



Up-to-date Practice Test with Latest Questions and Answers covering latest syllabus and topics of the exam. Makes you ready to face actual exam.



ISA-IEC-62443-IC33M Practice Questions  
ISA-IEC-62443-IC33M Practice Test  
ISA-IEC-62443-IC33M Practice Exam  
ISA-IEC-62443-IC33M Exam Questions  
ISA-IEC-62443-IC33M Study Guide



[killexams.com](https://killexams.com)

**ISA**

## ISA-IEC-62443-IC33M

ISA/IEC 62443 Cybersecurity Risk Assessment Specialist  
(Certificate 2)

ORDER FULL VERSION

<https://killexams.com/pass4sure/exam-detail/ISA-IEC-62443-IC33M>



**Question: 946**

A risk assessment team is preparing a report for a water treatment facility's IACS. The report must include a section on unmitigated risks per ISA/IEC 62443-3-2. What is a critical element that must be documented for each unmitigated risk?

- A. The CVSS temporal score for the vulnerability
- B. The business justification for accepting the risk
- C. The exact timestamp of the vulnerability discovery
- D. The vendor contact details for affected devices

Answer: B

Explanation: ISA/IEC 62443-3-2 requires that unmitigated risks in the risk assessment report include a business justification for accepting the risk. This ensures transparency and alignment with organizational risk tolerance. CVSS temporal scores, timestamps, or vendor details may be relevant but are not mandatory for unmitigated risks per the standard.

**Question: 947**

In a high-level risk assessment for a manufacturing plant's ICS, you are required to evaluate the risk of a ransomware attack on a programmable logic controller (PLC). Which parameter should be the primary focus to determine the risk severity as per ISA/IEC 62443?

- A. The cost of replacing the affected PLC hardware
- B. The number of employees with access to the PLC
- C. The likelihood of the ransomware exploiting known vulnerabilities
- D. The time required to restore operations after an attack

Answer: C

Explanation: Determining risk severity in a high-level assessment under ISA/IEC 62443 requires focusing on the likelihood of a threat exploiting vulnerabilities. For a ransomware attack, the presence of unpatched or known vulnerabilities in the PLC significantly increases the likelihood of a successful attack, making this the primary parameter to evaluate.

**Question: 948**

During a vulnerability assessment of a power generation facility, you are required to use the STRIDE model for threat modeling as per ISA/IEC 62443 recommendations. Which specific threat category would be most relevant when analyzing a scenario where an attacker gains unauthorized administrative access through a compromised operator account?

- A. Denial of Service
- B. Spoofing
- C. Information Disclosure
- D. Elevation of Privilege

Answer: D

Explanation: Elevation of Privilege is the most relevant threat category under the STRIDE model for a scenario where an attacker gains unauthorized administrative access through a compromised operator account. This category focuses on scenarios where an individual obtains higher-level permissions than authorized, posing a significant risk to the integrity and control of critical systems in an ICS environment, as highlighted in ISA/IEC 62443 threat modeling practices.

**Question: 949**

During a high-level risk assessment, an assessor identifies a vulnerable VPN gateway (CVE-2024-67890) in a conduit connecting two IACS zones. The consequence severity is 4, and likelihood is assumed as 1 per ISA/IEC 62443-3-2. What is the risk score, and what is the first mitigation step?

- A. Risk Score = 4, patch the VPN gateway
- B. Risk Score = 8, isolate the conduit
- C. Risk Score = 4, assign an SL-T
- D. Risk Score = 2, conduct a penetration test

Answer: C

Explanation: ISA/IEC 62443-3-2 initial risk assessment uses a likelihood of 1, so the risk score equals the consequence severity (4). The first step is to assign an SL-T to the conduit to prioritize mitigation based on security requirements. Patching, isolation, or penetration testing follows after SL-T assignment.

**Question: 950**

Which of the following is a critical piece of cybersecurity information to specify for an IACS assessment under ISA/IEC 62443 when evaluating access points?

