Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

CISSP MCQs
CISSP Exam Questions
CISSP Practice Test
CISSP TestPrep
CISSP Study Guide

PASS

killexams.com

ISC2

CISSP

Certified Information Systems Security Professional

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/CISSP

Question 1483

A security engineer is evaluating the strength of a symmetric encryption implementation. If the work factor to brute-force a key is represented as [2^n], where [n] is the key length, what is the impact on the security margin if the organization transitions from AES-128 to AES-256 in the context of Grover's algorithm?

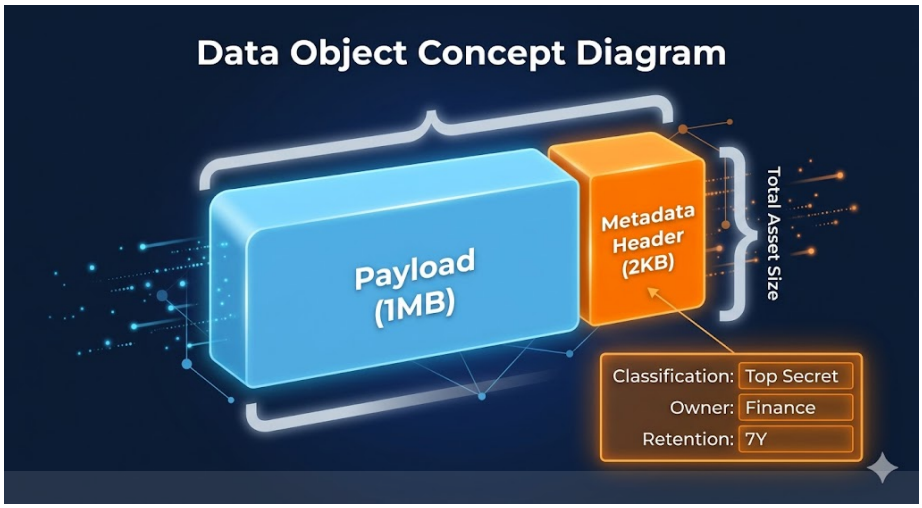
A. The effective security is doubled from 128 to 256 bits
B. The effective security remains significantly higher than RSA-2048
C. The effective security remains exactly the same
D. The effective security increases from 64 bits to 128 bits

Answer: D

Explanation: Grover's algorithm provides a quadratic speedup for quantum computers performing exhaustive key searches on symmetric ciphers. This effectively halves the bit-strength of the algorithm. Moving from AES-128 to AES-256 restores the security margin to a level equivalent to 128 bits of classical security, which is considered robust against quantum-enabled adversaries.

Question 1484

A security engineer is calculating the total storage overhead required to implement a robust data labeling and tagging system for a repository of [10^6] objects. Each object is [$1MB$] in size. The tagging system requires a fixed metadata header of [$2KB$] per object to support mandatory access control (MAC) and automated DLP scanning. What is the total size of the metadata that must be managed as part of the asset security strategy?



A. $200MB$ **B.** $500MB$ **C.** $20GB$ **D.** $2GB$

Answer: D

Explanation: The calculation is as follows: [$1,000,000 \text{ objects} \times 2,000 \text{ bytes per object} = 2,000,000,000 \text{ bytes}$]. To convert this to Gigabytes (using the standard decimal 10^9 for storage context), [$2,000,000,000 / 1,000,000,000 = 2GB$]. Managing asset security requires accounting for this metadata overhead, as it must be indexed, protected with the same integrity controls as the payload, and maintained throughout the data lifecycle. Inaccurate estimates of metadata size can lead to performance degradation in DLP systems and CASB solutions that must parse these headers in real-time.

Question 1485

When designing a wireless network for a warehouse, the engineer chooses to implement 802.11ax (Wi-Fi 6) over 802.11ac. Which specific security enhancement is a mandatory requirement for Wi-Fi 6 certification that improves protection against offline dictionary attacks?

A. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)

B. Temporal Key Integrity Protocol (TKIP)

C. Pre-Shared Key (PSK) with 256-bit AES

D. Simultaneous Authentication of Equals (SAE)

Answer: D

Explanation: Wi-Fi 6 (802.11ax) requires WPA3 certification. WPA3 replaces the vulnerable PSK 4-way handshake with Simultaneous Authentication of Equals (SAE), which is resistant to offline dictionary attacks and provides forward secrecy.

