最新ISO-IEC-27035-Lead-Incident-Manager考證，ISO-IEC-27035-Lead-Incident-Manager考證

從Google Drive中免費下載最新的KaoGuTi ISO-IEC-27035-Lead-Incident-Manager PDF版考試題庫：https://drive.google.com/open?id=1_-MzEsL2jFeZc7A-_z6eCIEZML1q1NaI

ISO-IEC-27035-Lead-Incident-Manager 認證基於 PECB 雄厚的技術實力，和不斷上升的市場佔有率的影響，其認證考試也有條不紊地在全國範圍逐步展開，越來越多的考生要參加 PECB 的ISO-IEC-27035-Lead-Incident-Manager 考試。作為權威的認證，ISO-IEC-27035-Lead-Incident-Manager 認證考試也是十分豐富的。ISO-IEC-27035-Lead-Incident-Manager考試整體來說還是不算複雜的，只要事先將擬真試題看好就沒有問題了。這樣的話，可以為你的考試節省很多的時間。

PECB ISO-IEC-27035-Lead-Incident-Manager 考試大綱：

主題	簡介
主題 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.
主題 2	• 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.
主題 3	• 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.

主題 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.
主題 5	• 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.

優秀的最新ISO-IEC-27035-Lead-Incident-Manager考證和認證考試的領導者材料與有實踐的ISO-IEC-27035-Lead-Incident-Manager考證

關於ISO-IEC-27035-Lead-Incident-Manager認證考試的相關資料，有很多網站都可以提供。但是，他們都不能保證考試資料的品質，同時也不能給你考試失敗就全額退款的保障。比起那些普通的參考資料，KaoGuTi的ISO-IEC-27035-Lead-Incident-Manager考古題完全是一個值得你利用的工具。在KaoGuTi的指導和幫助下，你完全可以充分地準備考試，並且可以輕鬆地通過考試。如果你想在IT行業有更大的發展，那你有必要參加IT認證考試。如果你想順利通過你的IT考試嗎，那麼你完全有必要使用KaoGuTi的考古題。

最新的 ISO 27001 ISO-IEC-27035-Lead-Incident-Manager 免費考試真題 (Q69-Q74):

問題 #69
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. No, the responsibilities of IRT do not include resolving incidents
- B. No, the responsibilities of IRT also include assessing events and declaring incidents
- C. Yes, IRT's responsibilities include identifying root causes, discovering hidden vulnerabilities, and resolving incidents quickly to minimize their impact

答案：B

解題說明：
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.
-

問題 #70
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 Based on scenario 7, which phase of forensic analysis did Paulina fail to conduct correctly?

- A. Analysis
- B. Reporting
- C. Collection

答案：C

解題說明：
Comprehensive and Detailed Explanation From Exact Extract:
As detailed in scenario 7 and reinforced in the previous question, Paulina began her forensic work after the system was restored-missing the critical Collection phase as defined in ISO/IEC 27043 and referenced in ISO/IEC 27035-2.
Forensic collection involves gathering volatile and non-volatile data (e.g., logs, RAM dumps, file artifacts) at the earliest possible moment in the incident lifecycle to avoid data loss. By waiting until after recovery, she likely compromised the chain of custody and the completeness of her evidence.
The scenario notes that her analysis and reporting were thorough, providing valuable insights and mitigation strategies. Thus, the failure lies in the timing and execution of the Collection phase.
Reference:
* ISO/IEC 27035-2:2016, Clause 6.4.2 and 7.2.3: "Collection activities should begin immediately upon identifying a potential incident and before recovery begins."
* ISO/IEC 27043:2015, Clause 8.2.1: "Forensic collection is critical to ensuring reliable analysis and admissible evidence." Correct

answer: A
-
-

問題 #71
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 ignored the trend and continued regular operations when the mean time between the same types of incidents decreased after a few occurrences. Is this acceptable?

- A. No, when the mean time between the same types of incidents decreases, a study should be conducted to discover why
- B. No, when the mean time between the same types of incidents decreases, a study should be necessary to confirm that the incidents are unrelated
- C. When the mean time between the same types of incidents decreases after a few occurrences, it shows that the incidents are becoming less significant

答案：A

解題說明：
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-1 encourages organizations to monitor metrics, such as the frequency of incident types, as part of continual improvement (Clause 7.3). A decreasing mean time between incidents (MTBI) may indicate increased threat frequency, weakened controls, or emerging vulnerabilities. Ignoring such trends can prevent timely corrective actions and weaken overall resilience. Instead of assuming the incidents are less significant, ISO guidance suggests conducting root cause analysis and trend evaluations when patterns like this emerge.
Reference:
ISO/IEC 27035-1:2016, Clause 7.3: "Monitoring and measurement of the incident management process should include trend analysis to identify recurring issues or new patterns." Correct answer: C
-

問題 #72
What roles do business managers play in relation to the Incident Management Team (IMT) and Incident Response Teams (IRTs)?

