DUMPSBOSS.

ISA/IEC 62443 Cybersecurity Fundamentals Specialist

ISA ISA-IEC-62443

Version Demo

Total Demo Questions: 24

Total Premium Questions: 246

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

What impact do increasing cybercrime attacks have?

A. They primarily target personal devices.

B. They focus solely on financial institutions.

C. They affect suppliers of essential services.

D. They lead to improved cybersecurity measures.

ANSWER: C

Explanation:

They affect suppliers of essential services. Increasing cybercrime creates a material operational and societal risk when it targets organizations that deliver or support critical services, such as energy, water, transportation, healthcare, and manufacturing. These organizations commonly depend on interconnected information technology and operational technology environments, including industrial automation and control systems. A successful attack can therefore extend beyond data loss or a single business interruption: it can impair production, delivery, safety-related operations, and the continuity of services on which communities and other organizations depend.

This impact is central to the ISA/IEC 62443 cybersecurity perspective. The standards address cybersecurity risk in industrial automation and control systems through a lifecycle approach involving asset owners, service providers, and product suppliers. Applying defined security requirements, segmentation concepts, risk assessment, and secure development practices helps essential-service suppliers manage the growing likelihood and consequences of cyber threats. The importance of protecting these sectors is also reflected in CISA's critical-infrastructure guidance and ENISA's reporting on the evolving threat landscape. See ISA/IEC 62443 certificate program and CISA Critical Infrastructure Security and Resilience.

QUESTION NO: 2

What is the primary purpose of the NIST Cybersecurity Framework (CSF)?

A. To create new cybersecurity technologies

B. To replace existing cybersecurity standards

C. To enhance the resilience of critical infrastructure

D. To provide a certification for organizations

ANSWER: C

Explanation:

To enhance the resilience of critical infrastructure is correct. The NIST Cybersecurity Framework was initially developed in response to a U.S. Executive Order calling for a common framework to reduce cyber risk to critical infrastructure. Its core purpose is to provide a flexible, risk-based structure that organizations can use to understand, manage, and communicate cybersecurity risks. The Framework helps organizations establish or improve cybersecurity programs by organizing activities around cybersecurity outcomes, rather than prescribing a single technology, product, or compliance method.

Although the CSF is broadly applicable to organizations of any size or sector, resilience remains central to its intended outcome: organizations should be better able to anticipate, withstand, recover from, and adapt to cyber incidents and changing threats. NIST CSF 2.0 expresses this through the six Functions—Govern, Identify, Protect, Detect, Respond, and Recover—which support management of cybersecurity risk across an organization. This risk-management orientation also makes the Framework useful in industrial and operational-technology environments addressed by ISA/IEC 62443 programs. See NIST's Cybersecurity Framework overview and the NIST CSF 2.0 publication.

QUESTION NO: 3

Which is a role of the application layer?

Available Choices (select all choices that are correct)

A. Includes protocols specific to network applications such as email, file transfer, and reading data registers in a PLC

B. Includes user applications specific to network applications such as email, file transfer, and reading data registers in a PLC

C. Provides the mechanism for opening, closing, and managing a session between end-user application processes

D. Delivers and formats information, possibly with encryption and security

ANSWER: A D

Explanation:

The application layer supplies network services and protocols that application processes use to exchange information. Therefore, “Includes protocols specific to network applications such as email, file transfer, and reading data registers in a PLC” is correct. In an industrial environment, this includes protocols and services through which a client requests operational data or commands from a device, such as accessing PLC registers. The application layer concerns the network-facing protocol function, rather than the end-user software application itself.

“Delivers and formats information, possibly with encryption and security” is also correct in the practical protocol-stack context used for industrial networking. Application-level protocols define how meaningful messages, requests, responses, and data objects are represented for the communicating applications. Modern application services can also use security capabilities, including authenticated and encrypted communications, to protect the information exchanged. Although OSI concepts are often presented as distinct layers, real protocol suites commonly combine responsibilities that are conceptually associated with adjacent upper layers. For cybersecurity assessments, recognizing application-protocol communication and its protection is important because those protocols carry the operational data and commands that affect industrial processes. See the ISA/IEC 62443 Cybersecurity Fundamentals Specialist program and Cisco’s overview of the OSI networking model.

