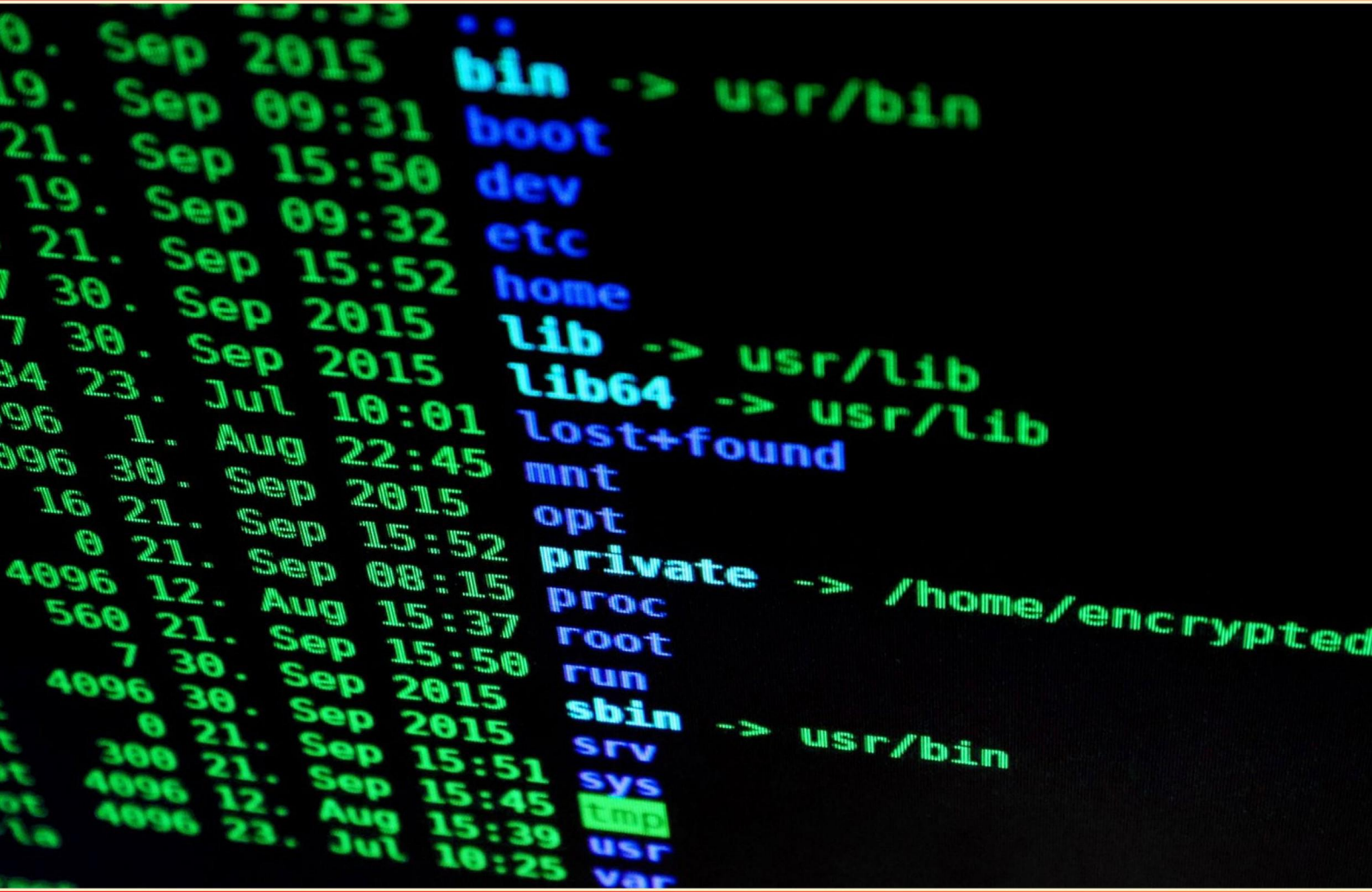
DISA ASSURED COMPLIANCE ASSESSMENT SOLUTION (ACAS) PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://disaacas.examzify.com

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 function of the dashboards in Tenable.sc?

