ISO-IEC-27035-Lead-Incident-Manager Unterlagen mit echte Prüfungsfragen der PECB Zertifizierung


PECB

BEYOND RECOGNITION

Professional Evaluation and Certification Board

hereby attests that

Ernestas Lipnickas

is awarded the title

PECB Certified ISO/IEC 27035 Lead Incident Manager

having met all the certification requirements, including all examination requirements, professional experience and adoption of the PECB Code of Ethics

Certificate Number: ISIMLM1000239-2022-10
Issue Date: 2022-10-24
This certificate is valid for three years for the purpose of PECB certification

Carolina Cabezas
Chief Compliance Officer

Wir versprechen, dass Sie die Prüfung zum ersten Mal mit unseren Schulungsunterlagen zur PECB ISO-IEC-27035-Lead-Incident-Manager Zertifizierungsprüfung bestehen können. Sonst erstatten wir Ihen die gesammte Summe zurück.

PECB ISO-IEC-27035-Lead-Incident-Manager Prüfungsplan:

Thema	Einzelheiten
Thema 1	• 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.
Thema 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.
Thema 3	• 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.
Thema 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.
Thema 5	• 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.

ISO-IEC-27035-Lead-Incident-Manager Fragen Und Antworten - ISO-IEC-27035-Lead-Incident-Manager Deutsch Prüfung

Unser PrüfungFrage ist international ganz berühmt. Die Anwendbarkeit von den Schulungsunterlagen ist sehr groß. Sie werden von den IT-Experten nach ihren Kenntnissen und Erfahrungen bearbeitet. Die Feedbacks von den Kandidaten haben sich gezeigt, dass unsere Prüdukte eher von guter Qualität sind. Wenn Sie einer der IT-Kandidaten sind, sollen Sie die Schulungsunterlagen zur PECB ISO-IEC-27035-Lead-Incident-Manager Zertifizierungsprüfung von PrüfungFrage ohne Zweifel wählen.

PECB Certified ISO/IEC 27035 Lead Incident Manager ISO-IEC-27035-Lead-Incident-Manager Prüfungsfragen mit Lösungen (Q37-Q42):

37. Frage
Why is it important to identify all impacted hosts during the eradication phase?

- A. To enhance overall security
- B. To optimize hardware performance
- C. To facilitate recovery efforts

Antwort: C

Begründung:
Comprehensive and Detailed Explanation From Exact Extract:
During the eradication phase of the information security incident management process, identifying all impacted hosts is essential to ensure that every element affected by the incident is addressed before proceeding to recovery. According to ISO/IEC 27035-2:2016, Clause 6.4.5, the eradication phase involves removing malware, disabling unauthorized access, and remediating vulnerabilities that led to the incident.
Identifying all impacted hosts ensures:
Comprehensive removal of malicious artifacts
Prevention of reinfection or further propagation
A smooth and complete transition into the recovery phase
This directly supports recovery planning because it helps teams understand which systems need to be restored, rebuilt, or validated.
Option B (optimizing hardware performance) is not a goal of incident management, and Option C (enhancing overall security) is a long-term objective but not the immediate goal of the eradication phase.
Reference:
ISO/IEC 27035-2:2016, Clause 6.4.5: "During eradication, it is important to identify all affected systems so that root causes and malicious components are removed prior to recovery." Correct answer: A
-

38. Frage
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 learn from the incident and improve future security measures
- C. To showcase the effectiveness of existing security protocols to stakeholders

Antwort: B

Begründung:
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
-

39. Frage
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 According to scenario 7, what type of incident has occurred at Konzolo?

- A. Critical severity incident
- B. High severity incident
- C. Medium severity incident

Antwort: B

Begründung:
Comprehensive and Detailed Explanation From Exact Extract:
Severity classification of an incident under ISO/IEC 27035-2:2016 is determined by factors such as potential data exposure, business disruption, and impact on critical services. In this scenario, the server downtime caused by a third-party breach and a vulnerability in cryptographic wallet software-capable of leading to asset exposure-signifies serious business and operational risks.

