

# Reliable ISO-IEC-27035-Lead-Incident-Manager Exam Practice | Reliable ISO-IEC-27035-Lead-Incident-Manager Test Tutorial



2026 Latest BraindumpStudy ISO-IEC-27035-Lead-Incident-Manager PDF Dumps and ISO-IEC-27035-Lead-Incident-Manager Exam Engine Free Share: [https://drive.google.com/open?id=1M7kJdQ71D1KQaV9P4yzruZbO\\_8zPxTMM](https://drive.google.com/open?id=1M7kJdQ71D1KQaV9P4yzruZbO_8zPxTMM)

Windows computers support the desktop practice test software. BraindumpStudy has a complete support team to fix issues of PECB ISO-IEC-27035-Lead-Incident-Manager practice test software users. BraindumpStudy practice tests (desktop and web-based) produce score report at the end of each attempt. So, that users get awareness of their PECB Certified ISO/IEC 27035 Lead Incident Manager (ISO-IEC-27035-Lead-Incident-Manager) preparation status and remove their mistakes.

Nowadays, there are more and more people realize the importance of ISO-IEC-27035-Lead-Incident-Manager, because more and more enterprise more and more attention it. If someone pass the ISO-IEC-27035-Lead-Incident-Manager exam and own relevant certificates that mean he had good grasp of this field of knowledge, that is to say, he will be popular and valued by more enterprise. In order to help most candidates who want to Pass ISO-IEC-27035-Lead-Incident-Manager Exam, so we compiled such a study materials to make exam simply. Our ISO-IEC-27035-Lead-Incident-Manager guide torrent has gone through strict analysis and summary according to the past exam papers and the popular trend in the industry and are revised and updated according to the change of the syllabus and the latest development conditions in the theory and the practice.

>> Reliable ISO-IEC-27035-Lead-Incident-Manager Exam Practice <<

## Pass Guaranteed 2026 Pass-Sure PECB ISO-IEC-27035-Lead-Incident-Manager: Reliable PECB Certified ISO/IEC 27035 Lead Incident Manager Exam Practice

You will get a lot of personal and professional benefits after passing the PECB ISO-IEC-27035-Lead-Incident-Manager test. The PECB ISO-IEC-27035-Lead-Incident-Manager exam is a valuable credential that will assist you to advance your career. The PECB ISO-IEC-27035-Lead-Incident-Manager is a way to increase your knowledge and skills. You can also trust on BraindumpStudy and start PECB Certified ISO/IEC 27035 Lead Incident Manager ISO-IEC-27035-Lead-Incident-Manager test preparation with PECB ISO-IEC-27035-Lead-Incident-Manager practice test material.

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

---

Topic	Details
Topic 1	<ul style="list-style-type: none"> <li>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.</li> </ul>
Topic 2	<ul style="list-style-type: none"> <li>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.</li> </ul>
Topic 3	<ul style="list-style-type: none"> <li>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.</li> </ul>

## PECB Certified ISO/IEC 27035 Lead Incident Manager Sample Questions (Q56-Q61):

### NEW QUESTION # 56

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 conducts continuous review of the incident management process to ensure the effectiveness of processes and procedures in place. Is this a good practice to follow?

- A. Yes, organizations should conduct continuous review of the incident management process to ensure the effectiveness of the processes and procedures in place
- B. No, organizations should conduct quarterly performance reviews of individual employees to ensure they follow incident management protocols
- C. No, organizations should regularly assess the physical security measures to ensure they align with incident management protocols

**Answer: A**

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

ISO/IEC 27035-1:2016 stresses the importance of continual review and improvement of the incident management process. Clause 7.1 specifically advises that organizations regularly evaluate their policies, procedures, and tools to ensure they remain effective in the face of evolving threats and business changes.

Moneda Vivo's continuous review aligns perfectly with this guidance, reinforcing preparedness and adaptability. Options A and C, while related to broader security or HR practices, are not directly aligned with ISO/IEC 27035's core recommendation regarding process review.

Reference:

ISO/IEC 27035-1:2016, Clause 7.1: "The organization should review the effectiveness of the information security incident management process regularly and in response to incidents and significant changes."

