OCFA SECURING UTILITIES PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://ocfasecuringutilities.examzify.com

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

SAMPLE

Table of Contents

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 5

Answers 8

Explanations 10

Next Steps 16

SAMPLE

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.

SAMPLE

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!

SAMPLE

Questions

SAMPLE

1. Which sequence constitutes a secure decommissioning of an OT asset?

A. Disconnect from network and delete the asset from accounting only.

B. Disconnect from network, wipe data, destroy credentials.

C. Physically destroy the asset without updating inventories.

D. Remove from network, wipe data, destroy credentials, collect proof of disposal, and update asset inventories and change logs.

2. Why is patch management particularly challenging in OT environments, and what two-phase approach improves safety?

A. OT devices patch automatically with no testing

B. OT devices may have vendor-specific firmware, real-time constraints, downtime risks; two-phase approach: test patches in a controlled lab and staged pilot before deployment; change control and rollback plans to minimize disruption

C. Patching is irrelevant in OT environments

D. Patch management is fully automated with no oversight

3. Commercial service lines can be up to how many psi?

A. up to 60 psi

B. up to 0.3 psi

C. up to 12 psi

D. up to 5 psi

4. What is a key SIEM challenge in OT environments?

A. They require no configuration.

B. They do not collect logs from OT devices.

C. OT-specific data sources require careful tuning and normalization.

D. They automatically remediate threats.

5. Why is coordination with public safety and emergency management agencies critical?

A. It is optional and adds complexity

B. It is only for weather events

C. They understand incident impact, coordinate response measures, and ensure public safety; miscoordination can worsen outages or hazards

D. It delays restoration

SAMPLE

6. What is defense-in-depth in securing utility networks, and which example illustrates its application across IT, DMZ, and OT zones?

A. Layered controls across IT, DMZ, and OT with IT firewalls and EDR, DMZ jump hosts and industrial gateways, OT isolation and monitoring

B. A single-layer firewall approach relying on perimeter defense

C. Only endpoint protection in IT, with no DMZ or OT considerations

D. Physical security measures without network controls

7. How is data integrity protected in OT data flows?

A. Rely on encryption only without integrity checks.

B. Only monitor data after it arrives at control center.

C. Data integrity is not a concern in OT.

D. Use checksums, digital signatures, and hash validation; implement redundant data paths and regular backups; ensure data in transit and at rest are protected.

8. Which monitoring tools are appropriate for detecting unusual OT activity?

A. Only antivirus on IT endpoints

B. SIEM, IDS, and anomaly detection

C. Manual review of logs once per year

D. No monitoring in OT networks

9. A pole with how many transformers is a good indicator of three-phase power use?

A. Two transformers

B. Three transformers

C. Four transformers

D. Five transformers

10. Which practice improves data integrity for historian data stores by detecting tampering?

A. Implement integrity checks

B. Encrypt data at rest

C. Restrict access by role

D. Secure connections

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which sequence constitutes a secure decommissioning of an OT asset?

A. Disconnect from network and delete the asset from accounting only.

B. Disconnect from network, wipe data, destroy credentials.

C. Physically destroy the asset without updating inventories.

D. Remove from network, wipe data, destroy credentials, collect proof of disposal, and update asset inventories and change logs.

Secure decommissioning of an OT asset combines removing all access, sanitizing data, ensuring there is verifiable disposal, and keeping accurate records. Disconnecting the asset from the network stops any ongoing or future remote control or monitoring, which is essential to prevent unauthorized access. Wiping the data eliminates sensitive configurations, logs, and other information that could be misused if recovered. Destroying credentials prevents any reuse of accounts or tokens tied to the asset, closing off entry points that could be exploited later. Collecting proof of disposal provides a verifiable trail for audits and compliance, ensuring stakeholders can confirm the asset was handled properly. Updating asset inventories and change logs ensures the organization's records reflect the disposal, prevents orphaned assets, and supports ongoing security governance. Other options miss one or more of these critical elements, creating gaps in security, traceability, or governance.

2. Why is patch management particularly challenging in OT environments, and what two-phase approach improves safety?

A. OT devices patch automatically with no testing

B. OT devices may have vendor-specific firmware, real-time constraints, downtime risks; two-phase approach: test patches in a controlled lab and staged pilot before deployment; change control and rollback plans to minimize disruption

C. Patching is irrelevant in OT environments

D. Patch management is fully automated with no oversight

OT environments face unique challenges because many devices run vendor-specific firmware and must meet strict real-time control requirements. A patch can alter timing, interoperability, or safety logic, and applying it often means downtime or reconfiguring control loops, which can disrupt the process or create safety risks. A two-phase approach helps manage that risk: first, test patches in a controlled lab that mirrors the OT system to verify compatibility and safety; then run a staged pilot on a limited set of devices to observe performance in real-world conditions before a full rollout. Coupled with formal change control and rollback plans, this approach provides a safe path to apply security updates without causing unexpected outages or unsafe behavior. Patching without testing or oversight, or assuming patching is irrelevant, would ignore the critical need to safeguard both safety and availability in OT operations.