Although the vulnerability was critical, no actual asset theft or breach was confirmed. Therefore, while serious, the incident does not reach the "critical" threshold (which would typically involve data exfiltration, irreversible loss, or public impact). The appropriate classification is "High Severity." Reference:
* ISO/IEC 27035-2:2016, Clause 6.3.1: "Severity is determined by the actual or potential impact on business operations, data, reputation, and legal obligations."
* Annex A (Example Severity Levels): "High-severity incidents involve confirmed vulnerabilities with significant potential for impact, such as financial loss or regulatory violations." Correct answer: B
-

40. Frage
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.
During a training session on incident management at Alura Hospital, staff members are presented with various roles and responsibilities. One staff member, a technician, was unsure about their role during a data integrity incident. According to the training objectives, did the manager take the correct action to ensure the technician was prepared?

- A. No, roles and responsibilities should be assigned based on seniority to ensure that more experienced staff handle complex scenarios
- B. Yes, roles and responsibilities should include rotational training to ensure all staff are versatile
- C. No, they should have provided the technician with specific role-playing exercises related to data integrity incidents

Antwort: B

Begründung:
Comprehensive and Detailed Explanation:
According to ISO/IEC 27035-2 and ISO/IEC 27002:2022 (A.6.3 - Information Security Awareness and Training), incident response training should aim to build both competence and adaptability. Cross-training and rotational exposure to different incident types prepare staff for a wide range of potential scenarios, enhancing organizational resilience.
Assigning roles not strictly based on current expertise fosters flexibility and supports development, particularly in incident response, where versatile response capabilities are critical.
Reference:
ISO/IEC 27035-2:2016, Clause 5.2.3: "Training should cover various incident scenarios and enable staff to take on different responsibilities as required." ISO/IEC 27002:2022, Control A.6.3: "Training should be ongoing and adaptive to emerging threats and varied incident types." Correct answer: A

41. Frage
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 Referring to scenario 7, Konzolo conducted a forensic analysis after all systems had been fully restored and normal operations resumed. Is this recommended?

- A. No, they should have conducted it before responding to the incident to understand its cause
- B. No, they should have conducted it concurrently with the response to preserve evidence
- C. Yes, they should conduct it after all systems have been fully restored and normal operations have resumed

Antwort: B

Begründung:
Comprehensive and Detailed Explanation From Exact Extract:
Forensic analysis is most effective when conducted during or immediately following the detection and containment phases-before recovery processes begin-so that critical evidence is preserved. ISO/IEC 27035-
2:2016, Clause 6.4.2 emphasizes the importance of conducting evidence collection early in the incident lifecycle to maintain integrity and avoid contamination.
Performing forensic analysis after systems are restored risks overwriting or losing crucial data such as logs, memory states, and malicious artifacts. Therefore, Paulina should have conducted the analysis concurrently with or directly after containment, not post-recovery.
Reference:
* ISO/IEC 27035-2:2016, Clause 6.4.2: "Evidence collection should begin as early as possible during incident detection and containment to preserve forensic integrity."
* ISO/IEC 27043:2015 (Digital Forensics), Clause 7.2.1: "Evidence should be collected prior to recovery to maintain chain of custody and ensure integrity." Correct answer: A
-

42. Frage
.....

□ ISO-IEC-27035-Lead-Incident-Manager Fragen Beantworten □ Suchen Sie auf der Webseite □ www.deutschpruefung.com □ nach 《 ISO-IEC-27035-Lead-Incident-Manager 》 und laden Sie es kostenlos herunter □ □ISO-IEC-27035-Lead-Incident-Manager Zertifizierung