### NEW QUESTION # 57

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 cyber attacks 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 responsibilities of which team in Alura Hospital were NOT defined correctly?

- A. The analysis team
- B. The planning team
- C. The monitoring team

**Answer: B**

Explanation:

Comprehensive and Detailed Explanation:

ISO/IEC 27035-2:2016 clearly outlines functional responsibilities for various roles in the incident management structure. The issue in the scenario lies in the description of the planning team.

The planning team, per ISO guidance, should focus on policy development, incident readiness planning, role assignments, and maintaining readiness through simulations and updates-not on communicating with external parties (which typically falls under the remit of the communications or coordination function within the incident response team).

Monitoring and analysis team responsibilities-such as applying patches, managing risk priorities, and analyzing vulnerabilities-are accurately described.

Reference:

ISO/IEC 27035-2:2016, Clause 5.2.3 - "The planning function should be responsible for developing and maintaining the plan, identifying resource needs, and ensuring team training." Correct answer: A

-

### NEW QUESTION # 58

During an ongoing cybersecurity incident investigation, the Incident Management Team (IMT) at a cybersecurity company identifies

a pattern similar to recent attacks on other organizations. According to best practices, what actions should the IMT take?

- **A. Proactively exchange technical information and incident insights with trusted Incident Response Teams (IRTs) from similar organizations while adhering to predefined information-sharing protocols to improve collective security postures**
- B. Focus on internal containment and eradication processes, consulting external experts strictly for legal and public relations management
- C. Delay any external communication until a thorough internal review is conducted, and the impact of the incident is fully understood to prevent any premature information leakage that could affect ongoing mitigation efforts

**Answer: A**

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

ISO/IEC 27035 strongly encourages information sharing among trusted parties to enhance collective incident response capabilities and reduce the broader impact of cyber threats. Clause 6.5.6 in ISO/IEC 27035-1 highlights the importance of cooperation and communication with external parties, including industry-specific information-sharing forums, CERTs/CSIRTs, and trusted partners. The practice of proactive information exchange allows organizations to:

Detect coordinated or widespread attacks

Accelerate response through shared indicators of compromise (IOCs)

Benefit from collective intelligence and incident analysis

Build sector-wide resilience

However, such exchanges must occur within well-defined protocols that preserve confidentiality, legal compliance, and operational integrity.

Option B and C reflect overly cautious or siloed approaches that may delay response or reduce the effectiveness of collaborative efforts.

Reference Extracts:

ISO/IEC 27035-1:2016, Clause 6.5.6: "Incident management should consider the importance of trusted collaboration, sharing of incident information, and threat intelligence between relevant entities." ENISA and FIRST.org also support this collaborative approach in their best practices.

Correct answer: A

-

## **NEW QUESTION # 59**

Scenario 4: ORingo is a company based in Krakow, Poland, specializing in developing and distributing electronic products for health monitoring and heart rate measurement applications. With a strong emphasis on innovation and technological advancement, ORingo has established itself as a trusted provider of high-quality, reliable devices that enhance the well being and healthcare capabilities of individuals and healthcare professionals alike.

As part of its commitment to maintaining the highest standards of information security, ORingo has established an information security incident management process. This process aims to ensure that any potential threats are swiftly identified, assessed, and addressed to protect systems and information. However, despite these measures, an incident response team member at ORingo recently detected a suspicious state in their systems operational data, leading to the decision to shut down the company-wide system until the anomaly could be thoroughly investigated. Upon detecting the threat, the company promptly established an incident response team to respond to the incident effectively. The team's responsibilities encompassed identifying root causes, uncovering hidden vulnerabilities, and implementing timely resolutions to mitigate the impact of the incident on ORingo's operations and customer trust.

In response to the threat detected across its cloud environments, ORingo employed a sophisticated security tool that broadened the scope of incident detection and mitigation. This tool covers network traffic, cloud environments, and potential attack vectors beyond traditional endpoints, enabling ORingo to proactively defend against evolving cybersecurity threats. During a routine check, the IT manager at ORingo discovered that multiple employees lacked awareness of proper procedures following the detection of a phishing email. In response, immediate training sessions on information security policies and incident response were scheduled for all employees, emphasizing the importance of vigilance and adherence to established protocols in safeguarding ORingo's sensitive data and assets.

