ISO-IEC-27035-Lead-Incident-Manager題庫下載 & ISO-IEC-27035-Lead-Incident-Manager真題

P.S. NewDumps在Google Drive上分享了免費的2025 PECB ISO-IEC-27035-Lead-Incident-Manager考試題庫：https://drive.google.com/open?id=149HQjUkOPqLfcAJwgiWGIb5pnykh2EJV

您是否在尋找可靠的學習資料來準備即將來的ISO-IEC-27035-Lead-Incident-Manager考試？如果是的話，您可以嘗試NewDumps的產品和服務。我們提供最新的PECB ISO-IEC-27035-Lead-Incident-Manager考古題是經過眾多考生和專家檢驗過的學習指南，保證成功率百分之百的考古題。對于購買ISO-IEC-27035-Lead-Incident-Manager題庫產品的客戶，我們還提供一年的免費更新服務。所以，您不必擔心，PECB ISO-IEC-27035-Lead-Incident-Manager學習指南不僅讓您更準確的了解考試的出題點，還能讓您更有范圍的學習相關知識，高效率的通過ISO-IEC-27035-Lead-Incident-Manager考試。

人生舞臺的大幕隨時都可能拉開，關鍵是你願意表演，還是選擇躲避，能把在面前行走的機會抓住的人，十有八九都是成功的。所以你必須抓住NewDumps這個機會，讓你隨時可以展現你的技能，NewDumps PECB的ISO-IEC-27035-Lead-Incident-Manager考試培訓資料就是你通過認證的最有效的方法，有了這個認證，你將在你人生的藍圖上隨意揮灑，實現你的夢想，走向成功。要做就做一個勇往直前的人，那樣的人生才有意義。

>> ISO-IEC-27035-Lead-Incident-Manager題庫下載 <<

準備充分的ISO-IEC-27035-Lead-Incident-Manager題庫下載和認證考試的領導者材料和認證的ISO-IEC-27035-Lead-Incident-Manager真題

通過很多已經使用NewDumps的些針對IT認證考試培訓資料的考生的回饋，證明了使用我們的NewDumps的產品通過It認證考試是很容易的。NewDumps最近研究出來了關於熱門的PECB ISO-IEC-27035-Lead-Incident-Manager 認證考試的培訓方案，包括一些針對性的測試題，可以幫助你鞏固知識，讓你為PECB ISO-IEC-27035-Lead-Incident-Manager 認證考試做好充分的準備。

最新的 ISO 27001 ISO-IEC-27035-Lead-Incident-Manager 免費考試真題 (Q54-Q59):

問題 #54
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. Yes, all phases of the incident management process were established according to the ISO/IEC 27035-1 guidelines
- C. No, the second phase of the incident management process should include the collection of information associated with the occurrences of information security events

答案：C

解題說明：
-
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.

問題 #55
Scenario 7: Located in central London, Konzolo has become a standout innovator in the cryptocurrency field.
By introducing its unique cryptocurrency, Konzolo has contributed to the variety of digital currencies and prioritized enhancing the security and reliability of its offerings.
Konzolo aimed to enhance its systems but faced challenges in monitoring the security of its own and third- party systems. These issues became especially evident during an incident that caused several hours of server downtime This downtime was primarily caused by a third-party service provider that failed to uphold strong security measures, allowing unauthorized access.
In response to this critical situation, Konzolo strengthened its information security infrastructure. The company initiated a comprehensive vulnerability scan of its cryptographic wallet software, a cornerstone of its digital currency offerings The scan revealed a critical vulnerability due to the software using outdated encryption algorithms that are susceptible to decryption by modern methods that posed a significant risk of asset exposure Noah, the IT manager, played a central role in this discovery With careful attention to detail, he documented the vulnerability and communicated the findings to the incident response team and management.
Acknowledging the need for expertise in navigating the complexities of information security incident management. Konzolo welcomed Paulina to the team. After addressing the vulnerability and updating the cryptographic algorithms, they recognized the importance of conducting a thorough investigation to prevent future vulnerabilities. This marked the stage for Paulina s crucial involvement. She performed a detailed forensic analysis of the incident, employing automated and manual methods during the collection phase. Her analysis provided crucial insights into the security breach, enabling Konzolo to understand the depth of the vulnerability and the actions required to mitigate it.
Paulina also played a crucial role in the reporting phase, as her comprehensive approach extended beyond analysis. By defining clear and actionable steps for future prevention and response, she contributed significantly to developing a resilient information security incident management system based on ISO/IEC
27035-1 and 27035-2 guidelines. This strategic initiative marked a significant milestone in Konzolo's quest to strengthen its defenses against cyber threats According to scenario 7, what type of incident has occurred at Konzolo?

