

最近更新的ISO-IEC-27035-Lead-Incident-Manager權威考題 & PECB最新ISO-IEC-27035-Lead-Incident-Manager考題：PECB Certified ISO/IEC 27035 Lead Incident Manager確認通過



P.S. KaoGuTi在Google Drive上分享了免費的2026 PECB ISO-IEC-27035-Lead-Incident-Manager考試題庫：https://drive.google.com/open?id=1P8EHI1DDMvRITvdgZYGmqoFFs_eAoqz

KaoGuTi為每個需要通過PECB的ISO-IEC-27035-Lead-Incident-Manager考試認證的考生提供了一個明確和卓越的解決方案，我們為你提供PECB的ISO-IEC-27035-Lead-Incident-Manager考試詳細的問題及答案，我們團隊的IT專家是最有經驗和資格的，我們的考試測試題及答案幾乎和真實得考試一樣，做到這樣的確很了不起，更重要的是我們KaoGuTi網站在全球範圍內執行這項考試培訓通過率最大。

KaoGuTi的資深專家團隊研究出了針對PECB ISO-IEC-27035-Lead-Incident-Manager考試的培訓教材。通過KaoGuTi提供的教材培訓和學習，通過PECB ISO-IEC-27035-Lead-Incident-Manager 認證考試將會很簡單。KaoGuTi能100%保證你首次參加PECB ISO-IEC-27035-Lead-Incident-Manager 認證考試就可以成功通過。我們給你提供的考試練習題和答案將在你考試的時候會出現。當你選擇了我們的幫助，KaoGuTi承諾給你一份準確而全面的考試資料，而且會給你提供一年的免費更新服務。

>> ISO-IEC-27035-Lead-Incident-Manager權威考題 <<

最新ISO-IEC-27035-Lead-Incident-Manager考題 & ISO-IEC-27035-Lead-Incident-Manager題庫分享

隨著社會的發展，現在PECB行業得到了人們的青睞，也有越來越多的人們想考取PECB方面的資格認證證書，在事業上更進一步。這個時候你應該想到的是KaoGuTi網站，它是你ISO-IEC-27035-Lead-Incident-Manager考試合格的好幫手。KaoGuTi的強大考古題是ISO-IEC-27035-Lead-Incident-Manager技術專家們多年來總結出來的經驗和結果，站在這些前人的肩膀上，會讓你離成功更進一步。

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

主題	簡介
主題 1	<ul style="list-style-type: none"> • 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 2	<ul style="list-style-type: none"> • 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 3	<ul style="list-style-type: none"> • 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.

最新的 ISO 27001 ISO-IEC-27035-Lead-Incident-Manager 免費考試真題 (Q12-Q17):

問題 #12

Scenario 6: EastCyber has established itself as a premier cyber security company that offers threat detection, vulnerability assessment, and penetration testing tailored to protect organizations from emerging cyber threats. The company effectively utilizes ISO/IEC 27035*1 and 27035-2 standards, enhancing its capability to manage information security incidents.

EastCyber appointed an information security management team led by Mike. Despite limited resources, Mike and the team implemented advanced monitoring protocols to ensure that every device within the company's purview is under constant surveillance. This monitoring approach is crucial for covering everything thoroughly, enabling the information security and cyber management team to proactively detect and respond to any sign of unauthorized access, modifications, or malicious activity within its systems and networks.

In addition, they focused on establishing an advanced network traffic monitoring system. This system carefully monitors network activity, quickly spotting and alerting the security team to unauthorized actions. This vigilance is pivotal in maintaining the integrity of EastCyber's digital infrastructure and ensuring the confidentiality, availability, and integrity of the data it protects.

Furthermore, the team focused on documentation management. They meticulously crafted a procedure to ensure thorough documentation of information security events. Based on this procedure, the company would document only the events that escalate into high-severity incidents and the subsequent actions. This documentation strategy streamlines the incident management process, enabling the team to allocate resources more effectively and focus on incidents that pose the greatest threat.

