# Reliable ISO-IEC-27035-Lead-Incident-Manager Test Tips - ISO-IEC-27035-Lead-Incident-Manager Learning Materials


As most of the people tend to use express delivery to save time, our ISO-IEC-27035-Lead-Incident-Manager preparation exam will be sent out within 5-10 minutes after purchasing. As long as you pay at our platform, we will deliver the relevant exam materials to your mailbox within the given time. Our company attaches great importance to overall services, if there is any problem about the delivery of ISO-IEC-27035-Lead-Incident-Manager Exam Materials: PECB Certified ISO/IEC 27035 Lead Incident Manager, please let us know, a message or an email will be available.

Usually, the questions of the real exam are almost the same with our ISO-IEC-27035-Lead-Incident-Manager exam questions. So you just need to memorize our correct questions and answers of the ISO-IEC-27035-Lead-Incident-Manager study materials. You absolutely can pass the exam. Also, we will offer good service to add you choose the most suitable ISO-IEC-27035-Lead-Incident-Manager Practice Braindumps since we have three different versions of every exam product. And you can free download the demos of the ISO-IEC-27035-Lead-Incident-Manager learning quiz.

**>> Reliable ISO-IEC-27035-Lead-Incident-Manager Test Tips <<**

## 100% Pass Quiz PECB - ISO-IEC-27035-Lead-Incident-Manager - High Pass-Rate Reliable PECB Certified ISO/IEC 27035 Lead Incident Manager Test Tips

Our ISO-IEC-27035-Lead-Incident-Manager exam questions are based on the actual situation to stimulate exam circumstance in order to provide you a high-quality and high-efficiency user experience. In addition, the ISO-IEC-27035-Lead-Incident-Manager exam guide function as a time-counter, and you can set fixed time to fulfill your task, so that promote your efficiency in real test. The key strong-point of our ISO-IEC-27035-Lead-Incident-Manager Test Guide is that we impart more important knowledge with fewer questions and answers, with those easily understandable ISO-IEC-27035-Lead-Incident-Manager study braindumps, you will find more interests in them and experience an easy learning process.

## PECB ISO-IEC-27035-Lead-Incident-Manager Exam Syllabus Topics:

| Topic | Details |
|---|---|
| Topic 1 | • Preparing and executing the incident response plan for information security incidents: This section of the exam measures skills of Incident Response Managers and covers the preparation and activation of incident response plans. It focuses on readiness activities such as team training, resource allocation, and simulation exercises, along with actual response execution when incidents occur. |
| Topic 2 | • Designing and developing an organizational incident management process based on ISO<br>• IEC 27035: This section of the exam measures skills of Information Security Analysts and covers how to tailor the ISO<br>• IEC 27035 framework to the unique needs of an organization, including policy development, role definition, and establishing workflows for handling incidents. |
| Topic 3 | • Improving the incident management processes and activities: This section of the exam measures skills of Incident Response Managers and covers the review and enhancement of existing incident management processes. It involves post-incident reviews, learning from past events, and refining tools, training, and techniques to improve future response efforts. |
| Topic 4 | • Fundamental principles and concepts of information security incident management: This section of the exam measures skills of Information Security Analysts and covers the core ideas behind incident management, including understanding what constitutes a security incident, why timely responses matter, and how to identify the early signs of potential threats. |

## PECB Certified ISO/IEC 27035 Lead Incident Manager Sample Questions (Q53-Q58):

**NEW QUESTION # 53**
Scenario 7: Located in central London, Konzolo has become a standout innovator in the cryptocurrency field.
The company faced challenges monitoring the security of its own and third-party systems. An incident involving server downtime exposed vulnerabilities in a third-party service provider's security posture, leading to unauthorized access.
In response, Konzolo launched a thorough vulnerability scan of its cryptographic wallet software and uncovered critical weaknesses due to outdated encryption algorithms. Noah, the IT manager, documented and communicated the findings. Paulina was brought in to lead a forensic investigation, provide actionable insights, and help enhance the company's overall incident response strategy based on ISO/IEC 27035 standards.
Based on the scenario above, answer the following question:
Which of the following steps for effective security monitoring did Konzolo NOT adhere to?

