Pass Guaranteed Quiz 2026 ISO-IEC-27035-Lead-Incident-Manager: High Hit-Rate PECB Certified ISO/IEC 27035 Lead Incident Manager New Real Test

BONUS!!! Download part of Lead2Passed ISO-IEC-27035-Lead-Incident-Manager dumps for free: https://drive.google.com/open?id=131_dOU8fFLavIiPq0auShSfr6AaIcyD6

We have professional technicians to check the website at times, therefore we can provide you with a clean and safe shopping environment if you buy ISO-IEC-27035-Lead-Incident-Manager training materials. In addition, we have free demo for you before purchasing, so that you can have a better understanding of what you are going to buying. Free update for 365 days is available, and you can get the latest information for the ISO-IEC-27035-Lead-Incident-Manager Exam Dumps without spending extra money. We have online and offline chat service stuff, and they possess the professional knowledge for the ISO-IEC-27035-Lead-Incident-Manager training materials, if you have any questions, just contact us.

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

Topic	Details
Topic 1	• 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 2	• Information security incident management process based on ISO • IEC 27035: This section of the exam measures skills of Incident Response Managers and covers the standardized steps and processes outlined in ISO • IEC 27035. It emphasizes how organizations should structure their incident response lifecycle from detection to closure in a consistent and effective manner.
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	• 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 5	- 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.

>> ISO-IEC-27035-Lead-Incident-Manager New Real Test <<

ISO-IEC-27035-Lead-Incident-Manager Test Certification Cost | Reliable ISO-IEC-27035-Lead-Incident-Manager Test Labs

There may be customers who are concerned about the installation or use of our ISO-IEC-27035-Lead-Incident-Manager study materials. You don't have to worry about this. In addition to high quality and high efficiency, considerate service is also a big advantage of our company. We will provide 24 - hour online after-sales service to every customer. If you have any questions about installing or using our ISO-IEC-27035-Lead-Incident-Manager Study Materials, our professional after-sales service staff will provide you with warm remote service.

PECB Certified ISO/IEC 27035 Lead Incident Manager Sample Questions (Q70-Q75):

NEW QUESTION # 70
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.
Scenario 8: Moneda Vivo, headquartered in Kuala Lumpur, Malaysia, is a distinguished name in the banking sector. It recently experienced a phishing attack, prompting the response team to conduct a detailed review.
The incident underscored the need for resilience and continuous improvement.
What is the primary goal of the information Moneda Vivo's incident report team gathered from the incident?

- A. To document the incident for legal compliance purposes
- B. To showcase the effectiveness of existing security protocols to stakeholders
- C. To learn from the incident and improve future security measures

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The core purpose of incident reporting, as outlined in ISO/IEC 27035-1:2016 (Clause 6.4.7), is to learn from the incident in order to improve future preparedness, resilience, and effectiveness. Lessons learned from an incident should feed into policy, process, and technical improvements. The scenario highlights how Moneda Vivo's team analyzed the phishing attack to understand entry points and weaknesses, directly aligning with this principle.

While legal compliance (Option B) and showcasing security (Option A) may be secondary benefits, the primary objective is always organizational learning and resilience enhancement.
Reference:
ISO/IEC 27035-1:2016, Clause 6.4.7: "The lessons learned phase involves identifying improvements to the information security incident management process and to other relevant processes and controls." Correct answer: C
-

NEW QUESTION # 71
What is the purpose of incident identification in the incident response process?

- A. To collect all data related to the incident, including information from affected systems, network logs, user accounts, and any other relevant sources
- B. To recognize incidents through various methods like intrusion detection systems and employee reports
- C. To conduct a preliminary assessment of the incident

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Incident identification is the first operational step in the incident response process. It involves detecting unusual or suspicious activity and recognizing whether it constitutes an information security incident. ISO
/IEC 27035-1:2016 describes various sources of detection, such as:
Security monitoring tools (e.g., IDS/IPS)
User reports or helpdesk notifications
Automated alerts from applications or infrastructure
The goal at this stage is not to collect detailed forensic data or conduct deep analysis, but rather to determine whether the activity warrants classification as a potential incident and to escalate accordingly.
Reference:
ISO/IEC 27035-1:2016, Clause 6.2.1: "Incident identification involves recognizing the occurrence of an event that could be an information security incident." Correct answer: C
-

NEW QUESTION # 72
Based on ISO/IEC 27035-2, which of the following is an example of evaluation activities used to evaluate the effectiveness of the incident management team?