Question 1486

A security administrator is tasked with selecting a sanitization method for a decommissioned magnetic tape library that contained highly classified government intelligence. The tapes will be sold at an auction. Which NIST-recognized method provides the highest level of assurance that data cannot be recovered by laboratory techniques?

A. Compaction

B. Purging

C. Degaussing

D. Clearing

Answer: B

Explanation: Purging is the correct answer as it is a level of sanitization that protects against "Laboratory Attack" (robust data recovery attempts). For magnetic media, purging can be achieved through degaussing with a sufficiently strong magnetic field or through specific multiple-pass overwriting (though degaussing is generally preferred for tapes). "Clearing" only protects against simple non-invasive data

recovery techniques. "Compaction" is a storage optimization technique, not a sanitization method. While degaussing is the *action* used to purge magnetic media, "Purging" is the standard category of sanitization required for media leaving organizational control.

Question 1487

A company is installing a fire detection system. They need a sensor that is highly sensitive and can detect a fire in its earliest "incipient" stage, before visible smoke or flames are present. Which type of detector should be selected?

A. Ionization smoke detector
B. Rate-of-rise heat detector
C. Fixed-temperature heat detector
D. Photoelectric smoke detector

Answer: A

Explanation: Ionization detectors are generally more sensitive to the small, invisible particles produced by "fast-flaming" fires or the incipient stage of a fire. Photoelectric detectors are better for "smoldering" fires with larger visible smoke particles. Heat detectors (fixed or rate-of-rise) only trigger after a significant temperature change, which usually occurs well after the fire has started.

Question 1488

During the "Lessons Learned" phase of a disaster recovery exercise, it was noted that the "Emergency Management" team failed to notify the regulatory body within the required 24-hour window because the compliance officer's contact information

was only stored on the internal Wiki, which was offline. This highlights a failure in which BCP/DRP component?

A. The communication plan
B. Off-site distribution of the plan
C. Personnel training and awareness
D. Assessment and restoration

Answer: B

Explanation: A fundamental requirement of BCP/DRP is that the plan (and all contact lists) must be available even if the primary IT infrastructure is unavailable. Hard copies or "out-of-band" digital copies (e.g., encrypted cloud storage or offline mobile devices) must be maintained.

Question 1489

During asset inventory automation, a bank's system flags 5,000 untagged databases. Tagging policy uses criticality scores. What formula BEST determines initial classification? Assume impact values: High=3, Medium=2, Low=1.

A. $[\text{Classification} = \max(\text{BIA Impact}, \text{Regulatory Level})]$ **B.** $[\text{Classification} = \sum(\text{Impact} \times \text{Volume in GB})]$ **C.** $[\text{Classification} = \text{Average}(\text{User Access Levels})]$ **D.** $[\text{Classification} = \text{Count}(\text{Access Logs per Day})]$

Answer: A

Explanation: Classification prioritizes highest risk driver—BIA impact or regulatory mandates—ensuring critical assets receive appropriate handling regardless of volume or usage metrics.

Question 1490

A security architect is reviewing an application that handles sensitive PII. The code shows that the application logs the full credit card number and CVV to a local text file for debugging purposes. Which secure coding principle is being violated?

A. Segregation of Duties
B. Availability
C. Least Privilege
D. Proper Error Handling

Answer: D

Explanation: Secure coding guidelines strictly prohibit the logging of sensitive information (like full PANs or CVVs). Secure logging requires that logs contain enough information for auditing and troubleshooting without creating a new repository of sensitive data that could be exploited if the log files are accessed by unauthorized parties.

Question 1491

Which of the following scenarios best illustrates the concept of "Separation of Duties" in an IAM lifecycle?

A. The person who creates a new user account cannot be the person who assigns permissions to that account
B. A system administrator uses one account for daily email and a separate account for server maintenance
C. The Policy Decision Point and the Policy Enforcement Point reside on different physical servers
D. Users must provide both a password and a fingerprint to access the data center

Answer: A

Explanation: Separation of Duties (SoD) is a security principle that requires more than one person to complete a critical task to prevent fraud or error. In IAM, if one person can both create an identity and assign its privileges, they could create "ghost accounts" with administrative rights. Dividing these tasks ensures that no single individual has total control over the provisioning process.