- A. Monitor the outsourced services
- B. Monitor security vulnerabilities
- C. Monitor behavioral analytics

**Answer: A**

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-1:2016 and ISO/IEC 27035-2:2016 emphasize the importance of monitoring not only internal systems but also third-party or outsourced services. Clause 7.3.2 of ISO/IEC 27035-2 specifically recommends that organizations establish mechanisms for the continuous monitoring of service providers and outsourced systems, particularly when such services process or store sensitive information.
In the scenario, Konzolo suffered an incident due to a failure by a third-party service provider to uphold security controls. This indicates that Konzolo had insufficient or no effective monitoring of outsourced services in place, which directly contributed to the breach and system downtime.
On the other hand:
Option A is incorrect because Konzolo did conduct a vulnerability scan, identifying and addressing cryptographic weaknesses.
Option B is also incorrect, as Paulina conducted forensic and behavioral analysis (both manual and automated) as part of the investigation process.
Reference Extracts:
ISO/IEC 27035-2:2016, Clause 7.3.2: "Monitoring should not be limited to internal infrastructure but should include third-party and outsourced services to ensure that they are operating within defined security parameters." ISO/IEC 27002:2022, Control 5.23:

"Information security should be addressed in agreements with third parties." Correct answer: C
-

**NEW QUESTION # 54**
Which document provides guidelines for planning and preparing for incident response and for learning lessons from the incident response process?

- A. ISO/IEC 27035-2
- B. ISO/IEC 27037
- C. ISO/IEC 27035-1

**Answer: A**

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-2:2016 is titled "Information security incident management - Part 2: Guidelines to plan and prepare for incident response." This document provides detailed guidance on establishing an incident response capability, planning for incident response, and implementing effective response actions. It also emphasizes the importance of post-incident analysis and lessons learned to improve future incident handling.
Key activities covered in ISO/IEC 27035-2 include:
* Planning and preparing for incident handling (e.g., policy development, roles and responsibilities)
* Establishing and training the incident response team (IRT)
* Developing communication strategies and escalation procedures
* Conducting root cause analysis and collecting lessons learned
* Applying improvements to prevent recurrence
By contrast:
* ISO/IEC 27035-1 provides high-level principles of incident management (Part 1: Principles).
* ISO/IEC 27037 relates to the handling of digital evidence and is focused more on forensic practices than incident response preparation.
Reference Extracts:
* ISO/IEC 27035-2:2016, Introduction: "This part provides guidance on the planning and preparation necessary for effective incident response and for learning lessons from incidents."
* ISO/IEC 27035-2:2016, Clause 6.5: "Lessons learned and reporting can help improve future incident response and provide input to risk assessments and control improvements."

**NEW QUESTION # 55**
Scenario 1: RoLawyers is a prominent legal firm based in Guadalajara, Mexico. It specializes in a wide range of legal services tailored to meet the diverse needs of its clients. Committed to excellence and integrity, RoLawyers has a reputation for providing legal representation and consultancy to individuals, businesses, and organizations across various sectors.
Recognizing the critical importance of information security in today's digital landscape, RoLawyers has embarked on a journey to enhance its information security measures. This company is implementing an information security incident management system aligned with ISO/IEC 27035-1 and ISO/IEC 27035-2 guidelines. This initiative aims to strengthen RoLawyers' protections against possible cyber threats by implementing a structured incident response process to provide guidance on establishing and maintaining a competent incident response team.
After transitioning its database from physical to online infrastructure to facilitate seamless information sharing among its branches, RoLawyers encountered a significant security incident. A malicious attack targeted the online database, overloading it with traffic and causing a system crash, making it impossible for employees to access it for several hours.
In response to this critical incident, RoLawyers quickly implemented new measures to mitigate the risk of future occurrences. These measures included the deployment of a robust intrusion detection system (IDS) designed to proactively identify and alert the IT security team of potential intrusions or suspicious activities across the network infrastructure. This approach empowers RoLawyers to respond quickly to security threats, minimizing the impact on their operations and ensuring the continuity of its legal services.
By being proactive about information security and incident management, RoLawyers shows its dedication to protecting sensitive data, keeping client information confidential, and earning the trust of its stakeholders.
Using the latest practices and technologies, RoLawyers stays ahead in legal innovation and is ready to handle cybersecurity threats with resilience and careful attention.
According to scenario 1, what information security incident did RoLawyers face?