As part of the training initiative, ORingo conducted a simulated phishing attack exercise to assess employee response and knowledge. However, an employee inadvertently informed an external partner about the 'attack' during the exercise, highlighting the importance of ongoing education and reinforcement of security awareness principles within the organization.

Through its proactive approach to incident management and commitment to fostering a culture of security awareness and readiness, ORingo reaffirms its dedication to safeguarding the integrity and confidentiality of its electronic products and ensuring the trust and confidence of its customers and stakeholders worldwide.

According to scenario 4, in response to a detected threat across its cloud environments, which tool did ORingo utilize to extend its threat detection and response capabilities beyond traditional endpoints?

- A. IPS
- B. SIEM
- C. XDR

**Answer: C**

Explanation:

Comprehensive and Detailed Explanation:

XDR (Extended Detection and Response) is a security solution that integrates and correlates data across multiple domains including endpoints, networks, cloud workloads, and more. In the scenario, the tool is described as capable of covering network traffic, cloud environments, and beyond-characteristics that align directly with the capabilities of XDR.

IPS (Intrusion Prevention System) focuses narrowly on network perimeter security.

SIEM (Security Information and Event Management) is primarily focused on log aggregation and analysis rather than real-time detection and automated response across multiple layers.

Reference:

NIST SP 800-207 and modern security frameworks define XDR as a centralized detection and response platform with cross-domain visibility.

Therefore, the correct answer is A: XDR

-

### NEW QUESTION # 60

What is the purpose of monitoring behavioral analytics in security monitoring?

- A. To establish a standard for normal user behavior and detect unusual activities
- B. To prioritize the treatment of security incidents
- C. To evaluate the effectiveness of security training programs

**Answer: A**

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Behavioral analytics refers to using baselines of user or system behavior to identify anomalies that may indicate potential threats. According to ISO/IEC 27035-2, behavioral monitoring is an essential proactive technique for detecting insider threats, account compromise, and lateral movement by attackers.

Once a baseline for "normal behavior" is established (e.g., login patterns, file access, network usage), deviations can trigger alerts or investigations. This allows earlier detection of suspicious activities before they escalate into full-blown incidents.

Option A is a separate initiative related to awareness programs. Option B is more aligned with the response phase, not monitoring.

Reference:

ISO/IEC 27035-2:2016, Clause 7.3.2: "Security monitoring should include behavioral analysis to detect anomalies from baseline user and system activity." Correct answer: C

-

### NEW QUESTION # 61

.....

As we know, everyone has opportunities to achieve their own value and life dream. And our ISO-IEC-27035-Lead-Incident-Manager can help them achieve all of these more easily and leisurely. Our ISO-IEC-27035-Lead-Incident-Manager exam materials are pleased to serve you as such an exam tool. With over a decade's endeavor, our ISO-IEC-27035-Lead-Incident-Manager Practice Guide successfully become the most reliable products in the industry. There is a great deal of advantages of our ISO-IEC-27035-Lead-Incident-Manager exam questions you can spare some time to get to know.

**Reliable ISO-IEC-27035-Lead-Incident-Manager Test Tutorial:** [https://www.braindumpstudy.com/ISO-IEC-27035-Lead-Incident-Manager\\_braindumps.html](https://www.braindumpstudy.com/ISO-IEC-27035-Lead-Incident-Manager_braindumps.html)

- First-grade Reliable ISO-IEC-27035-Lead-Incident-Manager Exam Practice - Passing ISO-IEC-27035-Lead-Incident-Manager Exam is No More a Challenging Task  Search for  ISO-IEC-27035-Lead-Incident-Manager  and download it for free on  [www.troytecdumps.com](http://www.troytecdumps.com)  website  Valid ISO-IEC-27035-Lead-Incident-Manager Test Labs
- Fast Download Reliable ISO-IEC-27035-Lead-Incident-Manager Exam Practice - Pass-Sure Reliable ISO-IEC-27035-