- A. The color coding of network cables
- B. The personal preferences of system operators
- C. The logical and physical access control mechanisms in place
- D. The warranty details of hardware components

Answer: C

Explanation: Specifying the logical and physical access control mechanisms in place is critical for an IACS assessment under ISA/IEC 62443. This information helps identify how access to the system is managed and secured, which is essential for assessing vulnerabilities at access points and mitigating unauthorized access risks.

**Question: 951**

You are conducting a vulnerability scan on an IACS using Nessus. The scan identifies a critical vulnerability (CVSS score 9.8) in an HMI running an outdated version of Apache (CVE-2023-25690).

The HMI is in a control zone with no internet access but is accessible from an engineering workstation zone. According to ISA/IEC 62443-3-2, what is the most appropriate next step?

- A. Apply a patch to the Apache server immediately
- B. Conduct a detailed risk assessment to evaluate the vulnerability's impact
- C. Disable the HMI to mitigate the vulnerability
- D. Reconfigure the firewall to block all traffic to the HMI

Answer: B

Explanation: A critical vulnerability like CVE-2023-25690 requires careful evaluation. ISA/IEC 62443-3-2 mandates a detailed risk assessment to determine the vulnerability's impact, considering factors like the HMI's role, network segmentation, and potential consequences of exploitation. Immediate patching or disabling the HMI could disrupt critical operations, and reconfiguring the firewall may not address the root issue if the vulnerability is exploitable within the zone. A risk assessment ensures a balanced approach to mitigation.

**Question: 952**

A detailed risk assessment identifies a PLC with a vulnerability (CVE-2023-45678, CVSS 8.4) exploitable via a specific network-based attack. The PLC is in a segmented zone, reducing likelihood to 0.7. The consequence severity is 5. What is the mitigated risk score?

- A. 3.5
- B. 5.0
- C. 8.4
- D. 42.0

Answer: A

Explanation: Per ISA/IEC 62443, the mitigated risk score is  $\text{Risk} = \text{Likelihood} \times \text{Consequence}$ . With a likelihood of 0.7 and consequence severity of 5, the risk score is  $0.7 \times 5 = 3.5$ . The CVSS score (8.4) is not used directly. The other options are incorrect.

**Question: 953**

You are reviewing a zone and conduit diagram for an ICS with a conduit connecting zones at SL-1 and SL-3. According to ISA/IEC 62443, what is the required configuration for the firewall settings on this conduit?

- A. Apply SL-1 settings for minimal restriction
- B. Apply SL-2 settings as a balanced approach
- C. Disable firewall settings for connectivity
- D. Apply SL-3 settings to match the highest level

Answer: D

Explanation: According to ISA/IEC 62443, firewall settings on a conduit connecting zones with different Security Levels must match the highest level, which is SL-3 in this case. This ensures that the security controls are stringent enough to protect the higher security zone. Applying lower settings or disabling the firewall would create vulnerabilities.

**Question: 954**

Under ISA/IEC 62443, what is a key method to identify cybersecurity vulnerabilities in IACS products during the assessment phase?

- A. Reviewing marketing materials for product features
- B. Performing penetration testing to exploit potential weaknesses
- C. Surveying employees about their user experience
- D. Checking the physical durability of hardware components

Answer: B

Explanation: Performing penetration testing to exploit potential weaknesses is a key method under ISA/IEC 62443 to identify cybersecurity vulnerabilities in IACS products. This active testing simulates real-world attacks to uncover design flaws or configuration issues that could compromise system security.

**Question: 955**

A risk assessment for a chemical plant's IACS identifies a threat where a brute-force attack compromises a DCS login. The likelihood is 0.2, and the consequence is a 4-hour outage costing \$400,000. What is the risk score and classification?

- A. 0.8, Moderate
- B. 0.8, Low
- C. 8.0, High
- D. 8.0, Critical

Answer: A

Explanation: Assuming a consequence score of 4 (based on significant financial impact), the risk score is  $0.2 \times 4 = 0.8$ . Per ISA/IEC 62443-3-2, this is a Moderate risk, requiring mitigation but not immediate action like High or Critical risks.

