ISO-IEC-27035-Lead-Incident-Manager權威認證 - ISO-IEC-27035-Lead-Incident-Manager學習資料

P.S. PDFExamDumps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=1nai3xcJOptIQuBBb5Fsp47l3Dwtgg9Zc

成千上萬的IT考生通過使用我們的產品成功通過考試，PECB ISO-IEC-27035-Lead-Incident-Manager考古題質量被廣大考試測試其是高品質的。我們從來不相信第二次機會，因此給您帶來的最好的PECB ISO-IEC-27035-Lead-Incident-Manager考古題幫助您首次就通過考試，并取得不錯的成績。PDFExamDumps網站幫助考生通過ISO-IEC-27035-Lead-Incident-Manager考試獲得認證，不僅可以節約很多時間，還能得到輕松通過ISO-IEC-27035-Lead-Incident-Manager考試的保證，這是IT認證考試中最重要的考試之一。

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

主題	簡介
主題 1	• 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 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.
主題 3	• 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 4	• 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 5	• 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.

ISO-IEC-27035-Lead-Incident-Manager學習資料 & ISO-IEC-27035-Lead-Incident-Manager證照信息

對於 PECB的ISO-IEC-27035-Lead-Incident-Manager考試認證每個考生都很迷茫。每個人都有自己不用的想法，不過總結的都是考試困難之類的，PECB的ISO-IEC-27035-Lead-Incident-Manager考試是比較難的一次考試認證，我相信大家都是耳目有染的，不過只要大家相信PDFExamDumps，這一切將不是問題，PDFExamDumps PECB的ISO-IEC-27035-Lead-Incident-Manager考試培訓資料是每個考生的必備品，它是我們PDFExamDumps為考生們量身訂做的，有了它絕對100%通過考試認證，如果你不相信，你進我們網站看一看你就知道，看了嚇一跳，每天購買率是最高的，你也別錯過，趕緊加入購物車吧。

最新的 ISO 27001 ISO-IEC-27035-Lead-Incident-Manager 免費考試真題 (Q35-Q40):

問題 #35
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 scenario 1, which information security principle was breached?

- A. Availability
- B. Confidentiality
- C. Integrity

答案：A

解題說明：
Comprehensive and Detailed Explanation From Exact Extract:
The three fundamental principles of information security are commonly known as the CIA Triad:

Confidentiality, Integrity, and Availability. ISO/IEC 27035 defines an information security incident as a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
In the provided scenario, RoLawyers experienced a cyber-attack in which their online database was overwhelmed by malicious traffic (likely a Denial-of-Service or DoS-type attack), which caused the system to crash and became inaccessible to employees for several hours. As a result, the employees were unable to access critical legal data and client information necessary for daily operations.
According to ISO/IEC 27035-1:2016, "Availability refers to the property of being accessible and usable upon demand by an authorized entity." (Ref: ISO/IEC 27000:2018, Clause 3.7.3). The scenario clearly reflects a breach in availability since authorized users (employees) were unable to access systems or data when needed.
There was no mention of unauthorized disclosure (which would affect confidentiality) or data alteration (which would affect integrity). Therefore, the primary principle that was violated in this incident is Availability.
This type of incident aligns with the definition and consequences outlined in the ISO/IEC 27035-1:2016 and ISO/IEC 27001:2022 standards, which identify availability loss as one of the main risks to be managed through an incident management process.
Reference Extracts from ISO/IEC Standards:
* ISO/IEC 27000:2018, Clause 3.7.3 - "Availability: property of being accessible and usable upon demand by an authorized entity."
* ISO/IEC 27035-1:2016, Clause 4.1 - "An information security incident can be any event that compromises the confidentiality, integrity or availability of information."
* ISO/IEC 27035-1:2016, Clause 5.1 - "Maintaining availability is critical to service continuity and information assurance."
Therefore, the correct answer is A: Availability.