- A. Analyzing the lessons learned once an information security incident has been handled and closed
- B. Evaluating the capabilities and services once they become operational
- C. Conducting information security testing, particularly vulnerability assessment

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-2:2016 Clause 7.4.3 emphasizes the role of lessons learned reviews as key evaluation activities for assessing the performance of incident response teams. This activity involves post-incident debriefs to evaluate what went right or wrong and how response processes or team functions could improve.
While options A and C are related to broader security or deployment procedures, Option B directly reflects a formal evaluation mechanism used to gauge incident team effectiveness.
Reference:
ISO/IEC 27035-2:2016 Clause 7.4.3: "Lessons learned should be documented and used to evaluate the effectiveness of the incident management process." Correct answer: B
-

NEW QUESTION # 73
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.
Based on scenario 1, which security control has RoLawyers implemented?

- A. Preventive controls
- B. Corrective controls
- C. Detective controls

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The deployment of an Intrusion Detection System (IDS) by RoLawyers following the incident is a classic example of implementing a detective control. According to ISO/IEC 27002:2022 (formerly 27002:2013), detective controls are designed to identify and report the occurrence of information security events in a timely manner. They help organizations discover that an event has occurred so that an appropriate response can be initiated.
The IDS mentioned in the scenario monitors the network for suspicious activity and alerts the IT security team when anomalies or intrusion attempts are detected. This aligns directly with the definition of detective controls.
By contrast:
Preventive controls are designed to prevent incidents from occurring in the first place (e.g., firewalls, access controls).
Corrective controls are actions taken after an incident to restore systems or data and prevent recurrence (e.g., patch management, backups).
Reference Extracts:
ISO/IEC 27002:2022, Clause 5.27 - "Detection controls should be implemented to identify incidents and anomalies in a timely manner." ISO/IEC 27035-1:2016, Clause 4.3.2 - "Detecting and reporting information security events and weaknesses are the first steps in the incident response process." RoLawyers' use of an IDS matches the description of a detective control designed to provide early warning signs of potential threats, making it easier for the organization to take timely action.
Therefore, the correct answer is B: Detective controls.

NEW QUESTION # 74
Scenario 2: NoSpace, a forward-thinking e-commerce store based in London, is renowned for its diverse products and advanced technology. To enhance its information security, NoSpace implemented an ISMS according to ISO/IEC 27001 to better protect customer data and ensure business continuity. Additionally, the company adopted ISO/IEC 27035-1 and ISO/IEC 27035-2 guidelines. Mark, the incident manager at NoSpace, strategically led the entire implementation. He played a crucial role in aligning the company's ISMS with the requirements specified in ISO/IEC 27001, using ISO/IEC 27035-1 guidelines as the foundation.
During a routine internal audit a minor anomaly was detected in the data traffic that could potentially indicate a security threat. Mark was immediately notified to assess the situation. Then, Mark and his team immediately escalated the incident to crisis management to handle the potential threat without further assessment. The decision was made to ensure a swift response.
After resolving the situation, Mark decided to update the incident management process. During the initial phase of incident management, Mark recognized the necessity of updating NoSpace's information security policies. This included revising policies related to risk management at the organizational level as well as for specific systems, services, or networks. The second phase of the updated incident management process included the assessment of the information associated with occurrences of information security events and the importance of classifying events and vulnerabilities as information security incidents. During this phase, he also introduced a 'count down' process to expedite the evaluation and classification of occurrences, determining whether they should be recognized as information security incidents.

Mark developed a new incident management policy to enhance the organization's resilience and adaptability in handling information security incidents. Starting with a strategic review session with key stakeholders, the team prioritized critical focus areas over less impactful threats, choosing not to include all potential threats in the policy document. This decision was made to keep the policy streamlined and actionable, focusing on the most significant risks identified through a risk assessment. The policy was shaped by integrating feedback from various department heads to ensure it was realistic and enforceable. Training and awareness initiatives were tailored to focus only on critical response roles, optimizing resource allocation and focusing on essential capabilities.
Based on scenario 2, NoSpace used the ISO/IEC 27035-1 guidelines to meet the ISMS requirements specified in ISO/IEC 27001. Is this acceptable?

