Introduction to Industrial Security Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Table of Contents

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- Practice answering questions under realistic conditions,
- Improve accuracy and speed,
- Review explanations to strengthen weak areas, and
- Approach the exam with greater confidence.

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There's no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

Questions

1. **What is a key benefit of network segmentation in an industrial control system environment?**

   A. It allows unrestricted access for all users.

   B. It ensures no monitoring is needed.

   C. It limits lateral movement of attackers, protects safety-critical networks, and simplifies monitoring.

   D. It eliminates the need for any physical security measures.

2. **Which of the following is NOT a common insider threat indicator?**

   A. Unusual access patterns

   B. Unexplained data transfers

   C. Regular policy compliance

   D. Suspected collusion or sabotage

3. **Which is a stage in policy lifecycle management?**

   A. Creation

   B. Incident response

   C. Training

   D. Budget approval

4. **The National Industrial Security Program (NISP) is an optional industry-run program with policy established by cleared contractor facilities. True or False?**

   A. True

   B. False

   C. Not sure

   D. Not applicable

5. **Which statement best describes the difference between business continuity planning and disaster recovery?**

   A. Maintaining essential operations during disruptions

   B. Restoring IT systems and data after a disruption

   C. Focusing solely on vendor management

   D. Eliminating all disruptions completely

6. Which activity is performed by the ISSP/SCA?

A. Perform Classified Information System assessments

B. Issue security policies

C. Manage physical access control

D. Conduct background investigations

7. The policy for NISP is established by cleared contractor facilities. True or False?

A. True

B. False

C. Not sure

D. Not applicable

8. Which term is used to designate an organization's eligibility to access classified information?

A. Facility Clearance (FCL)

B. Security Classification

C. Personnel Security Clearance (PCL)

D. Security Certification

9. Which of the following is a responsibility of the Insider Threat Program Senior Official (ITPSO)?

A. Conduct Information System awareness and training

B. Keep the Facility Security Officer involved in the Insider Threat Program

C. Approve security clearances

D. Manage physical access badges

10. Who performs classified Information System assessments?

A. Facility Security Officer (FSO)

B. Information System Security Manager (ISSM)

C. Program Manager

D. Defense Counterintelligence and Security Agency (DCSA)

Answers

1. C
2. C
3. A
4. A
5. A
6. A
7. A
8. A
9. B
10. A

Explanations

1. What is a key benefit of network segmentation in an industrial control system environment?

A. It allows unrestricted access for all users.

B. It ensures no monitoring is needed.

C. It limits lateral movement of attackers, protects safety-critical networks, and simplifies monitoring.

D. It eliminates the need for any physical security measures.

Network segmentation in an industrial control system environment helps contain breaches by dividing the network into zones with restricted communication between them. The key benefit is that it limits lateral movement of attackers, so compromising one segment doesn't easily allow access to safety-critical networks or essential control devices. It also makes monitoring more effective, since security tools and logging can be tailored to each zone, making anomalies easier to detect and respond to. In practice, segmentation reduces the impact radius of incidents and simplifies incident response by introducing architectural barriers between IT and OT functions and between general network traffic and safety-critical operations. Physical security remains important, and monitoring is still needed, but segmentation directly supports containment, protection of critical control networks, and clearer oversight.

2. Which of the following is NOT a common insider threat indicator?

A. Unusual access patterns

B. Unexplained data transfers

C. Regular policy compliance

D. Suspected collusion or sabotage

Insider threat indicators are signs that someone inside the organization might be acting in ways that could harm security or expose data. Unusual access patterns, such as logging in at odd hours or reaching systems or data beyond what their role requires, signal potential risk. Unexplained data transfers, especially large or frequent transfers to external destinations, are classic red flags that data could be leaking or being exfiltrated. Suspected collusion or sabotage points to coordinated or intentional harm by insiders. Regular policy compliance, on the other hand, is what you'd expect from a legitimate user who is following rules and procedures. It doesn't raise security concerns the way the other examples do. So it's the indicator that does not fit with insider-threat signals, making it the best choice here.

3. Which is a stage in policy lifecycle management?

A. Creation

B. Incident response

C. Training

D. Budget approval

Policy lifecycle management starts with the creation of a policy, where the initial draft outlines the purpose, scope, roles, and controls. This drafting stage sets the foundation for subsequent steps like review, approval, distribution, implementation, and ongoing revision. Incident response belongs to operations and is not a stage of developing and maintaining a policy. Training is essential for ensuring people follow the policy, but it happens after the policy exists and is not itself a lifecycle stage. Budget approval pertains to governance and resource planning for implementing policies, rather than a stage in the policy's lifecycle.

4. The National Industrial Security Program (NISP) is an optional industry-run program with policy established by cleared contractor facilities. True or False?