QUESTION NO: 4

Which is a commonly used protocol for managing secure data transmission on the Internet?

Available Choices (select all choices that are correct)

A. Datagram Transport Layer Security (DTLS)

B. Microsoft Point-to-Point Encryption

C. Secure Telnet

D. Secure Sockets Layer

ANSWER: A D

Explanation:

Datagram Transport Layer Security (DTLS) is a security protocol designed to protect application data carried over unreliable datagram transports, most notably UDP. It provides the essential security services needed for Internet communications: peer authentication, confidentiality through encryption, and integrity protection against undetected alteration. Its datagram-oriented design makes it suitable where applications need the characteristics of UDP while still requiring cryptographic protection.

Secure Sockets Layer is the historical protocol family commonly identified with securing Internet communications by establishing an encrypted, authenticated session between endpoints. In current implementations, TLS is the modern successor to SSL, and obsolete SSL versions must not be deployed. However, “Secure Sockets Layer” remains a commonly recognized term in foundational security material for the secure-session approach used by web services and other client-server communications. Both correct selections therefore identify protocols used to establish protected data transmission rather than merely identifying an application or encryption product. The IETF DTLS specification describes its security properties and use with datagram transport at RFC 6347; the current TLS standard is available at RFC 8446.

QUESTION NO: 5

What is TRUE regarding safety systems?

A. No dedicated malware has been found targeting safety systems specifically.

B. Even the most modern and sophisticated safety systems can be defeated by an attacker.

C. Safety systems are an independent protection layer and as such have no cybersecurity vulnerabilities.

D. By integrating control and safety systems via Modbus TCP, cybersecurity risks are at a tolerable level.

ANSWER: B

Explanation:

Even the most modern and sophisticated safety systems can be defeated by an attacker. Safety instrumented systems are designed to bring a process to, or maintain it in, a safe state when hazardous conditions arise. Their safety function is essential, but it does not make the equipment inherently immune to cyberattack. A capable adversary may target engineering workstations, safety controllers, communications paths, credentials, or the lifecycle processes used to configure and maintain the system. The TRITON/TRISIS incident demonstrated this risk in practice: malware was developed specifically to interact with Schneider Electric Triconex safety-instrumented-system controllers at an industrial site. This event established that attackers can deliberately pursue safety-system assets rather than merely affecting them as collateral damage. ISA/IEC 62443 therefore treats safety-related industrial automation and control system components as assets that require cybersecurity risk management, including secure architecture, access control, system hardening, monitoring, and controlled change management. Safety and cybersecurity must work together: the safety system provides a protective function for the physical process, while cybersecurity measures help preserve the integrity and availability of that function against intentional compromise. See the CISA TRITON malware alert and the ISA/IEC 62443 standards overview.

QUESTION NO: 6

Which organization is responsible for the ISA 62443 series of standards?

A. American National Standards Institute (ANSI)

B. International Electrotechnical Commission (IEC)

C. National Institute of Standards and Technology (NIST)

D. European Telecommunications Standards Institute (ETSI)

ANSWER: B

Explanation:

The **International Electrotechnical Commission (IEC)** is the correct answer because the IEC 62443 series is the internationally published set of standards for cybersecurity in industrial automation and control systems. These documents establish a common framework for securing industrial environments throughout their lifecycle, including concepts for security programs, risk assessment, system design, component requirements, and security levels. IEC standards are developed through international technical committees; IEC 62443 is maintained within IEC Technical Committee 65, which addresses industrial-process measurement, control, and automation. The series is commonly called ISA/IEC 62443 because its development has a close and ongoing relationship with ISA's ISA99 industrial cybersecurity standards work. However, IEC is the international standards organization that publishes the IEC 62443 documents and administers them as IEC international standards. This distinction matters in certification contexts: "ISA/IEC 62443" acknowledges the aligned ISA and IEC work, while "IEC 62443" identifies the formal international standards series. IEC's overview of industrial cybersecurity standards is available at https://www.iec.ch/cyber-security, and the IEC 62443 publication series can be found through the IEC Webstore search.

