Free PDF 2025 Useful PECB Reliable ISO-IEC-27035-Lead-Incident-Manager Exam Preparation

DOWNLOAD the newest PrepAwayPDF ISO-IEC-27035-Lead-Incident-Manager PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1ScoPjfg2yZzF-j95HzzzNRlbEtftDExM

We are conscious of the fact that most of the candidates have a tight schedule which makes it tough to prepare for the PECB Certified ISO/IEC 27035 Lead Incident Manager exam preparation. PrepAwayPDF provides you PECB ISO-IEC-27035-Lead-Incident-Manager Exam Questions in 3 different formats to open up your study options and suit your preparation tempo.

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

Topic	Details
Topic 1	• 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 2	• 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.
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	• 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.

Get Actual PECB ISO-IEC-27035-Lead-Incident-Manager PDF Questions For Better Exam Preparation

Can you imagine that you only need to review twenty hours to successfully obtain the PECB certification? Can you imagine that you don't have to stay up late to learn and get your boss's favor? With ISO-IEC-27035-Lead-Incident-Manager study materials, passing exams is no longer a dream. If you are an office worker, ISO-IEC-27035-Lead-Incident-Manager Study Materials can help you make better use of the scattered time to review. Just a mobile phone can let you do questions at any time.

PECB Certified ISO/IEC 27035 Lead Incident Manager Sample Questions (Q61-Q66):

NEW QUESTION # 61
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 has recently upgraded its digital banking platform. In line with the continual improvement process, Moneda Vivo has decided to review the information security incident management process for accuracy immediately after the software update. Is this recommended?

- A. No, the incident management process should be evaluated after a significant technological overhaul to ensure the system is up-to-date
- B. Yes, the incident management process should be reviewed after any minor software update
- C. No, the incident management process should be reviewed when the bank's annual audit is conducted

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
According to ISO/IEC 27035-1:2016, Clause 7.1 and ISO/IEC 27035-2:2016, Clause 7.3.3, it is advised to review and revise the information security incident management process following major organizational or technical changes. These changes include upgrades, system overhauls, and structural IT shifts. While minor updates may not necessitate a full review, significant technological updates, such as those affecting core digital banking platforms, should trigger immediate evaluation to ensure continued relevance

and effectiveness of incident response strategies.
In the scenario, Moneda Vivo recognized the need for a review but delayed it, which could pose risks. Option C accurately reflects ISO guidance.
Reference:
ISO/IEC 27035-1:2016 Clause 7.1: "Reviews should be performed after major changes or after information security incidents."
ISO/IEC 27035-2:2016 Clause 7.3.3 Correct answer: C
-

NEW QUESTION # 62
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 security vulnerabilities
- B. Monitor the outsourced services
- C. Monitor behavioral analytics

Answer: B

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 # 63
During the 'detect and report' phase of incident management at TechFlow, the incident response team began collecting detailed threat intelligence and conducting vulnerability assessments related to these login attempts.
Additionally, the incident response team classified a series of unusual login attempts as a potential security incident and distributed initial reports to the incident coordinator. Is this approach correct?

- A. No, because collecting detailed information about threats and vulnerabilities should occur in later phases
- B. No, because information security incidents cannot yet be classified as information security incidents in this phase
- C. Yes, because classifying events as information security incidents is essential during this phase

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The 'detect and report' phase, as defined in ISO/IEC 27035-1:2016 (Clause 6.2), includes the identification, classification, and initial

reporting of information security events. If events meet certain thresholds-such as multiple failed login attempts from unknown IP addresses or matching threat indicators-they can and should be classified as potential incidents.
It is also appropriate to begin collecting supporting information during this phase. Gathering threat intelligence and performing basic vulnerability assessments help in confirming the scope and nature of the threat, allowing faster escalation and response.
Option B is incorrect because while deep forensic collection occurs later, preliminary data collection should begin during detection.
Option C is incorrect as incident classification is explicitly allowed and encouraged in this phase.
Reference:
ISO/IEC 27035-1:2016, Clause 6.2.2: "Events should be assessed and classified to determine whether they qualify as information security incidents." Clause 6.2.3: "All relevant details should be collected to support early classification and reporting." Correct answer: A

NEW QUESTION # 64
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, did Mark follow the guidelines of ISO/IEC 27035 series regarding the incident management phases in the updated incident management process?

