written on a memo pad to log into a specific service.

When the information security officer inquires further as to why passwords are being written down, the response is that there are too many passwords to remember for all the different services the human resources department is required to use.

Additionally, each password has specific complexity requirements and different expiration time frames.

Which of the following would be the BEST solution for the information security officer to recommend?

a) Utilizing MFA
b) Implementing SSO
c) Deploying 802.1X
d) Pushing SAML adoption
e) Implementing TACACS

Answer: b

Question: 10

A security engineer is managing operational, excess, and available equipment for a customer. Three pieces of expensive leased equipment, which are supporting a highly confidential portion of the customer network, have recently been taken out of operation. The engineer determines the equipment lease runs for another 18 months.

Which of the following is the BEST course of action for the engineer to take to decommission the equipment properly?

a) Remove any labeling indicating the equipment was used to process confidential data and mark it as available for reuse.
b) Return the equipment to the leasing company and seek a refund for the unused time.
c) Redeploy the equipment to a less sensitive part of the network until the lease expires.
d) Securely wipe all device memory and store the equipment in a secure location until the end of the lease.

Answer: d

Study Guide to Crack CompTIA CASP+ CAS-003 Exam:

- Getting details of the CAS-003 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-003 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-003 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-003 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-003 practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for CAS-003 Certification

Make EduSum.com your best friend during your CompTIA Advanced Security Practitioner exam preparation. We provide authentic practice tests for the CAS-003 exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual CAS-003 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-003 exam.

Start Online practice of CAS-003 Exam by visiting URL
https://www.edusum.com/comptia/cas-003-comptia-advanced-security-practitioner