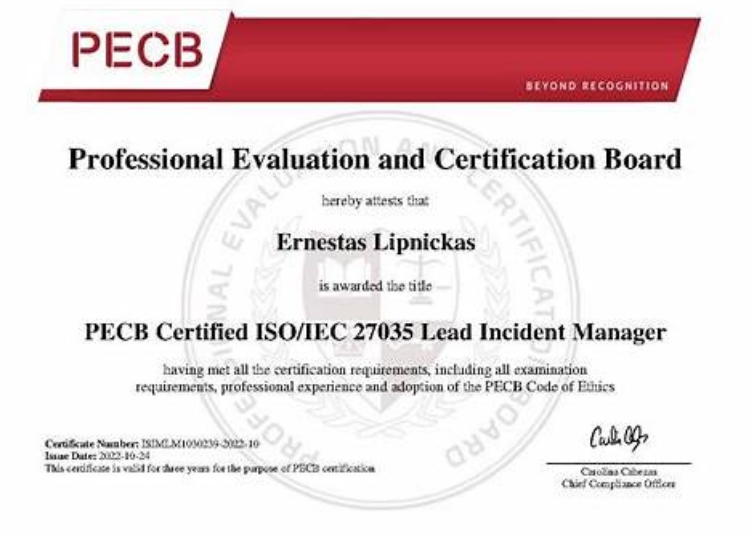
Reliable ISO-IEC-27035-Lead-Incident-Manager Test Notes & Latest ISO-IEC-27035-Lead-Incident-Manager Exam Discount



P.S. Free 2026 PECB ISO-IEC-27035-Lead-Incident-Manager dumps are available on Google Drive shared by FreePdfDump: https://drive.google.com/open?id=1L_LHZGpf48hnnx1pvqQdl78avUr_TOOm

The web-based format gives results at the end of every PECB ISO-IEC-27035-Lead-Incident-Manager practice test attempt and points the mistakes so you can get rid of them before the final attempt. This online format of the PECB Certified ISO/IEC 27035 Lead Incident Manager (ISO-IEC-27035-Lead-Incident-Manager) practice exam works well with Android, Mac, Windows, iOS, and Linux operating systems.

Do you want to pass the exam as soon as possible? ISO-IEC-27035-Lead-Incident-Manager exam dumps of us will give you such opportunity like this. You can pass your exam by spending about 48 to 72 hours on practicing ISO-IEC-27035-Lead-Incident-Manager exam dumps. With skilled experts to revise the exam dumps, the ISO-IEC-27035-Lead-Incident-Manager learning material is high-quality, and they will examine the ISO-IEC-27035-Lead-Incident-Manager Exam Dumps at times to guarantee the correctness. Besides, we offer you free update for 365 days after purchasing , and the update version for ISO-IEC-27035-Lead-Incident-Manager exam dumps will be sent to your email address automatically.

>> Reliable ISO-IEC-27035-Lead-Incident-Manager Test Notes <<

Latest ISO-IEC-27035-Lead-Incident-Manager Exam Discount & Practice ISO-IEC-27035-Lead-Incident-Manager Mock

FreePdfDump field is leaping up day by day and more people are pursuing it as a career than ever. Due to these reasons, candidates find it difficult to land their dream job and often face difficulty in finding the right career opportunities. But to overcome this issue, the ISO-IEC-27035-Lead-Incident-Manager Exam is introduced by PECB that provides candidates with a sustainable platform to examine their true capabilities and surf through their desired opportunities.

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	• 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	• Designing and developing an organizational incident management process based on ISO • IEC 27035: This section of the exam measures skills of Information Security Analysts and covers how to tailor the ISO • IEC 27035 framework to the unique needs of an organization, including policy development, role definition, and establishing workflows for handling incidents.