- A. Medium severity incident
- B. Critical severity incident
- C. High severity incident

答案：C

解題說明：
Comprehensive and Detailed Explanation From Exact Extract:
Severity classification of an incident under ISO/IEC 27035-2:2016 is determined by factors such as potential data exposure, business disruption, and impact on critical services. In this scenario, the server downtime caused by a third-party breach and a vulnerability in cryptographic wallet software-capable of leading to asset exposure-signifies serious business and operational risks. Although the vulnerability was critical, no actual asset theft or breach was confirmed. Therefore, while serious, the incident does not reach the "critical" threshold (which would typically involve data exfiltration, irreversible loss, or public impact). The appropriate classification is "High Severity." Reference:
* ISO/IEC 27035-2:2016, Clause 6.3.1: "Severity is determined by the actual or potential impact on business operations, data, reputation, and legal obligations."
* Annex A (Example Severity Levels): "High-severity incidents involve confirmed vulnerabilities with significant potential for impact, such as financial loss or regulatory violations." Correct answer: B
-

問題 #56
How is the impact of an information security event assessed?

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

答案：C

解題說明：
Comprehensive and Detailed Explanation From Exact Extract:
The impact of an information security event is assessed by evaluating how the event affects the CIA triad- Confidentiality, Integrity, and Availability-of information assets. This fundamental concept underpins all ISO/IEC 27000-series standards, including ISO/IEC 27035.
ISO/IEC 27035-1:2016, Clause 6.2.3 explicitly states that an event's severity and urgency are to be assessed by evaluating its

actual or potential impact on the organization's information security objectives, namely:
Confidentiality: Protection from unauthorized disclosure
Integrity: Protection from unauthorized modification
Availability: Assurance of timely and reliable access
This approach ensures consistent and risk-based decision-making during incident assessment. Options A and B are important steps, but they are part of the broader process; they do not directly measure impact.
Reference:
ISO/IEC 27035-1:2016, Clause 6.2.3: "The impact should be assessed based on the effect on confidentiality, integrity, and availability of the information assets affected." Correct answer: C
-

問題 #57
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 the scenario above, answer the following question:
After identifying a suspicious state in ORingo's system, a member of the IRT initiated a company-wide system shutdown until the anomaly was investigated. Is this acceptable?

- A. No, the IRT should have immediately informed all employees about the potential data breach
- B. No, the IRT should have determined the facts that enable detection of the event occurrence
- C. Yes, the correct action is to initiate a company-wide system shutdown until the anomaly is investigated

答案：B

解題說明：
Comprehensive and Detailed Explanation:
According to ISO/IEC 27035-1:2016, particularly in Clause 6.2.2 (Assess and Decide), the organization must first assess the reported event to determine whether it qualifies as a security incident before implementing disruptive responses such as a full system shutdown.
Initiating a shutdown without first determining the cause, impact, or whether it's a confirmed incident can lead to unnecessary operational disruption and loss of services. The proper approach is to collect evidence, analyze system behavior, and make informed decisions based on risk level and confirmed facts.
Option B best reflects the required approach: The IRT should first determine the facts that enable detection and validation of the event's occurrence and impact before initiating drastic action like shutting down critical systems.
Reference:
ISO/IEC 27035-1:2016, Clause 6.2.2 - "An analysis should be conducted to determine whether the event should be treated as an information security incident." Clause 6.2.3 - "Response should be proportionate to the impact and type of the incident." Therefore, the correct answer is B.

-

問題 #58
What is one of the requirements for an organization's technical means in supporting information security?

