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

ASIS-APP MCQs
ASIS-APP TestPrep
ASIS-APP Study Guide
ASIS-APP Practice Test
ASIS-APP Exam Questions

killexams.com

ASIS

# ASIS-APP

Associate Protection Professional - 202

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/ASIS-APP

**Question: 1113**

A security project manager is overseeing the installation of a new access control system. The project has a critical path duration of 12 weeks, with a budget of $100,000. If a delay in hardware delivery adds 2 weeks, which project management technique should be used to mitigate the impact?

A. Crashing the schedule by adding resources
B. Fast-tracking tasks to run concurrently
C. Reducing the project scope to exclude non-critical tasks
D. Updating the work breakdown structure (WBS) to reflect delays

Answer: A

Explanation: Crashing the schedule by adding resources reduces the project duration to meet the original timeline, addressing the 2-week delay. Fast-tracking risks quality by overlapping tasks. Reducing scope compromises deliverables. Updating the WBS documents delays but doesn't mitigate them.

**Question: 1114**

When evaluating a physical security program, which metrics should be used to assess compliance with ASIS Physical Asset Protection Standard?

A. Average time to resolve access control system alerts
B. Number of unauthorized access attempts detected
C. Total cost of security equipment purchases
D. Percentage of assets covered by surveillance systems

Answer: A,B,D

Explanation: Average time to resolve access control alerts, number of unauthorized access attempts detected, and percentage of assets covered by surveillance systems are direct metrics for assessing program effectiveness and compliance with ASIS standards. Total cost of equipment purchases is not a performance metric, as it does not measure operational outcomes.

**Question: 1115**

A security manager is tasked with establishing a continuity of operations plan (COOP) for a government agency. The agency's critical functions include public safety communications, which must resume within 2 hours of a disruption. Which of the following actions align with FEMA's Business Process Analysis and Business Impact Analysis User Guide for prioritizing critical functions?

A. Calculate the financial impact of downtime using FEMA's operational and financial impact worksheet

B. Identify dependencies between public safety communications and IT infrastructure
C. Map recovery strategies to a recovery point objective (RPO) of zero data loss
D. Train staff on manual workaround procedures during system outages

Answer: A,B,C,D

Explanation: FEMA's Business Process Analysis and Business Impact Analysis User Guide emphasizes a comprehensive approach to prioritizing critical functions. Calculating the financial impact using the worksheet helps quantify the cost of downtime, a key step in prioritizing recovery. Identifying dependencies ensures all supporting systems, like IT infrastructure, are accounted for in the COOP. Mapping recovery strategies to an RPO of zero data loss aligns with ensuring no data is lost for critical functions like communications. Training staff on manual workarounds prepares the agency for operational continuity during outages, a practical FEMA recommendation.

**Question: 1116**

A security manager calculates the Recovery Point Objective (RPO) for a critical system after a natural disaster. Which formula should be used?

A. RPO = Amount of Data Loss Acceptable / Recovery Cost
B. RPO = Time Between Last Backup and Incident
C. RPO = Total Downtime / Data Restoration Time
D. RPO = System Value / Recovery Priority

Answer: B

Explanation: The Recovery Point Objective (RPO) is calculated as the time between the last backup and the incident, representing the amount of data loss acceptable. This ensures recovery planning aligns with data loss tolerance. Other options do not accurately reflect RPO calculation principles.

**Question: 1117**

A security policy requires employees to report suspicious activities. Which components should be included in the guidelines to ensure effective reporting?

A. Anonymous reporting channels to protect whistleblowers
B. Clear definitions of what constitutes suspicious activity
C. Mandatory annual audits of reported incidents
D. Procedures for escalating reports to senior management

Answer: A,B,D

Explanation: Anonymous reporting channels encourage reporting by protecting whistleblowers. Clear definitions ensure employees understand what to report. Escalation procedures ensure timely handling of serious incidents. Annual audits are reactive and not a core component of reporting guidelines.

**Question: 1118**

A security consultant is designing a surveillance system for a high-risk facility. The system must integrate with an existing IDS and support real-time analytics. Which configuration ensures optimal performance?

A. Analog cameras with DVR and manual alerts
B. IP cameras with edge-based AI analytics
C. Hybrid system with cloud storage
D. PTZ cameras with centralized processing

Answer: B

Explanation: IP cameras with edge-based AI analytics provide real-time processing and IDS integration, optimizing performance. Analog cameras with DVR lack analytics. Hybrid systems are less efficient. PTZ cameras with centralized processing introduce latency, unsuitable for real-time needs.

**Question: 1119**

A security professional is designing a notification system for a high-risk facility. Which setting ensures compliance with emergency communication standards?