**Question: 956**

A high-level risk assessment identifies a critical PLC with no authentication controls, located in a zone with SL-T 3. The team needs to assign a foundational requirement (FR) per ISA/IEC 62443-3-3 to address this issue. Which FR is most relevant?

- A. FR 3: System Integrity
- B. FR 2: Use Control
- C. FR 1: Identification and Authentication Control
- D. FR 4: Data Confidentiality

Answer: C

Explanation: The lack of authentication controls on the PLC directly relates to FR 1: Identification and Authentication Control, which requires mechanisms to verify user and device identities. This is critical for securing the PLC in a zone with SL-T 3. The other FRs address different aspects (use control, integrity, confidentiality) not directly related to authentication.

**Question: 957**

During a detailed cyber risk assessment for an IACS, you identify a threat of ransomware exploiting a vulnerability in unpatched HMIs. Using the formula  $\text{Risk} = \text{Likelihood} \times \text{Consequence}$ , you assess likelihood as 0.8 (due to known exploits) and consequence as 10 (complete production halt). What is the risk value, and what is the priority action?

- A. Risk value 8, monitor the system
- B. Risk value 8, apply patches to HMIs
- C. Risk value 10, document the risk
- D. Risk value 18, update antivirus software

Answer: B

Explanation: Risk is calculated as  $0.8 \times 10 = 8$ , indicating a high risk per ISA/IEC 62443-2-1 methodology. Given the severity of ransomware and the potential for production halt, applying patches to HMIs addresses the root vulnerability, reducing likelihood and thus the overall risk. This is the priority action over monitoring or secondary measures.

**Question: 958**

In a Risk assessment for a power grid ICS, a threat scenario involves a potential SQL injection attack on a web-based HMI with a likelihood of 0.5 and consequence of 7 (on a 1-10 scale). What is the risk score, and what action is recommended if the tolerable risk is 3.0?

- A. Risk = 3.5, accept the risk as tolerable
- B. Risk = 3.5, implement mitigation measures
- C. Risk = 5.7, monitor without action
- D. Risk = 7.5, ignore due to low likelihood

Answer: B

Explanation: The risk score is 3.5 ( $0.5 \times 7$ ), which exceeds the tolerable risk of 3.0. Implementing mitigation measures is recommended to reduce the likelihood or consequence of a SQL injection attack

on the HMI, following ISA/IEC 62443 risk treatment strategies.

**Question: 959**

In a detailed risk assessment, a compromised HMI could cause a production halt costing \$10 million, with a likelihood of 0.05 after implementing two-factor authentication. What is the residual risk?

- A. \$500,000
- B. \$1,000,000
- C. \$2,500,000
- D. \$5,000,000

Answer: A

Explanation: Residual risk is consequence  $\times$  likelihood. Here,  $\$10,000,000 \times 0.05 = \$500,000$ , reflecting the risk after two-factor authentication, per ISA/IEC 62443-3-2.

**Question: 960**

An offshore platform is developing a CRS for an IACS controlling drilling operations. The system requires secure configuration management per ISA/IEC 62443-2-1 FR6: Restricted Access to Management Functions. Which requirement should be included?

- A. Require weekly configuration audits
- B. Use TLS 1.3 for configuration data transmission
- C. Deploy a configuration management database (CMDB)
- D. Implement role-based access control (RBAC) for configuration changes

Answer: D

Explanation: FR6 (Restricted Access to Management Functions) in ISA/IEC 62443-2-1 ensures that configuration changes are restricted to authorized personnel. Implementing RBAC for configuration changes directly addresses this requirement by enforcing access controls. TLS 1.3 relates to FR3, a CMDB is a tool not specific to FR6, and audits are a procedural practice, not a technical requirement.

**Question: 961**

Your organization is assessing a new physical access control system for a critical OT facility. The system costs \$120,000 to install, has an annual maintenance fee of \$10,000, and reduces unauthorized access risks by 85%. However, it requires integration with existing badge systems, adding a one-time cost of \$30,000 and increasing implementation complexity. The security budget is \$160,000, and the risk reduction target is 80%. What is the best course of action?

