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

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

killexams.com

ISC2

ISSMP

Information Systems Security Management Professional

ORDER FULL VERSION

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

Question: 2115

An organization decides to transfer a cyber risk via cyber insurance as a treatment option. Which key factor should be included in the cost-benefit analysis to evaluate effectiveness of this treatment?

A. Hardware upgrade costs for firewalls and IDS
B. Insurance premium cost versus potential payout limits and deductibles
C. Employee training expenses for phishing awareness
D. Cost to patch all vulnerable systems

Answer: B

Explanation: Evaluating cyber insurance as a risk treatment requires analyzing premium costs against potential payouts, policy limits, and deductibles to understand net financial impact and residual risk. The other costs relate to different controls.

Question: 2116

In a 2026 metaverse platform, VR headset spoofing via WebXR (pose matrix tampering). ISSMP analyzes using STRIDE model (Spoofing threat). Which alternatives ALE<500k?

A. Biometric liveness detection (iris scan FAR=1e-6, SDK: Tobii API), ALE 300k
B. Blockchain identity verification (DID: did:ethr:0x..., verifiable credentials JWT), ALE 400k
C. Haptic feedback anomaly checks (vibration pattern mismatch threshold 0.1s), ALE 450k
D. Zero-knowledge proofs for pose (zk-SNARK circuit depth 20, Groth16 params), ALE 200k

Answer: A, B, D

Explanation: WebXR spoofing's STRIDE analysis prioritizes low-ALE alternatives. Iris biometrics reduce FAR for auth. DID blockchain verifies without exposure. ZKPs prove pose integrity. Haptics lack robustness.

Question: 2117

For a cloud-based application under development, which step best integrates security throughout the project lifecycle?

A. Use Infrastructure as Code (IaC) with embedded security baseline checks during deployment automation
B. Apply manual security reviews only after cloud infrastructure is fully deployed
C. Treat cloud security as an operational issue separate from development
D. Outsource all security testing to third-party consultants post-launch

Answer: A

Explanation: Embedding security baseline checks in automated IaC deployments integrates security early and continuously throughout deployment cycles, reducing risk and improving compliance. Manual reviews post-deployment or segregating security from development delays detection; outsourcing post-launch risks vulnerabilities.

Question: 2118

You are designing security architecture for a multi-tier application requiring compliance with encryption at rest and in transit. Which architectural component is essential to meet these security design requirements?

A. Centralized logging with unencrypted storage to speed retrieval times
B. Implementation of antivirus software on application servers only
C. Integration of a hardware security module (HSM) for key management and TLS for data in transit
D. Use of basic authentication protocols for user access management

Answer: C

Explanation: Hardware security modules provide secure key storage vital for encryption at rest, while TLS protocols secure data in transit. These components directly satisfy encryption requirements, unlike antivirus or unencrypted logging which don't address encryption needs, and basic authentication which lacks robust security.

Question: 2119

After a homomorphic encryption (HE) scheme flaw in a privacy-preserving analytics

platform leaks query patterns, lessons learned using FAIR v3.0 quantifies risk. Which calcs and processes must update the DRP for HE resilience?

A. Risk decomposition: Loss event frequency= Threat_event_freq × Vulnerability, e.g., 0.1/year × 0.7=0.07, Loss magnitude= (data_exposed × $100/record)=50K×100=$5M, Primary loss= LExV=0.07×5M=$350K/year, appending to DRP section 4.2 with trigger if >$100K.
B. Control effectiveness: TE= (avoided_loss / potential_loss) × 100=60%, recommending CKKS scheme upgrade: Microsoft SEAL library --scheme=ckks --scale=2^40 --levels=5, with noise audit <2^20.
C. Static DRP without risk updates.
D. Simulation integration: Monte Carlo 10K runs in Python: numpy.random.normal(mean_risk=350K, std=100K), plotting 95th percentile <$500K, embedding in DRP appendix B for annual review.