A. To create new networking protocols

B. To generate reports for auditor purposes

C. To provide visual summaries and trends of network security

D. To establish network connections

2. Which icon is used for launching a scan or report?

A. Launch Button

B. Start Scan

C. Run Report

D. Execute Job

3. What types of data can ACAS collect during a scan?

A. Financial data and user passwords

B. Configuration data, vulnerability information, and compliance status

C. Network traffic and performance metrics

D. Intrusion detection alerts and malware signatures

4. Which of the following actions allows you to set an expiration date?

A. Add To Scratch Pad

B. Accept Risk

C. Launch Remediation Scan

D. Recast Risk

5. How does ACAS assist organizations during security incidents?

A. By providing detailed user training

B. By offering antivirus software at a discount

C. By providing rapid identification of vulnerabilities that may have been exploited

D. By directly responding to threats on behalf of organizations

6. What is a significant factor in ACAS's ability to enhance security measures?

A. Limited access to reports

B. Integration of automated vulnerability scans

C. Dependence on manual processes for all assessments

D. Scheduled downtime during assessments

7. Is the Nessus Network Monitor required as part of the task order?

A. True

B. False

C. Only for specific situations

D. It is optional

8. What target configurations can be included in your Freeze Window?

A. All Systems

B. Assets

C. IPs

D. All of the above

9. What type of reports does ACAS generate for compliance assessments?

A. Security analysis reports

B. Compliance reports against established security standards

C. Vulnerability assessment summaries

D. Network performance reports

10. Which security center role is responsible for creating an organization?

A. Administrator

B. Security Analyst

C. Security Manager

D. Executive

Answers

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

Explanations

1. What is a key function of the dashboards in Tenable.sc?

A. To create new networking protocols

B. To generate reports for auditor purposes

C. To provide visual summaries and trends of network security

D. To establish network connections

The key function of the dashboards in Tenable.sc is to provide visual summaries and trends of network security. Dashboards are designed to consolidate complex data into understandable visual formats, allowing users to quickly interpret the security posture of their networks. By presenting information through graphs, charts, and other visual aids, individuals and teams can identify security issues, trends over time, and areas that require attention, enabling more informed decision-making and proactive security management. This visualization capability is crucial in a cybersecurity context where timely insights can lead to quicker responses to threats and vulnerabilities. The ability to summarize vast amounts of security data in visually interpretable formats is foundational for effective monitoring and management of network security.

2. Which icon is used for launching a scan or report?

A. Launch Button

B. Start Scan

C. Run Report

D. Execute Job

The icon labeled "Launch Button" is used for initiating a scan or report in the ACAS framework. This terminology aligns with common user interface design conventions where a "Launch" or "Start" button typically signifies the action of beginning a process or executing a command. In many software environments, the term "Launch" indicates a broader function that encompasses various tasks, including starting scans and generating reports, making it an intuitive choice for users. The other options, while they may describe specific actions associated with scans or reports, are more descriptive commands rather than general user interface terminology for initiating a process. "Start Scan" and "Run Report" suggest specific tasks rather than the overarching action of launching, which could include both scanning and reporting functionalities. Similarly, "Execute Job" implies a more technical action that may not explicitly indicate scanning or reporting, making "Launch Button" the most appropriate choice for a general interface element used to initiate these actions.

3. What types of data can ACAS collect during a scan?

A. Financial data and user passwords

B. Configuration data, vulnerability information, and compliance status

C. Network traffic and performance metrics

D. Intrusion detection alerts and malware signatures

The correct choice highlights that ACAS is primarily focused on gathering information related to the security posture of systems within a network. Specifically, it collects configuration data, which includes information about system settings and software installations; vulnerability information, which identifies potential weaknesses in the system that could be exploited by attackers; and compliance status, which assesses whether systems adhere to established security standards and regulations. This focus on configuration, vulnerabilities, and compliance is essential for organizations to maintain a robust security framework and improve their cybersecurity posture. Understanding these aspects allows security personnel to manage risks effectively, ensuring that systems are configured securely and compliant with policies. The other options, while relevant to different aspects of cybersecurity, do not align with the specific functions of ACAS. Financial data and user passwords pertain to sensitive information that ACAS does not focus on collecting. Network traffic and performance metrics involve monitoring system performance rather than security assessments. Intrusion detection alerts and malware signatures are important for threat detection but fall outside the primary scope of what ACAS aims to collect during its scans.

