ISO-IEC-27035-Lead-Incident-Manager認證題庫 &最新 ISO-IEC-27035-Lead-Incident-Manager試題

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=1JDIJu8IB56qOBXejABQDDhRCTV92qmz6

KaoGuTi 的 ISO-IEC-27035-Lead-Incident-Manager 題庫是隨著 PECB 認證廠商對其做出的變化而變化的，確保了題庫的覆蓋率在96％以上，保證考生能順利通過 PECB ISO-IEC-27035-Lead-Incident-Manager 考試，獲取認證證書。我們的 PECB ISO-IEC-27035-Lead-Incident-Manager 模拟测试题具有最高的专业技术含量，供具有相关专业知识的专家和学者学习和研究之用。你還可以登陸我們題庫網站下載更多想要的認證考試題庫資料。

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

主題	簡介
主題 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.
主題 2	• 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 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.

主題 4	• 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 5	• 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.

最新ISO-IEC-27035-Lead-Incident-Manager試題 - ISO-IEC-27035-Lead-Incident-Manager考試重點

我們KaoGuTi配置提供給你最優質的PECB的ISO-IEC-27035-Lead-Incident-Manager考試考古題及答案，將你一步一步帶向成功，我們KaoGuTi PECB的ISO-IEC-27035-Lead-Incident-Manager考試認證資料絕對提供給你一個真實的考前準備，我們針對性很強，就如同為你量身定做一般，你一定會成為一個有實力的IT專家，我們KaoGuTi PECB的ISO-IEC-27035-Lead-Incident-Manager考試認證資料將是最適合你也是你最需要的培訓資料，趕緊註冊我們KaoGuTi網站，相信你會有意外的收穫。

最新的 ISO 27001 ISO-IEC-27035-Lead-Incident-Manager 免費考試真題 (Q45-Q50):

問題 #45
Scenario 3: L&K Associates is a graphic design firm headquartered in Johannesburg, South Africa. It specializes in providing innovative and creative design solutions to clients across various industries. With offices in multiple parts of the country, they effectively serve clients, delivering design solutions that meet their unique needs and preferences.
In its commitment to maintaining information security, L&K Associates is implementing an information security incident management process guided by ISO/IEC 27035-1 and ISO/IEC 27035-2. Leona, the designated leader overseeing the implementation of the incident management process, customized the scope of incident management to align with the organization's unique requirements. This involved specifying the IT systems, services, and personnel involved in the incident management process while excluding potential incident sources beyond those directly related to IT systems and services.
In scenario 3, which of the following risk identification approaches was used by L&K Associates?

- A. Both A and B
- B. Event-based approach
- C. Asset-based approach

答案：A

解題說明：
Comprehensive and Detailed Explanation From Exact Extract:
L&K Associates employed two distinct approaches as described in ISO/IEC 27005:2018 and referenced in ISO/IEC 27035-2:
Strategic scenario identification, which involves analyzing sources of risk and their impact on stakeholders and objectives. This is aligned with the event-based approach, which focuses on risk sources and events that may lead to incidents.
Operational scenario identification, which involves a thorough assessment of assets, threats, and vulnerabilities - aligning with the asset-based approach, where the focus is on critical assets and the threats that may exploit their weaknesses.
ISO/IEC 27005:2018, Clause 8.2.2, identifies multiple methods for risk identification, including:
Asset-based approach
Event-based (or threat-based) approach
Vulnerability-centered approach
In this scenario, both the asset- and event-based methods were clearly applied by Leona, which is encouraged in ISO risk management practices to provide a holistic view of risk.
Therefore, the correct answer is C: Both A and B.

問題 #46
What is the primary objective of an awareness program?

