Free PDF Quiz PECB - ISO-IEC-27035-Lead-Incident-Manager - Efficient Latest PECB Certified ISO/IEC 27035 Lead Incident Manager Exam Pass4sure

2026 Latest FreeCram ISO-IEC-27035-Lead-Incident-Manager PDF Dumps and ISO-IEC-27035-Lead-Incident-Manager Exam Engine Free Share: https://drive.google.com/open?id=1xcXLcsWTy7LSvOOrIJ5jYdqmPCwjd_iR

Our company constantly increases the capital investment on the research and innovation of our ISO-IEC-27035-Lead-Incident-Manager study materials and expands the influences of our study materials in the domestic and international market. Because the high quality and passing rate of our ISO-IEC-27035-Lead-Incident-Manager study materials more than 90 percent that clients choose to buy our study materials when they prepare for the test ISO-IEC-27035-Lead-Incident-Manager Certification. We have established a good reputation among the industry and the constantly-enlarged client base. Our sales volume and income are constantly increasing and the clients' credibility towards our ISO-IEC-27035-Lead-Incident-Manager study materials stay high.

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

Topic	Details
Topic 1	• 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 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	• 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.

>> Latest ISO-IEC-27035-Lead-Incident-Manager Exam Pass4sure <<

Testing ISO-IEC-27035-Lead-Incident-Manager Center | ISO-IEC-27035-Lead-Incident-Manager Downloadable PDF

To help you get to know the exam questions and knowledge of the ISO-IEC-27035-Lead-Incident-Manager practice exam successfully and smoothly, our experts just pick up the necessary and essential content in to our ISO-IEC-27035-Lead-Incident-Manager test guide with unequivocal content rather than trivia knowledge that exam do not test at all. To make you understand the content more efficient, our experts add charts, diagrams and examples in to ISO-IEC-27035-Lead-Incident-Manager Exam Questions to speed up you pace of gaining success. So these ISO-IEC-27035-Lead-Incident-Manager latest dumps will be a turning point in your life. And on your way to success, they can offer titanic help to make your review more relaxing and effective. Moreover, the passing certificate and all benefits coming along are not surreal dreams anymore.

PECB Certified ISO/IEC 27035 Lead Incident Manager Sample Questions (Q74-Q79):

NEW QUESTION # 74
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 # 75
Which method is used to examine a group of hosts or a network known for vulnerable services?

- A. Penetration testing
- B. Automated vulnerability scanning tool
- C. Security testing and evaluation

Answer: B

Explanation:
Comprehensive and Detailed Explanation:
An automated vulnerability scanning tool is designed specifically to scan systems, hosts, or networks for known vulnerabilities based on a maintained vulnerability database. These tools are efficient for covering large environments quickly and are commonly used in routine security assessments.
Security testing and evaluation (A) is broader and includes manual assessments. Penetration testing (C) simulates real-world attacks but is usually more targeted and time-intensive.
Reference:
ISO/IEC 27002:2022, Control A.5.27: "Automated vulnerability scanning should be used to identify technical vulnerabilities."
Correct answer: B
-