PECB Certified ISO/IEC 27035 Lead Incident Manager Sample Questions (Q24-Q29):

NEW QUESTION # 24
Scenario 7: Located in central London, Konzolo has become a standout innovator in the cryptocurrency field.
By introducing its unique cryptocurrency, Konzolo has contributed to the variety of digital currencies and prioritized enhancing the security and reliability of its offerings.
Konzolo aimed to enhance its systems but faced challenges in monitoring the security of its own and third- party systems. These issues became especially evident during an incident that caused several hours of server downtime This downtime was primarily caused by a third-party service provider that failed to uphold strong security measures, allowing unauthorized access.
In response to this critical situation, Konzolo strengthened its information security infrastructure. The company initiated a comprehensive vulnerability scan of its cryptographic wallet software, a cornerstone of its digital currency offerings The scan revealed a critical vulnerability due to the software using outdated encryption algorithms that are susceptible to decryption by modern methods that posed a significant risk of asset exposure Noah, the IT manager, played a central role in this discovery With careful attention to detail, he documented the vulnerability and communicated the findings to the incident response team and management.
Acknowledging the need for expertise in navigating the complexities of information security incident management. Konzolo welcomed Paulina to the team. After addressing the vulnerability and updating the cryptographic algorithms, they recognized the importance of conducting a thorough investigation to prevent future vulnerabilities. This marked the stage for Paulina s crucial involvement. She performed a detailed forensic analysis of the incident, employing automated and manual methods during the collection phase. Her analysis provided crucial insights into the security breach, enabling Konzolo to understand the depth of the vulnerability and the actions required to mitigate it.
Paulina also played a crucial role in the reporting phase, as her comprehensive approach extended beyond analysis. By defining clear and actionable steps for future prevention and response, she contributed significantly to developing a resilient information security incident management system based on ISO/IEC
27035-1 and 27035-2 guidelines. This strategic initiative marked a significant milestone in Konzolo's quest to strengthen its defenses against cyber threats Based on scenario 7, which phase of forensic analysis did Paulina fail to conduct correctly?

- A. Collection
- B. Reporting
- C. Analysis

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
As detailed in scenario 7 and reinforced in the previous question, Paulina began her forensic work after the system was restored-missing the critical Collection phase as defined in ISO/IEC 27043 and referenced in ISO/IEC 27035-2.
Forensic collection involves gathering volatile and non-volatile data (e.g., logs, RAM dumps, file artifacts) at the earliest possible moment in the incident lifecycle to avoid data loss. By waiting until after recovery, she likely compromised the chain of custody and the completeness of her evidence.
The scenario notes that her analysis and reporting were thorough, providing valuable insights and mitigation strategies. Thus, the failure lies in the timing and execution of the Collection phase.

Reference:
* ISO/IEC 27035-2:2016, Clause 6.4.2 and 7.2.3: "Collection activities should begin immediately upon identifying a potential incident and before recovery begins."
* ISO/IEC 27043:2015, Clause 8.2.1: "Forensic collection is critical to ensuring reliable analysis and admissible evidence." Correct answer: A
-
-

NEW QUESTION # 25
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.
According to scenario 8, which reporting dashboard did Moneda Vivo use?

- A. Strategic
- B. Tactical
- C. Operational

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The scenario mentions that Moneda Vivo uses a dashboard that offers "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." These characteristics are aligned with an operational dashboard. According to ISO/IEC 27035-2 and related best practices, operational dashboards track day-to-day activities, monitor KPIs related to incident management, and help frontline teams manage incidents in real time.
Strategic dashboards (Option A) are used by executives for long-term decision-making, while tactical dashboards (Option C) are used for mid-term planning and departmental coordination.
Reference:
ISO/IEC 27035-2:2016, Clause 7.4.6: "Dashboards can support monitoring of incident management activities at operational and tactical levels." Correct answer: B
-

NEW QUESTION # 26
What roles do business managers play in relation to the Incident Management Team (IMT) and Incident Response Teams (IRTs)?

- A. Guiding on liability and compliance issues to the IMT and IRT and advise on which incidents constitute mandatory data breach notifications
- B. Developing policies and procedures for managing internal employees found engaging in unauthorized or illegal computer activities

- C. Understanding how the IMT and IRTs support business processes and define authority over business systems