- A. Man-in-the-middle attack

- B. Malware attack
- C. Denial-of-service attack

**Answer: C**

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
According to ISO/IEC 27035-1:2016, an information security incident is any event that compromises the confidentiality, integrity, or availability of information. In this scenario, RoLawyers experienced an attack where their online database was overloaded with excessive traffic, resulting in a system crash. This incident made it impossible for employees to access the database for several hours. This type of event is characteristic of a Denial-of-Service (DoS) attack. ISO/IEC 27035-1 Annex B provides examples of typical incidents, and one example includes "network-based attacks, including denial-of-service attacks." A DoS attack typically aims to make a service or resource unavailable to its intended users by overwhelming it with traffic.
There is no indication in the scenario that the attackers were intercepting communications (as would be seen in a Man-in-the-Middle attack) or installing malware to damage or steal data. The nature of the attack- excess traffic causing a crash-clearly aligns with the definition of a DoS attack.
Reference Extracts:
ISO/IEC 27035-1:2016, Clause B.2.1 (Examples of incident types): "Denial-of-service (DoS) attacks cause disruption or degradation of services." ISO/IEC 27035-1:2016, Clause 4.1: "An incident can result from deliberate attacks such as DoS, malicious code, or unauthorized access." Therefore, the incident faced by RoLawyers was a Denial-of-Service attack.
-

**NEW QUESTION # 56**
What is the first step in planning the response to information security incidents?

- A. Developing processes that support the response to information security incidents
- B. Defining the response classification
- C. Assigning the response class based on incident information

**Answer: B**

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
In ISO/IEC 27035-2:2016, the planning phase of incident response starts with establishing a classification system. Response classification is essential to ensure that incidents are assessed and categorized in a consistent manner, allowing appropriate response measures to be applied. This classification forms the foundation for selecting the right procedures, team involvement, and communication protocols.
Assigning a response class (Option A) is a subsequent step that occurs once an incident is analyzed and matched to a pre-defined category. Developing response processes (Option B) is important but comes after the classification model is defined.
Reference Extracts:
ISO/IEC 27035-2:2016, Clause 6.3.2: "The response planning process begins with the classification of potential incidents to determine the required actions and responsibilities." Clause 7.2.2: "Defining response classes helps the organization decide how to handle specific categories of incidents." Correct answer: C
-

**NEW QUESTION # 57**
How should vulnerabilities lacking corresponding threats be handled?

- A. They still require controls and should be promptly addressed
- B. They should be disregarded as they pose no risk
- C. They may not require controls but should be analyzed and monitored for changes

**Answer: C**

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
According to ISO/IEC 27005:2018 (which supports ISO/IEC 27035 in risk management and threat assessment processes), vulnerabilities that are not currently associated with known threats do not necessarily need immediate remediation or technical control measures. However, they cannot be ignored entirely either.

Such vulnerabilities may not pose an active risk at the present time, but that can change quickly if a new threat emerges that can exploit them. Therefore, these vulnerabilities should be documented, assessed in context, and monitored over time. This process ensures that if the threat landscape evolves, the organization can respond proactively.
The standard emphasizes a risk-based approach, which includes:
* Analyzing vulnerabilities in relation to assets and threat likelihood
* Monitoring the environment for changes that may introduce new threats
* Avoiding unnecessary or unjustified resource expenditure on low-risk issues Option A is incorrect because it suggests addressing all vulnerabilities without considering risk context.
Option B is risky and contradicts ISO best practices, which emphasize continuous risk monitoring.
Reference Extracts:
* ISO/IEC 27005:2018, Clause 8.2.2: "Vulnerabilities without known threats may not require treatment immediately but should be monitored regularly."
* ISO/IEC 27001:2022, Annex A, Control A.8.8 - "Management of technical vulnerabilities should be risk- based and responsive to changes." Therefore, the correct answer is C: They may not require controls but should be analyzed and monitored for changes.
-

**NEW QUESTION # 58**
.....

If you plan to apply for the PECB Certified ISO/IEC 27035 Lead Incident Manager (ISO-IEC-27035-Lead-Incident-Manager) certification exam, you need the best ISO-IEC-27035-Lead-Incident-Manager practice test material that can help you maximize your chances of success. You cannot rely on invalid ISO-IEC-27035-Lead-Incident-Manager Materials and then expect the results to be great. So, you must prepare from the updated PECB ISO-IEC-27035-Lead-Incident-Manager Exam Dumps to crack the ISO-IEC-27035-Lead-Incident-Manager exam.

**ISO-IEC-27035-Lead-Incident-Manager Learning Materials**: https://www.examslabs.com/PECB/ISO-27001/best-ISO-IEC-27035-Lead-Incident-Manager-exam-dumps.html