- A. No, the decision on whether to classify events as information security incidents should be assessed before initiating the incident management process
- B. No, the second phase of the incident management process should include the collection of information associated with the occurrences of information security events
- C. Yes, all phases of the incident management process were established according to the ISO/IEC 27035-1 guidelines

Answer: B

Explanation:
-
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-1:2016 outlines a structured five-phase approach to information security incident management, which includes:
1. Prepare
2. Identify (or detect and report)
3. Assess and Decide
4. Respond
5. Lessons Learned
According to the standard, the "Assess and Decide" phase must include the collection, review, and analysis of information associated with the occurrence of a potential incident. This phase ensures that the organization bases its classification decisions on factual data and contextual analysis, allowing the organization to determine whether the event should be categorized as a formal security incident.
In the scenario, Mark does introduce an accelerated "count down" process to evaluate and classify incidents, which is a commendable improvement in efficiency. However, there is no mention of gathering or documenting the actual event data prior to classification. This oversight fails to fully align with the standard.
Option A is incorrect because not all phases were implemented as defined-specifically, phase 3 ("Assess and Decide") lacks an

essential component: the collection of evidence/information from the anomaly or event.
Option C is also incorrect. According to ISO/IEC 27035, assessment and classification take place within the formal incident management process-not before it. The initiation of the process includes the evaluation of whether a security event becomes an incident.
Reference Extracts:
* ISO/IEC 27035-1:2016, Clause 6.2.2: "The assessment and decision process involves analyzing the information associated with reported events to decide whether they should be treated as incidents."
* ISO/IEC 27035-2:2016, Clause 7.3: "This phase includes collecting information from available sources...
such as logs, reports, and alerts, to support classification and response decisions." Therefore, the correct answer is B: No, the second phase of the incident management process should include the collection of information associated with the occurrences of information security events.

NEW QUESTION # 65
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. Yes, it is recommended that immediate training on these topics be provided to ensure employees know how to respond correctly to phishing emails
- B. No, the IT manager should handle the incident without involving other employees
- C. No, providing training is unnecessary; the employees' ignorance of proper procedures regarding phishing emails is a minor issue

Answer: A

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 # 66

.....

Taking PrepAwayPDF PECB Certified ISO/IEC 27035 Lead Incident Manager (ISO-IEC-27035-Lead-Incident-Manager) practice test questions are also important. These PECB ISO-IEC-27035-Lead-Incident-Manager practice exams include questions that are based on a similar pattern as the finals. This makes it easy for the candidates to understand the PECB Certified ISO/IEC 27035 Lead Incident Manager (ISO-IEC-27035-Lead-Incident-Manager) exam question paper and manage the time. It is indeed a booster for the people who work hard and do not want to leave any chance of clearing the ISO-IEC-27035-Lead-Incident-Manager exam with brilliant scores.

Test ISO-IEC-27035-Lead-Incident-Manager Questions: https://www.prepawaypdf.com/PECB/ISO-IEC-27035-Lead-Incident-Manager-practice-exam-dumps.html