- A. No, guidelines provided in ISO/IEC 27035-1 do not apply to ISMS requirements specified in ISO/IEC 27001
- B. No, ISO/IEC 27035-1 is designed for incident management and response and does not address the broader scope of ISMS requirements specified in ISO/IEC 27001
- C. Yes, another objective associated with ISO/IEC 27035-1 is to provide guidance on meeting the ISMS requirements specified in ISO/IEC 27001

Answer: C

Explanation:
-
Comprehensive and Detailed Explanation From Exact Extract:
Yes, the use of ISO/IEC 27035-1 to support compliance with ISO/IEC 27001 ISMS requirements is fully acceptable and encouraged. ISO/IEC 27035-1:2016 is explicitly designed to support organizations in establishing and maintaining effective information security incident management processes. These processes are a crucial component of a well-functioning Information Security Management System (ISMS), which is governed by ISO/IEC 27001.
Clause 6.1.3 and Clause A.16.1 of ISO/IEC 27001:2022 (formerly 2013) require that organizations establish and respond to information security incidents, including detection, response, and learning from such events.
ISO/IEC 27035-1 directly supports these controls by providing specific guidance on how to identify, manage, and learn from information security incidents in a structured and repeatable way.
Moreover, ISO/IEC 27035-1 is referenced by ISO/IEC 27001 Annex A (specifically A.5.24 to A.5.27 and A. 5.31 in the 2022 version), supporting requirements related to incident management, monitoring, and improvement. The ISO 27035 series acts as a detailed implementation guide for these controls, helping organizations meet both the management and operational requirements of the ISMS.
Therefore, Mark's decision to use ISO/IEC 27035-1 guidelines to align and enhance the incident management aspects of the ISMS is both appropriate and aligned with international best practices.
Reference Extracts:
* ISO/IEC 27035-1:2016, Clause 0.2: "This document also supports the information security requirements defined in ISO/IEC 27001 and provides detailed guidance on incident management activities relevant to an ISMS."
* ISO/IEC 27001:2022, Annex A (A.5.24-A.5.27): "Information security incident management should be based on established processes for detection, response, and learning."
* ISO/IEC 27001:2022, Clause 6.1.3: "Information security risks must be identified and treated as part of the ISMS." Therefore, the correct answer is A: Yes, another objective associated with ISO/IEC 27035-1 is to provide guidance on meeting the ISMS requirements specified in ISO/IEC 27001.

NEW QUESTION # 75
......

In today's technological world, more and more students are taking the PECB Certified ISO/IEC 27035 Lead Incident Manager (ISO-IEC-27035-Lead-Incident-Manager) exam online. While this can be a convenient way to take an PECB Certified ISO/IEC 27035 Lead Incident Manager (ISO-IEC-27035-Lead-Incident-Manager) exam dumps, it can also be stressful. Luckily, Lead2Passed's best PECB Certified ISO/IEC 27035 Lead Incident Manager (ISO-IEC-27035-Lead-Incident-Manager) exam questions can help you prepare for your PECB Certified ISO/IEC 27035 Lead Incident Manager (ISO-IEC-27035-Lead-Incident-Manager) certification exam and reduce your stress.

ISO-IEC-27035-Lead-Incident-Manager Test Certification Cost: https://www.lead2passed.com/PECB/ISO-IEC-27035-Lead-Incident-Manager-practice-exam-dumps.html

- Vce ISO-IEC-27035-Lead-Incident-Manager File □ ISO-IEC-27035-Lead-Incident-Manager Guaranteed Success □ ISO-IEC-27035-Lead-Incident-Manager Valid Exam Topics □ Easily obtain 「 ISO-IEC-27035-Lead-Incident-Manager 」 for free download through □ www.examcollectionpass.com □ □ISO-IEC-27035-Lead-Incident-Manager

