Certificate PECB ISO-IEC-27035-Lead-Incident-Manager Exam, ISO-IEC-27035-Lead-Incident-Manager Online Training Materials

DOWNLOAD the newest Pass4training ISO-IEC-27035-Lead-Incident-Manager PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1NLSrNm4k6zEatEYuYLW4Fc0ZSEWfkgp6

Pass4training ISO-IEC-27035-Lead-Incident-Manager desktop and web-based practice exams are distinguished by their excellent features. The ISO-IEC-27035-Lead-Incident-Manager web-based practice exam is supported by all operating systems and can be taken through popular browsers including Chrome, MS Edge, Internet Explorer, Opera, Firefox, and Safari. Windows computers can run the desktop PECB ISO-IEC-27035-Lead-Incident-Manager Practice Test software. You won't require a live internet connection to use the desktop PECB exam simulation software once you've verified the product's license.

Are you preparing for the PECB ISO-IEC-27035-Lead-Incident-Manager certification exam? Whether you're an experienced professional PECB ISO-IEC-27035-Lead-Incident-Manager looking to take your career to the next level or a recent graduate trying to break into the tech field, the road to PECB ISO-IEC-27035-Lead-Incident-Manager Certification can be a long and challenging one. The good news is that you do not have to navigate it alone.

>> Certificate PECB ISO-IEC-27035-Lead-Incident-Manager Exam <<

PECB ISO-IEC-27035-Lead-Incident-Manager Online Training Materials | Reliable ISO-IEC-27035-Lead-Incident-Manager Exam Questions

The PECB Certified ISO/IEC 27035 Lead Incident Manager (ISO-IEC-27035-Lead-Incident-Manager) web-based practice test is compatible with these browsers: Chrome, Safari, Internet Explorer, MS Edge, Firefox, and Opera. This PECB Certified ISO/IEC 27035 Lead Incident Manager (ISO-IEC-27035-Lead-Incident-Manager) practice exam does not require any software installation as it is web-based. It has similar specifications to the PECB ISO-IEC-27035-Lead-Incident-Manager desktop-based practice exam software, but it requires an internet connection.

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	• 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	• 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.

PECB Certified ISO/IEC 27035 Lead Incident Manager Sample Questions (Q20-Q25):

NEW QUESTION # 20
Scenario 7: Located in central London, Konzolo has become a standout innovator in the cryptocurrency field.
The company faced challenges monitoring the security of its own and third-party systems. An incident involving server downtime exposed vulnerabilities in a third-party service provider's security posture, leading to unauthorized access.
In response, Konzolo launched a thorough vulnerability scan of its cryptographic wallet software and uncovered critical weaknesses due to outdated encryption algorithms. Noah, the IT manager, documented and communicated the findings. Paulina was brought in to lead a forensic investigation, provide actionable insights, and help enhance the company's overall incident response strategy based on ISO/IEC 27035 standards.
Based on the scenario above, answer the following question:
Which of the following steps for effective security monitoring did Konzolo NOT adhere to?

- A. Monitor the outsourced services
- B. Monitor behavioral analytics
- C. Monitor security vulnerabilities

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-1:2016 and ISO/IEC 27035-2:2016 emphasize the importance of monitoring not only internal systems but also third-party or outsourced services. Clause 7.3.2 of ISO/IEC 27035-2 specifically recommends that organizations establish mechanisms for the continuous monitoring of service providers and outsourced systems, particularly when such services process or store sensitive information.
In the scenario, Konzolo suffered an incident due to a failure by a third-party service provider to uphold security controls. This indicates that Konzolo had insufficient or no effective monitoring of outsourced services in place, which directly contributed to the breach and system downtime.
On the other hand:
Option A is incorrect because Konzolo did conduct a vulnerability scan, identifying and addressing cryptographic weaknesses.
Option B is also incorrect, as Paulina conducted forensic and behavioral analysis (both manual and automated) as part of the investigation process.
Reference Extracts:
ISO/IEC 27035-2:2016, Clause 7.3.2: "Monitoring should not be limited to internal infrastructure but should include third-party and outsourced services to ensure that they are operating within defined security parameters." ISO/IEC 27002:2022, Control 5.23:

"Information security should be addressed in agreements with third parties." Correct answer: C
-

NEW QUESTION # 21
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. Yes, the information security incident management policy was appropriately developed
- B. No, the purpose of the information security incident management policy was not appropriately defined, as it failed to address all potential threats
- C. No, he should have outlined any awareness and training initiatives within the organization that are related to incident management

Answer: A

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 # 22
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.
Based on scenario 4, are the responsibilities of the incident response team (IRT) established according to the ISO/IEC 27035-2 guidelines?