Question 1492

When configuring a CI/CD pipeline, why is it important to use "Immutable Build Artifacts"?

A. It allows the build server to use less disk space by overwriting old artifacts
B. It prevents the use of version control for the application's source code
C. It ensures that the code can be modified easily even after it has been deployed
D. It ensures that the exact same binary that was tested in staging is the one deployed to production

Answer: D

Explanation: Immutability means the artifact (e.g., a Docker image or a JAR file) does not change after it is created. This ensures consistency across environments. If you test "version 1.0" in staging and then re-build "version 1.0" for production, there is a risk that a dependency or environment change could result in a different, untested binary. Immutable artifacts mitigate this risk.

Question 1493

A developer is using a serverless architecture where functions are triggered by asynchronous events. The security architect is concerned about "Function-Level Over-Privilege." Which strategy is BEST for mitigating this risk while maintaining the scalability of the serverless model?

A. Deploying all functions within a single VPC subnet
B. Applying a single IAM role to all functions within the account
C. Creating granular execution roles for each individual function
D. Implementing a traditional firewall at the function perimeter

Answer: C

Explanation: Serverless security relies heavily on the principle of least privilege applied at the function level. By creating specific Identity and Access Management (IAM) roles for each function, the architect ensures that a compromise of one function does not grant the attacker access to resources required by other parts of the application.

Question 1494

An organization is calculating the risk of a legacy application that lacks input validation. The cost of a successful SQL injection attack is estimated at $250,000. The probability of an attack is estimated at 0.4 per year. The cost to implement a robust Change Management process and update the code is $40,000 per year. What is the Return on Security Investment (ROSI) for this control?

A. $[(\$250,000 \times 0.4) + \$40,000] / \$250,000 = 0.56$ **B.** $[(\$250,000 \times 0.4) - \$40,000] / \$40,000 = 1.5$ **C.** $\$40,000 / (\$250,000 \times 0.4) = 0.4$ **D.** $\$250,000 - (\$40,000 / 0.4) = \$150,000$

Answer: B

Explanation: The Return on Security Investment (ROSI) is calculated using the formula: $ROSI = [(ALE \times Mitigation Effectiveness) - Cost of Control] / Cost of Control$. Assuming the mitigation effectiveness is 100%, the Annualized Loss Expectancy (ALE) is $\$250,000 \times 0.4 = \$100,000$. Subtracting the cost of the control $(\$40,000)$ gives a net savings of $\$60,000$. Dividing this by the cost of the control $(\$40,000)$ results in a ROSI of 1.5 (or 150%).

Question 1495

In a multinational healthcare organization complying with HIPAA and GDPR, the Chief Medical Officer identifies patient records containing PHI as needing 10-year retention post-discharge. The IT Director implements backups and encryption, while a cloud vendor in Europe processes anonymized data subsets for analytics. During an audit, who bears ultimate accountability for classifying these records and approving their retention period?

