# ISO-IEC-27035-Lead-Incident-Manager Exam Pattern - ISO-IEC-27035-Lead-Incident-Manager Authorized Exam Dumps


BONUS!!! Download part of FreePdfDump ISO-IEC-27035-Lead-Incident-Manager dumps for free: https://drive.google.com/open?id=1bPIsgKSwxDR5N4Ep9hCE2acU6q0OBP6-

For candidates who are looking for ISO-IEC-27035-Lead-Incident-Manager exam braindumps, they pay much attention to the quality. With experienced experts to compile and verify, ISO-IEC-27035-Lead-Incident-Manager exam materials are high quality, and you can pass your exam and get the corresponding certification successfully. In addition, we recommend you to try free demo for ISO-IEC-27035-Lead-Incident-Manager Exam Dumps before purchasing, so that you can know what the complete version is like. We have online and offline service. If you have any questions for ISO-IEC-27035-Lead-Incident-Manager exam materials, you can consult us, and we will give you reply as quickly as we can.

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

| Topic | Details |
|---|---|
| Topic 1 | • 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. |
| Topic 2 | • Implementing incident management processes and managing information security incidents: This section of the exam measures skills of Information Security Analysts and covers the practical implementation of incident management strategies. It looks at ongoing incident tracking, communication during crises, and ensuring incidents are resolved in accordance with established protocols. |
| Topic 3 | • 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 4 | • 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. |

**>> ISO-IEC-27035-Lead-Incident-Manager Exam Pattern <<**

# ISO-IEC-27035-Lead-Incident-Manager PDF Dumps [2026] For Productive Exam Preparation

The page of our ISO-IEC-27035-Lead-Incident-Manager simulating materials provides demo which are sample questions. The purpose of providing demo is to let customers understand our part of the topic and what is the form of our study materials when it is opened? In our minds, these two things are that customers who care about the ISO-IEC-27035-Lead-Incident-Manager Exam may be concerned about most. We will give you our software which is a clickable website that you can visit the product page. Red box marked in our ISO-IEC-27035-Lead-Incident-Manager exam practice is demo; you can download PDF version for free, and you can click all three formats to see.

# PECB Certified ISO/IEC 27035 Lead Incident Manager Sample Questions (Q54-Q59):

**NEW QUESTION # 54**
Scenario 5: Located in Istanbul, Turkey, Alura Hospital is a leading medical institution specializing in advanced eye surgery and vision care. Renowned for its modern facilities, cutting-edge technology, and highly skilled staff, Alura Hospital is committed to delivering exceptional patient care. Additionally, Alura Hospital has implemented the ISO/IEC 27035 standards to enhance its information security incident management practices.
At Alura Hospital, the information security incident management plan is a critical component of safeguarding patient data and maintaining the integrity of its medical services. This comprehensive plan includes instructions for handling vulnerabilities discovered during incident management. According to this plan, when new vulnerabilities are discovered, Mehmet is appointed as the incident handler and is authorized to patch the vulnerabilities without assessing their potential impact on the current incident, prioritizing patient data security above all else.
Recognizing the importance of a structured approach to incident management, Alura Hospital has established four teams dedicated to various aspects of incident response. The planning team focuses on implementing security processes and communicating with external organizations. The monitoring team is responsible for security patches, upgrades, and security policy implementation. The analysis team adjusts risk priorities and manages vulnerability reports, while the test and evaluation team organizes and performs incident response tests to ensure preparedness.
During an incident management training session, staff members at Alura Hospital were provided with clear roles and responsibilities. However, a technician expressed uncertainty about their role during a data integrity incident, as the manager assigned them a role unrelated to their expertise. This decision was made to ensure that all staff members possess versatile skills and are prepared to handle various scenarios effectively.
Additionally, Alura Hospital realized it needed to communicate better with stakeholders during security incidents. The hospital discovered it was not adequately informing stakeholders and that relevant information must be provided using formats, language, and media that meet their needs. This would enable them to participate fully in the incident response process and stay informed about potential risks and mitigation strategies.
Also, the hospital has experienced frequent network performance issues affecting critical hospital systems and increased sophisticated cyberattacks designed to bypass traditional security measures. So, it has deployed an external firewall. This action is intended to strengthen the hospital's network security by helping detect threats that have already breached the perimeter defenses. The firewall's implementation is a part of the hospital's broader strategy to maintain a robust and secure IT infrastructure, which is crucial for protecting sensitive patient data and ensuring the reliability of critical hospital systems. Alura Hospital remains committed to integrating state-of-the-art technology solutions to uphold the highest patient care and data security standards.
Based on scenario 5, the hospital decided to deploy an external firewall to detect threats that have already breached the perimeter defenses in response to frequent network performance issues affecting critical hospital systems. Is this recommended?

