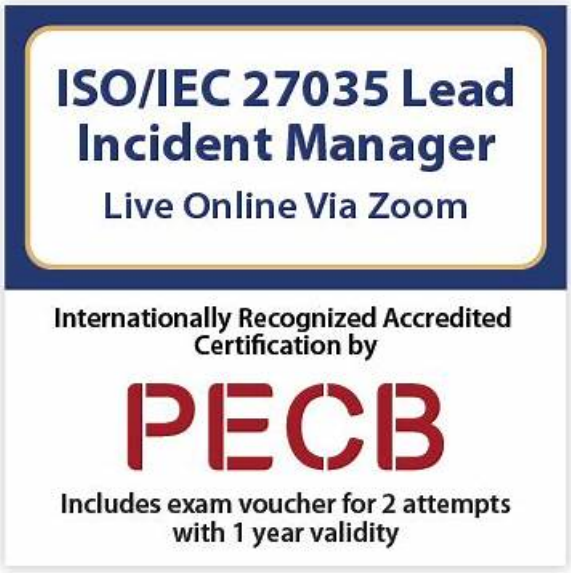
Need for PECB ISO-IEC-27035-Lead-Incident-Manager Exam Questions in Your Preparation



BONUS!!! Download part of PracticeVCE ISO-IEC-27035-Lead-Incident-Manager dumps for free: https://drive.google.com/open?id=1LbnALjlyGgy4eyqkG_gz3ZfuyXBcsXTW

The ISO-IEC-27035-Lead-Incident-Manager PDF file contains the real, valid, and updated PECB ISO-IEC-27035-Lead-Incident-Manager exam practice questions. These are the real ISO-IEC-27035-Lead-Incident-Manager exam questions that surely will appear in the upcoming exam and by preparing with them you can easily pass the final exam. The ISO-IEC-27035-Lead-Incident-Manager PDF Questions file is easy to use and install. You can use the ISO-IEC-27035-Lead-Incident-Manager PDF practice questions on your laptop, desktop, tabs, or even on your smartphone and start ISO-IEC-27035-Lead-Incident-Manager exam preparation right now.

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	• 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 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.

>> Certification ISO-IEC-27035-Lead-Incident-Manager Cost <<

Utilizing The Certification ISO-IEC-27035-Lead-Incident-Manager Cost Means that You Have Passed Half of PECB Certified ISO/IEC 27035 Lead Incident Manager

This kind of polished approach is beneficial for a commendable grade in the PECB Certified ISO/IEC 27035 Lead Incident Manager (ISO-IEC-27035-Lead-Incident-Manager) exam. While attempting the exam, take heed of the clock ticking, so that you manage the PECB Certified ISO/IEC 27035 Lead Incident Manager (ISO-IEC-27035-Lead-Incident-Manager) questions in a time-efficient way. Even if you are completely sure of the correct answer to a question, first eliminate the incorrect ones, so that you may prevent blunders due to human error.

PECB Certified ISO/IEC 27035 Lead Incident Manager Sample Questions (Q17-Q22):

NEW QUESTION # 17
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 regularly assess the physical security measures to ensure they align with incident management protocols
- C. No, organizations should conduct quarterly performance reviews of individual employees to ensure they follow 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 # 18
What is the primary input for the information security risk treatment process?

- A. A prioritized list of IT systems for security upgrades
- B. A prioritized set of risks to be treated based on risk criteria
- C. A prioritized list of all assets within the organization

Answer: B

Explanation:
Comprehensive and Detailed Explanation:
According to ISO/IEC 27005:2018, the risk treatment process begins after risk analysis and evaluation. The main input to this phase is a prioritized set of identified and assessed risks, chosen based on the organization's risk acceptance criteria. These risks are then assigned treatments such as mitigation, avoidance, or acceptance.
Reference:
ISO/IEC 27005:2018, Clause 8.4: "Risk treatment is based on a set of prioritized risks resulting from the risk assessment process."
Correct answer: B
-

NEW QUESTION # 19
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. Deploying an external firewall to detect threats that have already breached the perimeter defenses
- B. No, they should have deployed an intrusion detection system to identify and alert the incident response team of the breach
- C. No, they should have implemented a cloud-based antivirus solution instead of deploying an external firewall

Answer: A

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 # 20
What is the purpose of incident identification in the incident response process?

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

Answer: A

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 # 21
How is the impact of an information security event assessed?

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

Answer: B

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 # 22
.....

Aspiring PECB professionals strive to excel in PECB ISO-IEC-27035-Lead-Incident-Manager exams such as the PECB Certified ISO/IEC 27035 Lead Incident Manager (ISO-IEC-27035-Lead-Incident-Manager) to achieve their dream careers. However, passing the ISO-IEC-27035-Lead-Incident-Manager Exam can be challenging, especially with a demanding schedule that leaves little time for preparation.

Incident-Manager □ for free by simply searching on ➥ www.exams4collection.com □ □ISO-IEC-27035-Lead-Incident-Manager Updated Demo

- ISO-IEC-27035-Lead-Incident-Manager Latest Exam Guide □ Latest ISO-IEC-27035-Lead-Incident-Manager Exam Preparation □ ISO-IEC-27035-Lead-Incident-Manager Latest Exam Forum □ Download ⇛ ISO-IEC-27035-Lead-Incident-Manager ⇚ for free by simply entering □ www.pdfvce.com □ website □ISO-IEC-27035-Lead-Incident-Manager Downloadable PDF
- ISO-IEC-27035-Lead-Incident-Manager Exam Bible □ Latest ISO-IEC-27035-Lead-Incident-Manager Test Voucher □ ISO-IEC-27035-Lead-Incident-Manager New Braindumps Questions □ Download （ ISO-IEC-27035-Lead-Incident-Manager ） for free by simply searching on ☀ www.prep4pass.com □☀□ □Latest ISO-IEC-27035-Lead-Incident-Manager Exam Registration
- New ISO-IEC-27035-Lead-Incident-Manager Exam Test □ ISO-IEC-27035-Lead-Incident-Manager New Braindumps Questions □ ISO-IEC-27035-Lead-Incident-Manager Exam Bible □ Download □ ISO-IEC-27035-Lead-Incident-Manager □ for free by simply entering ☀ www.pdfvce.com □☀□ website □Latest ISO-IEC-27035-Lead-Incident-Manager Test Voucher
- Free PDF Quiz PECB - ISO-IEC-27035-Lead-Incident-Manager Authoritative Certification Cost □ Search for ➠ ISO-IEC-27035-Lead-Incident-Manager □ and download exam materials for free through （ www.prep4pass.com ） □ □ISO-IEC-27035-Lead-Incident-Manager Latest Exam Guide
- yxy99.top, 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, lms.ait.edu.za, tedcole945.laowaiblog.com, 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, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, adamree449.bluxeblog.com, www.olt.wang, adamree449.aboutyoublog.com, nogorweb.com, Disposable vapes

BONUS!!! Download part of PracticeVCE ISO-IEC-27035-Lead-Incident-Manager dumps for free: https://drive.google.com/open?id=1LbnALjlyGgy4eyqkG_gz3ZfuyXBcsXTW