A. Chief Medical Officer

B. Data processor

C. Cloud vendor

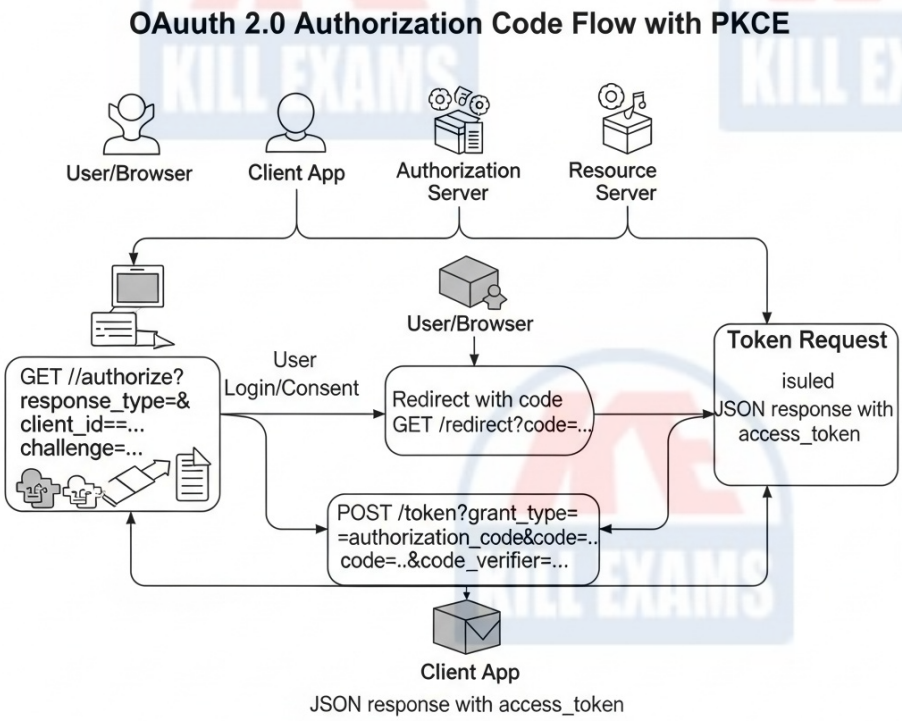
D. IT Director

Answer: A

Explanation: The Chief Medical Officer, as data owner, holds ultimate accountability for classifying patient records based on sensitivity and business needs, and for determining the retention period to meet regulatory requirements like HIPAA's 10-year standard for PHI. The IT Director functions as data custodian by handling technical protections such as backups and encryption but lacks authority over classification decisions. The cloud vendor acts as data processor, executing tasks like analytics on directed data subsets without owning classification or retention choices. Anonymization does not transfer accountability, as original records remain classified by the owner.

Question 1496

An organization is implementing a new API-first strategy for its SaaS platform. The development team has opted for an OAuth 2.0 implementation using the Authorization Code Grant flow with PKCE (Proof Key for Code Exchange). A security auditor is reviewing the message exchange to ensure it mitigates common API security threats.



Which of the following represents the most significant security failure in this specific implementation of the ecosystem?

A. Failure to use the Implicit Grant flow, which is more secure for modern single-page applications

B. Use of a public client without a client secret, rendering PKCE ineffective for the Authorization Server

C. Lack of transport layer security (TLS) for the transmission of the code verifier and tokens

D. Improperly configured CORS (Cross-Origin Resource Sharing) policies on the Resource Server

Answer: C

Explanation: In modern secure coding and API security, the Authorization Code Flow with PKCE is the gold standard for both public and confidential clients. However, its security rests entirely on the confidentiality of the tokens and the verifiers. Transmitting the 'code_verifier' or 'access_token' over an unencrypted HTTP connection (lack of TLS) exposes the application to person-in-the-middle (PITM) attacks and token theft. Even with PKCE, if the verifier is intercepted in transit, an attacker can complete the exchange. The Implicit Grant is actually deprecated and less secure. PKCE specifically exists to secure public clients that cannot maintain a client secret, so the lack of a secret is not the failure; the lack of encryption is.

Question 1497

An organization uses a Centralized Remote Access Service (RAS) and wants to implement a protocol that provides encrypted communication between the NAS and the daemon, while also separating the authentication, authorization, and accounting functions. Which protocol is the BEST choice?

A. TACACS+

B. RADIUS

C. LDAP

D. DIAMETER

Answer: A

Explanation: TACACS+ (Terminal Access Controller Access-Control System Plus) is a Cisco-proprietary protocol (though widely supported) that encrypts the entire body of the packet, whereas RADIUS only encrypts the password. Most importantly for this scenario, TACACS+ uses a modular architecture that strictly separates Authentication, Authorization, and Accounting (AAA), allowing for more granular control compared to RADIUS, which combines authentication and authorization.

Question 1498

A security operations center (SOC) analyst notices a high number of failed login attempts followed by a successful login from a different IP address for a high-level executive. The executive is currently on a business trip. What is the first priority for the analyst according to personnel safety and security best practices?

A. Disable the executive's account immediately to prevent further data loss.
B. Initiate a remote wipe of the executive’s laptop.
C. Contact the executive via a pre-verified out-of-band communication channel to verify their safety and status.
D. Reset the password and email the new credentials to the executive.

Answer: C

Explanation: In CISSP Domain 7, personnel safety is the top priority. A compromised account for a traveling executive could indicate "tiger-teaming" or a physical kidnapping/extortion attempt (duress). Before taking technical actions that might alert an adversary or leave the executive stranded without communications, the SOC must attempt to verify the executive's physical safety and whether they are

acting under duress.

Question 1499

In the context of Asset Security, which role is primarily responsible for determining the classification level of a dataset and defining the business requirements for its protection?