- A. Public disclosure of contact register details for transparency
- B. Immediate deletion of all incident reports for security purposes
- C. Quick acquisition of information security event/incident/vulnerability reports

答案：C

解題說明：
Comprehensive and Detailed Explanation From Exact Extract:
According to ISO/IEC 27035-2:2016, one of the technical requirements to support effective incident management is the capability to rapidly detect, collect, and process information about security events, incidents, and vulnerabilities. Timely acquisition of this data allows the organization to assess threats, determine the scope of incidents, and execute response measures quickly.
Clause 7.4.1 emphasizes the need for adequate tools and infrastructure to support the detection and acquisition of information security events and vulnerability reports. The collected data becomes the foundation for risk assessment, root cause analysis, and corrective action planning.
Option A (public disclosure of contact details) might be relevant for CERT/CSIRT public coordination but is not a core requirement in technical incident response. Option B (immediate deletion of reports) is contrary to best practices, as incident reports are critical for audits, compliance, and continuous improvement.
Reference Extracts:
ISO/IEC 27035-2:2016, Clause 7.4.1: "Organizations should ensure that technical means are in place to allow quick acquisition and analysis of information related to events, incidents, and vulnerabilities." Correct answer: C
-

問題 #59
.....

現在許多公司正要求員工接受減薪，然而雇員可能抱怨幾年前增加的不足百分之四或五的薪水，持有當前的 IT 認證不能保證您不面對減薪。但擁有特別的認證包括 GAQM、EMC、ISC證書，就會使員工具有獲得被付高薪的資格。而 NewDumps 為你提供的 PECB ISO-IEC-27035-Lead-Incident-Manager 練習題和答案能使你順利通過考試。PECB ISO-IEC-27035-Lead-Incident-Manager 考古題是考試之前的模擬考試時很有必要的，也是很有效的。如果你選擇了它，你可以100%通過 ISO-IEC-27035-Lead-Incident-Manager 考試。

ISO-IEC-27035-Lead-Incident-Manager真題: https://www.newdumpspdf.com/ISO-IEC-27035-Lead-Incident-Manager-exam-new-dumps.html

PECB ISO-IEC-27035-Lead-Incident-Manager題庫下載 如果你回答“是”，那趕緊來參加考試吧，我們為您提供涵蓋真實測試的題目和答案的試題，快將我們NewDumps ISO-IEC-27035-Lead-Incident-Manager真題的產品收入囊中吧，通過我們專家團隊編寫的PECB ISO-IEC-27035-Lead-Incident-Manager全真題庫練習就是最好的捷徑，我們的NewDumps ISO-IEC-27035-Lead-Incident-Manager真題在任何時間下都可以幫您快速解決這個問題，PECB ISO-IEC-27035-Lead-Incident-Manager題庫下載 總結經常被自己遺漏而導致做錯題的知識點，並做好記錄，NewDumps就是一個可以滿足很多參加PECB ISO-IEC-27035-Lead-Incident-Manager 認證考試的IT人士的需求的網站，NewDumps的專家團隊以他們的豐富的專業知識和經驗幫助你增長知識，並且給你能提供ISO-IEC-27035-Lead-Incident-Manager 認證考試的相關練習題和答案。

謝謝妳，我叫李雪，我本來是為了助大師壹臂之力的，真的是沒有想到是既然將它放跑了，如果你回答“是”，那趕緊來參加考試吧，我們為您提供涵蓋真實測試的題目和答案的試題，快將我們NewDumps的產品收入囊中吧，通過我們專家團隊編寫的PECB ISO-IEC-27035-Lead-Incident-Manager全真題庫練習就是最好的捷徑。

高質量的ISO-IEC-27035-Lead-Incident-Manager題庫下載和準確的PECB認證培訓 - 通過無憂PECB PECB Certified ISO/IEC 27035 Lead Incident Manager

我們的NewDumps在任何時間下ISO-IEC-27035-Lead-Incident-Manager都可以幫您快速解決這個問題，總結經常被自己遺漏而導致做錯題的知識點，並做好記錄。