4. Which of the following actions allows you to set an expiration date?

A. Add To Scratch Pad

B. Accept Risk

C. Launch Remediation Scan

D. Recast Risk

Setting an expiration date is typically associated with the management of identified risks and how those risks are tracked over time. When you accept a risk, you are formally acknowledging the presence of that risk and deciding that it does not require immediate remediation, often accompanied by a decision on how long that acceptance is valid. This process involves a determined timeframe during which the risk will be monitored, thus necessitating an expiration date. By defining when the risk acceptance will be reevaluated or reviewed, you can effectively manage your compliance and assurance activities. The other actions mentioned do not inherently pertain to the assignment of an expiration date to risks. Adding items to a scratch pad is often used for temporary storage of information or tasks but does not impact risk management timelines. Launching a remediation scan focuses on identifying or resolving vulnerabilities rather than managing risks explicitly. Recasting risk typically involves reassessing or redefining a risk rather than assigning an expiration to it. Therefore, the action of accepting risk directly aligns with the establishment of an expiration date within the context of risk management in compliance assessments.

5. How does ACAS assist organizations during security incidents?

A. By providing detailed user training

B. By offering antivirus software at a discount

C. By providing rapid identification of vulnerabilities that may have been exploited

D. By directly responding to threats on behalf of organizations

ACAS (Assured Compliance Assessment Solution) plays a critical role in assisting organizations during security incidents primarily by offering rapid identification of vulnerabilities that may have been exploited. In the context of a security incident, the ability to quickly diagnose existing vulnerabilities allows organizations to respond effectively and prioritize their remediation efforts. This rapid identification is vital for limiting the damage caused by a security breach, as it enables organizations to understand which systems and assets are at risk and require immediate attention. The focus of ACAS is on assessing and reporting the compliance status of systems against established security configurations and best practices. When a security incident occurs, having a robust tool like ACAS allows security teams to quickly determine if any previously known vulnerabilities were targeted. This proactive approach helps them to not only mitigate the current threat but also to strengthen their defenses against future attacks. In comparison, options like providing detailed user training, offering antivirus software at a discount, or directly responding to threats miss the essential function of ACAS in vulnerability management during security incidents. While training and software solutions are important components of an overall security posture, they do not address the immediate need for detection and assessment that is critical during or immediately following a security incident.

6. What is a significant factor in ACAS's ability to enhance security measures?

A. Limited access to reports

B. Integration of automated vulnerability scans

C. Dependence on manual processes for all assessments

D. Scheduled downtime during assessments

The integration of automated vulnerability scans is a significant factor in ACAS's ability to enhance security measures. Automated scans allow for consistent and comprehensive examination of systems to identify vulnerabilities quickly and efficiently. By leveraging automation, ACAS can conduct regular assessments, ensuring that security measures are continuously updated and that potential weaknesses are identified and addressed promptly. This proactive approach significantly strengthens an organization's overall security posture by reducing the time and effort needed for manual assessments while increasing the frequency and depth of vulnerability detection. In contrast, limited access to reports would hinder transparency and the ability to take informed actions based on the assessment results. Dependence on manual processes for all assessments would slow down the evaluation and remediation cycles, as manual checks are often more time-consuming and less thorough compared to automated scans. Scheduled downtime during assessments could disrupt critical operations and limit the assessment process, ultimately lowering the effectiveness of the security evaluation. Therefore, the integration of automated vulnerability scans stands out as the most impactful element in bolstering security within the ACAS framework.