Answer: C

Explanation:
-
Comprehensive and Detailed Explanation From Exact Extract:
According to ISO/IEC 27035-1:2016 and ISO/IEC 27035-2:2016, business managers have a vital governance and operational oversight role in relation to information security incident response. Their main function is to ensure that incident management activities align with the organization's business processes and risk management strategies.
Clause 7.2.1 of ISO/IEC 27035-2 highlights that business managers are responsible for ensuring that the incident response teams (IRTs) understand business priorities, and that response activities reflect the criticality of affected systems and services. Business managers also help define the operational boundaries and authority of IMTs and IRTs when incidents impact key business systems. Their involvement ensures that decisions made during response efforts support overall organizational resilience and legal compliance.
Option A is more aligned with human resources or legal/compliance functions, not core business manager responsibilities. Option B relates more closely to legal counsel or data privacy officers who are tasked with interpreting laws and regulations concerning breach notifications and liability.
Reference Extracts:
ISO/IEC 27035-2:2016, Clause 7.2.1: "Business managers are responsible for ensuring the coordination between business requirements and incident response activities, and for defining authority over the systems under their management." Clause 6.1.1: "Incident response activities must be aligned with business continuity plans and critical asset protection priorities." Therefore, the correct and most comprehensive answer is: C - Understanding how the IMT and IRTs support business processes and define authority over business systems.
-

NEW QUESTION # 27
How is the impact of an information security event assessed?

- A. By evaluating the effect on the confidentiality, integrity, and availability of information
- B. By identifying the assets affected by the event
- C. By determining if the event is an information security incident

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The impact of an information security event is assessed by evaluating how the event affects the CIA triad- Confidentiality, Integrity, and Availability-of information assets. This fundamental concept underpins all ISO/IEC 27000-series standards, including ISO/IEC 27035.
ISO/IEC 27035-1:2016, Clause 6.2.3 explicitly states that an event's severity and urgency are to be assessed by evaluating its actual or potential impact on the organization's information security objectives, namely:
Confidentiality: Protection from unauthorized disclosure
Integrity: Protection from unauthorized modification
Availability: Assurance of timely and reliable access
This approach ensures consistent and risk-based decision-making during incident assessment. Options A and B are important steps, but they are part of the broader process; they do not directly measure impact.
Reference:
ISO/IEC 27035-1:2016, Clause 6.2.3: "The impact should be assessed based on the effect on confidentiality, integrity, and availability of the information assets affected." Correct answer: C
-

NEW QUESTION # 28
According to scenario 4, what is the next action ORingo should take to prevent escalation when conducting exercises?

- A. Inform all participants and external entities involved that this was a simulated scenario and not a real threat immediately
- B. Proceed with the exercise as planned, considering this as a part of the learning process
- C. Wait until the exercise is completed to clarify the situation with all parties involved

Answer: A

Explanation:
Comprehensive and Detailed Explanation:
According to ISO/IEC 27035-2:2016, incident response exercises (including simulations such as phishing campaigns) must be carefully controlled to avoid confusion, escalation, or reputational damage. If an exercise is misunderstood by employees or external parties, it could lead to unintended consequences including external escalation, customer concern, or media involvement.
The best practice is to ensure that all involved-especially external stakeholders-are informed as soon as possible if they are exposed to simulated elements. Transparency ensures the organization maintains trust and mitigates potential fallout. This is part of effective communication during planned exercises.
Reference:
ISO/IEC 27035-2:2016, Clause 7.5 - "Exercises should be clearly identified, controlled, and followed by communication plans that inform affected parties of their simulated nature." Correct answer: C
-

NEW QUESTION # 29
.....

We promise during the process of installment and payment of our ISO-IEC-27035-Lead-Incident-Manager prep torrent, the security of your computer or cellphone can be guaranteed, which means that you will be not afraid of virus intrusion and personal information leakage. Besides we have the right to protect your email address and not release your details to the 3rd parties.

- Online ISO-IEC-27035-Lead-Incident-Manager Version □ Reliable ISO-IEC-27035-Lead-Incident-Manager Test Cram □ New ISO-IEC-27035-Lead-Incident-Manager Test Vce □ Immediately open ▹ www.practicevce.com ◃ and search for { ISO-IEC-27035-Lead-Incident-Manager } to obtain a free download □Valid ISO-IEC-27035-Lead-Incident-Manager Test Preparation
- bbs.ucwm.com, ronorp.net, www.stes.tyc.edu.tw, hhi.instructure.com, www.ted.com, www.fundable.com, www.fundable.com, globalsathi.in, www.stes.tyc.edu.tw, medcz.net, Disposable vapes

What's more, part of that FreePdfDump ISO-IEC-27035-Lead-Incident-Manager dumps now are free: https://drive.google.com/open?id=1L_LHZGpf48hnnx1pvqQdl78avUr_TOOm