- A. Yes, IRT's responsibilities include identifying root causes, discovering hidden vulnerabilities, and resolving incidents quickly to minimize their impact
- B. No, the responsibilities of IRT also include assessing events and declaring incidents
- C. No, the responsibilities of IRT do not include resolving incidents

Answer: B

Explanation:
Comprehensive and Detailed Explanation:
ISO/IEC 27035-2:2016 outlines comprehensive responsibilities for an incident response team, which include not just response and mitigation but also:
Assessing and classifying reported events
Determining if they qualify as incidents
Coordinating containment, eradication, and recovery actions
Conducting root cause analysis and lessons learned
While the scenario highlights the team's strengths in root cause analysis and resolution, it omits one key responsibility: the proper assessment and classification of the anomaly before response. This makes option C the most accurate.
Reference:
ISO/IEC 27035-2:2016, Clause 5.2.2 - "The IRT should assess events, determine whether they are incidents, and take appropriate actions." Therefore, the correct answer is C.
-

NEW QUESTION # 23
Who is responsible for approving an organization's information security incident management policy?

- A. Incident manager

- B. Incident coordinator
- C. Top management

Answer: C

Explanation:
Comprehensive and Detailed Explanation:
According to ISO/IEC 27001:2022 and ISO/IEC 27035-2:2016, top management holds accountability for ensuring the alignment of security policies with organizational objectives. Policy approval, particularly for something as critical as incident management, must be authorized by top-level decision-makers to ensure authority, enforcement, and resource support.
Reference:
ISO/IEC 27001:2022, Clause 5.1: "Top management shall demonstrate leadership and commitment...
including approval of the information security policy."
ISO/IEC 27035-2:2016, Clause 4.3: "The policy should be approved and issued by top management." Correct answer: A
-

NEW QUESTION # 24
Scenario 1: RoLawyers is a prominent legal firm based in Guadalajara, Mexico. It specializes in a wide range of legal services tailored to meet the diverse needs of its clients. Committed to excellence and integrity, RoLawyers has a reputation for providing legal representation and consultancy to individuals, businesses, and organizations across various sectors.
Recognizing the critical importance of information security in today's digital landscape, RoLawyers has embarked on a journey to enhance its information security measures. This company is implementing an information security incident management system aligned with ISO/IEC 27035-1 and ISO/IEC 27035-2 guidelines. This initiative aims to strengthen RoLawyers' protections against possible cyber threats by implementing a structured incident response process to provide guidance on establishing and maintaining a competent incident response team.
After transitioning its database from physical to online infrastructure to facilitate seamless information sharing among its branches, RoLawyers encountered a significant security incident. A malicious attack targeted the online database, overloading it with traffic and causing a system crash, making it impossible for employees to access it for several hours.
In response to this critical incident, RoLawyers quickly implemented new measures to mitigate the risk of future occurrences. These measures included the deployment of a robust intrusion detection system (IDS) designed to proactively identify and alert the IT security team of potential intrusions or suspicious activities across the network infrastructure. This approach empowers RoLawyers to respond quickly to security threats, minimizing the impact on their operations and ensuring the continuity of its legal services.
By being proactive about information security and incident management, RoLawyers shows its dedication to protecting sensitive data, keeping client information confidential, and earning the trust of its stakeholders.
Using the latest practices and technologies, RoLawyers stays ahead in legal innovation and is ready to handle cybersecurity threats with resilience and careful attention.
According to scenario 1, what information security incident did RoLawyers face?

- A. Malware attack
- B. Man-in-the-middle attack
- C. Denial-of-service attack

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
According to ISO/IEC 27035-1:2016, an information security incident is any event that compromises the confidentiality, integrity, or availability of information. In this scenario, RoLawyers experienced an attack where their online database was overloaded with excessive traffic, resulting in a system crash. This incident made it impossible for employees to access the database for several hours. This type of event is characteristic of a Denial-of-Service (DoS) attack. ISO/IEC 27035-1 Annex B provides examples of typical incidents, and one example includes "network-based attacks, including denial-of-service attacks." A DoS attack typically aims to make a service or resource unavailable to its intended users by overwhelming it with traffic.
There is no indication in the scenario that the attackers were intercepting communications (as would be seen in a Man-in-the-Middle attack) or installing malware to damage or steal data. The nature of the attack- excess traffic causing a crash-clearly aligns with the definition of a DoS attack.
Reference Extracts:
ISO/IEC 27035-1:2016, Clause B.2.1 (Examples of incident types): "Denial-of-service (DoS) attacks cause disruption or degradation of services." ISO/IEC 27035-1:2016, Clause 4.1: "An incident can result from deliberate attacks such as DoS, malicious code, or unauthorized access." Therefore, the incident faced by RoLawyers was a Denial-of-Service attack.
-

NEW QUESTION # 25

.....

If you prepare ISO-IEC-27035-Lead-Incident-Manager real exam with our training materials, we guarantee your success in the first attempt. Our test engine enables you practice ISO-IEC-27035-Lead-Incident-Manager exam questions in the mode of the formal test and enjoy the atmosphere of the actual test. Our ISO-IEC-27035-Lead-Incident-Manager Practice Test is a way of exam simulation that will mark your mistakes and remind you when you practice dump next time.