- A. Enhancing the efficiency of the company's IT infrastructure
- B. Introducing new security technology to the IT department
- C. Reinforcing or modifying behavior and attitudes toward security

答案：C

解題說明：
Comprehensive and Detailed Explanation From Exact Extract:
The core purpose of a security awareness program, as outlined in ISO/IEC 27035 and ISO/IEC 27001, is to influence behavior and attitudes toward security, making staff more conscious of threats and their responsibilities in preventing incidents. An effective awareness program helps reduce human errors, enhances response readiness, and builds a security-conscious culture.
ISO/IEC 27035-2:2016 clearly differentiates awareness from training. While training focuses on skills and procedures, awareness is about shaping the mindset, ensuring that employees understand the importance of security in their daily tasks.
Option A (technology introduction) and option C (IT efficiency) are not primary goals of awareness programs.
Reference Extracts:
ISO/IEC 27035-2:2016, Clause 7.3.1: "The objective of awareness activities is to change behavior and enhance understanding of security threats and how to prevent them." ISO/IEC 27001:2022, Control 6.3 and Annex A: "Personnel should be made aware of the importance of information security and their responsibilities in supporting it." Correct answer: B
-

問題 #47
What can documenting recovery options and associated data loss/recovery timeframes assist with during incident response?

- A. Accelerating the incident response process
- B. Minimizing the impact on system performance
- C. Making informed decisions about containment and recovery

答案：C

解題說明：
Comprehensive and Detailed Explanation From Exact Extract:
Documenting recovery options and estimating recovery time objectives (RTOs) and data loss tolerances (Recovery Point Objectives - RPOs) is a crucial planning activity that supports decision-making during the containment and recovery phases. ISO/IEC 27035-2:2016, Clause 6.4.6 emphasizes that such documentation allows teams to:
Evaluate trade-offs between containment scope and data loss
Determine acceptable downtime for critical services
Select the most appropriate recovery strategy based on business impact
This documentation supports strategic thinking rather than rushed action, reducing the likelihood of costly decisions. It does not necessarily accelerate the process (Option C), nor is it designed to optimize performance (Option A).
Reference:
ISO/IEC 27035-2:2016, Clause 6.4.6: "Recovery planning should consider documented recovery procedures, acceptable data loss, and system downtime to support business continuity." Correct answer: B

問題 #48
What role does the incident coordinator play during the response phase?

- A. Initiating the response actions immediately
- B. Coordinating the activities of IRTs and monitoring response time
- C. Assessing if the event is a potential or confirmed security incident

答案：B

解題說明：
Comprehensive and Detailed Explanation From Exact Extract:
The incident coordinator plays a vital managerial and operational role in guiding and synchronizing the efforts of Incident Response

Teams (IRTs). ISO/IEC 27035-2:2016, Clause 7.2.2 describes the role as one that involves coordination of resources, communication, and oversight to ensure that all phases of the response are executed according to procedure and within acceptable timelines.
Responsibilities include:
Assigning roles and responsibilities
Overseeing containment, eradication, and recovery efforts
Communicating with stakeholders
Tracking incident metrics and resolution progress
Initiating the response (Option B) is typically a decision taken collectively or by senior management or the IMT after classification.
Assessing the nature of an event (Option C) falls under the detection and classification phase, not the coordinator's primary role during response.
Reference:
ISO/IEC 27035-2:2016, Clause 7.2.2: "The incident coordinator is responsible for leading and coordinating the incident response process, ensuring timely and efficient execution." Correct answer: A
-

問題 #49
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 behavioral analytics
- C. Monitor the outsourced services

答案：C

解題說明：
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
-

問題 #50
.....

錯。在您購買PECB ISO-IEC-27035-Lead-Incident-Manager考古題之前，我們所有的題庫都有提供對應免費試用的demo，您覺得適合在購買，這樣您可以更好的了解我們產品的品質。