Answer: A, B, D

Explanation: FAIR decomps yield annualized losses, triggering DRP thresholds for proactive budgeting in analytics platforms. TE metrics validate scheme upgrades, SEAL params bounding noise for HE accuracy. Monte Carlo sims forecast tails, visualizing percentiles for review cycles, dynamically enhancing DRP over static versions ignoring evolving privacy risks.

Question: 2120

To enforce policy compliance in a change enabling serverless functions on AWS Lambda with API Gateway integrations for a logistics firm's tracking API, the ISSMP configures continuous monitoring. Which monitoring setups detect non-compliance with internal policies mandating least privilege IAM roles?

A. CloudWatch alarms on Lambda metrics (e.g., Errors >5/min) correlated with GuardDuty findings for privilege escalations, triggering Lambda@Edge for just-in-time role assumption
B. Enable AWS Config conformance packs for Lambda, checking policies against custom rules (e.g., no wildcard actions in role ARNs), with SNS notifications for drifts exceeding 1% deviation
C. Integrate Datadog agents for API Gateway logs, setting anomaly detection thresholds on 4xx errors indicative of auth failures, dashboarding compliance scores against policy KPIs like 95% success rate
D. Schedule AWS Security Hub insights quarterly, aggregating findings from Macie for

PII scans in function code, remediating via CodePipeline stages that fail on high-severity violations

Answer: A, B, C

Explanation: Continuous monitoring for serverless changes must proactively flag IAM deviations to uphold least privilege, preventing over-permissions in APIs handling sensitive logistics data like shipment manifests. CloudWatch alarms on Lambda errors (>5/min) integrated with GuardDuty detect escalations (e.g., unusual AssumeRole calls), invoking Lambda@Edge for dynamic role tweaks (e.g., sts:AssumeRoleWithWebIdentity with duration 900s), enforcing real-time compliance per NIST 800-53 AC-6 (least privilege). AWS Config packs evaluate roles against rules denying wildcards (e.g., "Effect": "Deny", "Action": "*"), notifying via SNS on drifts to maintain baseline integrity, supporting CA-7 through automated evaluations. Datadog's log analytics on Gateway 4xx spikes—thresholds tuned to auth patterns—visualize compliance via dashboards (e.g., pie charts of role usage vs. policy allowances at 95%), enabling trend-based adjustments. These layered detections ensure ongoing adherence, critical for logistics where non-compliance could expose supply chain disruptions under frameworks like ISO 27001.

Question: 2121

A compliance exception related to insufficient endpoint security requires monitoring. Which metric best supports validating implemented mitigation actions?

A. Percentage of endpoints with updated threat detection signatures relative to baseline
B. Number of helpdesk tickets unrelated to endpoint security
C. Total volume of network traffic passing through endpoint firewalls
D. Number of new software versions released by the vendor monthly

Answer: A

Explanation: Tracking the percentage of endpoints with updated threat detection signatures supports validation by showing progress in improving endpoint security, which directly addresses the identified exception risk.

Question: 2122

Scenario: An energy firm using edge AI for predictive maintenance identifies controls for

model drift. Per 2026 AI trends, which?

A. Drift detection: KL-divergence threshold <0.05 between model versions
B. Retraining pipelines: Trigger if accuracy drop >5%, using MLOps in Kubeflow
C. Data lineage tracking: Provenance graphs in Apache Atlas, coverage 100%
D. Periodic manual checks

Answer: A, B, C

Explanation: AI trends emphasize automated drift management. KL-divergence quantifies shifts. Pipelines automate retraining. Lineage ensures traceability; manuals are inefficient.

Question: 2123

In developing a metric to drive improvements in the security incident response program, which calculation would be most relevant?

A. Number of new security tools deployed each quarter
B. {MTTR} = {Total downtime}\{Number of incidents}
C. Percentage of incidents that triggered compliance reporting
D. Ratio of incidents resolved without escalation

Answer: B

Explanation: Mean Time To Repair (MTTR) or resolution indicates average downtime per incident, directly measuring response effectiveness and guiding improvements. Deployment count and ratios provide less actionable detail on operational impact.