- ISO-IEC-27035-Lead-Incident-Manager: PECB Certified ISO/IEC 27035 Lead Incident Manager Dumps - PassGuide ISO-IEC-27035-Lead-Incident-Manager Examen □ Erhalten Sie den kostenlosen Download von ▷ ISO-IEC-27035-Lead-Incident-Manager ◁ mühelos über ➥ www.itzert.com □ □ISO-IEC-27035-Lead-Incident-Manager Prüfung
- ISO-IEC-27035-Lead-Incident-Manager Trainingsunterlagen □ ISO-IEC-27035-Lead-Incident-Manager Fragen&Antworten □ ISO-IEC-27035-Lead-Incident-Manager Fragen&Antworten □ URL kopieren ➥ www.itzert.com □ Öffnen und suchen Sie 「 ISO-IEC-27035-Lead-Incident-Manager 」 Kostenloser Download □ □ISO-IEC-27035-Lead-Incident-Manager Fragen Beantworten
- ISO-IEC-27035-Lead-Incident-Manager Pass Dumps - PassGuide ISO-IEC-27035-Lead-Incident-Manager Prüfung - ISO-IEC-27035-Lead-Incident-Manager Guide ⌨ Öffnen Sie die Webseite ➤ www.itzert.com □ und suchen Sie nach kostenloser Download von （ ISO-IEC-27035-Lead-Incident-Manager ） ☯ISO-IEC-27035-Lead-Incident-Manager PDF
- ISO-IEC-27035-Lead-Incident-Manager Zertifikatsdemo □ ISO-IEC-27035-Lead-Incident-Manager PDF ♥ ISO-IEC-27035-Lead-Incident-Manager Zertifizierung □ Suchen Sie jetzt auf □ de.fast2test.com □ nach □ ISO-IEC-27035-Lead-Incident-Manager □ um den kostenlosen Download zu erhalten □ISO-IEC-27035-Lead-Incident-Manager Online Tests
- ISO-IEC-27035-Lead-Incident-Manager Zertifizierung □ ISO-IEC-27035-Lead-Incident-Manager Zertifikatsdemo □ ISO-IEC-27035-Lead-Incident-Manager Zertifizierungsantworten □ Erhalten Sie den kostenlosen Download von 《 ISO-IEC-27035-Lead-Incident-Manager 》 mühelos über ➥ www.itzert.com □ □ISO-IEC-27035-Lead-Incident-Manager Deutsch Prüfungsfragen
- ISO-IEC-27035-Lead-Incident-Manager Exam Fragen □ ISO-IEC-27035-Lead-Incident-Manager Demotesten □ ISO-IEC-27035-Lead-Incident-Manager Prüfung □ Geben Sie ➽ www.zertpruefung.ch □ ein und suchen Sie nach kostenloser Download von ▷ ISO-IEC-27035-Lead-Incident-Manager ◁ □ISO-IEC-27035-Lead-Incident-Manager Online Tests
- ISO-IEC-27035-Lead-Incident-Manager Prüfungsinformationen □ ISO-IEC-27035-Lead-Incident-Manager Fragen&Antworten □ ISO-IEC-27035-Lead-Incident-Manager Pruefungssimulationen □ Geben Sie “ www.itzert.com ” ein und suchen Sie nach kostenloser Download von “ ISO-IEC-27035-Lead-Incident-Manager ” □ISO-IEC-27035-Lead-Incident-Manager Exam Fragen
- ISO-IEC-27035-Lead-Incident-Manager Pass Dumps - PassGuide ISO-IEC-27035-Lead-Incident-Manager Prüfung - ISO-IEC-27035-Lead-Incident-Manager Guide □ Suchen Sie jetzt auf ➡ www.itzert.com □□□ nach 「 ISO-IEC-27035-Lead-Incident-Manager 」 um den kostenlosen Download zu erhalten □ISO-IEC-27035-Lead-Incident-Manager Zertifikatsdemo
- ISO-IEC-27035-Lead-Incident-Manager Dumps □ ISO-IEC-27035-Lead-Incident-Manager Schulungsunterlagen ↗ ISO-IEC-27035-Lead-Incident-Manager Fragen Beantworten □ Erhalten Sie den kostenlosen Download von ▷ ISO-IEC-27035-Lead-Incident-Manager ◁ mühelos über ➤ www.itzert.com □ □ISO-IEC-27035-Lead-Incident-Manager Buch
- ISO-IEC-27035-Lead-Incident-Manager Dumps □ ISO-IEC-27035-Lead-Incident-Manager Vorbereitung □ ISO-IEC-27035-Lead-Incident-Manager Demotesten ⧗ Öffnen Sie die Webseite ➡ www.zertpruefung.ch □□□ und suchen Sie nach kostenloser Download von ⇛ ISO-IEC-27035-Lead-Incident-Manager ⇚ □ISO-IEC-27035-Lead-Incident-Manager Testing Engine
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, www.stes.tyc.edu.tw, Disposable vapes