ISO-IEC-27035-Lead-Incident-Manager - PECB Certified ISO/IEC 27035 Lead Incident Manager–The Best Accurate Prep Material

BONUS!!! Download part of VCEEngine ISO-IEC-27035-Lead-Incident-Manager dumps for free: https://drive.google.com/open?id=1tcXFOSJuYnPcHzuK1cbSs_CVQAF1DA_R

Our exam prep material is famous among ISO-IEC-27035-Lead-Incident-Manager exam candidates which help to polish the knowledge required to pass the PECB ISO-IEC-27035-Lead-Incident-Manager exam. The certification is organized by ISO-IEC-27035-Lead-Incident-Manager internationally. Our PECB ISO-IEC-27035-Lead-Incident-Manager exam questions are the most cost-effective as we understand that you need low-cost material but are authentic and updated. VCEEngine provides its PECB ISO-IEC-27035-Lead-Incident-Manager Exam Questions in three forms, one is PDF eBook, the second is practice exam software for Windows-based systems, and the third is an online practice test.

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	• 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.

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	• 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 5	• 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.

Reliable ISO-IEC-27035-Lead-Incident-Manager Braindumps Ebook, Latest ISO-IEC-27035-Lead-Incident-Manager Exam Discount

In order to meet the time requirement of our customers, our experts carefully designed our ISO-IEC-27035-Lead-Incident-Manager test torrent to help customers pass the exam in a lot less time. If you purchase our ISO-IEC-27035-Lead-Incident-Manager guide torrent, we can make sure that you just need to spend twenty to thirty hours on preparing for your exam before you take the exam, it will be very easy for you to save your time and energy. So do not hesitate and buy our ISO-IEC-27035-Lead-Incident-Manager study torrent, we believe it will give you a surprise, and it will not be a dream for you to pass your PECB Certified ISO/IEC 27035 Lead Incident Manager exam and get your certification in the shortest time.

PECB Certified ISO/IEC 27035 Lead Incident Manager Sample Questions (Q39-Q44):

NEW QUESTION # 39
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. No, they should have implemented a cloud-based antivirus solution instead of deploying an external firewall
- C. Deploying an external firewall to detect threats that have already breached the perimeter defenses

Answer: C

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 # 40
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, a vulnerability scan at Konzolo revealed a critical vulnerability in the cryptographic wallet

software that could lead to asset exposure. Noah, the IT manager, documented the event and communicated it to the incident response team and management. Is this acceptable?

- A. No, he should have postponed the documentation process until a full investigation is completed
- B. No, he should have waited for confirmation of an actual asset exposure before documenting and communicating the vulnerability
- C. Yes, he should document the event and communicate it to the incident response team and management

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
According to ISO/IEC 27035-1:2016, an information security event should be documented and communicated as soon as it is identified-particularly if it has the potential to escalate into an incident. Timely documentation and escalation enable the organization to take immediate and coordinated actions, which are essential to managing risk effectively.
Clause 6.2.1 of ISO/IEC 27035-1 states that events, even before confirmation as incidents, must be logged and assessed to determine appropriate response measures. Waiting until after a breach occurs or delaying documentation may violate both internal policies and regulatory requirements, especially in high-risk domains like cryptocurrency.
Therefore, Noah's actions align fully with the recommended practices outlined in ISO/IEC 27035.
Reference:
* ISO/IEC 27035-1:2016, Clause 6.2.1: "All identified information security events should be recorded and communicated to ensure appropriate assessment and response."
* Clause 6.2.2: "Early communication and documentation are crucial to managing potential incidents effectively." Correct answer: C
-

NEW QUESTION # 41
What is a key activity in the response phase of information security incident management?

- A. Ensuring the change control regime covers information security incident tracking
- B. Logging all activities, results, and related decisions for later analysis
- C. Restoring systems to normal operation

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
During the response phase, one of the most critical activities-according to ISO/IEC 27035-1 and 27035-2- is the documentation of actions, decisions, and results. Clause 6.4.6 of ISO/IEC 27035-1 emphasizes that all activities must be logged to support post-incident analysis, audit trails, and lessons learned. This ensures that:
Accountability is maintained
Decisions can be reviewed
Investigations are legally sound (especially in regulated environments) While restoring systems (Option C) typically occurs in the recovery phase, logging activities and outcomes is essential during the actual response. Change control processes (Option B) are supporting functions but are not core to the immediate response phase.
Reference:
ISO/IEC 27035-1:2016, Clause 6.4.6: "All incident response actions and decisions should be recorded to enable traceability and facilitate future improvement." Correct answer: A
-

NEW QUESTION # 42
Which factor of change should be monitored when maintaining incident management documentation?

- A. Employee attendance records
- B. Market trends
- C. Test results

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
When maintaining documentation for information security incident management, test results are critical indicators of how well current plans and controls are functioning. According to ISO/IEC 27035-2:2016 Clause 7.3.3, organizations must update documents based on test outcomes, incident experiences, or environmental changes.
Market trends (Option A) and attendance records (Option B) are not directly relevant to the content or accuracy of incident documentation.
Reference:
ISO/IEC 27035-2:2016 Clause 7.3.3: "Changes in the environment or test results should be used as input for reviewing documentation." Correct answer: C
-

NEW QUESTION # 43
Which of the following statements regarding the principles for digital evidence gathering is correct?