Question: 2124

In applying a traditional incident management methodology, what is the correct order of activities following incident identification?

A. Eradication → Containment → Recovery → Post-Mortem
B. Containment → Eradication → Recovery → Lessons Learned
C. Recovery → Containment → Eradication → Analysis
D. Lessons Learned → Recovery → Containment → Eradication

Answer: B

Explanation: The generally accepted sequence is containment to limit damage, eradication to remove threats, recovery to restore systems, and lessons learned to improve future responses.

Question: 2125

A central bank piloting CBDC on a permissioned ledger detects potential attacks via SIEM logs showing unusual quorum certificate validations. To categorize these in the threat intelligence program, advanced methods must distinguish between internal errors and external manipulations. Which approaches ensure precise identification?

A. Categorize using ATT&CK-Enterprise (TA0007: Discovery via Network Service Scanning), apply ML clustering (K-means on log entropy > H=4.5), label as 'Manipulation' if silhouette score >0.6
B. Leverage CWE-20 (Improper Input Validation) for ledger code, score with EPSS (Exploit Prediction Scoring System) >0.8, categorize as 'External' via graph anomaly detection GNN P(edge|context) <0.01
C. Use simple rule-based NIST categories (e.g., Unauthorized Access) without ML, for quick triage
D. Map to CAPEC-219 (Observing Response Time), Bayesian network for P(attack|logs) = ? P(node|parents), with priors from 2026 CBDC red team exercises

Answer: A, B, D

Explanation: CBDC anomalies are categorized against ATT&CK TA0007 (Discovery: Scanning for validator endpoints), using K-means clustering on log entropy (H >4.5 bits/symbol) to group outliers, labeling 'Manipulation' if silhouette coefficient >0.6 indicates tight clusters, distinguishing insider tweaks from external probes. CWE-20 flags input flaws in quorum certs, prioritized by EPSS >0.8 (predicted exploit likelihood), with Graph Neural Networks detecting anomalous edges P(unusual_link | topology) <0.01 to classify as external via validator graph deviations. CAPEC-219 (Timing Attacks on validations) feeds Bayesian networks—P(attack | log_sequence) = ∏_i P(state_i | parents_i)—initialized with priors from simulated 2026 red teams (e.g., P(external)=0.7), enabling high-fidelity categorization for ledger integrity.

Question: 2126

You are developing a detailed recovery plan using alternatives analysis. Scenario: Two recovery sites A and B have different failover capabilities. Site A can restore applications in 1 hour but has limited storage. Site B has ample storage but a 6-hour restore time. Which setting best defines a strategy for critical and non-critical systems?

A. Use Site B for all systems due to better storage capacity
B. Assign critical systems to Site A and non-critical systems to Site B
C. Assign both critical and non-critical systems to Site A to optimize restore speed
D. Rotate sites monthly to balance workload

Answer: B

Explanation: Critical systems benefit from the faster restore times at Site A, while non-critical systems can be allocated to Site B to leverage storage capacity, optimizing resource use based on system priority.

Question: 2127

Which parameter is crucial when quantifying customer impact after a personal data breach to comply with GDPR?

A. Number of data subjects affected
B. Total packet captures collected during the incident
C. Duration of firewall downtime
D. Number of privileged accounts locked out

Answer: A

Explanation: GDPR requires disclosure based on the number of data subjects whose personal data was compromised to assess breach severity and notify regulatory bodies properly. Packet captures and operational metrics do not address regulatory requirements.

Question: 2128

Cloud provider's 2026 HITRUST r2 Domain 9 crypto non-FIPS for EU data. Workaround module swap. Which?