QUESTION NO: 7

A network-security review identifies communications that are not required for control operations. Which two measures BEST support restricted data flow between IACS zones? Select two.

A. Allow only approved hosts, protocols, ports, and communication directions.

B. Remove unnecessary services and communication paths.

C. Permit all traffic between zones to simplify troubleshooting.

D. Use one shared administrator account for both zones.

ANSWER: A B

Explanation:

Restricted data flow is supported by allowing only explicitly required communications and by enforcing those rules at controlled zone boundaries. Firewall or equivalent boundary rules can limit traffic by source, destination, protocol, port, and direction. Removing unnecessary services and communications reduces the attack surface and limits opportunities for lateral movement.

Permitting all traffic for convenience defeats the purpose of segmentation. Using one shared administrator account does not restrict data flow and weakens accountability and access control.

QUESTION NO: 8

An asset owner is preparing the scope for an IACS cybersecurity risk assessment. Which two items provide the MOST useful basis for defining the assessment boundaries and potential consequences? Select two.

A. An accurate inventory of IACS assets and their connections

B. Process-hazard information describing potential consequences

C. A list of antivirus signatures installed on office computers

D. A corporate marketing plan for the next financial year

ANSWER: A B

Explanation:

An accurate asset inventory and documented process-hazard information are essential inputs. The inventory identifies the control-system hardware, software, communications, interfaces, and supporting assets that are within scope. Process-hazard information helps the assessment team understand the possible safety, environmental, production, and equipment consequences if cybersecurity affects the process.

A list of current antivirus signatures does not establish the system boundary or process consequence. A corporate marketing plan is not a meaningful source for determining IACS cybersecurity scope or operational impact.

QUESTION NO: 9

Which protocol is commonly used for managing the security of message transmission on the Internet via web browsers?

A. TLS

B. L2TP

C. PPTP

D. IPsec

ANSWER: A

Explanation:

TLS is correct because it is the standard protocol browsers use to establish protected web sessions, most visibly through HTTPS. When a user connects to an HTTPS website, the browser and server use TLS to authenticate the server through digital certificates and to negotiate cryptographic parameters and session keys. TLS then protects data in transit by providing confidentiality, so transmitted information cannot readily be read by an unauthorized party, and integrity, so unauthorized modification can be detected. Modern browser security depends on TLS for activities such as signing in to sites, submitting forms, viewing sensitive operational dashboards, and accessing cloud services.

Within an industrial cybersecurity context, secure communications are an important part of protecting data flows between users, applications, and systems. TLS is particularly applicable when those flows use web technologies, including browser-based human-machine interfaces, management portals, and web APIs. The current TLS specification is TLS 1.3, defined by the Internet Engineering Task Force; HTTPS is defined as HTTP operating over TLS. See IETF RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3 and IETF RFC 9110: HTTPS.

QUESTION NO: 10

Which of the following technologies is no longer considered secure?

A. Secure Sockets Layer (SSL)

B. Transport Layer Security (TLS)

C. Digital Encryption Standard (DES)

D. Advanced Encryption Standard (AES)

ANSWER: A

Explanation:

Secure Sockets Layer (SSL) is no longer considered secure because its protocol versions have fundamental design and cryptographic weaknesses that permit practical attacks against confidentiality and connection integrity. SSL 2.0 has long been obsolete, and SSL 3.0 was shown to be vulnerable to attacks such as POODLE, which can expose portions of protected communications under certain conditions. The Internet Engineering Task Force formally deprecated SSL 3.0 and states that SSL 3.0 must not be used; this direction also reflects the broader industry move away from every SSL version. See RFC 7568: Deprecating Secure Sockets Layer Version 3.0. Secure communications should instead use a currently supported Transport Layer Security configuration, typically TLS 1.2 or TLS 1.3, with approved cipher suites and appropriate certificate validation. NIST's guidance for TLS implementations likewise requires support for TLS 1.2 and recommends TLS 1.3, while prohibiting obsolete SSL protocol versions in government TLS deployments. See NIST SP 800-52 Rev. 2. Therefore, Secure Sockets Layer (SSL) is the intended technology that is no longer considered secure.