A. True

B. False

C. Not sure

D. Not applicable

National Industrial Security Program establishes government-set security requirements for industry handling classified information, and participation is mandatory for cleared facilities. The policy is created by government agencies, not by the contractors themselves, and the program is administered under the NISPOM by the Defense Counterintelligence and Security Agency (DCSA) and other government offices. Contractors implement the requirements, but they do not set the policy. Therefore, this statement is false.

5. Which statement best describes the difference between business continuity planning and disaster recovery?

A. Maintaining essential operations during disruptions

B. Restoring IT systems and data after a disruption

C. Focusing solely on vendor management

D. Eliminating all disruptions completely

The main idea is that business continuity planning aims to keep essential operations running during disruptions, while disaster recovery focuses on restoring IT systems and data after an outage. A business continuity plan takes a broad view of the organization: it covers people, processes, facilities, suppliers, and communications, and it outlines how critical functions will continue or quickly resume when something goes wrong. Disaster recovery, by contrast, is a more IT-specific effort within that broader plan, dealing with getting servers, networks, and data back online after an incident. Since the goal of business continuity is to maintain ongoing operations, the statement describing maintaining essential operations during disruptions best captures the difference. The other options point to IT restoration, vendor management, or eliminating all disruptions, which are narrower or unrealistic in scope.

6. Which activity is performed by the ISSP/SCA?

A. Perform Classified Information System assessments

B. Issue security policies

C. Manage physical access control

D. Conduct background investigations

Security control assessments of Classified Information Systems are what ISSP and Security Control Assessor teams focus on. In the RMF framework, these roles are responsible for evaluating the security controls that protect systems handling classified data. They plan, execute, and document assessments to verify that safeguards are properly implemented, functioning, and in line with required standards, supporting the authorization decision and ongoing monitoring. This direct focus on testing and validating the system's security posture is why this activity is the best match. Other tasks—issuing security policies, managing physical access control, and conducting background investigations—are handled by different roles such as policy owners, physical security personnel, and personnel security investigators.

7. The policy for NISP is established by cleared contractor facilities. True or False?

A. True

B. False

C. Not sure

D. Not applicable

In the National Industrial Security Program, the facility that holds or handles classified information is responsible for implementing and maintaining the security program. This means the cleared contractor facility develops its own internal security policies, procedures, and controls that are aligned with NISPOM and the contract requirements, and then executes them on a day-to-day basis under government oversight. So the policy framework you operate under is established at the facility level by the contractor, while the government provides the overarching requirements and standards. That alignment is why the statement is true: the policy for NISP is established and enforced at the cleared contractor facility level.

8. Which term is used to designate an organization's eligibility to access classified information?

A. Facility Clearance (FCL)

B. Security Classification

C. Personnel Security Clearance (PCL)

D. Security Certification

The central idea is that an organization earns the right to handle classified information through a facility clearance. This formal designation, granted by the government after evaluating the organization's safeguarding practices, security procedures, and overall readiness to protect sensitive material, shows the organization is authorized to access and work with classified contracts. Once the organization has this clearance, its cleared personnel can handle information under the organization's security program. In contrast, security classification refers to the level of sensitivity of the information itself (such as top secret or secret), not to who or what can access it. A personnel security clearance belongs to an individual, not the organization, and security certification isn't the standard term for organizational eligibility to access classified data.

9. Which of the following is a responsibility of the Insider Threat Program Senior Official (ITPSO)?

A. Conduct Information System awareness and training

B. Keep the Facility Security Officer involved in the Insider Threat Program

C. Approve security clearances

D. Manage physical access badges

Understanding the role of the Insider Threat Program Senior Official centers on governance and coordination of the insider threat program. The ITPSO is the senior leader who ensures the program is integrated with the facility's security operations. Keeping the Facility Security Officer involved is essential because the FSO oversees day-to-day facility security, including operations that touch insider threat indicators, reporting, and coordination with security governance. This partnership ensures insider threat activities align with overall security posture and that there's a clear, consistent line of communication to leadership. The other tasks—conducting system awareness and training, approving security clearances, and managing physical access badges—are typically handled by other security, personnel, or facilities roles, not by the ITPSO.

10. Who performs classified Information System assessments?

A. Facility Security Officer (FSO)

B. Information System Security Manager (ISSM)

C. Program Manager

D. Defense Counterintelligence and Security Agency (DCSA)

The on-site Facility Security Officer is responsible for the facility's security program, including ensuring classified information systems are properly reviewed. The FSO coordinates and often conducts the classified Information System assessments to verify that access controls, procedures, physical protection, and incident response practices meet requirements and that any findings are tracked and remediated. The Information System Security Manager handles the technical security of the information system but work under the facility's security leadership to implement controls, not as the primary on-site assessor. The Defense Counterintelligence and Security Agency provides external oversight and audits, not day-to-day assessments performed at the facility, and the Program Manager focuses on mission execution rather than security assessments. So the Facility Security Officer is the best fit to perform these assessments.

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://introtoindustrialsec.examzify.com

We wish you the very best on your exam journey. You've got this!