NEW QUESTION # 76
Scenario 4: ORingo is a company based in Krakow, Poland, specializing in developing and distributing electronic products for health monitoring and heart rate measurement applications. With a strong emphasis on innovation and technological advancement, ORingo has established itself as a trusted provider of high-quality, reliable devices that enhance the well being and healthcare capabilities of individuals and healthcare professionals alike.
As part of its commitment to maintaining the highest standards of information security, ORingo has established an information security incident management process This process aims to ensure that any potential threats are swiftly identified, assessed, and addressed to protect systems and information. However, despite these measures, an incident response team member at ORingo recently detected a suspicious state in their systems operational data, leading to the decision to shut down the company-wide system until the anomaly could be thoroughly investigated Upon detecting the threat, the company promptly established an incident response team to respond to the incident effectively. The team's responsibilities encompassed identifying root causes, uncovering hidden vulnerabilities, and implementing timely resolutions to mitigate the impact of the incident on ORingo's operations and customer trust.
In response to the threat detected across its cloud environments. ORingo employed a sophisticated security tool that broadened the scope of incident detection and mitigation This tool covers network traffic, doud environments, and potential attack vectors beyond traditional endpoints, enabling ORingo to proactively defend against evolving cybersecurity threats During a routine check, the IT manager at ORingo discovered that multiple employees lacked awareness of proper procedures following the detection of a phishing email. In response, immediate training sessions on information security policies and incident response were scheduled for all employees, emphasizing the importance of vigilance and adherence to established protocols in safeguarding ORingo's sensitive data and assets.
As part of the training initiative. ORingo conducted a simulated phishing attack exercise to assess employee response and knowledge. However, an employee inadvertently informed an external partner about the 'attack" during the exercise, highlighting the importance of ongoing education and reinforcement of security awareness principles within the organization.
Through its proactive approach to incident management and commitment to fostering a culture of security awareness and readiness. ORingo reaffirms its dedication to safeguarding the integrity and confidentiality of its electronic products and ensuring the trust and confidence of its customers and stakeholders worldwide.
In scenario 4, during a routine check, the IT manager discovered that multiple employees were unaware of the proper procedures following the detection of a phishing email and scheduled immediate training for all employees on information security policies and incident response. Is this recommended?

- A. No, providing training is unnecessary; the employees' ignorance of proper procedures regarding phishing emails is a minor issue
- B. Yes, it is recommended that immediate training on these topics be provided to ensure employees know how to respond correctly to phishing emails
- C. No, the IT manager should handle the incident without involving other employees

Answer: B

Explanation:
Comprehensive and Detailed Explanation:
Phishing is one of the most common entry points for cybersecurity incidents. ISO/IEC 27035 and ISO/IEC
27002 both recommend security awareness training as a key preventive control. When users do not understand proper response procedures, the risk of successful attacks increases significantly.
Providing immediate training, especially following the identification of a knowledge gap, is considered best practice. This aligns with ISO/IEC 27001:2022 Annex A.6.3 and A.5.36, which emphasize the need for education and continuous awareness on security topics, including how to handle phishing attempts.
Reference:
ISO/IEC 27035-1:2016, Clause 6.1 - "Preparation includes awareness training to reduce the likelihood and impact of incidents."
ISO/IEC 27002:2022, Control A.6.3 - "Personnel should receive appropriate awareness education and training to carry out their information security responsibilities." Therefore, the correct answer is A.

NEW QUESTION # 77
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, was Mark's information security incident management policy appropriately developed?

- A. No, the purpose of the information security incident management policy was not appropriately defined, as it failed to address all potential threats
- B. No, he should have outlined any awareness and training initiatives within the organization that are related to incident management
- C. Yes, the information security incident management policy was appropriately developed

Answer: C

Explanation:
-
Comprehensive and Detailed Explanation From Exact Extract:
Yes, Mark's approach to developing NoSpace's information security incident management policy was aligned with the structured guidelines outlined in ISO/IEC 27035-1 and ISO/IEC 27035-2. These standards emphasize the importance of establishing an effective and realistic policy framework that supports the identification, management, and learning from information security incidents.
ISO/IEC 27035-1:2016, Clause 6.1, outlines the core components of the "Prepare" phase of the incident management lifecycle. A well-developed incident management policy should:
* Define the purpose, scope, and applicability of the policy
* Focus on critical assets and threats identified through a formal risk assessment
* Be shaped by stakeholder input
* Be realistic, enforceable, and capable of being integrated across departments
* Include training and awareness tailored to relevant personnel
In this scenario, Mark held a strategic session with stakeholders, ensured the policy was risk-based, and tailored training initiatives to critical roles only - which aligns precisely with ISO guidance on optimizing resource allocation and ensuring enforceability.
Option A is incorrect because the scenario clearly states that Mark implemented training and awareness initiatives tailored to critical response roles, which meets ISO/IEC 27035-1 expectations.
Option B is incorrect because ISO/IEC 27035-1 emphasizes prioritization of high-risk threats rather than attempting to address all potential threats equally. A focused and actionable policy that targets the most significant risks is more practical and aligns with international best practices.
Reference Extracts:
* ISO/IEC 27035-1:2016, Clause 6.1: "The preparation phase should include the definition of incident management policy, development of procedures, and awareness/training initiatives."
* ISO/IEC 27035-2:2016, Clause 5.1: "The policy should be concise, focused on relevant threats, and shaped by organizational structure and risk appetite."
* ISO/IEC 27001:2022, Annex A.5.25 & A.5.27: "Clear roles, responsibilities, and awareness should be assigned and supported through training."
Therefore, the correct answer is: C. Yes, the information security incident management policy was appropriately developed.