A. Configure alerts to send only to senior management
B. Set up geo-targeted alerts based on employee location data
C. Use a single SMS provider to simplify maintenance
D. Disable acknowledgment features to expedite delivery

Answer: B

Explanation: Geo-targeted alerts based on employee location data ensure relevant, timely notifications, aligning with standards like NFPA 72 for emergency communications. Limiting alerts to senior management excludes critical personnel, a single SMS provider risks delivery failure, and disabling acknowledgment features prevents confirmation of receipt.

**Question: 1120**

A security professional is tasked with implementing a legal hold for a pending lawsuit. Which of the following steps is critical to ensure compliance?

A. Deleting irrelevant records to streamline the process
B. Notifying all relevant custodians of the legal hold
C. Storing records on an unsecured external drive
D. Allowing routine backups to overwrite relevant data

Answer: B

Explanation: Notifying all relevant custodians of the legal hold ensures they preserve necessary records, complying with legal requirements. Deleting irrelevant records risks destroying potentially relevant evidence. Storing records on an unsecured external drive compromises security. Allowing routine backups to overwrite relevant data violates legal hold obligations by risking data loss.

**Question: 1121**

A security team is collecting evidence after a cyber intrusion. Which tool should be used to create a forensic image of a compromised device?

A. DD command with a write-blocker to create a bit-by-bit copy
B. FileZilla to transfer files to a secure server
C. Notepad++ to document file contents
D. Windows Backup to create a system restore point

Answer: A

Explanation: The DD command with a write-blocker creates a forensically sound bit-by-bit copy of a device, preserving all data without modification. FileZilla is for file transfers, not forensic imaging. Notepad++ is for text editing, and Windows Backup does not create forensic images suitable for evidence.

**Question: 1122**

A multinational corporation is conducting a threat assessment for its new data center in a politically unstable region. The security team must prioritize threats based on potential consequences using a quantitative risk assessment model. The team identifies a potential cyberattack with a likelihood of 0.3 (30%) and an impact cost of $10 million, and a physical intrusion with a likelihood of 0.1 (10%) and an impact cost of $15 million. Using the formula Risk = Likelihood × Impact, which threat should be prioritized?

A. Cyberattack due to higher likelihood
B. Cyberattack due to lower impact cost
C. Physical intrusion due to higher impact cost
D. Physical intrusion due to lower likelihood

Answer: C

Explanation: Using the formula Risk = Likelihood × Impact, the risk for the cyberattack is 0.3 × $10,000,000 = $3,000,000, and for the physical intrusion, it is 0.1 × $15,000,000 = $1,500,000. Although the cyberattack has a higher likelihood, the physical intrusion has a higher impact cost. However, prioritizing threats based solely on impact cost, as the question emphasizes potential consequences, leads to selecting physical intrusion due to higher impact cost ($15 million vs. $10 million). Thus, physical intrusion due to higher impact cost is the correct choice.

**Question: 1123**

During an investigation, you find that proprietary data was accessed via a compromised API. Which steps should you take to secure the API?

A. Implement OAuth 2.0 with access token expiration after 1 hour
B. Configure rate limiting to 100 API calls per minute per client
C. Allow anonymous API access to simplify integration
D. Enable logging of all API requests with a retention period of 90 days

Answer: A,B,D

Explanation: OAuth 2.0 with token expiration secures API access. Rate limiting prevents abuse. Logging API requests enables auditing and incident analysis. Anonymous API access is insecure and unsuitable for protecting proprietary data.

**Question: 1124**

In a scenario where a security breach leads to litigation, which evidence protection technique ensures the integrity of digital logs?

A. Storing logs on a write-once, read-many (WORM) device
B. Copying logs to a shared cloud storage platform
C. Allowing administrators to edit logs for clarity
D. Backing up logs on an unencrypted external drive

Answer: A

Explanation: Storing logs on a write-once, read-many (WORM) device prevents alterations, ensuring their integrity for litigation. Copying logs to a shared cloud storage platform risks unauthorized access or tampering. Allowing administrators to edit logs compromises their authenticity. Backing up logs on an unencrypted external drive exposes them to security risks, undermining their legal validity.

**Question: 1125**

A financial institution's BCP requires a recovery strategy for its trading platform, with an RTO of 2 hours. A recent gap analysis shows the current recovery time is 4 hours due to manual failover processes. Which of the following solutions should be implemented to meet the RTO?

A. Automate failover to a hot site with real-time data replication
B. Train staff to execute manual failover faster
C. Increase the RTO to 4 hours in the BCP
D. Outsource trading platform operations to a third party

Answer: A

Explanation: Automating failover to a hot site with real-time data replication ensures the trading platform can be restored within the 2-hour RTO by eliminating manual delays. Training staff to speed up manual processes is unlikely to consistently achieve the required RTO. Increasing the RTO compromises the BCP's objectives. Outsourcing introduces risks and may not guarantee the 2-hour RTO.