A. Mod: yum install dracut-fips; dracut -f --regenerate-all; grub2-mkconfig -o /boot/grub2/grub.cfg;
B. Risk: Entropy = -sum p_i log2(p_i) = 3.2 bits/byte, target 4.0;

C. Report to assessor with FIPS validation cert #1234.
D. Validate: fipscheck -f /bin/ls;

Answer: A, B, C

Explanation: HITRUST gap uses dracut for FIPS. Entropy measures. Assessor reports. fipscheck validates.

Question: 2129

In determining residual risk, which variable is primarily affected by control effectiveness?

A. Threat actor motivation
B. Asset value
C. Vulnerability likelihood
D. Risk appetite

Answer: C

Explanation: Control effectiveness reduces vulnerability likelihood by diminishing the chances that threats exploit weaknesses.

Question: 2130

A media streaming service suffers a wiper attack on their CDN edge servers (Akamai + CloudFront), wiping 20PB of cached content during prime-time, with RTO=15min. To implement DRP under SOC 2 Type II, which execution commands and thresholds must be applied for rapid orchestration?

A. Trigger Lambda function for auto-remediation: aws lambda invoke --function-name dr-orchestrator --payload '{"event":"wiper_detected","threshold":95%_wipe","region":"us-east-1"}', logging to CloudWatch with metric filter pattern [error,wipe].
B. Execute multi-region failover script: terraform apply -var="failover=true" -var="rto_threshold=15" -var="backup_bucket=dr-backups-2026", monitoring via Prometheus query: up{job="cdn"} == 0.
C. Manually rebuild caches from primary origin without thresholds, to save costs.
D. Deploy chaos engineering test post-execution: kubectl apply -f chaos-mesh.yaml --set

duration=300s --set target=50% pods, to validate resilience.

Answer: A, B, D

Explanation: Lambda invocations automate detection and response at wipe thresholds, integrating with CloudWatch for SOC 2 audit logs, enabling sub-minute orchestration in high-volume CDNs. Terraform applies ensure idempotent failovers across regions, enforcing RTO via variables and Prometheus monitoring for availability drops. Chaos tests simulate failures post-execution, hardening against recurrences per SOC 2's continuous monitoring, over cost-driven manual rebuilds that exceed RTO and amplify downtime during peaks.

Question: 2131

A smart city initiative must manage accountability for traffic AI under NISTIR 8354 2024. Operators ignore model drift alerts, planners lack integration metrics. The urban security chief needs controls. Which controls should the chief activate?

A. Drift detection in TensorFlow Extended, accountability alerts to operators
B. KPI frameworks with (Accuracy Drift / Baseline) * 100, planner reviews
C. AI governance training with city-specific scenarios, 100% certification
D. City API gateways enforcing role-based drift thresholds

Answer: A, B, C

Explanation: Managing city AI accountability requires detection, KPIs, and training for NISTIR. Alerts notify. Formulas review. Training certifies. Gateways enforce.

Question: 2132

Assigning roles for recovery operations, you find overlapping responsibilities causing task conflicts. What corrective step least mitigates this issue?

A. Revising role descriptions with distinct tasks and boundaries
B. Allowing staff to self-assign tasks dynamically
C. Establishing escalation procedures for conflicts
D. Providing training focused on role clarity

Answer: B

Explanation: Allowing self-assignment without structure may increase confusion. Clear role definitions, escalation, and training minimize overlap and conflicts more effectively.

Question: 2133

A space tech firm developing satellite constellations must define roles for orbital debris mitigation under FCC Part 25 2024 rules. Roles overlap in propulsion system security between aerospace engineers and cyber teams for TT&C links. The mission security officer must clarify for launch certifications. Which methodologies should the officer employ?

A. Hazard analysis critical control points (HACCP) adapted for space, with role assignments for debris probability calculations (e.g., P_Collision = Density * Velocity * Area)
B. Orbital simulations in STK software, validating role responses to cyber-induced maneuvers
C. Role charters compliant with FCC, with syntax for TT&C encryption (AES-256 min)
D. Maturity assessments per NIST SP 800-53A, scoring control effectiveness 1-5

Answer: A, B, C

Explanation: Defining space roles needs risk-adapted analysis and simulation for FCC) HACCP assigns with formulas. Simulations test. Charters specify encryption. Assessments evaluate.