- A. No, they should have deployed an intrusion detection system to identify and alert the incident response team of the breach
- B. Deploying an external firewall to detect threats that have already breached the perimeter defenses
- C. No, they should have implemented a cloud-based antivirus solution instead of deploying an external firewall

**Answer: B**

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-2:2016 (Information Security Incident Management - Part 2: Guidelines to Plan and Prepare for Incident Response) provides specific guidance on implementing protective technologies that enhance detection, prevention, and response to

information security incidents. Among the recommendations, deploying firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and other layered security mechanisms are considered essential practices in ensuring network and system resilience.
In this case, Alura Hospital experienced repeated network performance issues and targeted cyberattacks. Their decision to deploy an external firewall is appropriate and aligns with best practices outlined in ISO/IEC
27035-2, especially for a healthcare institution handling sensitive patient data. External firewalls act as a network barrier that not only prevents unauthorized access but also helps monitor and detect anomalies or threats that may have already breached traditional perimeter defenses. This is particularly important in environments where traditional safeguards are being bypassed by sophisticated attackers.
While intrusion detection systems (option C) are also important, the scenario mentions that the firewall is being used as part of a broader layered defense system and is meant to detect already-breached threats. Cloud- based antivirus solutions (option B) are not a substitute for firewalls in terms of network protection and would not adequately address the complex, targeted threats that Alura is facing.
Reference Extracts from ISO/IEC 27035-2:2016:
Clause 7.3.2: "Organizations should implement network and system security controls such as firewalls, IDS
/IPS, and anti-malware tools to monitor and restrict unauthorized access." Annex B (Example Preparatory Activities): "Firewalls are vital components in detecting and preventing unauthorized traffic, especially when placed at external network perimeters." Thus, deploying an external firewall in this context is a recommended and justified security measure. The correct answer is: A.
-

**NEW QUESTION # 55**
Which method is used to examine a group of hosts or a network known for vulnerable services?

- A. Automated vulnerability scanning tool
- B. Penetration testing
- C. Security testing and evaluation

**Answer: A**

Explanation:
Comprehensive and Detailed Explanation:
An automated vulnerability scanning tool is designed specifically to scan systems, hosts, or networks for known vulnerabilities based on a maintained vulnerability database. These tools are efficient for covering large environments quickly and are commonly used in routine security assessments.
Security testing and evaluation (A) is broader and includes manual assessments. Penetration testing (C) simulates real-world attacks but is usually more targeted and time-intensive.
Reference:
ISO/IEC 27002:2022, Control A.5.27: "Automated vulnerability scanning should be used to identify technical vulnerabilities."
Correct answer: B
-

**NEW QUESTION # 56**
What does the Incident Cause Analysis Method (ICAM) promote?

- A. A disciplined approach to incident analysis by emphasizing five key areas: people, environment, equipment, procedures, and the organization
- B. The analysis of incidents through the creation of a detailed timeline of events leading up to the incident
- C. An emphasis on evaluating and reporting the financial impact of incidents on the organization

**Answer: A**

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The Incident Cause Analysis Method (ICAM) is a root cause analysis technique used across various industries, including cybersecurity, to understand underlying issues behind incidents. It promotes a holistic and structured approach by examining five critical dimensions:
People (human error, behavior, awareness)
Environment (physical or digital conditions)
Equipment (hardware, software, tools)

Procedures (policies, guidelines, workflows)
Organization (culture, leadership, resourcing)
This comprehensive model helps organizations identify both immediate and systemic causes, allowing them to implement more effective corrective actions and prevent recurrence.
Reference:
ICAM Framework (adapted for cyber from industrial safety): "The ICAM methodology provides a structured approach to incident analysis using five contributing factor categories." ISO/IEC 27035-2 supports root cause analysis practices as part of the post-incident review (Clause 6.4.7).
Correct answer: A
-

**NEW QUESTION # 57**
Scenario 8: Moneda Vivo, headquartered in Kuala Lumpur. Malaysia, is a distinguished name in the banking sector. It is renowned for its innovative approach to digital banking and unwavering commitment to information security. Moneda Vivo stands out by offering various banking services designed to meet the needs of its clients. Central to its operations is an information security incident management process that adheres to the recommendations of ISO/IEC 27035-1 and 27035-2.
Recently. Moneda Vivo experienced a phishing attack aimed at its employees Despite the bank's swift identification and containment of the attack, the incident led to temporary service outages and data access issues, underscoring the need for improved resilience The response team compiled a detailed review of the attack, offering valuable insights into the techniques and entry points used and identifying areas for enhancing their preparedness.
Shortly after the attack, the bank strengthened its defense by implementing a continuous review process to ensure its incident management procedures and systems remain effective and appropriate While monitoring the incident management process, a trend became apparent. The mean time between similar incidents decreased after a few occurrences; however, Moneda Vivo strategically ignored the trend and continued with regular operations This decision was rooted in a deep confidence in its existing security measures and incident management protocols, which had proven effective in quick detection and resolution of issues Moneda Vivo's commitment to transparency and continual improvement is exemplified by its utilization of a comprehensive dashboard. This tool provides real time insights into the progress of its information security incident management, helping control operational activities and ensure that processes stay within the targets of productivity, quality, and efficiency. However, securing its digital banking platform proved challenging.
Following a recent upgrade, which included a user interface change to its digital banking platform and a software update, Moneda Vivo recognized the need to immediately review its incident management process for accuracy and completeness. The top management postponed the review due to financial and time constraints.
Based on scenario 8, Moneda Vivo has recently upgraded its digital banking platform. In line with the continual improvement process, Moneda Vivo has decided to review the information security incident management process for accuracy immediately after the software update. Is this recommended?

