Pass4sure PECB ISO-IEC-27035-Lead-Incident-Manager Dumps Pdf - ISO-IEC-27035-Lead-Incident-Manager Exam Cram Questions

BTW, DOWNLOAD part of VCE4Plus ISO-IEC-27035-Lead-Incident-Manager dumps from Cloud Storage: https://drive.google.com/open?id=1LXNgNrjODTZxyOC0vs3EnZxiFeZ-3woq

Through all these years' experience, our ISO-IEC-27035-Lead-Incident-Manager training materials are becoming more and more prefect. Moreover, we hold considerate after-sales services and sense-and-respond tenet all these years. So if you get any questions of our ISO-IEC-27035-Lead-Incident-Manager learning guide, please get us informed. It means we will deal with your doubts with our ISO-IEC-27035-Lead-Incident-Manager practice materials 24/7 with efficiency and patience.

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	• 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 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.

ISO-IEC-27035-Lead-Incident-Manager Exam Cram Questions - ISO-IEC-27035-Lead-Incident-Manager Test Simulator Online

If you use the trial version of our ISO-IEC-27035-Lead-Incident-Manager study materials, you will find that our products are very useful for you to pass your exam and get the certification. Though the trail version of our ISO-IEC-27035-Lead-Incident-Manager learning guide only contains a small part of the exam questions and answers, but it shows the quality and validity. If you buy our ISO-IEC-27035-Lead-Incident-Manager Exam Questions, we can promise that you will pass the exam for sure and gain the according the certification.

PECB Certified ISO/IEC 27035 Lead Incident Manager Sample Questions (Q76-Q81):

NEW QUESTION # 76
What role does the incident coordinator play during the response phase?

- A. Initiating the response actions immediately
- B. Assessing if the event is a potential or confirmed security incident
- C. Coordinating the activities of IRTs and monitoring response time

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The incident coordinator plays a vital managerial and operational role in guiding and synchronizing the efforts of Incident Response Teams (IRTs). ISO/IEC 27035-2:2016, Clause 7.2.2 describes the role as one that involves coordination of resources, communication, and oversight to ensure that all phases of the response are executed according to procedure and within acceptable timelines.
Responsibilities include:
Assigning roles and responsibilities
Overseeing containment, eradication, and recovery efforts
Communicating with stakeholders
Tracking incident metrics and resolution progress
Initiating the response (Option B) is typically a decision taken collectively or by senior management or the IMT after classification.
Assessing the nature of an event (Option C) falls under the detection and classification phase, not the coordinator's primary role during response.
Reference:
ISO/IEC 27035-2:2016, Clause 7.2.2: "The incident coordinator is responsible for leading and coordinating the incident response process, ensuring timely and efficient execution." Correct answer: A
-

NEW QUESTION # 77
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. Tactical
- B. Strategic
- 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 # 78
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 # 79
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 implemented a cloud-based antivirus solution instead of deploying an external firewall
- B. No, they should have deployed an intrusion detection system to identify and alert the incident response team of the breach
- 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 # 80

Based on the categorization of information security incidents, incidents such as abuse of rights, denial of actions, and misoperations are categorized as:

- A. Compromise of functions incident
- B. Breach of rule incident
- C. Compromise of information incident

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-1 classifies incidents into several categories based on the nature of their impact. Incidents involving the abuse of user rights, denial of authorized activities, or improper system use are considered violations of internal policies or rules. These fall under the category of "Breach of Rule" incidents.
This category emphasizes that while data or functionality may not be directly compromised, internal governance, permissions, or acceptable use policies have been violated. These incidents are crucial to detect as they often indicate insider threats or misconfigured permissions.
Reference:
ISO/IEC 27035-1:2016, Annex A.2.3: "Breach of Rule" incidents include abuse of privileges, unauthorized activities, and actions violating organizational policies.
Correct answer: C
-

NEW QUESTION # 81

......

Our ISO-IEC-27035-Lead-Incident-Manager study materials are designed carefully. We have taken all your worries into consideration. Also, we adopt the useful suggestions about our ISO-IEC-27035-Lead-Incident-Manager study materials from our customers. Now, our study materials are out of supply. Thousands of people will crowd into our website to choose the ISO-IEC-27035-Lead-Incident-Manager study materials. So people are different from the past. Learning has become popular among different age groups. Our ISO-IEC-27035-Lead-Incident-Manager Study Materials truly offer you the most useful knowledge. You can totally trust us. We are trying our best to meet your demands. Why not give our PECB study materials a chance? Our products will live up to your expectations.