7. Is the Nessus Network Monitor required as part of the task order?

A. True

B. False

C. Only for specific situations

D. It is optional

The Nessus Network Monitor is indeed required as part of the task order because it plays a crucial role in providing continuous monitoring and assessment of the network security posture. This tool is designed to detect vulnerabilities and misconfigurations within the network, which is essential for maintaining compliance with security standards and frameworks. In the context of the DISA Assured Compliance Assessment Solution (ACAS), having a reliable monitoring tool like Nessus Network Monitor ensures that organizations can proactively identify security risks and apply necessary remediation measures. The requirement for this tool underscores the importance of real-time visibility into network security, making it a foundational element of the ACAS framework. While other options might suggest the tool is only needed in certain scenarios or that it could be optional, the standardized processes and compliance needs dictate that it is a necessary component to effectively fulfill the security assessment objectives outlined in the task order. This comprehensive approach helps organizations meet their security obligations and enhances the overall integrity of their systems.

8. What target configurations can be included in your Freeze Window?

A. All Systems

B. Assets

C. IPs

D. All of the above

In the context of the Freeze Window in the DISA Assured Compliance Assessment Solution (ACAS), the correct answer encompasses all mentioned categories: systems, assets, and IPs. A Freeze Window is a designated timeframe during which changes to configurations are restricted to ensure system stability and compliance verification. Including "All Systems" allows for a broad application across various devices and platforms within an organization. When you include "Assets," it's focusing on the specific items that need to be monitored or assessed within that timeframe, ensuring all critical components are accounted for. By incorporating "IPs," you can specify or monitor specific network addresses that are crucial to compliance and security checks. Therefore, the inclusion of all these elements — systems, assets, and IPs — enables comprehensive coverage and enhances compliance readiness during the Freeze Window. This approach facilitates better management and oversight of potential changes that could impact the security posture or compliance state of the organization. It is essential in maintaining an effective compliance program, as it ensures every relevant aspect is reviewed without external modifications during the assessment period.

9. What type of reports does ACAS generate for compliance assessments?

A. Security analysis reports

B. Compliance reports against established security standards

C. Vulnerability assessment summaries

D. Network performance reports

The ACAS generates compliance reports against established security standards as part of its functionality in assessing compliance with various mandates and regulations. These compliance reports are crucial for organizations to ensure that their systems and operations meet specific security and operational standards defined by authorities such as the Department of Defense or other regulatory entities. The reports can highlight areas of compliance or non-compliance, providing organizations with actionable insights and a clear understanding of their security posture regarding established policies and guidelines. This focus on compliance reports underscores the solution's role in maintaining regulatory adherence and helps organizations prepare for audits. It reassures stakeholders that effective risk management practices are being implemented while engaging in a systematic approach to ongoing security assessments. In contrast, while security analysis reports, vulnerability assessment summaries, and network performance reports provide valuable insights into different aspects of an organization's security infrastructure, they do not specifically focus on compliance with established security standards. Thus, they serve different purposes in the larger context of network and information security management.

10. Which security center role is responsible for creating an organization?

A. Administrator

B. Security Analyst

C. Security Manager

D. Executive

The Administrator role in a security center is primarily responsible for setting up and managing the organization's infrastructure within the security system. This encompasses creating and configuring the organization itself, which includes defining the structure, roles, and permissions that are essential for the system's operational effectiveness. The Administrator ensures that the security framework aligns with the organization's policies and compliance requirements. This role is foundational, as it lays the groundwork for how security procedures are implemented and who has access to what within the organization. The effectiveness of the security program is heavily reliant on the Administrator's ability to establish a robust and secure organization setup. As such, the Administrator's tasks often involve not just initial setup, but ongoing management and updates to adapt to new security challenges or structural changes within the organization. The other roles, while integral to the security center's operations, have different focuses; for example, the Security Analyst investigates and responds to security incidents, the Security Manager oversees the security protocols and strategies, and the Executive focuses on high-level oversight, strategic decisions, and stakeholder engagement.

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://disaacas.examzify.com

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