A recent incident involving unauthorized access to company phones highlighted the critical nature of incident management. Nate, the incident coordinator, quickly prepared an exhaustive incident report. His report detailed an analysis of the situation, identifying the problem and its cause. However, it became evident that assessing the seriousness and the urgency of a response was inadvertently overlooked.

In response to the incident, EastCyber addressed the exploited vulnerabilities. This action started the eradication phase, aimed at systematically eliminating the elements of the incident. This approach addresses the immediate concerns and strengthens EastCyber's defenses against similar threats in the future.

Scenario 6: EastCyber has established itself as a premier cybersecurity company that offers threat detection, vulnerability assessment, and penetration testing tailored to protect organizations from emerging cyber threats. The company effectively utilizes ISO/IEC 27035-1 and 27035-2 standards, enhancing its capability to manage information security incidents.

EastCyber appointed an information security management team led by Mike. Despite limited resources, Mike and the team implemented advanced monitoring protocols to ensure that every device within the company's purview is under constant surveillance. This monitoring approach is crucial for covering everything thoroughly, enabling the information security and cyber management team to proactively detect and respond to any sign of unauthorized access, modifications, or malicious activity within its systems and networks.

Based on the scenario above, answer the following question:

While implementing monitoring protocols, Mike ensured that every device within the company's purview was under constant surveillance. Is this a recommended practice?

- A. No, Mike should have focused on the essential components to reduce the clutter and noise in the data collected
- B. Yes. Mike defined the objective of network monitoring correctly

- C. No, Mike should have focused on new devices, as they are more likely to have undetected vulnerabilities

答案: B

解題說明:

Comprehensive and Detailed Explanation From Exact Extract:

According to ISO/IEC 27035-2:2016, Clause 7.3.2, implementing continuous monitoring across all critical assets and endpoints is a key component of proactive incident detection. Organizations are encouraged to establish real-time detection mechanisms that allow prompt identification of unauthorized or abnormal behavior.

Mike's approach-ensuring all systems are under constant surveillance-is consistent with this recommendation. Comprehensive monitoring allows the early identification of security events that may otherwise go unnoticed, especially in environments where advanced persistent threats (APTs) or insider threats are concerns.

While focusing only on new devices or limiting monitoring to certain components may reduce noise, it creates gaps in coverage and increases the risk of missed threats.

Reference:

ISO/IEC 27035-2:2016, Clause 7.3.2: "Monitoring systems and activities should be established and maintained to detect deviations that may indicate a security incident." ISO/IEC 27001:2022, Control A.5.28: "Monitoring systems should cover all devices that process or store sensitive information." Correct answer: A

-

問題 #13

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

答案: B

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 #14

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.

Based on the scenario above, answer the following question:

Considering its industry and services, is the guidance provided in ISO/IEC 27035-1 applicable for RoLawyers?

- **A. Yes, it applies to all organizations, regardless of their size, type, or nature**
- B. No, it is specific to organizations providing incident management services
- C. No, it is specific to organizations in the information security industry

答案： A

解題說明：

Comprehensive and Detailed Explanation From Exact Extract:

ISO/IEC 27035-1:2016 is titled "Information security incident management - Part 1: Principles of incident management". This standard provides a comprehensive framework for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving incident management within an organization.

The scope of ISO/IEC 27035-1 is explicitly broad and designed to be applicable to all organizations, regardless of their size, type, or nature, as stated in the standard's introduction and scope sections. The principles laid out in the document are intended to be flexible and scalable so that organizations from any sector can adopt and implement incident management processes suitable to their specific context.

The document clearly emphasizes that information security incidents can impact any organization that processes, stores, or transmits information digitally - including law firms like RoLawyers. The guidance addresses the creation of an incident response capability to detect, respond, and recover from information security incidents effectively.