- A. Reliability implies that all processes used in handling digital evidence should be unique and not necessarily reproducible
- B. Sufficiency means that only a minimal amount of material should be gathered to avoid unnecessary auditing and justification efforts
- C. Relevance means that the DEFR should be able to describe the procedures followed and justify the decision to acquire each item based on its value to the investigation

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Digital evidence gathering, as outlined in ISO/IEC 27037 and referenced in ISO/IEC 27035-2, must adhere to several core principles-reliability, sufficiency, relevance, and integrity. Relevance, in particular, means that the Digital Evidence First Responder (DEFR) must ensure that any item collected has direct or potential bearing on the investigation.
Relevance also requires:
Clear justification for why an item was acquired
Ability to trace the decision-making process
Alignment with investigation objectives
Option A misrepresents "sufficiency," which does not mean minimal collection but rather collecting enough evidence to support conclusions without overburdening the investigation. Option B contradicts the principle of reliability, which requires that processes be standardized and reproducible.
Reference:
ISO/IEC 27037:2012, Clause 6.2.2.4: "Relevance is determined by the value of the digital evidence in addressing the objectives of the investigation." ISO/IEC 27035-2:2016 references this standard in Clause 7.4.4 regarding forensic evidence handling.
Correct answer: C
-

NEW QUESTION # 44
.....

We have a special technical customer service staff to solve all kinds of consumers' problems on our ISO-IEC-27035-Lead-Incident-Manager exam questions. If you have questions when installing or using our ISO-IEC-27035-Lead-Incident-Manager practice engine, you can always contact our customer service staff via email or online consultation. They will solve your questions about ISO-IEC-27035-Lead-Incident-Manager Preparation materials with enthusiasm and professionalism, giving you a timely response whenever you contact them.

Incident-Manager Tool

- ISO-IEC-27035-Lead-Incident-Manager Exam Accurate Prep Material - Newest Reliable ISO-IEC-27035-Lead-Incident-Manager Braindumps Ebook Pass Success □ Search for ➽ ISO-IEC-27035-Lead-Incident-Manager □ and obtain a free download on ☀ www.practicevce.com □☀□ □Real ISO-IEC-27035-Lead-Incident-Manager Question
- Study ISO-IEC-27035-Lead-Incident-Manager Tool □ ISO-IEC-27035-Lead-Incident-Manager Actual Tests □ ISO-IEC-27035-Lead-Incident-Manager Actual Tests □ Simply search for 《 ISO-IEC-27035-Lead-Incident-Manager 》 for free download on （ www.pdfvce.com ） □ISO-IEC-27035-Lead-Incident-Manager Reliable Test Materials
- PECB ISO-IEC-27035-Lead-Incident-Manager Accurate Prep Material: PECB Certified ISO/IEC 27035 Lead Incident Manager - www.practicevce.com Test Engine Simulation ❊ Search on ➠ www.practicevce.com □ for （ ISO-IEC-27035-Lead-Incident-Manager ） to obtain exam materials for free download □Reliable ISO-IEC-27035-Lead-Incident-Manager Study Plan
- PECB ISO-IEC-27035-Lead-Incident-Manager Accurate Prep Material: PECB Certified ISO/IEC 27035 Lead Incident Manager - Pdfvce Test Engine Simulation □ Search for ➥ ISO-IEC-27035-Lead-Incident-Manager □ on □ www.pdfvce.com □ immediately to obtain a free download ☣ISO-IEC-27035-Lead-Incident-Manager Exam Dump
- ISO-IEC-27035-Lead-Incident-Manager Accurate Prep Material Free PDF | Valid Reliable ISO-IEC-27035-Lead-Incident-Manager Braindumps Ebook: PECB Certified ISO/IEC 27035 Lead Incident Manager □ Easily obtain □ ISO-IEC-27035-Lead-Incident-Manager □ for free download through ☀ www.troytecdumps.com □☀□ □ISO-IEC-27035-Lead-Incident-Manager Reliable Exam Online
- New ISO-IEC-27035-Lead-Incident-Manager Test Test □ ISO-IEC-27035-Lead-Incident-Manager PDF VCE □ New ISO-IEC-27035-Lead-Incident-Manager Exam Notes □ Search for ▹ ISO-IEC-27035-Lead-Incident-Manager ◃ and download it for free on ➤ www.pdfvce.com □ website □Reliable ISO-IEC-27035-Lead-Incident-Manager Study Plan
- Switch Your Nervousness in ISO-IEC-27035-Lead-Incident-Manager Exam by Using PECB ISO-IEC-27035-Lead-Incident-Manager Exam □ Search for [ISO-IEC-27035-Lead-Incident-Manager] and obtain a free download on [www.prep4away.com] □Valid Test ISO-IEC-27035-Lead-Incident-Manager Fee
- 2026 ISO-IEC-27035-Lead-Incident-Manager Accurate Prep Material | Latest 100% Free Reliable ISO-IEC-27035-Lead-Incident-Manager Braindumps Ebook □ Search for ▹ ISO-IEC-27035-Lead-Incident-Manager ◃ and easily obtain a free download on { www.pdfvce.com } □Reliable ISO-IEC-27035-Lead-Incident-Manager Exam Syllabus
- New ISO-IEC-27035-Lead-Incident-Manager Exam Notes □ ISO-IEC-27035-Lead-Incident-Manager Actual Tests □ □ ISO-IEC-27035-Lead-Incident-Manager Reliable Exam Online □ The page for free download of “ ISO-IEC-27035-Lead-Incident-Manager ” on □ www.examcollectionpass.com □ will open immediately □Latest ISO-IEC-27035-Lead-Incident-Manager Study Plan
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, p1.me-page.org, www.stes.tyc.edu.tw, 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, connect.garmin.com, www.stes.tyc.edu.tw, Disposable vapes

BONUS!!! Download part of VCEEngine ISO-IEC-27035-Lead-Incident-Manager dumps for free: https://drive.google.com/open?id=1tcXFOSJuYnPcHzuK1cbSs_CVQAF1DA_R