ISO-IEC-27035-Lead-Incident-Manager Exam Cram Questions: https://www.vce4plus.com/PECB/ISO-IEC-27035-Lead-Incident-Manager-valid-vce-dumps.html

- ISO-IEC-27035-Lead-Incident-Manager Testking Learning Materials □ ISO-IEC-27035-Lead-Incident-Manager Latest Questions □ ISO-IEC-27035-Lead-Incident-Manager Test Price □ Go to website ➽ www.prep4away.com □ open and search for ➡ ISO-IEC-27035-Lead-Incident-Manager □□□ to download for free □ISO-IEC-27035-Lead-Incident-Manager Test Result
- ISO-IEC-27035-Lead-Incident-Manager Demo Test □ ISO-IEC-27035-Lead-Incident-Manager Exam Collection □ ISO-IEC-27035-Lead-Incident-Manager Detailed Study Dumps □ Enter ▶ www.pdfvce.com ◀ and search for ☀ ISO-IEC-27035-Lead-Incident-Manager □☀□ to download for free □ISO-IEC-27035-Lead-Incident-Manager Dumps PDF
- Free PDF Quiz ISO-IEC-27035-Lead-Incident-Manager - High-quality Pass4sure PECB Certified ISO/IEC 27035 Lead Incident Manager Dumps Pdf □ Download ☀ ISO-IEC-27035-Lead-Incident-Manager □☀□ for free by simply searching on ➡ www.prepawaypdf.com □□□ □Reliable ISO-IEC-27035-Lead-Incident-Manager Study Guide
- Real ISO-IEC-27035-Lead-Incident-Manager Braindumps □ ISO-IEC-27035-Lead-Incident-Manager Latest Questions □ Training ISO-IEC-27035-Lead-Incident-Manager Tools □ Search for ⇛ ISO-IEC-27035-Lead-Incident-Manager ⇚ and download it for free immediately on ▶ www.pdfvce.com ◀ □Real ISO-IEC-27035-Lead-Incident-Manager Braindumps
- ISO-IEC-27035-Lead-Incident-Manager Reliable Test Dumps □ Training ISO-IEC-27035-Lead-Incident-Manager Tools □ ISO-IEC-27035-Lead-Incident-Manager Detailed Study Dumps □ Download （ ISO-IEC-27035-Lead-Incident-Manager ） for free by simply entering □ www.vce4dumps.com □ website □Real ISO-IEC-27035-Lead-Incident-Manager Braindumps
- Interactive ISO-IEC-27035-Lead-Incident-Manager Practice Exam □ Real ISO-IEC-27035-Lead-Incident-Manager Braindumps □ ISO-IEC-27035-Lead-Incident-Manager Test Price □ Search for ⇛ ISO-IEC-27035-Lead-Incident-Manager ⇚ and easily obtain a free download on ▶ www.pdfvce.com ◀ □ISO-IEC-27035-Lead-Incident-Manager Latest Questions

- Web-Based PECB ISO-IEC-27035-Lead-Incident-Manager Practice Exam - Compatible with all OS □ Go to website 【 www.testkingpass.com 】 open and search for ▹ ISO-IEC-27035-Lead-Incident-Manager ◃ to download for free □ □ISO-IEC-27035-Lead-Incident-Manager Detailed Study Dumps
- Free PDF Quiz ISO-IEC-27035-Lead-Incident-Manager - High-quality Pass4sure PECB Certified ISO/IEC 27035 Lead Incident Manager Dumps Pdf □ Download （ ISO-IEC-27035-Lead-Incident-Manager ） for free by simply searching on ☀ www.pdfvce.com □☀□ □Real ISO-IEC-27035-Lead-Incident-Manager Braindumps
- Tested Material Used To PECB Get Ahead ISO-IEC-27035-Lead-Incident-Manager Pass4sure Dumps Pdf □ Download 「 ISO-IEC-27035-Lead-Incident-Manager 」 for free by simply entering 《 www.testkingpass.com 》 website □ISO-IEC-27035-Lead-Incident-Manager Updated Testkings
- Pass4sure ISO-IEC-27035-Lead-Incident-Manager Dumps Pdf - 100% Pass Quiz 2026 PECB First-grade ISO-IEC-27035-Lead-Incident-Manager: PECB Certified ISO/IEC 27035 Lead Incident Manager Exam Cram Questions □ Simply search for 《 ISO-IEC-27035-Lead-Incident-Manager 》 for free download on [www.pdfvce.com] □Reliable ISO-IEC-27035-Lead-Incident-Manager Test Sample
- Tested Material Used To PECB Get Ahead ISO-IEC-27035-Lead-Incident-Manager Pass4sure Dumps Pdf □ Search on ➠ www.pdfdumps.com □ for " ISO-IEC-27035-Lead-Incident-Manager " to obtain exam materials for free download □ □ISO-IEC-27035-Lead-Incident-Manager Reliable Test Dumps
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, ycs.instructure.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, elgonihi.com, www.stes.tyc.edu.tw, Disposable vapes

What's more, part of that VCE4Plus ISO-IEC-27035-Lead-Incident-Manager dumps now are free: https://drive.google.com/open?id=1LXNgNrjODTZxyOC0vs3EnZxiFeZ-3woq