Question: 2134

During 2026 AR training rollout, the edtech firm metrics AR Session Security (ARS) = (Secure Sessions / Total) × Privacy Compliance Score, at 87%. Associating uses formulas for XR privacy. Which?

A. Privacy Score Calculation = (GDPR Controls Met / Total) × 100, >95
B. Session Hijack Attempts = (Blocked / Total) × 100, <0.1%
C. AR Device Firmware Compliance = (Updated Devices / Total) × 100, 100%
D. User Consent Granularity = Average Consent Options Accepted / Session, >3

Answer: A, B

Explanation: ARS low 87% ties to privacy gaps. Privacy Score (>95%) directly factors. Session Hijack (<0.1%) secures sessions. Compliance and Granularity enable but not core security.

Question: 2135

You have multiple recovery alternatives to restore a cloud database service after failure. Which parameter is *most* critical to analyze when recommending the recovery strategy?

A. Color branding of the cloud provider
B. Latency between the primary and recovery geographic regions
C. Number of cloud vendors in the market
D. User satisfaction with mobile app interfaces

Answer: B

Explanation: Latency between geographic regions affects replication speed and data consistency during failover in cloud recovery scenarios, making it a critical parameter for recovery strategy recommendation.

Question: 2136

A energy sector OT system with Modbus TCP integrates security in implementation per IEC 62443-4-2. Which controls?

A. Configure firewalls with rules permit tcp src 192.168.1.0/24 dst 10.0.0.1 port 502 modbus_function_code=03 only
B. Implement integrity checks with CRC16 validation in modbus_read_holding_registers response, rejecting if crc_mismatch >0
C. Deploy HARTING PLC guards with zone segmentation vlan_id=100 for OT, acl deny interzone unless explicit
D. Monitor with Snort rules alert tcp any any -> $OT_NET 502 (msg:"Modbus Write"; content:"00 01";)

Answer: A, B, C

Explanation: Implementation secures protocols with firewall rules, CRC for integrity, and

segmentation. Snort is monitoring.

Question: 2137

A firm integrates quantum-safe cryptography algorithms into its security infrastructure. Which step is critical to ensure operational continuity during this transition?

A. Using quantum-safe cryptography only for low-risk transactions
B. Immediately disabling all classical cryptographic algorithms
C. Encrypting all legacy data solely with post-quantum cryptography without backups
D. Implementing hybrid cryptographic schemes combining classical and quantum-safe algorithms

Answer: D

Explanation: Hybrid schemes allow gradual migration by enabling classical and quantum-safe algorithms to operate simultaneously, preserving compatibility and security. Abruptly disabling classical algorithms or ignoring backups risks service failures.

Question: 2138

You have been instructed to select risk treatment options for a newly identified risk of ransomware targeting outdated backup systems. Which sequence correctly orders treatment options by decreasing preference according to best practices?

A. Mitigate, Transfer, Accept, Avoid
B. Avoid, Mitigate, Transfer, Accept
C. Accept, Transfer, Mitigate, Avoid
D. Transfer, Avoid, Accept, Mitigate

Answer: B

Explanation: Effective risk treatment prioritizes avoiding the risk first by eliminating its cause, then mitigating by implementing controls, transferring risk (e.g., insurance), and as a last resort accepting the risk if it falls within tolerance.

Question: 2139

OT ISSMP reports per FSSCC: monitor threats. $15M budget (13% of $115M IT), KPI: engagement min replies 5. Evolving: 27% transient, adjust via X keyword search.