A. Data Owner
B. Privacy Officer
C. Custodian
D. System Administrator

Answer: A

Explanation: The Data Owner (or Information Owner) is typically a senior manager or executive who has ultimate responsibility for a specific set of data. Their duties include determining the initial classification of the data, periodically reviewing the classification, and defining the security requirements and business rules for the data's use. The Custodian (often IT or System Admin) is responsible for implementing the technical controls defined by the owner.

Question 1500

When assessing the security impact of "Commercial-off-the-shelf" (COTS) software, an organization discovers the product has reached its "End of Life" (EOL). What should be the primary security concern?

A. The immediate cessation of all functional features within the software

B. The software will no longer be compatible with the current version of Windows
C. A sudden increase in the licensing costs for the software
D. The loss of vendor support and the unavailability of future security patches

Answer: D

Explanation: The most critical security impact of EOL software is that the vendor no longer monitors for or remediates vulnerabilities. If a "zero-day" flaw is discovered in an EOL product, the organization will remain permanently vulnerable unless they have implemented compensating controls or replaced the software.

Question 1501

An organization is implementing an ingress/egress monitoring strategy at its network edge. They want to detect data exfiltration that utilizes DNS tunneling. Which observation would most likely indicate a DNS tunneling attempt is in progress?

A. Frequent DNS A-record lookups for the organization's own public web server
B. Large TXT or NULL records in DNS responses originating from an unknown external nameserver
C. A decrease in the total number of DNS packets sent during peak business hours
D. A high volume of DNS queries for common domains like google.com or office.com

Answer: B

Explanation: DNS tunneling encodes data within DNS queries and responses. Since standard A-records (IP lookups) are small, attackers often use TXT, SRV, or NULL records to carry the larger payloads required for exfiltration or command-and-control (C2) communication. Monitoring for unusually large DNS records or a high

frequency of subdomains for a single, suspicious domain is a key technique for detecting this type of egress violation.

Question 1502

A DevSecOps team is implementing Static Application Security Testing (SAST) within their GitLab CI pipeline. They find that the SAST tool is generating thousands of alerts, most of which are low-risk or irrelevant to the specific application context, causing "alert fatigue" among developers. What is the best strategy to improve the effectiveness of the assessment?

A. Tuning the SAST rulesets to match the specific framework and coding standards used by the team
B. Moving the SAST scan to a monthly manual process instead of an automated pipeline step
C. Configuring the SAST tool to only scan for "Critical" and "High" severity vulnerabilities
D. Replacing the SAST tool with a DAST tool to ensure only exploitable vulnerabilities are reported

Answer: A

Explanation: The most effective way to handle high volumes of false positives or irrelevant data in SAST is tuning. By refining the rulesets to ignore irrelevant patterns and focus on the specific frameworks (e.g., Spring, Django) and coding standards used by the developers, the tool becomes more accurate. Reducing the scope to only "High" might miss important "Medium" risks, and moving to a manual process loses the benefits of continuous integration. DAST and SAST are complementary, not interchangeable.

Question 1503

An organization utilizes a "Data Processor" to handle its payroll. The contract specifies that the processor must destroy all records within 90 days of contract termination. The processor uses a cloud-based backup service that keeps snapshots for 180 days. After the contract ends, the processor deletes the active records but the snapshots remain for the full 180 days. Is the processor in compliance?

A. Yes, because backup data is exempt from retention policies
B. No, because the snapshots constitute "data remanence" beyond the agreed 90-day window
C. No, because they did not use a degausser on the cloud storage
D. Yes, because the active production data was deleted within 90 days

Answer: B

Explanation: Data destruction requirements apply to all copies of the data, including backups and snapshots. If the contract mandates destruction within 90 days, the processor is responsible for ensuring that the data is unrecoverable from all media, including secondary storage, within that timeframe. Failure to clear backups is a common compliance gap in data lifecycle management.

Question 1504

Which of the following physical security controls is best suited to prevent "Tailgating" in a high-traffic entrance?

A. A sign that says "No Tailgating Allowed"
B. A revolving door or "Mantrap" (Optical turnstile)

C. A CCTV camera with AI-based facial recognition

D. An armed guard checking IDs at a desk

Answer: B

Explanation: A mantrap or specialized turnstiles are designed to allow only one person through at a time. While a guard can watch for tailgating, they can be distracted or social-engineered. A physical barrier like a mantrap provides a technical/physical control that enforces the "one person per authentication" rule.