NEW QUESTION # 78
Scenario 3: L&K Associates is a graphic design firm headquartered in Johannesburg, South Africa. It specializes in providing innovative and creative design solutions to clients across various industries. With offices in multiple parts of the country, they effectively serve clients, delivering design solutions that meet their unique needs and preferences.
In its commitment to maintaining information security, L&K Associates is implementing an information security incident management process guided by ISO/IEC 27035-1 and ISO/IEC 27035-2. Leona, the designated leader overseeing the implementation of the incident management process, customized the scope of incident management to align with the organization's unique requirements. This involved specifying the IT systems, services, and personnel involved in the incident management process while excluding potential incident sources beyond those directly related to IT systems and services.

Based on the scenario above, answer the following question:
Is the incident management scope correctly determined at L&K Associates?

- A. No, the incident management scope is overly restrictive, excluding potential incident sources beyond those directly related to IT systems and services
- B. Yes, the incident management scope is customized to align with the organization's unique needs
- C. No, the incident management scope is too broad, encompassing all IT systems regardless of relevance

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-1:2016 encourages organizations to define the scope of incident management based on their own risk environment, business model, and available resources. This scope should be tailored to focus on the systems, services, and personnel that are most critical and relevant to the organization's operations.
In this scenario, Leona appropriately aligned the scope with L&K Associates' specific IT infrastructure and business processes, deliberately including relevant IT systems and associated personnel while excluding unrelated sources. This customization is consistent with best practices and ensures that the incident management process remains focused, efficient, and manageable.
ISO/IEC 27035-2, Clause 4.2, emphasizes that "the scope of incident management should be defined in a way that it supports the organization's objectives and risk environment." Therefore, the correct answer is A: Yes, the incident management scope is customized to align with the organization's unique needs.
-

NEW QUESTION # 79
.....

27035-Lead-Incident-Manager □ to download exam materials for free □ISO-IEC-27035-Lead-Incident-Manager Exam Study Guide

- ISO-IEC-27035-Lead-Incident-Manager Exams Training □ ISO-IEC-27035-Lead-Incident-Manager Exams Training □ □ Test ISO-IEC-27035-Lead-Incident-Manager Valid □ Easily obtain ➥ ISO-IEC-27035-Lead-Incident-Manager □ for free download through ➤ www.pdfdumps.com □ □ISO-IEC-27035-Lead-Incident-Manager Top Dumps
- Latest ISO-IEC-27035-Lead-Incident-Manager Learning Materials □ Reliable ISO-IEC-27035-Lead-Incident-Manager Guide Files ☃ High ISO-IEC-27035-Lead-Incident-Manager Passing Score □ Easily obtain free download of □ ISO-IEC-27035-Lead-Incident-Manager □ by searching on ➥ www.pdfvce.com □ □High ISO-IEC-27035-Lead-Incident-Manager Passing Score
- PECB ISO-IEC-27035-Lead-Incident-Manager - PECB Certified ISO/IEC 27035 Lead Incident Manager First-grade Latest Exam Pass4sure □ Search for " ISO-IEC-27035-Lead-Incident-Manager " and obtain a free download on （ www.practicevce.com ） □ISO-IEC-27035-Lead-Incident-Manager Exam Details
- 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.drnehaarora.com, 47.92.5.61:8080, creativeacademy.online, www.callcentersindia.co.in, pink88.cc, 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, alaa-essam.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, Disposable vapes

BTW, DOWNLOAD part of FreeCram ISO-IEC-27035-Lead-Incident-Manager dumps from Cloud Storage: https://drive.google.com/open?id=1xcXLcsWTy7LSvOOrIJ5jYdqmPCwjd_iR