SAMPLE

3. Commercial service lines can be up to how many psi?

A. up to 60 psi

B. up to 0.3 psi

C. up to 12 psi

D. up to 5 psi

Gas service lines to commercial buildings are treated as low-pressure conduits. They're designed so the utility can regulate the pressure down to safe, appliance-friendly levels, and five pounds per square inch represents the upper limit typically allowed for a service connection. This keeps the line within the range that standard regulators and safety practices can manage. Pressures above this are not considered service lines and require different handling and equipment. So five psi is the standard maximum for commercial service lines, which is why that option is the best fit.

4. What is a key SIEM challenge in OT environments?

A. They require no configuration.

B. They do not collect logs from OT devices.

C. OT-specific data sources require careful tuning and normalization.

D. They automatically remediate threats.

In OT environments, the data feeding a SIEM comes from a variety of specialized sources—PLCs, historians, HMIs, engineering workstations, and industrial gateways—each with its own log formats and event meanings. This diversity means the SIEM must be carefully configured to collect from these sources and, crucially, to normalize and map the data into a common structure so that events from different devices can be correlated meaningfully. You also need to tune parsers, time references, and field mappings, and establish baselines for normal OT behavior, so alerts reflect real anomaly or intrusion patterns rather than noise from unfamiliar OT activity. Without this normalization and tuning, you can't reliably detect cross-device sequences that indicate threats in an OT setup. Other statements miss the reality of OT SIEMs: you do configure collectors and parsers because OT devices use varied formats; OT logs can indeed be collected, but they typically require specialized connectors and normalization to be useful; and SIEMs focus on detection and alerting rather than automatically remediating threats, with remediation usually handled by other security controls or SOC playbooks.

5. Why is coordination with public safety and emergency management agencies critical?

A. It is optional and adds complexity

B. It is only for weather events

C. They understand incident impact, coordinate response measures, and ensure public safety; miscoordination can worsen outages or hazards

D. It delays restoration

Cooperation with public safety and emergency management agencies is essential because they provide the big-picture view of how an incident affects people and critical infrastructure. They understand the incident's impact across sectors, help set restoration priorities that protect life and safety, and coordinate response actions across many responders. This ensures field crews aren't duplicating efforts, road blocks and safety protocols are managed, and resources are allocated where they're most needed. Sharing information through a common command framework improves situational awareness and speeds up safe, effective restoration. It's relevant for all types of incidents, not just weather events, and without this coordination, actions can conflict, hazards can worsen, and outages can last longer.

SAMPLE

6. What is defense-in-depth in securing utility networks, and which example illustrates its application across IT, DMZ, and OT zones?

A. Layered controls across IT, DMZ, and OT with IT firewalls and EDR, DMZ jump hosts and industrial gateways, OT isolation and monitoring

B. A single-layer firewall approach relying on perimeter defense

C. Only endpoint protection in IT, with no DMZ or OT considerations

D. Physical security measures without network controls

Defense-in-depth means building multiple, complementary layers of security that protect different parts of the network so that a breach in one area doesn't lead to a full compromise. In securing utility networks, this concept is applied by layering protections across IT, DMZ, and OT zones, each with controls suited to that zone's role and risk. In the IT zone, you strengthen the human-machine layer with strong firewalls and endpoint detection and response, plus solid access controls and secure configurations. This reduces the chance that a compromised user device or server can be used to reach deeper into the network. The DMZ acts as a protective buffer between IT and OT. Here you introduce mechanisms to tightly control and monitor traffic crossing the boundary, such as jump hosts for administrator access and specialized gateways that enforce protocol and authentication policies. This prevents direct, unfettered access from IT to OT. In the OT zone, you emphasize isolation and continuous monitoring. Segmentation limits the spread of any intrusion, and ongoing surveillance detects unusual or unauthorized activity quickly, enabling rapid containment. This layered approach is why the defense-in-depth idea is so effective for utility networks: it reduces reliance on a single perimeter, provides multiple opportunities to detect and block attacks, and supports safer remote access and change management across critical operations. A single-layer perimeter defense or focusing only on IT endpoints misses the need for segmentation and monitoring across DMZ and OT, and physical security measures without network controls don't address the actual traffic and behavior on the network.