- A. No, the incident management process should be evaluated after a significant technological overhaul to ensure the system is up-to-date
- B. Yes, the incident management process should be reviewed after any minor software update
- C. No, the incident management process should be reviewed when the bank's annual audit is conducted

**Answer: A**

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
According to ISO/IEC 27035-1:2016, Clause 7.1 and ISO/IEC 27035-2:2016, Clause 7.3.3, it is advised to review and revise the information security incident management process following major organizational or technical changes. These changes include upgrades, system overhauls, and structural IT shifts. While minor updates may not necessitate a full review, significant technological updates, such as those affecting core digital banking platforms, should trigger immediate evaluation to ensure continued relevance and effectiveness of incident response strategies.
In the scenario, Moneda Vivo recognized the need for a review but delayed it, which could pose risks. Option C accurately reflects ISO guidance.
Reference:
ISO/IEC 27035-1:2016 Clause 7.1: "Reviews should be performed after major changes or after information security incidents."
ISO/IEC 27035-2:2016 Clause 7.3.3 Correct answer: C
-

**NEW QUESTION # 58**

Which action is NOT involved in the process of improving controls in incident management?

- A. Documenting risk assessment results
- B. Updating the incident management policy
- C. Implementing new or updated controls

**Answer: A**

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Improving controls in incident management is a proactive activity focused on directly adjusting and strengthening existing defenses. As per ISO/IEC 27035-2:2016, Clause 7.4, this process typically involves identifying deficiencies, updating or implementing new technical or procedural controls, and revising policies.
While risk assessments inform control decisions, simply documenting their results does not constitute direct improvement of controls. Hence, Option A is not part of the control improvement process itself.
Reference:
ISO/IEC 27035-2:2016 Clause 7.4: "Actions to improve controls include analyzing causes of incidents and updating procedures and policies accordingly." Correct answer: A
-

**NEW QUESTION # 59**
.....

You surely desire the ISO-IEC-27035-Lead-Incident-Manager certification. So with a tool as good as our ISO-IEC-27035-Lead-Incident-Manager exam material, why not study and practice for just 20 to 30 hours and then pass the examination? With our great efforts, our ISO-IEC-27035-Lead-Incident-Manager study materials have been narrowed down and targeted to the examination. So you don't need to worry about wasting your time on useless ISO-IEC-27035-Lead-Incident-Manager Exam Materials information. We can ensure you a pass rate as high as 98% to 100%.

Practice Questions

- ISO-IEC-27035-Lead-Incident-Manager Certification Materials □ ISO-IEC-27035-Lead-Incident-Manager Valid Exam Fee □ ISO-IEC-27035-Lead-Incident-Manager Reliable Test Bootcamp □ Download ➥ ISO-IEC-27035-Lead-Incident-Manager □ for free by simply entering ➠ www.exam4labs.com □ website □ISO-IEC-27035-Lead-Incident-Manager Test Passing Score
- ISO-IEC-27035-Lead-Incident-Manager Practice Test: PECB Certified ISO/IEC 27035 Lead Incident Manager - ISO-IEC-27035-Lead-Incident-Manager Exam Braindumps □ Open website ➠ www.pdfvce.com □ and search for [ ISO-IEC-27035-Lead-Incident-Manager ] for free download □ISO-IEC-27035-Lead-Incident-Manager Exam Engine
- ISO-IEC-27035-Lead-Incident-Manager Exam Engine □ Latest ISO-IEC-27035-Lead-Incident-Manager Test Testking □ □ Latest ISO-IEC-27035-Lead-Incident-Manager Practice Questions □ Open □ www.prepawayete.com □ and search for □ ISO-IEC-27035-Lead-Incident-Manager □ to download exam materials for free □ISO-IEC-27035-Lead-Incident-Manager Study Guide Pdf
- agendabookmarks.com, 45listing.com, mollymmqj249110.blogdosaga.com, jemimakxrl822287.plpwiki.com, mathezajn625821.law-wiki.com, ianorpc425790.theisblog.com, naturalbookmarks.com, 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, graysonkcsm257519.wikibyby.com, karimwlbu854019.tusblogos.com, Disposable vapes

BONUS!!! Download part of FreePdfDump ISO-IEC-27035-Lead-Incident-Manager dumps for free: https://drive.google.com/open?id=1bPIsgKSwxDR5N4Ep9hCE2acU6q0OBP6-