- A. Guiding on liability and compliance issues to the IMT and IRT and advise on which incidents constitute mandatory data breach notifications
- B. Developing policies and procedures for managing internal employees found engaging in unauthorized or illegal computer activities
- C. Understanding how the IMT and IRTs support business processes and define authority over business systems

答案：C

解題說明：
-
Comprehensive and Detailed Explanation From Exact Extract:
According to ISO/IEC 27035-1:2016 and ISO/IEC 27035-2:2016, business managers have a vital governance and operational oversight role in relation to information security incident response. Their main function is to ensure that incident management activities align with the organization's business processes and risk management strategies.
Clause 7.2.1 of ISO/IEC 27035-2 highlights that business managers are responsible for ensuring that the incident response teams (IRTs) understand business priorities, and that response activities reflect the criticality of affected systems and services. Business managers also help define the operational boundaries and authority of IMTs and IRTs when incidents impact key business systems. Their involvement ensures that decisions made during response efforts support overall organizational resilience and legal compliance.
Option A is more aligned with human resources or legal/compliance functions, not core business manager responsibilities. Option B relates more closely to legal counsel or data privacy officers who are tasked with interpreting laws and regulations concerning breach notifications and liability.
Reference Extracts:
ISO/IEC 27035-2:2016, Clause 7.2.1: "Business managers are responsible for ensuring the coordination between business requirements and incident response activities, and for defining authority over the systems under their management." Clause 6.1.1: "Incident response activities must be aligned with business continuity plans and critical asset protection priorities." Therefore, the correct and most comprehensive answer is: C - Understanding how the IMT and IRTs support business processes and define authority over business systems.
-

問題 #73
How should vulnerabilities lacking corresponding threats be handled?

- A. They may not require controls but should be analyzed and monitored for changes
- B. They should be disregarded as they pose no risk
- C. They still require controls and should be promptly addressed

答案：A

解題說明：
Comprehensive and Detailed Explanation From Exact Extract:
According to ISO/IEC 27005:2018 (which supports ISO/IEC 27035 in risk management and threat assessment processes), vulnerabilities that are not currently associated with known threats do not necessarily need immediate remediation or technical control measures. However, they cannot be ignored entirely either.
Such vulnerabilities may not pose an active risk at the present time, but that can change quickly if a new threat emerges that can exploit them. Therefore, these vulnerabilities should be documented, assessed in context, and monitored over time. This process ensures that if the threat landscape evolves, the organization can respond proactively.
The standard emphasizes a risk-based approach, which includes:
* Analyzing vulnerabilities in relation to assets and threat likelihood
* Monitoring the environment for changes that may introduce new threats
* Avoiding unnecessary or unjustified resource expenditure on low-risk issues Option A is incorrect because it suggests addressing all vulnerabilities without considering risk context.
Option B is risky and contradicts ISO best practices, which emphasize continuous risk monitoring.
Reference Extracts:
* ISO/IEC 27005:2018, Clause 8.2.2: "Vulnerabilities without known threats may not require treatment immediately but should be monitored regularly."
* ISO/IEC 27001:2022, Annex A, Control A.8.8 - "Management of technical vulnerabilities should be risk- based and responsive to changes." Therefore, the correct answer is C: They may not require controls but should be analyzed and monitored for changes.
-

問題 #74
.....

ISO-IEC-27035-Lead-Incident-Manager考證: https://www.kaoguti.com/ISO-IEC-27035-Lead-Incident-Manager_exam-pdf.html