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

- ISO-IEC-27035-Lead-Incident-Manager認證題庫 - 通過PECB Certified ISO/IEC 27035 Lead Incident Manager立刻馬上 □ 複製網址[tw.fast2test.com]打開並搜索⇛ ISO-IEC-27035-Lead-Incident-Manager ⇚免費下載最新ISO-IEC-27035-Lead-Incident-Manager題庫
- ISO-IEC-27035-Lead-Incident-Manager試題 □ ISO-IEC-27035-Lead-Incident-Manager PDF □ ISO-IEC-27035-Lead-Incident-Manager認證考試 □ 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學習筆記
- ISO-IEC-27035-Lead-Incident-Manager認證題庫將是您最好的助手-關于PECB Certified ISO/IEC 27035 Lead Incident Manager考試 □ 進入➥ www.newdumpspdf.com □搜尋✔ ISO-IEC-27035-Lead-Incident-Manager □✔□ 免費下載ISO-IEC-27035-Lead-Incident-Manager PDF
- ISO-IEC-27035-Lead-Incident-Manager學習筆記 □ ISO-IEC-27035-Lead-Incident-Manager學習筆記 □ ISO-IEC-27035-Lead-Incident-Manager認證 □ 透過✔ www.newdumpspdf.com □✔□搜索➤ ISO-IEC-27035-Lead-Incident-Manager □免費下載考試資料最新ISO-IEC-27035-Lead-Incident-Manager題庫
- 最受歡迎的ISO-IEC-27035-Lead-Incident-Manager認證題庫，PECB ISO 27001認證ISO-IEC-27035-Lead-Incident-Manager考試題庫提供免費下載 □ 開啟➡ tw.fast2test.com □□□輸入▹ ISO-IEC-27035-Lead-Incident-Manager ◃並獲取免費下載ISO-IEC-27035-Lead-Incident-Manager指南
- 最新ISO-IEC-27035-Lead-Incident-Manager題庫 □ ISO-IEC-27035-Lead-Incident-Manager試題 □ 新版ISO-IEC-27035-Lead-Incident-Manager題庫上線 □ 在[www.newdumpspdf.com]網站上免費搜索▹ ISO-IEC-27035-Lead-Incident-Manager ◃題庫ISO-IEC-27035-Lead-Incident-Manager學習筆記
- 高通過率的ISO-IEC-27035-Lead-Incident-Manager認證題庫 - PECB 最新ISO-IEC-27035-Lead-Incident-Manager試題：PECB Certified ISO/IEC 27035 Lead Incident Manager最新發布 □ 免費下載□ ISO-IEC-27035-Lead-Incident-Manager □只需在{ tw.fast2test.com }上搜索ISO-IEC-27035-Lead-Incident-Manager認證
- 最受歡迎的ISO-IEC-27035-Lead-Incident-Manager認證題庫，PECB ISO 27001認證ISO-IEC-27035-Lead-Incident-Manager考試題庫提供免費下載 □ 到☀ www.newdumpspdf.com □☀□搜尋（ ISO-IEC-27035-Lead-Incident-Manager ）以獲取免費下載考試資料ISO-IEC-27035-Lead-Incident-Manager指南
- ISO-IEC-27035-Lead-Incident-Manager認證題庫 |高通過率的考試材料丨ISO-IEC-27035-Lead-Incident-Manager：PECB Certified ISO/IEC 27035 Lead Incident Manager □ ▸ www.kaoguti.com ◂是獲取➽ ISO-IEC-27035-Lead-Incident-Manager □免費下載的最佳網站最新ISO-IEC-27035-Lead-Incident-Manager考古題
- ISO-IEC-27035-Lead-Incident-Manager認證考試 □ ISO-IEC-27035-Lead-Incident-Manager題庫最新資訊 □ ISO-IEC-27035-Lead-Incident-Manager認證 □ 到⇛ www.newdumpspdf.com ⇚搜尋➽ ISO-IEC-27035-Lead-Incident-Manager □以獲取免費下載考試資料ISO-IEC-27035-Lead-Incident-Manager認證
- ISO-IEC-27035-Lead-Incident-Manager學習資料 □ ISO-IEC-27035-Lead-Incident-Manager認證考試 □ ISO-IEC-27035-Lead-Incident-Manager指南 □ 立即打開（ tw.fast2test.com ）並搜索☀ ISO-IEC-27035-Lead-Incident-Manager □☀□以獲取免費下載ISO-IEC-27035-Lead-Incident-Manager學習筆記
- pct.edu.pk, 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, csem.online, motionentrance.edu.np, 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, lineage9527.官網.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, 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, Disposable vapes

P.S. KaoGuTi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=1JDIJu8IB56qOBXejABQDDhRCTV92qmz6