Furthermore, the standard stresses that incident management is a vital part of maintaining information security resilience, minimizing damage, and protecting the confidentiality, integrity, and availability of information assets, which is crucial for organizations handling sensitive data, such as legal firms.

Hence, ISO/IEC 27035-1 is not limited to IT or information security service providers alone; instead, it supports any organization's need to manage information security incidents systematically. RoLawyers, given its reliance on digital data and the critical nature of its information, can and should apply the standard's principles to safeguard its assets and clients.

Reference Extracts from ISO/IEC 27035-1:2016:

* Scope (Section 1): "The principles provided in this document are intended to be applicable to all organizations, irrespective of type, size or nature."

* Introduction (Section 0.1): "Effective incident management helps organizations to reduce the consequences of incidents and limit the damage caused to information and information systems."

* General (Section 4): "This document provides guidance for establishing, implementing, operating, monitoring, reviewing, maintaining and improving incident management processes within an organization." Thus, based on ISO/IEC 27035-1, the guidance is fully applicable to RoLawyers, aligning with their objective to improve information security and incident management practices.

問題 #15

What is the purpose of monitoring behavioral analytics in security monitoring?

- A. To evaluate the effectiveness of security training programs
- **B. To establish a standard for normal user behavior and detect unusual activities**
- C. To prioritize the treatment of security incidents

答案： B

解題說明：

Comprehensive and Detailed Explanation From Exact Extract:

Behavioral analytics refers to using baselines of user or system behavior to identify anomalies that may indicate potential threats. According to ISO/IEC 27035-2, behavioral monitoring is an essential proactive technique for detecting insider threats, account compromise, and lateral movement by attackers.

Once a baseline for "normal behavior" is established (e.g., login patterns, file access, network usage), deviations can trigger alerts or investigations. This allows earlier detection of suspicious activities before they escalate into full-blown incidents.

Option A is a separate initiative related to awareness programs. Option B is more aligned with the response phase, not monitoring.

Reference:

ISO/IEC 27035-2:2016, Clause 7.3.2: "Security monitoring should include behavioral analysis to detect anomalies from baseline user and system activity." Correct answer: C

-

問題 #16

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 technique did L&K Associates use for its risk analysis process?

- A. Qualitative risk analysis
- B. Quantitative risk analysis
- C. Semi-quantitative risk analysis

答案： B

解題說明：

Comprehensive and Detailed Explanation From Exact Extract:

In the scenario, Leona used a methodology that estimates "practical values for consequences and their probabilities," which clearly points to a quantitative risk analysis approach.

Quantitative risk analysis, as defined in ISO/IEC 27005:2018, involves assigning numerical values (e.g., monetary impact, frequency rates) to both the probability and consequence of risks. This allows for risk prioritization based on actual or estimated figures, enabling data-driven decisions on mitigation strategies.

Qualitative analysis uses descriptive categories (e.g., high/medium/low), and semi-quantitative methods mix ranking scales with partial numeric estimations - neither of which are described in this scenario.

Reference:

ISO/IEC 27005:2018, Clause 8.3.3: "Quantitative risk analysis estimates the probability and impact of risk using numerical values to derive a risk level." Therefore, the correct answer is C: Quantitative risk analysis.

-

問題 #17

.....

如果你仍然在努力獲得PECB的ISO-IEC-27035-Lead-Incident-Manager考試認證，我們KaoGuTi為你實現你的夢想，KaoGuTi PECB的ISO-IEC-27035-Lead-Incident-Manager考試培訓資料是品質最好的培訓資料，為你提供了一個好的學習平臺，問題是你如何準備這個考試，以確保你百分百成功，答案是非常簡單的，如果你有適當的時間學習，那就選擇我們KaoGuTi PECB的ISO-IEC-27035-Lead-Incident-Manager考試培訓資料，有了它，你將快樂輕鬆的準備考試。

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

- 最優良的ISO-IEC-27035-Lead-Incident-Manager權威考題 | 第一次嘗試輕鬆學習並通過考試和可信任的PECB

