ISA-IEC-62443 Q&As

ISA/IEC 62443 Cybersecurity Fundamentals Specialist

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

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/isa-iec-62443.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by ISA Official Exam Center

Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers

QUESTION 1

Which is a common pitfall when initiating a CSMS program?

Available Choices (select all choices that are correct)

A. Organizational lack of communication

B. Failure to relate to the mission of the organization

C. Insufficient documentation due to lack of good follow-up

D. Immediate jump into detailed risk assessment

Correct Answer: D

"A common pitfall is to attempt to initiate a CSMS program without at least a high-level rationale that relates cyber security to the specific organization and its mission." A CSMS program is a Cybersecurity Management System program that follows the IEC 62443 standards for securing industrial control systems (ICS)1. A common pitfall when initiating a CSMS program is D. Immediate jump into detailed risk assessment. This is because a detailed risk assessment requires a clear definition of the system under consideration (SuC), the allocation of IACS assets to zones and conduits, and the identification of threats, vulnerabilities, and consequences for each zone and conduit2. These steps are part of the assess phase of the CSMS program, which is the first phase of the security program development process2. However, before starting the assess phase, it is important to have the management team\\'s support to ensure the CSMS program will have sufficient financial and organizational resources to implement necessary actions2. Therefore, jumping into detailed risk assessment without having the management buy-in is a common mistake that can jeopardize the success of the CSMS program.

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

Which layer specifies the rules for Modbus Application Protocol

Available Choices (select all choices that are correct)

A. Data link layer

B. Session layer

C. Presentation layer

D. Application layer

Correct Answer: D

The Modbus Application Protocol is a messaging protocol that provides client/server communication between devices connected on different types of buses or networks. It is positioned at level 7 of the OSI model, which is the application layer. The application layer is the highest level of the OSI model and defines the rules and formats for data exchange between applications. The Modbus Application Protocol is independent of the underlying communication layers and can be implemented using different transport protocols, such as TCP/IP, serial, or Modbus Plus. The Modbus Application Protocol defines the function codes, data formats, and error codes for Modbus transactions123 References: MODBUS APPLICATION PROTOCOL SPECIFICATION V1 Modbus - Wikipedia Overview of Modbus -- EPICS support for Modbus - GitHub Pages

QUESTION 4

Which of the following is an industry sector-specific standard?

Available Choices (select all choices that are correct)

A. ISA-62443 (EC 62443)

B. NIST SP800-82

C. API 1164

D. D. ISO 27001

Correct Answer: C

API 1164 is an industry sector-specific standard that provides guidance on the cybersecurity of pipeline supervisory control and data acquisition (SCADA) systems. API stands for American Petroleum Institute, which is the largest U.S. trade association for the oil and natural gas industry. API 1164 was first published in 2004 and revised in 2009 and 2021. The latest version of the standard aligns with the ISA/IEC 62443 series of standards and incorporates the concepts of security levels, zones, and conduits. API 1164 covers the security lifecycle of pipeline SCADA systems, from risk assessment and policy development to implementation and maintenance. The standard also defines roles and responsibilities, security requirements, security controls, and security assessment methods for pipeline SCADA systems. References: API 1164: Pipeline SCADA Security, Fourth Edition, September 2021 ISA/IEC 62443 Cybersecurity Fundamentals Specialist Study Guide, Section 2.2.2, Industry Sector-Specific Standards ISA/IEC 62443 Cybersecurity Fundamentals Specialist Exam Specification, Section 2.2.2, Industry Sector-Specific Standards

QUESTION 5

After receiving an approved patch from the JACS vendor, what is BEST practice for the asset owner to follow?

A. If a low priority, there is no need to apply the patch.

B. If a medium priority, schedule the installation within three months after receipt.

C. If a high priority, apply the patch at the first unscheduled outage.

D. If no problems are experienced with the current IACS, it is not necessary to apply the patch.

Correct Answer: C

According to the ISA/IEC 62443 Cybersecurity Fundamentals Specialist resources, patches are software updates that fix bugs, vulnerabilities, or improve performance of a system. Patches are classified into three categories based on their urgency and impact: low, medium, and high. Low priority patches are those that have minimal or no impact on the system functionality or security, and can be applied at the next scheduled maintenance. Medium priority patches are those that have moderate impact on the system functionality or security, and should be applied within a reasonable time frame, such as three months. High priority patches are those that have significant or criticalimpact on the system functionality or security, and should be applied as soon as possible, preferably at the first unscheduled outage. Applying patches in a timely manner is a best practice for maintaining the security and reliability of an industrial automation and control system (IACS). References: ISA/IEC 62443 Cybersecurity Fundamentals Specialist Study Guide, Section 4.3.2, Patch Management 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 5.3.2.2, Patch management ISA/IEC 62443-3-3:2013, Security for industrial automation and control systems - Part 3-3: System security requirements and security levels, Clause 4.3.3.6.2, Patch management

ISA-IEC-62443 VCE Dumps ISA-IEC-62443 Practice Test ISA-IEC-62443 Exam Questions