- ISO-IEC-27035-Lead-Incident-Manager考試備考經驗 ↖ ISO-IEC-27035-Lead-Incident-Manager最新題庫 □ ISO-IEC-27035-Lead-Incident-Manager考試備考經驗 □ 開啟【 www.vcesoft.com 】輸入▸ ISO-IEC-27035-Lead-Incident-Manager ◂並獲取免費下載ISO-IEC-27035-Lead-Incident-Manager PDF題庫
- ISO-IEC-27035-Lead-Incident-Manager認證考試資料匯總 □ 立即到➽ www.newdumpspdf.com □上搜索☀ ISO-IEC-27035-Lead-Incident-Manager □☀□以獲取免費下載ISO-IEC-27035-Lead-Incident-Manager考題
- ISO-IEC-27035-Lead-Incident-Manager考試心得 □ ISO-IEC-27035-Lead-Incident-Manager考試證照 □ ISO-IEC-27035-Lead-Incident-Manager參考資料 □ ▹ www.vcesoft.com ◃最新➡ ISO-IEC-27035-Lead-Incident-Manager □□□問題集合最新ISO-IEC-27035-Lead-Incident-Manager試題
- 選擇我們有效的ISO-IEC-27035-Lead-Incident-Manager題庫下載: PECB Certified ISO/IEC 27035 Lead Incident Manager，PECB ISO-IEC-27035-Lead-Incident-Manager當然很簡單通過 □ 透過□ www.newdumpspdf.com □輕鬆獲取⇛ ISO-IEC-27035-Lead-Incident-Manager ⇚免費下載ISO-IEC-27035-Lead-Incident-Manager考試心得
- ISO-IEC-27035-Lead-Incident-Manager考題 □ 新版ISO-IEC-27035-Lead-Incident-Manager題庫 □ ISO-IEC-27035-Lead-Incident-Manager考試證照 □ 打開網站⇛ tw.fast2test.com ⇚搜索☀ ISO-IEC-27035-Lead-Incident-Manager □☀□免費下載ISO-IEC-27035-Lead-Incident-Manager考試心得
- 正確的ISO-IEC-27035-Lead-Incident-Manager題庫下載擁有模擬真實考試環境與場境的軟件VCE版本＆專業的ISO-IEC-27035-Lead-Incident-Manager：PECB Certified ISO/IEC 27035 Lead Incident Manager □ 請在➽ www.newdumpspdf.com □網站上免費下載➡ ISO-IEC-27035-Lead-Incident-Manager □□□題庫ISO-IEC-27035-Lead-Incident-Manager PDF題庫
- ISO-IEC-27035-Lead-Incident-Manager熱門證照 □ ISO-IEC-27035-Lead-Incident-Manager PDF題庫 □ ISO-IEC-27035-Lead-Incident-Manager考試證照 ☂ 立即在➤ tw.fast2test.com □上搜尋➽ ISO-IEC-27035-Lead-Incident-Manager □並免費下載ISO-IEC-27035-Lead-Incident-Manager PDF題庫
- 正確的ISO-IEC-27035-Lead-Incident-Manager題庫下載擁有模擬真實考試環境與場境的軟件VCE版本＆專業的ISO-IEC-27035-Lead-Incident-Manager：PECB Certified ISO/IEC 27035 Lead Incident Manager □ 立即打開⇛ www.newdumpspdf.com ⇚並搜索【 ISO-IEC-27035-Lead-Incident-Manager 】以獲取免費下載ISO-IEC-27035-Lead-Incident-Manager考試心得
- ISO-IEC-27035-Lead-Incident-Manager證照資訊 □ ISO-IEC-27035-Lead-Incident-Manager權威認證 □ ISO-IEC-27035-Lead-Incident-Manager考試心得 □ ➽ tw.fast2test.com □上的免費下載□ ISO-IEC-27035-Lead-Incident-Manager □頁面立即打開ISO-IEC-27035-Lead-Incident-Manager考試心得
- ISO-IEC-27035-Lead-Incident-Manager參考資料 □ ISO-IEC-27035-Lead-Incident-Manager熱門證照 □ ISO-IEC-27035-Lead-Incident-Manager真題材料 □ ▸ www.newdumpspdf.com ◂網站搜索▹ ISO-IEC-27035-Lead-Incident-Manager ◃並免費下載ISO-IEC-27035-Lead-Incident-Manager權威認證
- ISO-IEC-27035-Lead-Incident-Manager參考資料 □ ISO-IEC-27035-Lead-Incident-Manager最新題庫資源 □ ISO-IEC-27035-Lead-Incident-Manager最新題庫資源 □ ▸ www.newdumpspdf.com ◂網站搜索□ ISO-IEC-27035-Lead-Incident-Manager □並免費下載ISO-IEC-27035-Lead-Incident-Manager軟件版
- shufaii.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.xunshuzhilian.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, study.stcs.edu.np, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

2025 NewDumps最新的ISO-IEC-27035-Lead-Incident-Manager PDF版考試題庫和ISO-IEC-27035-Lead-Incident-Manager考試問題和答案免費分享：https://drive.google.com/open?id=149HQjUkOPqLfcAJwgiWGIb5pnykh2EJV