Question 1505

A cloud service provider is negotiating a contract with a new enterprise client. The client requires a guarantee that the service will be available 99.99% of the time and specifies the financial penalties if the provider fails to meet this target. In which document should these specific uptime requirements and penalties be recorded?

A. Operational Level Agreement (OLA)

B. Business Impact Analysis (BIA)

C. Service Level Agreement (SLA)

D. Memorandum of Understanding (MOU)

Answer: C

Explanation: A Service Level Agreement (SLA) is a formal contract between a service provider and a customer that defines the expected level of service, including metrics like uptime, and the remedies or penalties if those levels are not achieved. While an OLA is an internal agreement, the SLA is the external, legally binding document.

Question 1506

A security engineer is configuring a SIEM to prioritize alerts. The engineer wants to use the "Risk Score" formula: $\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Impact}$. If a specific asset has a critical vulnerability (Value: 1.0) but is located in a segmented network with no external threat actors currently targeting it (Value: 0.1), and the business impact is high (Value: 10), what is the calculated risk score?

A. 11
B. 1.0
C. 1.1
D. 10

Answer: B

Explanation: Using the provided formula: $1.0(\text{Vulnerability}) \times 0.1(\text{Threat}) \times 10(\text{Impact}) = 1.0$. This demonstrates that even if a vulnerability is critical and the impact is high, the overall risk remains low if the threat is minimal or the asset is sufficiently isolated.

Question 1507

What is the primary difference between "Identification" and "Authentication" in the IAM lifecycle?

A. Identification uses "something you know," while Authentication uses "something you are."
B. Identification is the process of granting permissions; Authentication is the process of identifying the user.
C. Identification occurs after Authentication is successful.

D. Authentication is the process of proving a claimed identity; Identification is the claim itself.

Answer: D

Explanation: Identification is the act of a subject claiming an identity (e.g., entering a username). Authentication is the process of verifying that the claim is true (e.g., providing a password or biometric that matches the username). Identification must always precede authentication.

Question 1508

A company wants to implement a security control that prevents "Man-in-the-Middle" (MitM) attacks on their API communications. Which of the following is the most effective technical control?

A. Restricting API access to specific geographic locations
B. Implementing strong password complexity requirements
C. Requiring all API calls to use TLS 1.3 with Certificate Pinning
D. Using a CAPTCHA on the login page

Answer: C

Explanation: TLS 1.3 provides encryption and server authentication. Certificate Pinning adds an extra layer of security by telling the client to only trust a specific, pre-defined certificate or public key, preventing an attacker from using a fraudulent certificate issued by a compromised or rogue Certificate Authority (CA) to intercept the traffic.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Exam Questions Based on Current Exam Objectives

Killexams.com provides exam questions aligned with the latest official exam objectives and latest syllabus. Our content is reviewed and updated regularly to reflect recent changes announced by certification vendors. By studying these questions, candidates will become cover the structure, difficulty level, and topic coverage of the actual exam, helping them prepare more effectively and efficiently.

Comprehensive Exam MCQs (PDF Format)

Killexams.com offers multiple-choice questions (MCQs) in easy-to-read PDF format, covering all major domains of the exam. Each PDF contains a structured collection of questions and verified answers designed to support focused study. These MCQs help candidates reinforce key concepts, identify knowledge gaps, and improve exam readiness through consistent practice.

Realistic Practice Tests (Online & Desktop)

To support hands-on preparation, Killexams.com provides practice tests through both an Online Test Engine and a Desktop Exam Simulator. These tools are designed to simulate a real exam environment, allowing candidates to practice under exam-like conditions. Performance tracking, test history, and result analysis help users evaluate their progress and focus on areas that need improvement.

Risk-Free Purchase Policy

Killexams.com follows a transparent and customer-friendly purchase policy. If users are not satisfied with the study materials, they may request assistance or a refund in accordance with our published terms and conditions. This policy reflects our commitment to customer satisfaction, fairness, and confidence in our preparation resources.

Regularly Updated Content

Our question bank is reviewed and updated on an ongoing basis to stay aligned with the latest exam outlines and vendor updates. This ensures candidates are studying relevant material and preparing with content that reflects current exam expectations, helping them stay confident and well-prepared.