ISA-IEC-62443$^{Q\&As}$

ISA/IEC 62443 Cybersecurity Fundamentals Specialist

Pass ISA ISA-IEC-62443 Exam with 100% Guarantee

QUESTION 1

Which of the following is the BEST reason for periodic audits?

Available Choices (select all choices that are correct)

A. To confirm audit procedures

B. To meet regulations

C. To validate that security policies and procedures are performing

D. To adhere to a published or approved schedule

Correct Answer: C

Periodic audits are an essential part of the ISA/IEC 62443 cybersecurity standards, as they help to verify the effectiveness and compliance of the security program. According to the ISA/IEC 62443-2-1 standard, periodic audits should be conducted to evaluate the following aspects1: The security policies and procedures are consistent with the security requirements and objectives of the organization The security policies and procedures are implemented and enforced in accordance with the security program The security policies and procedures are reviewed and updated regularly to reflect changes in the threat landscape, the IACS environment, and the business needs The security performance indicators and metrics are measured and reported to the relevant stakeholders The security incidents and vulnerabilities are identified, analyzed, and resolved in a timely manner The security awareness and training programs are effective and aligned with the security roles and responsibilities of the personnel The security audits and assessments are conducted by qualified and independent auditors The security audit and assessment results are documented and communicated to the appropriate parties The security audit and assessment findings and recommendations are addressed and implemented in a prioritized and systematic way Periodic audits are not only a means to meet regulations or adhere to a schedule, but also a way to validate that the security policies and procedures are performing as intended and achieving the desired security outcomes. Periodic audits also help to identify gaps and weaknesses in the security program and provide opportunities for improvement and enhancement. References: Periodic audits are an essential part of the ISA/IEC 62443 cybersecurity standards, as they help to verify the effectiveness and compliance of the security program. According to the ISA/IEC 62443-2-1 standard, periodic audits should be conducted to evaluate the following aspects1: The security policies and procedures are consistent with the security requirements and objectives of the organization The security policies and procedures are implemented and enforced in accordance with the security program The security policies and procedures are reviewed and updated regularly to reflect changes in the threat landscape, the IACS environment, and the business needs The security performance indicators and metrics are measured and reported to the relevant stakeholders The security incidents and vulnerabilities are identified, analyzed, and resolved in a timely manner The security awareness and training programs are effective and aligned with the security roles and responsibilities of the personnel The security audits and assessments are conducted by qualified and independent auditors The security audit and assessment results are documented and communicated to the appropriate parties The security audit and assessment findings and recommendations are addressed and implemented in a prioritized and systematic way Periodic audits are not only a means to meet regulations or adhere to a schedule, but also a way to validate that the security policies and procedures are performing as intended and achieving the desired security outcomes. Periodic audits also help to identify gaps and weaknesses in the security program and provide opportunities for improvement and enhancement. References:

QUESTION 2

Which of the following is an activity that should trigger a review of the CSMS?

Available Choices (select all choices that are correct)

A. Budgeting

B. New technical controls

C. Organizational restructuring

D. Security incident exposing previously unknown risk.

Correct Answer: BCD

According to the ISA/IEC 62443-2-1 standard, a review of the CSMS should be triggered by any changes that affect the cybersecurity risk of the industrial automation and control system (IACS), such as new technical controls, organizational restructuring, or security incidents1. Budgeting is not a trigger for CSMS review, unless it impacts the cybersecurity risk level or the CSMS itself2. References: 1: ISA/IEC 62443-2-1:2010, Section 4.3.3.3 2: A Practical Approach to Adopting the IEC 62443 Standards, ISAGCA Blog3

QUESTION 3

What does Layer 1 of the ISO/OSI protocol stack provide?