- Monitor Your Progress with ISO-IEC-27035-Lead-Incident-Manager Practice Test Software □ " www.free4dump.com " is best website to obtain ⇛ ISO-IEC-27035-Lead-Incident-Manager ⇚ for free download □ISO-IEC-27035-Lead-Incident-Manager Cert Guide
- Test ISO-IEC-27035-Lead-Incident-Manager Tutorials □ New ISO-IEC-27035-Lead-Incident-Manager Practice Materials □ New ISO-IEC-27035-Lead-Incident-Manager Test Pass4sure □ Search for ➽ ISO-IEC-27035-Lead-Incident-Manager □ and obtain a free download on （ www.pdfvce.com ） □Reliable ISO-IEC-27035-Lead-Incident-Manager Test Syllabus
- Pass Guaranteed Quiz Latest PECB - Reliable ISO-IEC-27035-Lead-Incident-Manager Exam Preparation □ Search on ▹ www.actual4labs.com ◃ for ☀ ISO-IEC-27035-Lead-Incident-Manager □☀□ to obtain exam materials for free download □ISO-IEC-27035-Lead-Incident-Manager Cert Guide
- Real PECB ISO-IEC-27035-Lead-Incident-Manager Exam Questions [2025]-Secrets To Pass Exam In First Try □ Search for 「 ISO-IEC-27035-Lead-Incident-Manager 」 and download it for free immediately on ➤ www.pdfvce.com □ □New ISO-IEC-27035-Lead-Incident-Manager Exam Objectives
- Efficient Reliable ISO-IEC-27035-Lead-Incident-Manager Exam Preparation - Pass ISO-IEC-27035-Lead-Incident-Manager Exam □ Simply search for ☀ ISO-IEC-27035-Lead-Incident-Manager □☀□ for free download on ➥ www.prep4pass.com □ □ISO-IEC-27035-Lead-Incident-Manager Study Group
- Real PECB ISO-IEC-27035-Lead-Incident-Manager Exam Questions [2025]-Secrets To Pass Exam In First Try □ The page for free download of ➽ ISO-IEC-27035-Lead-Incident-Manager □ on ➡ www.pdfvce.com □□□ will open immediately □Pdf ISO-IEC-27035-Lead-Incident-Manager Files
- ISO-IEC-27035-Lead-Incident-Manager Valid Test Answers □ Reliable ISO-IEC-27035-Lead-Incident-Manager Test Syllabus □ Pdf ISO-IEC-27035-Lead-Incident-Manager Files □ Search for ➠ ISO-IEC-27035-Lead-Incident-Manager □ and download exam materials for free through ➽ www.dumps4pdf.com □ ⛄New ISO-IEC-27035-Lead-Incident-Manager Practice Materials
- ISO-IEC-27035-Lead-Incident-Manager Cert Guide □ ISO-IEC-27035-Lead-Incident-Manager Cert Guide ✍ ISO-IEC-27035-Lead-Incident-Manager Study Group □ Copy URL " www.pdfvce.com " open and search for ▸ ISO-IEC-27035-Lead-Incident-Manager ◂ to download for free □High ISO-IEC-27035-Lead-Incident-Manager Passing Score
- ISO-IEC-27035-Lead-Incident-Manager Study Group □ Reliable ISO-IEC-27035-Lead-Incident-Manager Dumps □ ISO-IEC-27035-Lead-Incident-Manager Latest Test Materials □ Immediately open ▸ www.prep4away.com ◂ and search for [ISO-IEC-27035-Lead-Incident-Manager] to obtain a free download □Pdf ISO-IEC-27035-Lead-Incident-Manager Files
- Get The UP-To-Date PECB ISO-IEC-27035-Lead-Incident-Manager Exam Questions □ 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 Test Guide Online
- Pass Guaranteed 2025 Authoritative PECB ISO-IEC-27035-Lead-Incident-Manager: Reliable PECB Certified ISO/IEC 27035 Lead Incident Manager Exam Preparation □ Immediately open ▹ www.dumps4pdf.com ◃ and search for ➠ ISO-IEC-27035-Lead-Incident-Manager □ to obtain a free download □ISO-IEC-27035-Lead-Incident-Manager Exam Study Solutions
- mdtaschool.org, www.stes.tyc.edu.tw, dkpacademy.in, lms.ait.edu.za, cou.alnoor.edu.iq, ncon.edu.sa, study.stcs.edu.np, learn.akrmind.com, cobe2go.com, hindi.sachpress.com, Disposable vapes

2025 Latest PrepAwayPDF 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=1ScoPjfg2yZzF-j95HzzzNRlbEtftDExM