QUESTION NO: 11

Security Levels (SLs) are broken down into which three types?

A. Target, capacity, and availability

B. Target, capacity, and achieved

C. Target, capability, and availability

D. Target, capability, and achieved

ANSWER: D

Explanation:

Target, capability, and achieved is correct because the ISA/IEC 62443 model distinguishes the security level that is needed, the level a solution is able to provide, and the level that is actually realized in operation. Target Security Level (SL-T) is established from the asset owner's risk assessment and defines the required degree of protection for a zone or conduit. Capability Security Level (SL-C) describes the security capability that a product, component, or system can provide when properly configured and used within its intended scope. Achieved Security Level (SL-A) represents the protection that has been implemented and verified in the deployed environment. These three concepts support a practical lifecycle process: determine the required protection, select and engineer capabilities that can meet it, and validate the implemented result. They also enable meaningful gap analysis between the required level and the operationally achieved level. The terminology originates in the foundational ISA/IEC 62443 security-level model and is used across the standards family's risk-based approach to industrial automation and control system cybersecurity. See the IEC 62443-1-1 publication record and ISA's ISA99/IEC 62443 standards overview.

QUESTION NO: 12

A remote service provider requires occasional access to an engineering workstation for approved maintenance. Which two measures BEST support secure remote access in an IACS environment? Select two.

A. Require unique, individually assigned accounts for remote personnel

B. Route remote sessions through a managed access point in a controlled zone

C. Permit direct Internet access to the engineering workstation during support periods

D. Provide a shared vendor account so that support can continue during personnel changes

E. Grant permanent remote access to avoid delays during future maintenance

ANSWER: A B

Explanation:

Remote access should be restricted to authorized users and tightly controlled paths. Requiring unique authenticated accounts supports accountability and prevents the loss of traceability associated with shared credentials. Routing access through a managed intermediary in a controlled zone supports segmentation, monitoring, and the enforcement of approved communications between the external party and the engineering workstation.

Directly exposing the engineering workstation increases attack surface and bypasses defense-in-depth controls. Permanent access and shared credentials are inconsistent with least privilege, access review, and effective accountability.

QUESTION NO: 13

What does Foundational Requirement 6 (FR 6) - Timely Response to Events (TRE) require?

A. Control access to information

B. Protect against unauthorized operation

C. Notify the proper authority about security violations

D. Ensure adequate responses to network resource requests

ANSWER: C

Explanation:

Notify the proper authority about security violations is correct because Timely Response to Events addresses the capability of an industrial automation and control system to react to detected security-relevant events quickly enough to support effective incident handling. In the ISA/IEC 62443 framework, this includes making relevant event information available and notifying the appropriate responsible personnel or authority when a security violation occurs. Timely notification enables personnel to investigate the event, determine its operational and safety implications, initiate containment measures, and coordinate recovery activities before the incident creates greater impact. The requirement is not limited to generating a

technical alert; notification must reach the party with the responsibility and authority to act on the event. This aligns with industrial-control-system incident-response practice, where prompt awareness and escalation are essential because cyber events can affect availability, process integrity, equipment, and safe operation. ISA identifies timely response to events as one of the foundational requirements used to structure cybersecurity capabilities for automation and control systems. See ISA's overview of the ISA/IEC 62443 standards and NIST's Guide to Operational Technology Security for OT event monitoring and incident-response guidance.

QUESTION NO: 14

Electronic security, as defined in ANSI/ISA-99.00.01:2007. includes which of the following?

Available Choices (select all choices that are correct)

A. Security guidelines for the proper configuration of IACS computers and operating systems

B. Computers, networks, operating systems, applications, and other programmable configurable components of the system

C. Personnel, policies, and procedures related to the security of computers, networks. PLCs, and other programmable configurable components of the system

D. Security guidelines for the proper configuration of IACS PLCs and other programmable configurable components of the system

ANSWER: B C

Explanation:

Electronic security in the ANSI/ISA-99.00.01:2007 industrial automation and control systems context is intentionally broad. It encompasses the technical assets that process, transmit, store, or control information, including "Computers, networks, operating systems, applications, and other programmable configurable components of the system." These interconnected components provide the electronic functionality that must be protected to maintain the secure operation of an IACS.