- Latest Released Reliable ISO-IEC-27035-Lead-Incident-Manager Test Tips - PECB ISO-IEC-27035-Lead-Incident-Manager Learning Materials: PECB Certified ISO/IEC 27035 Lead Incident Manager □ Open ✔ www.examsreviews.com □✔□ and search for ➠ ISO-IEC-27035-Lead-Incident-Manager □ to download exam materials for free □Free ISO-IEC-27035-Lead-Incident-Manager Braindumps
- Vce ISO-IEC-27035-Lead-Incident-Manager Test Simulator □ ISO-IEC-27035-Lead-Incident-Manager Valid Test Vce □ ISO-IEC-27035-Lead-Incident-Manager Valid Test Vce Free □ Simply search for □ ISO-IEC-27035-Lead-Incident-Manager □ for free download on ▹ www.pdfvce.com ◃ □ISO-IEC-27035-Lead-Incident-Manager Exam Flashcards
- PECB ISO-IEC-27035-Lead-Incident-Manager Questions - Latest ISO-IEC-27035-Lead-Incident-Manager Dumps [2025] □ Search for " ISO-IEC-27035-Lead-Incident-Manager " and obtain a free download on { www.real4dumps.com } □100% ISO-IEC-27035-Lead-Incident-Manager Accuracy
- Latest ISO-IEC-27035-Lead-Incident-Manager Dumps Ppt □ ISO-IEC-27035-Lead-Incident-Manager Valid Test Vce Free □ Real ISO-IEC-27035-Lead-Incident-Manager Braindumps □ Download ▹ ISO-IEC-27035-Lead-Incident-Manager ◃ for free by simply searching on ⇛ www.pdfvce.com ⇚ □ISO-IEC-27035-Lead-Incident-Manager New Real Exam
- ISO-IEC-27035-Lead-Incident-Manager Valid Mock Test □ Vce ISO-IEC-27035-Lead-Incident-Manager Test Simulator □ ISO-IEC-27035-Lead-Incident-Manager Upgrade Dumps □ Open □ www.torrentvalid.com □ and search for [ ISO-IEC-27035-Lead-Incident-Manager ] to download exam materials for free □Exam ISO-IEC-27035-Lead-Incident-Manager Question
- ISO-IEC-27035-Lead-Incident-Manager Valid Mock Test □ Real ISO-IEC-27035-Lead-Incident-Manager Braindumps □ Exam ISO-IEC-27035-Lead-Incident-Manager Question □ Download ➽ ISO-IEC-27035-Lead-Incident-Manager □ for free by simply searching on { www.pdfvce.com } □Latest ISO-IEC-27035-Lead-Incident-Manager Exam Camp
- Vce ISO-IEC-27035-Lead-Incident-Manager Test Simulator □ ISO-IEC-27035-Lead-Incident-Manager Valid Exam Braindumps □ ISO-IEC-27035-Lead-Incident-Manager Upgrade Dumps □ Open website □ www.prep4away.com □ and search for ⇛ ISO-IEC-27035-Lead-Incident-Manager ⇚ for free download □ISO-IEC-27035-Lead-Incident-Manager Valid Mock Test
- ISO-IEC-27035-Lead-Incident-Manager Test Score Report □ ISO-IEC-27035-Lead-Incident-Manager New Real Exam □ 100% ISO-IEC-27035-Lead-Incident-Manager Accuracy □ Easily obtain 「 ISO-IEC-27035-Lead-Incident-Manager 」 for free download through 「 www.pdfvce.com 」 □ISO-IEC-27035-Lead-Incident-Manager Valid Test Vce
- ISO-IEC-27035-Lead-Incident-Manager Updated Test Cram 👆 100% ISO-IEC-27035-Lead-Incident-Manager Accuracy □ Real ISO-IEC-27035-Lead-Incident-Manager Braindumps □ Open □ www.prep4away.com □ enter " ISO-

IEC-27035-Lead-Incident-Manager " and obtain a free download Guaranteed ISO-IEC-27035-Lead-Incident-Manager Success

- ISO-IEC-27035-Lead-Incident-Manager Valid Exam Braindumps  ISO-IEC-27035-Lead-Incident-Manager Exam Flashcards  ISO-IEC-27035-Lead-Incident-Manager New Real Exam  Search for ✔ ISO-IEC-27035-Lead-Incident-Manager ✔ on  www.pdfvce.com  immediately to obtain a free download Free ISO-IEC-27035-Lead-Incident-Manager Braindumps
- Latest Released Reliable ISO-IEC-27035-Lead-Incident-Manager Test Tips - PECB ISO-IEC-27035-Lead-Incident-Manager Learning Materials: PECB Certified ISO/IEC 27035 Lead Incident Manager  Enter ➤ www.real4dumps.com  and search for { ISO-IEC-27035-Lead-Incident-Manager } to download for free ✉ 100% ISO-IEC-27035-Lead-Incident-Manager Accuracy
- www.myvrgame.cn, actual4testcert.blogspot.com, universityofapprointernational.com, graaphi.com, www.yiwang.shop, cou.alnoor.edu.iq, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, ncon.edu.sa, www.stes.tyc.edu.tw, Disposable vapes