ISO-IEC-27035-Lead-Incident-Manager Online Training Materials: https://www.pass4training.com/ISO-IEC-27035-Lead-Incident-Manager-pass-exam-training.html

- ISO-IEC-27035-Lead-Incident-Manager Latest Version □ Latest ISO-IEC-27035-Lead-Incident-Manager Version □ ISO-IEC-27035-Lead-Incident-Manager Latest Exam Registration □ Go to website （ www.vceengine.com ） open and search for 【 ISO-IEC-27035-Lead-Incident-Manager 】 to download for free □ISO-IEC-27035-Lead-Incident-Manager Latest Exam Answers
- Free PDF 2026 High-quality PECB Certificate ISO-IEC-27035-Lead-Incident-Manager Exam □ Enter □ www.pdfvce.com □ and search for ⇛ ISO-IEC-27035-Lead-Incident-Manager ⇚ to download for free □ISO-IEC-27035-Lead-Incident-Manager Latest Version
- ISO-IEC-27035-Lead-Incident-Manager New Learning Materials □ Demo ISO-IEC-27035-Lead-Incident-Manager Test □ ISO-IEC-27035-Lead-Incident-Manager Trustworthy Exam Content □ Search for ➥ ISO-IEC-27035-Lead-Incident-Manager □ and download it for free immediately on ⇛ www.testkingpass.com ⇚ □ISO-IEC-27035-Lead-Incident-Manager Latest Test Labs
- ISO-IEC-27035-Lead-Incident-Manager Practice Exam Materials: PECB Certified ISO/IEC 27035 Lead Incident Manager and ISO-IEC-27035-Lead-Incident-Manager Study Guide - Pdfvce □ Search for 「 ISO-IEC-27035-Lead-Incident-Manager 」 and download it for free immediately on ▸ www.pdfvce.com ◂ □Demo ISO-IEC-27035-Lead-Incident-Manager Test
- Certificate ISO-IEC-27035-Lead-Incident-Manager Exam - 100% Realistic Questions Pool ℹ Search for ⇛ ISO-IEC-27035-Lead-Incident-Manager ⇚ and download it for free on " www.torrentvce.com " website □ISO-IEC-27035-Lead-Incident-Manager Valid Exam Pass4sure
- Free PDF 2026 High-quality PECB Certificate ISO-IEC-27035-Lead-Incident-Manager Exam □ Open □ www.pdfvce.com □ enter ➡ ISO-IEC-27035-Lead-Incident-Manager □□□ and obtain a free download □ISO-IEC-27035-Lead-Incident-Manager Trustworthy Exam Content
- 100% Pass 2026 PECB - ISO-IEC-27035-Lead-Incident-Manager - Certificate PECB Certified ISO/IEC 27035 Lead Incident Manager Exam □ Search for □ ISO-IEC-27035-Lead-Incident-Manager □ on ➽ www.troytecdumps.com □ immediately to obtain a free download □ISO-IEC-27035-Lead-Incident-Manager Valid Exam Pass4sure
- ISO-IEC-27035-Lead-Incident-Manager Latest Exam Answers 👆 ISO-IEC-27035-Lead-Incident-Manager Latest Version □ Demo ISO-IEC-27035-Lead-Incident-Manager Test □ Copy URL ▹ www.pdfvce.com ◃ open and search for ➡ ISO-IEC-27035-Lead-Incident-Manager □□□ to download for free □ISO-IEC-27035-Lead-Incident-Manager New Study Questions
- Pass Guaranteed Marvelous ISO-IEC-27035-Lead-Incident-Manager Certificate PECB Certified ISO/IEC 27035 Lead Incident Manager Exam □ Copy URL { www.examcollectionpass.com } open and search for ➠ ISO-IEC-27035-Lead-Incident-Manager □ to download for free □ISO-IEC-27035-Lead-Incident-Manager New Exam Braindumps
- ISO-IEC-27035-Lead-Incident-Manager Practice Exam Materials: PECB Certified ISO/IEC 27035 Lead Incident Manager and ISO-IEC-27035-Lead-Incident-Manager Study Guide - Pdfvce □ Copy URL ✔ www.pdfvce.com □✔□ open and search for 「 ISO-IEC-27035-Lead-Incident-Manager 」 to download for free □ISO-IEC-27035-Lead-Incident-Manager New Exam Braindumps
- Free PDF PECB - Professional ISO-IEC-27035-Lead-Incident-Manager - Certificate PECB Certified ISO/IEC 27035 Lead Incident Manager Exam □ Search for □ ISO-IEC-27035-Lead-Incident-Manager □ on ▹ www.exam4labs.com ◃ immediately to obtain a free download □ISO-IEC-27035-Lead-Incident-Manager Simulation Questions
- learnonline.sprintlearn.net, 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, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.estudystudio.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, hashnode.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, maliwebcourse.com, Disposable vapes

What's more, part of that Pass4training ISO-IEC-27035-Lead-Incident-Manager dumps now are free: https://drive.google.com/open?id=1NLSrNm4k6zEatEYuYLW4Fc0ZSEWfkgp6