The definition also includes "Personnel, policies, and procedures related to the security of computers, networks. PLCs, and other programmable configurable components of the system." This recognizes that effective electronic security is not solely a product or technology feature. It depends on people performing defined responsibilities and on organizational policies and procedures that govern secure administration, operation, maintenance, access, and response. Together, the technical-system scope and the people/process scope reflect the defense-in-depth and lifecycle-oriented approach used throughout the ISA/IEC 62443 series. ISA identifies the ISA/IEC 62443 standards as a framework for securing industrial automation and control systems: ISA/IEC 62443 Series of Standards. This comprehensive view also aligns with NIST's treatment of security as protection involving information systems and the organizational measures used to manage them: NIST Information Security Glossary.

QUESTION NO: 15

A review finds that unauthorized users can download confidential production recipes and that authorized operators can modify control setpoints beyond their assigned duties. Which two foundational requirements are MOST directly implicated? Select two.

A. Data confidentiality

B. Use control

C. Timely response to events

D. Resource availability

ANSWER: A B

Explanation:

Data confidentiality is implicated because confidential production recipes are being disclosed to unauthorized users. Use control is implicated because operators are able to exercise privileges beyond their authorized duties. Use control includes authorization enforcement, least privilege, and restrictions on actions that authenticated users may perform.

Timely response to events concerns notification and response to security-relevant events. Resource availability concerns the ability of the system to provide required resources and services, not the unauthorized disclosure of recipes or excessive user privileges.

QUESTION NO: 16

Which of the following is a cause for the increase in attacks on IACS?

Available Choices (select all choices that are correct)

A. Use of proprietary communications protocols

B. The move away from commercial off the shelf (COTS) systems, protocols, and networks

C. Knowledge of exploits and tools readily available on the Internet

D. Fewer personnel with system knowledge having access to IACS

ANSWER: A C D

Explanation:

“Use of proprietary communications protocols,” “Knowledge of exploits and tools readily available on the Internet,” and “Fewer personnel with system knowledge having access to IACS” are contributing factors to the growth in successful attacks against industrial automation and control systems. Historically, proprietary protocols and products were frequently deployed with an assumption of isolation or obscurity rather than robust, independently validated security controls. As connectivity increases, weaknesses in those protocols can be identified, documented, and reused by attackers. The public availability of vulnerability research, proof-of-concept code, scanning capabilities, and exploitation frameworks also lowers the effort and specialized knowledge needed to identify and target exposed industrial assets. In addition, a shrinking pool of personnel who possess detailed, system-specific operational knowledge can make it harder for an organization to securely configure, maintain, monitor, patch, and recover its control environment. This operational knowledge gap is significant because industrial environments often contain long-lived technologies and specialized processes. ISA/IEC 62443 emphasizes managing cybersecurity risk across the lifecycle of these systems, including the people, processes, and technology involved. See the ISA/IEC 62443 overview and CISA’s Industrial Control Systems resources.

QUESTION NO: 17

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

ANSWER: C

Explanation:

Cyber Security Management System is the correct expansion of CSMS in ISA/IEC 62443-2-1. This part of the ISA/IEC 62443 series addresses the establishment of an industrial automation and control systems (IACS) security program. A CSMS provides the organized management framework through which an asset owner establishes, implements, maintains, and continually improves cybersecurity for IACS.

In practice, the CSMS is not a single technical product or monitoring capability. It encompasses the governance and lifecycle processes needed to manage cybersecurity systematically, including security policy, roles and responsibilities, risk assessment and treatment, security awareness and training, incident response, access management, change management, audit activities, and ongoing improvement. The purpose is to ensure that cybersecurity is managed consistently across the organization and throughout the lifecycle of its industrial systems.

ISA identifies the ISA/IEC 62443 standards as a comprehensive framework for securing industrial automation and control systems, and IEC 62443-2-1 specifically concerns establishing an IACS security program. See the ISA/IEC 62443 series overview and the IEC 62443-2-1 publication page.

QUESTION NO: 18

Which is an important difference between IT systems and IACS?