7. How is data integrity protected in OT data flows?

A. Rely on encryption only without integrity checks.

B. Only monitor data after it arrives at control center.

C. Data integrity is not a concern in OT.

D. Use checksums, digital signatures, and hash validation; implement redundant data paths and regular backups; ensure data in transit and at rest are protected.

In OT environments, keeping data trustworthy as it moves from sensors and controllers through networks to storage is essential because inaccurate or tampered data can lead to unsafe operations. Protecting data integrity involves several layers that work together. Use checksums, hash functions, and digital signatures to detect any changes to data in transit or at rest; these allow the receiving system to verify that the data received is exactly what was sent and to identify tampering or corruption. Pairing these with secure channels that provide integrity guarantees (often via authenticated encryption or message authentication codes) helps prevent undetected modifications while data is moving. Build in redundancy with multiple data paths so there are independent routes for verification and delivery, and maintain regular backups so you can restore from a known-good state if integrity is compromised. Protecting data both in transit and at rest, plus maintaining logs and audit trails, helps detect and respond to integrity issues promptly. Relying on encryption alone won't catch all alterations, monitoring only after data arrives misses in-flight tampering, and claiming integrity isn't a concern ignores the safety-critical need to trust OT data.

SAMPLE

8. Which monitoring tools are appropriate for detecting unusual OT activity?

A. Only antivirus on IT endpoints

B. SIEM, IDS, and anomaly detection

C. Manual review of logs once per year

D. No monitoring in OT networks

Detecting unusual OT activity relies on layered monitoring that provides real-time visibility into OT networks and devices, plus the ability to recognize deviations from normal operations. SIEM, IDS, and anomaly detection work together to achieve this. SIEM collects and correlates logs from OT and IT sources, giving a centralized view and enabling alerts when events match suspicious patterns or show unusual sequences. IDS monitors network traffic and can detect known attack signatures or abnormal communication patterns across OT protocols like Modbus, DNP3, or IEC 60870-5. Anomaly detection builds a baseline of normal OT behavior—things like typical command frequencies, device interactions, and setpoint changes—and flags deviations that may indicate malware, misconfigurations, or unsafe changes. Using all three creates timely, actionable detections across the control network. For example, a sudden surge of write commands to a PLC, combined with unusual command sequences and an unexpected login, might trigger SIEM correlations and IDS alerts, while anomaly detection would flag behavior that falls outside the established OT baseline. This kind of coordinated visibility is essential in OT, where threats can impact safety and operations. Relying only on antivirus on IT endpoints misses OT-specific threats and protocols, as OT devices may not run standard antivirus or expose the same attack surfaces. Reviewing logs only once a year is far too slow to catch fast-moving threats or zero-days. And having no monitoring at all leaves OT networks blind to intrusions and anomalous behavior.

9. A pole with how many transformers is a good indicator of three-phase power use?

A. Two transformers

B. Three transformers

C. Four transformers

D. Five transformers

Three-phase power is distributed using three separate phase voltages, offset from one another by 120 degrees. A common and clear way utilities do this is to mount one transformer for each phase on the same pole, forming a three-transformer bank. So, when you see three transformers on a single pole, that visual setup is a strong indicator that the line is carrying three-phase power, since each transformer is handling one of the three phases. If you see only two transformers on a pole, that usually points to a single-phase setup or a subset of services rather than a full three-phase bank. Seeing four or five transformers on one pole is not the standard arrangement for indicating three-phase distribution, so it's less reliable as a cue for three-phase power.

SAMPLE

10. Which practice improves data integrity for historian data stores by detecting tampering?

A. Implement integrity checks

B. Encrypt data at rest

C. Restrict access by role

D. Secure connections

Detecting tampering and preserving data integrity in historian data stores relies on implementing integrity checks. These checks create a verifiable fingerprint of the data, such as cryptographic hashes or checksums, at the moment data is captured and later re-verified to confirm nothing has changed. By storing baseline digests in a secure, tamper-evident location and periodically recalculating and comparing hashes, you can quickly detect any alteration. Techniques like append-only or WORM storage, combined with tamper-evident logs or auditable records, make changes visible and support reliable audit trails. For large amounts of time-series data, scalable approaches like Merkle trees or batched hash manifests help verify integrity without slowing down access. This focus on verifying that stored data remains exactly as it was, over time, is what enables prompt detection of tampering. Encrypting data at rest protects confidentiality, not necessarily the ability to detect changes after the fact. Restricting access by role reduces the chance of unauthorized modification but doesn't provide ongoing verification of data integrity. Securing connections protects data in transit, but the stored data's integrity over time requires these fingerprinting and verification mechanisms.

SAMPLE

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://ocfasecuringutilities.examzify.com

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

SAMPLE