- ISO-IEC-27035-Lead-Incident-Manager考題資訊 □ ISO-IEC-27035-Lead-Incident-Manager考題資訊 □ ISO-IEC-27035-Lead-Incident-Manager考試資訊 □ 到□ www.newdumpspdf.com □搜索【 ISO-IEC-27035-Lead-Incident-Manager 】輕鬆取得免費下載ISO-IEC-27035-Lead-Incident-Manager認證考試解析
- 热门的ISO-IEC-27035-Lead-Incident-Manager認證考試最新考古题产品 - 提供免费ISO-IEC-27035-Lead-Incident-Manager题库demo下載 □ （ www.newdumpspdf.com ）提供免費➠ ISO-IEC-27035-Lead-Incident-Manager □問題收集ISO-IEC-27035-Lead-Incident-Manager在線考題
- 頂尖的PECB 最新ISO-IEC-27035-Lead-Incident-Manager考證＆權威的www.kaoguti.com - 認證考試材料的領導者 □ 在□ www.kaoguti.com □上搜索➡ ISO-IEC-27035-Lead-Incident-Manager □□□並獲取免費下載ISO-IEC-27035-Lead-Incident-Manager考試
- 熱門的最新ISO-IEC-27035-Lead-Incident-Manager考證和有效的PECB認證培訓 - 100％合格率PECB PECB Certified ISO/IEC 27035 Lead Incident Manager □ 免費下載【 ISO-IEC-27035-Lead-Incident-Manager 】只需在▹ www.newdumpspdf.com ◃上搜索ISO-IEC-27035-Lead-Incident-Manager熱門證照
- 热门的ISO-IEC-27035-Lead-Incident-Manager認證考試最新考古题产品 - 提供免费ISO-IEC-27035-Lead-Incident-Manager题库demo下載 □ 在➽ tw.fast2test.com □上搜索➤ ISO-IEC-27035-Lead-Incident-Manager □並獲取免費下載ISO-IEC-27035-Lead-Incident-Manager認證考試
- ISO-IEC-27035-Lead-Incident-Manager資料 □ ISO-IEC-27035-Lead-Incident-Manager在線考題 □ ISO-IEC-27035-Lead-Incident-Manager真題 □ ✔ www.newdumpspdf.com □✔□是獲取➡ ISO-IEC-27035-Lead-Incident-Manager □□□免費下載的最佳網站ISO-IEC-27035-Lead-Incident-Manager考試資訊
- 可靠的最新ISO-IEC-27035-Lead-Incident-Manager考證＆認證考試材料領導者和更新的ISO-IEC-27035-Lead-Incident-Manager考證 □ 進入□ www.newdumpspdf.com □搜尋□ ISO-IEC-27035-Lead-Incident-Manager □免費下載ISO-IEC-27035-Lead-Incident-Manager熱門證照
- ISO-IEC-27035-Lead-Incident-Manager下載 □ ISO-IEC-27035-Lead-Incident-Manager最新試題 □ ISO-IEC-27035-Lead-Incident-Manager題庫下載 □ 免費下載➠ ISO-IEC-27035-Lead-Incident-Manager □只需在☀ www.newdumpspdf.com □☀□上搜索ISO-IEC-27035-Lead-Incident-Manager真題
- 最受歡迎的最新ISO-IEC-27035-Lead-Incident-Manager考證，免費下載ISO-IEC-27035-Lead-Incident-Manager考試資料得到妳想要的PECB證書 □ 來自網站【 www.pdfexamdumps.com 】打開並搜索➠ ISO-IEC-27035-Lead-Incident-Manager □免費下載ISO-IEC-27035-Lead-Incident-Manager考證
- ISO-IEC-27035-Lead-Incident-Manager考試資訊 □ 新版ISO-IEC-27035-Lead-Incident-Manager題庫上線 □ ISO-IEC-27035-Lead-Incident-Manager題庫下載 □ 到⇛ www.newdumpspdf.com ⇚搜尋▹ ISO-IEC-27035-Lead-Incident-Manager ◃以獲取免費下載考試資料新版ISO-IEC-27035-Lead-Incident-Manager題庫上線
- 已驗證的PECB 最新ISO-IEC-27035-Lead-Incident-Manager考證和最佳的www.testpdf.net - 認證考試材料的領導者 □ “www.testpdf.net ”是獲取□ ISO-IEC-27035-Lead-Incident-Manager □免費下載的最佳網站ISO-IEC-27035-Lead-Incident-Manager題庫下載
- webookmarks.com, orlandoshhj531583.topbloghub.com, www.sgz13.cn, learn.designoriel.com, cruxbookmarks.com, aprilnkwb247616.law-wiki.com, nelsonohhq435406.laowaiblog.com, www.stes.tyc.edu.tw, tasneemcgie903227.ourcodeblog.com, onelifesocial.com, Disposable vapes

此外，這些KaoGuTi ISO-IEC-27035-Lead-Incident-Manager考試題庫的部分內容現在是免費的：https://drive.google.com/open?id=1_-MzEsL2jFeZc7A-_z6eCIEZML1q1NaI