**Question: 1126**

A company's warehouse is vulnerable to theft. Which prevention tactics should be implemented to enhance security?

A. Deploy guards with overlapping patrol schedules
B. Install a biometric access control system
C. Perform regular inventory audits
D. Use motion-activated lighting around the perimeter

Answer: A,B,D

Explanation: Deploying guards with overlapping patrol schedules ensures continuous monitoring. Installing a biometric access control system restricts unauthorized entry. Using motion-activated lighting deters intruders, all aligning with ASIS physical security prevention tactics. Regular inventory audits are detective, not preventive.

**Question: 1127**

A protection professional is integrating guards with a new VMS. Which features ensure effective coordination?

A. Mobile app for real-time video access
B. Manual camera control for guards
C. Real-time alerts for suspicious activity
D. Static camera feeds for post-event review

Answer: A, C

Explanation: A mobile app for real-time video access enables guards to monitor live feeds. Real-time alerts ensure rapid response to incidents. Manual camera control is inefficient for guards. Static feeds are less useful for real-time coordination.

**Question: 1128**

A retail chain in South Africa is addressing shoplifting through a partnership with the South African Police Service (SAPS). Which method fosters effective working relationships under SAPS's community policing framework?

A. Deploy private security to conduct independent arrests
B. Host joint community outreach events to build trust
C. Require SAPS to prioritize retail theft over other crimes
D. Share proprietary surveillance footage without legal agreements

Answer: B

Explanation: Hosting joint community outreach events aligns with SAPS's community policing framework, building trust and collaboration. Independent arrests by private security may violate legal boundaries, prioritizing retail theft is unrealistic, and sharing footage without agreements risks privacy violations.

**Question: 1129**

A protection professional is developing a training program for executive protection personnel. Which skill should be emphasized for high-threat scenarios?

A. Basic customer service training
B. Advanced evasive driving techniques
C. General office administration skills
D. Standard first aid certification

Answer: B

Explanation: Advanced evasive driving techniques are critical for navigating high-threat scenarios, such as ambushes. Customer service, office administration, and standard first aid are less relevant to immediate threat response.

**Question: 1130**

To enhance the organization's threat intelligence analysis, a security manager integrates a machine learning model to predict potential threats. Which Python library should be used to implement a supervised learning model for this purpose?

A. NumPy
B. Pandas
C. Scikit-learn
D. Matplotlib

Answer: C

Explanation: Scikit-learn is a Python library designed for implementing supervised learning models, such as classification or regression, suitable for predicting potential threats. NumPy is used for numerical computations, not machine learning. Pandas is for data manipulation, not model training. Matplotlib is for data visualization, not predictive modeling.

**Question: 1131**

A security manager is selecting a vendor for a surveillance system. Which qualification criterion ensures the vendor can handle complex installations?

A. Certification in project management (PMP)
B. Experience with installations in similar environments
C. Lowest bid price
D. Vendor's annual revenue

Answer: A,B

Explanation: Certification in project management (PMP) indicates the vendor’s ability to manage complex installations effectively. Experience with installations in similar environments demonstrates relevant expertise. Lowest bid price and annual revenue do not directly correlate with installation capability.

**Question: 1132**

During a high-risk international executive travel assignment to a politically unstable region, the protection team must implement a layered travel security program. Which components should be prioritized to ensure comprehensive protection?

A. Conducting real-time social media monitoring for threat indicators
B. Deploying a single advance agent to confirm hotel security measures
C. Establishing a 24/7 command center for continuous situational awareness
D. Utilizing encrypted communication devices for all team interactions

Answer: A,C,D

Explanation: Conducting real-time social media monitoring for threat indicators is critical in unstable regions to identify emerging threats like protests or targeted attacks. Establishing a 24/7 command center ensures continuous situational awareness, enabling rapid response to changing conditions. Utilizing encrypted communication devices protects sensitive communications from interception, which is vital in high-risk areas. Deploying a single advance agent, while useful, is insufficient for comprehensive hotel security confirmation, as it lacks redundancy and depth for such a high-risk environment.

**Question: 1133**

When preparing a budget for a security department, which steps ensure compliance with financial reporting standards?

A. Align budget with GAAP principles
B. Include only qualitative risk assessments
C. Reconcile budget with general ledger
D. Use standardized financial templates

Answer: A,C,D

Explanation: Aligning with GAAP ensures compliance with accounting standards, reconciling with the general ledger verifies accuracy, and standardized templates ensure consistency. Qualitative risk assessments are not directly related to financial reporting standards.

**Question: 1134**

During a security audit, the team identifies a gap in the organization's incident response metrics. Which of the following should be included in a continuous assessment process to measure incident response effectiveness?