A. Allocate 30% to transient device protections
B. Include FSSCC alerts in monthly reports
C. Request 15% for intel sharing
D. Low engagement; ignore

Answer: A, B, C

Explanation: Per 27% transients, allocate 30% protections, report FSSCC alerts, request 15% for X-based intel (replies >5). This enhances OCC-coordinated monitoring, fortifying 2026 OT against U.S. financial threats.

Question: 2140

During implementation of an updated security strategy, your project team wants to ensure rapid incident response. Which management task best supports this goal?

A. Scheduling quarterly vulnerability scans without immediate follow-up
B. Establishing an integrated Security Orchestration, Automation, and Response (SOAR) platform with predefined playbooks
C. Defining perimeter firewall rules only and ignoring endpoint alerts
D. Mandating monthly password changes without multi-factor authentication

Answer: B

Explanation: SOAR platforms automate response workflows and enable rapid, consistent incident handling, critical for timely response. Merely scheduling scans without follow-up or focusing only on firewall rules doesn't ensure incident readiness, and enforcing password changes without MFA is insufficient security management.

Question: 2141

A vendor proposes to change a security configuration to bypass certain authentication steps because "industry best practices" are not clear. What is your ethical obligation?

A. Accept changes based on vendor expertise

B. Evaluate changes against organizational risk policies and advocate for secure configurations
C. Implement immediately to reduce operational friction
D. Ignore proposed changes and continue current practices

Answer: B

Explanation: Ethical responsibility involves critical evaluation of vendor proposals, aligning with internal policies and risk appetite rather than blindly accepting claims, ensuring security and accountability.

Question: 2142

A MSSP's SOC documentation per Softenger 2026 best practices outlines 24/7 monitoring shifts. Which models and plans detail staffing?

A. Model: Rotation=8-hour shifts, covering 24/7 with overlap=1hr for handovers, MSSP backup for peaks
B. Plan: AI alerts reduction via params=auto_filter=low_severity, escalation=notify via Slack in <2min
C. Training: Continuous with modules='AI Monitoring, IR', frequency=monthly, documented in LMS
D. Staffing via informal rosters

Answer: A, B, C

Explanation: 24/7 SOCs need rotations with overlaps for continuity. AI params filter noise, speeding responses. Monthly LMS-documented training ensures skills for 2026 threats like AI attacks.

Question: 2143

In a 2026 ISO 22301 BCMS audit for a logistics firm, the DR site failover test fails RTO=4h due to bandwidth caps. As ISSMP, workaround with hybrid cloud burst. Which?

A. AWS CLI: aws ec2 modify-instance-attribute --instance-id i-123 --attribute-group reserved-instances --groups "burst-group"; aws directconnect create-connection --location EqDC2 --bandwidth 100;
B. Document with MTTD formula: MTTD = Total Incidents / Detection Rate, 50 inc/12.5

det/month = 4 days, post-workaround 2 days.
C. Report waiver to certification body with signed addendum including RTO variance analysis.
D. Monitor: Prometheus query rate(failover_success[5m]) > 0.95;

Answer: A, B, C

Explanation: ISO 22301 RTO gap uses AWS CLI for burst. MTTD calc shows improvement. Addendum reports/approves. Prometheus monitors.

Question: 2144

A security architect is tasked with integrating a next-gen firewall capable of AI threat detection into the enterprise's existing security ecosystem. Which integration aspect is most essential?

A. Providing real-time telemetry data feeds from the firewall to central security analytics
B. Isolating the firewall from existing SIEM tools to reduce noise
C. Disabling automated threat prevention modes initially
D. Removing legacy firewalls immediately to avoid conflicts

Answer: A

Explanation: Real-time telemetry feeding into central analytics enables correlation and enhanced threat detection. Isolation reduces insight, disabling features delays benefits, and immediate removal may create gaps.

Question: 2145

In an agile transformation for a retail bank's fraud detection ML model, the ISSMP integrates security using SAFe framework. Program increment (PI) planning shows quality risks from unvetted data pipelines, with timeline at 5 PIs (20 weeks) and $2.8M budget. Which SAFe practices and metrics should be enforced to analyze and incorporate security?