- A. Reject the system due to high integration costs
- B. Delay implementation until integration complexity is reduced
- C. Approve the system as it meets the risk reduction target within budget

D. Seek a less complex alternative with similar effectiveness

Answer: C

Explanation: The physical access control system achieves an 85% reduction in unauthorized access risks, surpassing the organization's target of 80%. The total first-year cost of \$160,000 (\$120,000 installation, \$30,000 integration, and \$10,000 maintenance) fits within the allocated budget of \$160,000. While integration complexity is a concern, the system's effectiveness and budget compliance make it a viable solution for enhancing security at the OT facility.

**Question: 962**

A team is conducting a cyber criticality assessment for an IACS in a pharmaceutical plant. The assessment requires ranking assets based on their impact on regulatory compliance. Which formula should be used to calculate the criticality score?

- A. Criticality = Max(Regulatory Impact, Operational Impact, Financial Impact)
- B. Criticality = Regulatory Impact + Operational Impact + Financial Impact
- C. Criticality = (Regulatory Impact × 0.6) + (Operational Impact × 0.3) + (Financial Impact × 0.1)
- D. Criticality = (Regulatory Impact × Operational Impact × Financial Impact)<sup>(1/3)</sup>

Answer: C

Explanation: The weighted formula (Regulatory Impact × 0.6) + (Operational Impact × 0.3) + (Financial Impact × 0.1) prioritizes regulatory impact, which is critical in pharmaceutical IACS due to compliance requirements, while considering operational and financial impacts. This aligns with ISA/IEC 62443's risk assessment methodology. Summation, maximum value, or geometric mean approaches do not reflect the prioritized weighting needed for accurate criticality scoring.

**Question: 963**

In preparing for a cybersecurity risk assessment of an Industrial Automation and Control System (IACS), you are tasked with defining the scope of the assessment for a large-scale chemical processing plant. The plant has multiple interconnected systems, including legacy equipment with outdated firmware. Which step should be prioritized to ensure the scope accurately reflects the critical assets and potential risks?

- A. Conducting a preliminary vulnerability scan on all networked devices to identify immediate threats
- B. Creating a detailed IACS asset inventory, categorizing assets by criticality and connectivity
- C. Developing a risk matrix without stakeholder input to expedite the process
- D. Focusing solely on the newest systems to minimize assessment complexity

Answer: B

Explanation: Creating a detailed IACS asset inventory is the foundational step in defining the scope of a cybersecurity risk assessment. Categorizing assets by criticality and connectivity ensures that all components, including legacy equipment, are accounted for and prioritized based on their potential

impact on operations. This approach aligns with the ISA/IEC 62443 standard's emphasis on comprehensive asset identification as a precursor to risk evaluation.

**Question: 964**

As part of pre-assessment planning for a cybersecurity risk evaluation in a chemical processing plant, which step should be executed first to ensure compliance with ISA/IEC 62443-3-2 and to establish a baseline for the System Under Consideration (SUC)?

- A. Conduct a penetration test on critical assets
- B. Develop a detailed incident response plan
- C. Define the scope and boundaries of the SUC
- D. Implement temporary security controls

Answer: C

Explanation: Defining the scope and boundaries of the System Under Consideration (SUC) is the first critical step in pre-assessment planning under ISA/IEC 62443-3-2. This involves identifying the specific systems, assets, and processes to be assessed, ensuring that the evaluation is focused and aligned with organizational risk criteria. This step establishes a clear baseline for subsequent risk assessment activities and ensures compliance with the standard's structured approach.

**Question: 965**

In pre-assessment research for an IACS, you need to identify vulnerabilities in a Yokogawa DCS. Which NVD query syntax would yield the most precise results for 2024 vulnerabilities?

- A. yokogawa dcs cve-2024-\*
- B. cve yokogawa 2024
- C. yokogawa dcs vulnerability
- D. vendor:yokogawa product:dcx year:2024

Answer: D

Explanation: The structured query vendor:yokogawa product:dcx year:2024 targets Yokogawa DCS vulnerabilities in 2024, ensuring precision in the NIST NVD. Other options are less specific or incorrect for NVD's search interface.