A. Mean time to detect (MTTD) incidents
B. Mean time to respond (MTTR) to incidents
C. Number of incidents reported annually
D. Total cost of incident response training

Answer: A,B

Explanation: Mean time to detect (MTTD) incidents and mean time to respond (MTTR) to incidents are key performance indicators that measure the efficiency of incident response processes. Number of incidents reported annually is a volume metric, not a performance indicator. Total cost of incident response training is a financial metric, not directly related to response effectiveness.

**Question: 1135**

Which law governs the protection of employee whistleblower rights in the U.S.?

A. Dodd-Frank Act
B. General Data Protection Regulation (GDPR)
C. Health Insurance Portability and Accountability Act (HIPAA)
D. Sarbanes-Oxley Act (SOX)

Answer: A

Explanation: The Dodd-Frank Act protects employee whistleblowers in the U.S., particularly for reporting financial misconduct. GDPR governs data protection in the EU, HIPAA protects health information, and SOX focuses on financial reporting but has limited whistleblower provisions compared to Dodd-Frank.

**Question: 1136**

A facility receives a bomb threat, and the incident commander must implement a contingency plan. Which sequence of steps should be followed to ensure compliance with ASIS standards for bomb threat

response?

A. Assess threat credibility, evacuate personnel, conduct a sweep, notify law enforcement
B. Conduct a sweep, notify law enforcement, assess threat credibility, evacuate personnel
C. Evacuate personnel, notify law enforcement, conduct a sweep, assess threat credibility
D. Notify law enforcement, evacuate personnel, assess threat credibility, conduct a sweep

Answer: A

Explanation: ASIS standards prioritize assessing threat credibility first to determine the appropriate response level, followed by evacuating personnel for safety, conducting a sweep to identify suspicious items, and notifying law enforcement to coordinate external support. This sequence ensures a structured and prioritized response. Other options disrupt this logical flow, potentially compromising safety or efficiency.

**Question: 1137**

Which non-verbal communication training topic is most critical for employees interacting with external vendors in a high-stakes environment?

A. Facial expressions indicating stress or deception
B. Hand gesture frequency
C. Posture alignment with corporate branding
D. Walking speed during meetings

Answer: A

Explanation: Facial expressions indicating stress or deception are critical for detecting vendor malintent in high-stakes interactions. Hand gestures, posture alignment, and walking speed are less relevant to security outcomes.

**Question: 1138**

During negotiations with a security vendor, a clause is proposed that requires the vendor to maintain a 99.9% uptime for access control systems. Which contractual term should be included to enforce this requirement?

A. Indemnification for system downtime exceeding 0.1%
B. Liquidated damages for failure to meet uptime requirements
C. Performance bond to cover vendor insolvency
D. Termination clause for repeated non-compliance

Answer: B

Explanation: Liquidated damages for failure to meet uptime requirements directly address the financial consequences of the vendor not achieving the 99.9% uptime, providing a measurable penalty for non-compliance. Indemnification for system downtime exceeding 0.1% may cover losses but is less specific than liquidated damages for enforcing uptime. A performance bond to cover vendor insolvency addresses financial stability, not uptime performance. A termination clause for repeated non-compliance is a remedy but does not directly enforce the uptime requirement.

**Question: 1139**

A security manager is preparing a financial report for a security project. Which principle ensures accurate reporting of project costs? (Single Answer)

A. Conservatism
B. Consistency
C. Materiality
D. Objectivity

Answer: B

Explanation: Consistency ensures that financial reporting methods remain uniform across periods, allowing accurate comparison of project costs. Conservatism prioritizes caution, materiality focuses on significant items, and objectivity ensures unbiased reporting but not necessarily cost accuracy.

**Question: 1140**

A security team is setting security awareness program objectives. Which objective is SMART (Specific, Measurable, Achievable, Relevant, Time-bound)?

A. Improve employee security knowledge
B. Reduce insider threat incidents by 20% in 12 months
C. Conduct more training sessions
D. Enhance organizational security culture

Answer: B

Explanation: Reducing insider threat incidents by 20% in 12 months is SMART, with clear metrics and a timeline. Improving knowledge, conducting more sessions, and enhancing culture lack specificity or measurability.

**Question: 1141**

A security manager is implementing a notification protocol for a data breach affecting customer information. Which regulatory requirement must be addressed in the notification process?

A. Notify affected customers within 72 hours of breach discovery, per GDPR
B. Post a public announcement on the company website within 24 hours
C. Delay notification until the breach is fully contained to avoid panic
D. Send notifications only to senior management to maintain confidentiality

Answer: A

Explanation: The General Data Protection Regulation (GDPR) mandates notifying affected customers within 72 hours of discovering a data breach to ensure transparency and compliance. Public announcements may be required but are not time-bound under GDPR. Delaying notification violates regulatory requirements, and notifying only senior management fails to inform affected individuals.

# 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.