A. Define enablers in the ART backlog for data lineage with Collibra governance, setting OKR: 100% traceable pipelines by PI 2, weighted 20% in IP iteration
B. Apply WSJF for features: Defer low-score items if WSJF < 5, calculating as (Bv + Tc + Rr + Oe) / Js to balance scope against 85% velocity target

C. Run PI system demos only for business stakeholders, excluding security teams to streamline timelines and reduce demo overhead by 12%
D. Fix budget rigidly without EVM tracking, assuming scaled agile inherently controls variances

Answer: A,B

Explanation: Enablers in the ART backlog using Collibra for 100% data lineage traceability by PI 2, weighted at 20% in IP iterations, embeds security governance early in SAFe's scaled agile, mitigating fraud detection risks and sustaining the 20-week timeline within $2.8M. WSJF prioritization—(Business Value + Time Criticality + Risk Reduction + Opportunity Enablement) / Job Size < 5 for deferral—optimizes scope to hit 85% velocity, ensuring quality ML pipelines without budget dilution. Excluding security from PI demos fragments feedback, undermining SAFe's collaborative ethos and inviting compliance gaps, while rigid budgets sans EVM ignore scaled complexities, fostering uncontrolled overruns.

Question: 2146

A newly appointed Security Program Manager needs to define roles across a decentralized organization with multiple business units. Which strategy ensures roles are consistent yet adaptable for specific unit needs?

A. Create independent role definitions for each business unit
B. Develop a global role taxonomy with unit-level customizable sub-roles
C. Assign generic roles with no customization
D. Rely solely on government regulatory role guidelines

Answer: B

Explanation: A global role taxonomy provides a common framework for role definitions, while customizable sub-roles allow individual units to tailor responsibilities to their needs. Independent role definitions risk inconsistency, generic roles may lack specificity, and regulation-based roles alone do not address operational complexities.

Question: 2147

Your organization's code of ethics forbids accepting gifts from vendors above nominal value. A vendor offers expensive software licenses as a special incentive. How should

you respond ethically?

A. Decline the gift and disclose the offer to management per ethics guidelines
B. Accept the licenses to benefit the organization
C. Accept and report after use to justify benefits
D. Request the vendor to reduce the value to an acceptable amount

Answer: A

Explanation: Ethical guidelines prevent conflicts of interest and undue influence; declining and disclosing preserves transparency and integrity. Accepting or manipulating values undermines trust.

Question: 2148

You are leading the development of incident management program documentation for a healthcare conglomerate facing rising disruptive extortion and AI-assisted insider threats in 2026. The documentation must outline integration with SIEM systems for centralized log aggregation and real-time threat detection, per NIST's updated Incident Response Recommendations. Which advanced documentation techniques should be employed to embed employee training protocols and cyber tabletop exercises with quantifiable metrics?

A. Structured outlines for training modules using Gantt charts with milestones: Week 1: Awareness (80% completion rate); Week 4: Tabletop (participation >=90%, post-exercise score >85% on scenario recall formula: Recall = Correct Responses / Total Questions)
B. Code snippets for SIEM rule configurations in SPL (Splunk Processing Language): index=health_logs sourcetype="insider_activity" | stats count by user_id | where count > threshold=50 | eval risk=if(extortion_indicator=="true", 9.5, 7.0) | alert action=notify_ir_team
C. Appendix with formulas for exercise efficacy: Efficacy Score = (Pre-Test Avg - Post-Test Avg) / Pre-Test Avg * 100, targeting >20% improvement in detection of AI-manipulated alerts during hybrid work simulations
D. Narrative sections on external communication plans without metrics, emphasizing empathetic stakeholder notifications post-incident