Available Choices (select all choices that are correct)

A. The IACS security priority is integrity.

B. The IT security priority is availability.

C. IACS cybersecurity must address safety issues.

D. Routers are not used in IACS networks.

ANSWER: A C

Explanation:

IACS cybersecurity assigns especially high importance to integrity because industrial control decisions depend on trustworthy commands, measurements, configurations, and logic. Integrity means that information and system functions remain accurate, complete, and protected from unauthorized modification. In an industrial environment, altered sensor values, setpoints, control logic, or device configurations can cause the process to operate outside safe limits. Consequently, integrity protections such as authenticated access, change control, configuration management, and verification of control-system data are central to a defensible IACS security program.

IACS cybersecurity must also address safety issues because cyber compromise can create physical consequences. Unlike many conventional information-system incidents, a successful attack on industrial automation can affect machinery, process conditions, people, property, and the environment. ISA/IEC 62443 addresses cybersecurity for industrial automation and control systems across their lifecycle and recognizes the need to manage cybersecurity in the context of operational and safety risks. Security controls should therefore be selected and operated so they preserve the safe, reliable performance of the industrial process while protecting the IACS from cyber threats. See the ISA/IEC 62443 overview and NIST's Guide to Operational Technology Security.

QUESTION NO: 19

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 found in periodic reassessments

D. Review of system logs and other key data files

ANSWER: A C D

Explanation:

“Increase in staff training and security awareness,” “Significant changes in identified risk found in periodic reassessments,” and “Review of system logs and other key data files” are elements that support the continual monitoring and improvement of a cybersecurity management system (CSMS). A CSMS is not static: the organization must monitor its performance, identify changes affecting cybersecurity risk, and take improvement actions. Training and awareness strengthen personnel competency and help ensure that personnel continue to recognize, report, and appropriately handle cybersecurity concerns. Periodic risk reassessments, as well as reassessments prompted by significant changes, keep the risk picture current and provide input for updates to controls, policies, and priorities. Reviewing logs and relevant system data provides operational monitoring evidence, supports detection and investigation of cybersecurity events, and helps identify trends requiring corrective action or further improvement.

These practices align with the management-system lifecycle embodied in IEC 62443-2-1, including monitoring, review, assessment, corrective action, and continual improvement. The standard is described by the IEC 62443-2-1 publication page; ISA also describes the CSMS concepts and lifecycle in its ISA/IEC 62443 certificate program.

QUESTION NO: 20

Which of the following activities is NOT listed under the â€œPatch Testingâ€□ phase in the asset owner requirements?

A. Notification

B. File authenticity

C. Removal procedure

D. Qualification and verification

E. None of the above; all of these activities are listed under Patch Testing.

ANSWER: E

Explanation:

None of the listed activities is excluded from the Patch Testing phase. The asset-owner patch-management requirements treat notification, verification of file authenticity, qualification and verification, and a removal procedure as patch-testing considerations. Testing is not limited to determining whether a patch installs successfully: it also establishes that the patch package can be trusted, is suitable for the intended industrial environment, has been properly validated, and can be removed or reversed in a controlled manner if operational issues occur. Notification supports coordination of the testing activity and communication of its outcome; file-authenticity checks help ensure the test uses a genuine, unaltered vendor patch; qualification and verification confirm the patch is appropriate and performs acceptably; and testing the removal procedure helps demonstrate that recovery can be performed safely. Therefore, the only accurate single-choice response is “None of the above; all of these activities are listed under Patch Testing.” This is consistent with the patch-management expectations in ISA/IEC 62443-2-1, which defines requirements for establishing an industrial automation and control systems security program. See the standard listing at IEC 62443-2-1 and ISA’s ISA/IEC 62443 standards overview.

QUESTION NO: 21

Which ISA/IEC 62443 part covers technical security requirements used by product suppliers, integration service providers, and asset owners?