**Question: 966**

A team is preparing for an ISA/IEC 62443-3-2 assessment and needs to document the cybersecurity requirements specification (CRS). Which element must be included in the CRS to comply with the standard?

- A. Security Level Target (SL-T) for each zone
- B. Detailed patch management procedures

- C. List of all known vulnerabilities
- D. Incident response plan details

Answer: A

Explanation: The cybersecurity requirements specification (CRS) in ISA/IEC 62443-3-2 must include the Security Level Target (SL-T) for each zone to define the required protection levels. Patch management, vulnerability lists, and incident response plans are developed later or separately, not as part of the CRS.

**Question: 967**

While critiquing a cybersecurity requirements specification (CRS), you find a requirement for "regular updates" to IACS software but no defined frequency or process for validation. What is the most critical improvement needed?

- A. Adding a requirement for manual updates
- B. Defining a specific update frequency and validation process
- C. Including a rollback mechanism only
- D. Specifying vendor contact for updates

Answer: B

Explanation: ISA/IEC 62443 requires clear and actionable security specifications. Defining a specific update frequency (e.g., monthly) and a validation process ensures that updates are applied consistently and verified for compatibility, reducing the risk of unpatched vulnerabilities or system instability.

**Question: 968**

A network diagram for an IACS shows a conduit between two zones with a data flow rate of 500 Mbps, but no encryption details are provided. Why is this a concern under ISA/IEC 62443?

- A. It hinders evaluation of data confidentiality protection
- B. It affects the physical cabling requirements
- C. It impacts the cost of network hardware
- D. It prevents accurate firmware tracking

Answer: A

Explanation: The lack of encryption details hinders the evaluation of data confidentiality protection, which is critical under ISA/IEC 62443. Unencrypted data flows through conduits can be intercepted, posing a significant risk to the security of the IACS.

**Question: 969**

A team is documenting cybersecurity requirements for an IACS in a steel mill. The system requires

Security Level 4 (SL-4) for data confidentiality. Which ISA/IEC 62443-3-3 requirement must be prioritized?

- A. FR1: Identification and Authentication Control
- B. FR3: System Integrity
- C. FR4: Data Confidentiality
- D. FR5: Restricted Data Flow

Answer: C

Explanation: For Security Level 4 (SL-4) with a focus on data confidentiality, ISA/IEC 62443-3-3 prioritizes FR4: Data Confidentiality, which ensures encryption and protection of sensitive data during transmission and storage.

**Question: 970**

During a risk assessment for an oil refinery's IACS, the team identifies a SCADA system communicating over an unencrypted Modbus/TCP protocol. A threat scenario involves an attacker intercepting and modifying control commands to cause a pressure surge in a pipeline. Which method should the team use to evaluate the likelihood of this threat scenario?

- A. Use a qualitative risk matrix based on expert judgment and threat intelligence
- B. Calculate the likelihood using historical attack data from the refinery's logs
- C. Perform a penetration test to simulate the interception and modification
- D. Assume a threat likelihood of 1 and focus on consequence severity

Answer: A

Explanation: ISA/IEC 62443-3-2 recommends a qualitative approach for evaluating threat likelihood in IACS environments due to the lack of reliable historical cybersecurity incident data. A qualitative risk matrix, informed by expert judgment and current threat intelligence, allows the team to assess the likelihood of an attacker intercepting and modifying Modbus/TCP communications while considering the specific context of the refinery's network and threat landscape.

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including Exam Questions, 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.



## Practice Exam Questions Based on Current Exam Objectives

Killexams.com provides practice 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 practice questions, candidates will cover the structure, difficulty level, and topics of the actual exam, helping them prepare more effectively and efficiently.

## Comprehensive Practice Exams (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 practice 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 Test Engine & Desktop Test Engine)

To support hands-on preparation, Killexams.com provides practice tests through both an Online Test Engine and a Desktop Test Engine. These tools are designed to simulate a real exam environment, allowing candidates to practice under exam-like conditions, with latest syllabus and topics of the exam. 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 practice 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 up-to-date, relevant material, and preparing with content that reflects current exam expectations, helping them stay confident and well-prepared.