Answer: A, B, C

Explanation: Structured outlines using Gantt charts for training modules ensure phased rollout with measurable completion rates (e.g., 80% for awareness, 90% participation in tabletops) and recall formulas, directly supporting NIST's preparation phase by

quantifying training effectiveness and preparing staff for AI-assisted threats through structured, trackable programs that reduce human error in 2026's evolving landscape. Code snippets in SPL for SIEM rules enable automated detection of anomalous insider activity exceeding thresholds (e.g., count >50), assigning high risk scores (9.5 for extortion indicators) and triggering notifications, which embeds advanced analytics into documentation for centralized log management and swift identification as mandated by updated NIST guidance. The efficacy score formula measures tabletop improvements (>20% in pre/post-test deltas) for scenarios like AI-manipulated alerts, providing data-driven validation of exercises to refine protocols and enhance resilience against insider threats, ensuring the documentation serves as a living tool for continuous improvement.

Question: 2149

During security requirements identification for a new AI-driven analytics platform, what constitutes a high-priority control given the sensitivity of data processing?

A. Disable logging to conserve storage space
B. Enable only generic antivirus across all servers
C. Allow unrestricted data export by default for user convenience
D. Design and implement fine-grained access controls based on data classification and usage patterns

Answer: D

Explanation: Fine-grained access controls tailored to classified data and usage minimize exposure risk inherent in sensitive AI processing. Generic antivirus, unrestricted data export, or disabled logging undermine confidentiality and accountability.

Question: 2150

In vulnerability scanning configuration, which setting reduces scan duration but risks missing intermittent vulnerabilities?

A. Using full credentialed scans
B. Increasing scan timeout values
C. Scheduling scans during off-peak hours
D. Limiting scan to critical ports only

Answer: D

Explanation: Limiting scans to critical ports reduces scan time but risks missing vulnerabilities on non-standard or intermittent ports relevant to attack vectors. Credentialed scans, scheduling, and timeout adjustments impact coverage differently.

Question: 2151

Retail's 2026 RFID with AI inventory, EPC Gen2, risks cloning. With CRC-16-CCITT, which?

A. Mutual auth with challenge-response, nonce 128 bits.
B. AI track with Kalman $x_k = F x + w$, R=0.1 noise.
C. Encrypt TID AES-128, key per tag.
D. Backscatter modulation ASK 2, data rate 128kHz.

Answer: A, C

Explanation: CRC verifies, mutual auth/nonce prevents clone replay. AES-TID per-tag secures unique IDs. Kalman tracks but assumes auth. Modulation physical.

Question: 2152

Which control identification method best applies when integrating continuous automated assessment tools for cloud infrastructure security?

A. Manually reviewing cloud provider security reports quarterly
B. Defining API-based control points aligned with compliance frameworks
C. Relying on endpoint antivirus status only
D. Scheduling annual penetration tests only

Answer: B

Explanation: Defining API-based control points enables automated, continuous security checks aligned with compliance, ideal for fast-changing cloud environments. Manual or annual reviews are not continuous and lack automation.

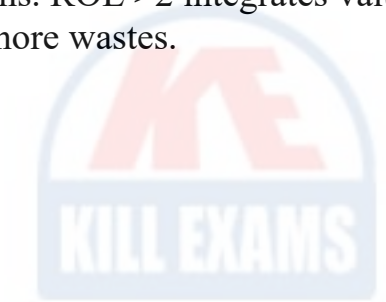
Question: 2153

Agile for quantum key distro net, ISSMP DAD framework. Discovery spikes for threats, timeline 14 months, budget $5.2M, quality 98%. Which?

A. Spikes: Timeboxed 20% sprint for threat models, acceptance if coverage >90%
B. Delivery patterns: If spike ROE >2, integrate to main backlog
C. No spikes, full sprints
D. ROE ignore, all integrate

Answer: A,B

Explanation: 20% timeboxed spikes at >90% coverage embed DAD discovery in agile for 14 months. ROE >2 integrates valuable threats to $5.2M at 98% quality. No spikes rushes risks, ignore wastes.



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:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.