New Study Notes

- New ISO-IEC-27035-Lead-Incident-Manager Exam Pass4sure □ Latest Test ISO-IEC-27035-Lead-Incident-Manager Simulations □ ISO-IEC-27035-Lead-Incident-Manager Valid Exam Topics □ Easily obtain free download of □ ISO-IEC-27035-Lead-Incident-Manager □ by searching on ➥ www.pdfvce.com □ □ISO-IEC-27035-Lead-Incident-Manager Valid Exam Topics
- PECB ISO-IEC-27035-Lead-Incident-Manager Unparalleled New Real Test □ Search for ➠ ISO-IEC-27035-Lead-Incident-Manager □ and download exam materials for free through ➠ www.prepawaypdf.com □ □Latest Test ISO-IEC-27035-Lead-Incident-Manager Simulations
- Exam Discount ISO-IEC-27035-Lead-Incident-Manager Voucher □ ISO-IEC-27035-Lead-Incident-Manager Actual Exam Dumps □ New ISO-IEC-27035-Lead-Incident-Manager Dumps Sheet □ Simply search for ➡ ISO-IEC-27035-Lead-Incident-Manager □□□ for free download on ➡ www.pdfvce.com □□□ □ISO-IEC-27035-Lead-Incident-Manager Certification Torrent
- ISO-IEC-27035-Lead-Incident-Manager Test Online □ Top ISO-IEC-27035-Lead-Incident-Manager Questions □ New ISO-IEC-27035-Lead-Incident-Manager Dumps Sheet □ The page for free download of ➻ ISO-IEC-27035-Lead-Incident-Manager □ on 《 www.pass4test.com 》 will open immediately □New ISO-IEC-27035-Lead-Incident-Manager Dumps Sheet
- New ISO-IEC-27035-Lead-Incident-Manager Exam Labs □ ISO-IEC-27035-Lead-Incident-Manager Actual Exam Dumps □ New ISO-IEC-27035-Lead-Incident-Manager Exam Pass4sure □ The page for free download of ➡ ISO-IEC-27035-Lead-Incident-Manager □□□ on “ www.pdfvce.com ” will open immediately □ISO-IEC-27035-Lead-Incident-Manager Free Test Questions
- ISO-IEC-27035-Lead-Incident-Manager Desktop Practice Exam Software □ Immediately open 「 www.verifieddumps.com 」 and search for ▷ ISO-IEC-27035-Lead-Incident-Manager ◁ to obtain a free download □Vce ISO-IEC-27035-Lead-Incident-Manager File
- ISO-IEC-27035-Lead-Incident-Manager Guaranteed Success □ New ISO-IEC-27035-Lead-Incident-Manager Exam Pass4sure □ ISO-IEC-27035-Lead-Incident-Manager Certification Torrent □ The page for free download of ✔ ISO-IEC-27035-Lead-Incident-Manager □✔□ on 「 www.pdfvce.com 」 will open immediately □ISO-IEC-27035-Lead-Incident-Manager Guaranteed Success
- The Benefits of ISO-IEC-27035-Lead-Incident-Manager Certification □ Go to website ✔ www.practicevce.com □✔□ open and search for ▷ ISO-IEC-27035-Lead-Incident-Manager ◁ to download for free □Reliable ISO-IEC-27035-Lead-Incident-Manager Test Practice
- 100% Pass Quiz 2026 Realistic PECB ISO-IEC-27035-Lead-Incident-Manager New Real Test □ Simply search for ➻ ISO-IEC-27035-Lead-Incident-Manager □ for free download on 【 www.pdfvce.com 】 □Download ISO-IEC-27035-Lead-Incident-Manager Fee
- New ISO-IEC-27035-Lead-Incident-Manager Exam Labs □ Valid ISO-IEC-27035-Lead-Incident-Manager Mock Exam □ ISO-IEC-27035-Lead-Incident-Manager Valid Exam Topics □ Search for ☀ ISO-IEC-27035-Lead-Incident-Manager □☀□ and download it for free on □ www.verifieddumps.com □ website □Reliable ISO-IEC-27035-Lead-Incident-Manager Test Practice
- 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, www.stes.tyc.edu.tw, easierandsofterway.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, marciealfredo.blogspot.com, chesscoach.lk, 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, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free 2025 PECB ISO-IEC-27035-Lead-Incident-Manager dumps are available on Google Drive shared by Lead2Passed: https://drive.google.com/open?id=13l_dOU8fFLavIiPq0auShSfr6AaIcyD6