Available Choices (select all choices that are correct)

A. Data encryption, routing, and end-to-end connectivity

B. Framing, converting electrical signals to data, and error checking

C. The electrical and physical specifications of the data connection

D. User applications specific to network applications such as reading data registers in a PLC

Correct Answer: C

Layer 1 of the ISO/OSI protocol stack is the physical layer, which provides the means of transmitting and receiving raw data bits over a physical medium. It defines the electrical and physical specifications of the data connection, such as the voltage levels, signal timing, cable types, connectors, and pin assignments. It does not perform any data encryption, routing, end-to-end connectivity, framing, error checking, or user applications. These functions are performed by higher layers of the protocol stack, such as the data link layer, the network layer, the transport layer, and the application layer. References: ISO/IEC 7498-1:1994, Section 6.11; ISA/IEC 62443 Cybersecurity Fundamentals Specialist Study Guide, Section 3.1.12

QUESTION 4

Which of the following is an element of monitoring and improving a CSMS?

Available Choices (select all choices that are correct)

A. Increase in staff training and security awareness

B. Restricted access to the industrial control system to an as-needed basis

C. Significant changes in identified risk round in periodic reassessments

D. Review of system logs and other key data files

Correct Answer: ACD

According to the ISA/IEC 62443 Cybersecurity Fundamentals Specialist resources, a CSMS is a Cybersecurity Management System that defines the policies, procedures, and practices for managing the security of an industrial automation and control system (IACS). A CSMS should be monitored and improved continuously to ensure its effectiveness and alignment with the changing risk environment and business objectives. Some of the elements of monitoring and improving a CSMS are: Increase in staff training and security awareness: This element involves providing regular and updated training and awareness programs for the staff involved in the operation, maintenance, and security of the IACS. Training and awareness can help improve the skills, knowledge, and behavior of the staff, and reduce the likelihood and impact of human errors, negligence, or malicious actions. Training and awareness can also help foster a positive security culture and increase the staff\\'s engagement and commitment to the CSMS12 Significant changes in identified risk found in periodic reassessments: This element involves conducting periodic risk assessments to identify and evaluate the current and emerging threats, vulnerabilities, and consequences that may affect the IACS. Risk assessments can help determine the appropriate security levels (SLs) and security requirements for the system under control (SuC) and its components. Risk assessments can also help identify any gaps or weaknesses in the existing security measures and controls, and prioritize the actions for risk mitigation or acceptance. Periodic risk assessments can help ensure that the CSMS is responsive and adaptive to the changing risk landscape and business needs13 Review of system logs and other key data files: This element involves collecting, analyzing, and reviewing the system logs and other key data files that record the events and activities related to the IACS. System logs and data files can provide valuable information and insights for security monitoring, detection, response, and recovery. They can also help identify any anomalies, incidents, or breaches that may compromise the security or performance of the IACS. System logs and data files can also help measure and evaluate the effectiveness and efficiency of the CSMS and its processes, and provide feedback and recommendations for improvement14 References: ISA/IEC 62443 Cybersecurity Fundamentals Specialist Study Guide, Section 4.3, Cybersecurity Management System (CSMS) ISA/IEC 62443-2-1:2009, Security for industrial automation and control systems - Part 2-1: Establishing an industrial automation and control systems security program, Clause 5.3.2.1, Training and awareness ISA/IEC 62443-3-2:2020, Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design, Clause 4, Security risk assessment process ISA/IEC 62443-4-2:2019, Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components, Clause 4.3.3.7, Audit and accountabilit

QUESTION 5

What does the abbreviation CSMS round in ISA 62443-2-1 represent?

Available Choices (select all choices that are correct)

A. Control System Management System

B. Control System Monitoring System

C. Cyber Security Management System

D. Cyber Security Monitoring System

Correct Answer: C

The abbreviation CSMS stands for Cyber Security Management System in ISA 62443-2-1. This standard defines the elements necessary to establish a CSMS for industrial automation and control systems (IACS) and provides guidance on how to develop those elements123. A CSMS is a collection of policies, procedures, practices, and personnel that are responsible for ensuring the security of IACS throughout their lifecycle24. References: 1: ISA/IEC 62443 Series of Standards - ISA 2: ISA 62443-2-1 - Security for industrial automation and control systems, Part 2-1: Establishing an Industrial Automation and Control Systems Security Program | GlobalSpec 3: IEC 62443-2-1:2010 | IEC Webstore | cyber security, smart city 4: Structuring the ISA/IEC 62443 Standards - ISAGCA

Latest ISA-IEC-62443 Dumps

ISA-IEC-62443 VCE Dumps

ISA-IEC-62443 Practice Test