A. ISA/IEC 62443-2-1

B. ISA/IEC 62443-2-4

C. ISA/IEC 62443-3-3

D. ISA/IEC 62443-4-2

ANSWER: C

Explanation:

ISA/IEC 62443-3-3 is correct because it defines the system-level security requirements and security levels for industrial automation and control systems. It translates the ISA/IEC 62443 foundational requirements—such as identification and authentication control, use control, system integrity, data confidentiality, restricted data flow, timely response to events, and resource availability—into detailed technical requirements for a control system. These requirements provide a common basis for specifying, designing, integrating, operating, and assessing the cybersecurity capabilities of an IACS solution. Consequently, asset owners can use the part when defining system requirements and target security levels, integration service providers can use it when implementing and validating system architectures, and product suppliers can use it to understand how components support security in the overall system. The requirements are organized by security level, allowing them to be selected in accordance with the risk-based security objectives established for a particular zone or conduit. ISA identifies this document as the standard addressing system security requirements and security levels; its application is central to a defense-in-depth IACS cybersecurity program. See the ISA/IEC 62443-3-3 standard listing and the IEC webstore publication entry.

QUESTION NO: 22

Which policies and procedures publication is titled Patch Manaqement in the IACS Environment?

Available Choices (select all choices that are correct)

A. ISA-TR62443-2-3

B. ISA-TR62443-1-4

C. ISA-62443-3-3

D. ISA-62443-4-2

ANSWER: A

Explanation:

ISA-TR62443-2-3 is correct because its formal title is *Security for industrial automation and control systems—Part 2-3: Patch management in the IACS environment*. The “TR” designation identifies it as a technical report within the ISA/IEC 62443 family. It addresses the patch-management lifecycle for industrial automation and control systems, including the coordination needed between asset owners and product suppliers to identify, assess, test, deploy, document, and monitor patches. In an IACS environment, patching must be handled through a managed process because availability, safety, production requirements, system dependencies, and the potential operational impact of changes all need to be considered alongside vulnerability remediation. The report therefore provides guidance for establishing and maintaining an IACS patch-management program and for communicating relevant patch information among the involved parties. ISA describes the ISA/IEC 62443 series as the standards framework for industrial automation and control system cybersecurity at ISA/IEC 62443 Series of Standards. The publication can also be located through the IEC standards catalogue by searching for its designation at IEC Webstore search.

QUESTION NO: 23

A plant is replacing a legacy engineering workstation with a supported platform. Which two activities BEST support secure change management for the replacement? Select two.

A. Test the replacement in a representative environment where feasible.

B. Update the approved configuration and recovery information.

C. Place the replacement into production before validating its operation.

D. Retain all legacy accounts and permissions without review.

ANSWER: A B

Explanation:

The replacement should be assessed for its effects on the IACS and tested against the intended configuration before it is placed into production. The change should also be documented, authorized, and supported by a recovery plan. These activities help ensure that security improvements do not introduce unacceptable availability, interoperability, or safety risks.

Using the workstation immediately after installation without validation can introduce unrecognized operational problems. Retaining obsolete accounts and permissions increases the risk of unauthorized access and does not support secure change management.

QUESTION NO: 24

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.

ANSWER: B C D

Explanation:

A cybersecurity management system (CSMS) must be reviewed whenever meaningful change or new information could alter the organization's industrial automation and control system (IACS) cybersecurity risk posture, the suitability of established controls, or the adequacy of risk treatment decisions. **New technical controls** are a review trigger because their introduction can change system architecture, interfaces, access paths, monitoring capabilities, operational dependencies, and residual risk. The CSMS should ensure that such controls are properly governed, assessed, documented, and maintained.

Organizational restructuring is also a trigger because it can change cybersecurity roles, authorities, accountabilities, staffing, segregation of duties, service-provider relationships, and escalation paths. The CSMS needs to remain aligned with the organization that operates it so that ownership and management responsibilities remain clear and effective.

A **security incident exposing previously unknown risk** provides direct evidence that existing assumptions, threat assessments, safeguards, or response arrangements may need adjustment. Reviewing the CSMS after this type of event supports lessons learned, updates to risk assessment and treatment, and continual improvement of cybersecurity governance. This change-driven review approach is consistent with the CSMS lifecycle addressed by ISA/IEC 62443-2-1 and the IEC publication record for the standard. See ISA/IEC 62443 and IEC 62443-2-1:2010.