問題 #36
Scenario 5: Located in Istanbul, Turkey, Alura Hospital is a leading medical institution specializing in advanced eye surgery and vision care. Renowned for its modern facilities, cutting-edge technology, and highly skilled staff, Alura Hospital is committed to delivering exceptional patient care. Additionally, Alura Hospital has implemented the ISO/IEC 27035 standards to enhance its information security incident management practices.
At Alura Hospital, the information security incident management plan is a critical component of safeguarding patient data and maintaining the integrity of its medical services. This comprehensive plan includes instructions for handling vulnerabilities discovered during incident management. According to this plan, when new vulnerabilities are discovered, Mehmet is appointed as the incident handler and is authorized to patch the vulnerabilities without assessing their potential impact on the current incident, prioritizing patient data security above all else.
Recognizing the importance of a structured approach to incident management, Alura Hospital has established four teams dedicated to various aspects of incident response. The planning team focuses on implementing security processes and communicating with external organizations. The monitoring team is responsible for security patches, upgrades, and security policy implementation. The analysis team adjusts risk priorities and manages vulnerability reports, while the test and evaluation team organizes and performs incident response tests to ensure preparedness.
During an incident management training session, staff members at Alura Hospital were provided with clear roles and responsibilities. However, a technician expressed uncertainty about their role during a data integrity incident, as the manager assigned them a role unrelated to their expertise. This decision was made to ensure that all staff members possess versatile skills and are prepared to handle various scenarios effectively.
Additionally, Alura Hospital realized it needed to communicate better with stakeholders during security incidents. The hospital discovered it was not adequately informing stakeholders and that relevant information must be provided using formats, language, and media that meet their needs. This would enable them to participate fully in the incident response process and stay informed about potential risks and mitigation strategies.
Also, the hospital has experienced frequent network performance issues affecting critical hospital systems and increased sophisticated cyberattacks designed to bypass traditional security measures. So, it has deployed an external firewall. This action is intended to strengthen the hospital's network security by helping detect threats that have already breached the perimeter defenses. The firewall's implementation is a part of the hospital's broader strategy to maintain a robust and secure IT infrastructure, which is crucial for protecting sensitive patient data and ensuring the reliability of critical hospital systems. Alura Hospital remains committed to integrating state-of-the-art technology solutions to uphold the highest patient care and data security standards.
According to scenario 5, which of the following principles of efficient communication did Alura Hospital NOT adhere to?

- A. Credibility
- B. Appropriateness
- C. Responsiveness

答案：B

解題說明：
Comprehensive and Detailed Explanation From Exact Extract:

According to ISO/IEC 27035-1:2016 (Information Security Incident Management - Part 1: Principles of Incident Management), one of the core principles of effective communication in incident management is
"appropriateness." This refers to ensuring that the right information is shared with the right stakeholders using the appropriate channels, language, format, and timing. The objective is to guarantee that communication is both understandable and actionable by its recipients.
In the scenario, Alura Hospital recognized that they were not adequately informing stakeholders during security incidents. They identified a gap in providing relevant information using suitable formats, media, or language. This failure points directly to a lack of "appropriateness" in their communication strategy.
According to ISO/IEC 27035-1, Section 6.4 (Communication), it is essential to tailor incident communication to stakeholder needs to ensure informed decision-making and engagement.
The other options-credibility and responsiveness-are not indicated as the failing areas. There is no mention that the information provided lacked credibility or that the hospital failed to respond to incidents or communicate in a timely manner. Rather, the issue lies with the medium, clarity, and stakeholder alignment- hallmarks of appropriateness.
Reference Extracts from ISO/IEC 27035-1:2016:
Clause 6.4: "Communication must be timely, relevant, accurate, and appropriate for the target audience." Clause 7.2.4: "Stakeholders should be informed using formats and channels that they can easily access and understand." Therefore, the principle not adhered to by Alura Hospital is clearly: Appropriateness (C).
-

問題 #37
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 conducts continuous review of the incident management process to ensure the effectiveness of processes and procedures in place. Is this a good practice to follow?

- A. No, organizations should regularly assess the physical security measures to ensure they align with incident management protocols
- B. No, organizations should conduct quarterly performance reviews of individual employees to ensure they follow incident management protocols
- C. Yes, organizations should conduct continuous review of the incident management process to ensure the effectiveness of the processes and procedures in place

答案：C

解題說明：
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-1:2016 stresses the importance of continual review and improvement of the incident management process. Clause 7.1 specifically advises that organizations regularly evaluate their policies, procedures, and tools to ensure they remain effective in the face of evolving threats and business changes.
Moneda Vivo's continuous review aligns perfectly with this guidance, reinforcing preparedness and adaptability. Options A and C, while related to broader security or HR practices, are not directly aligned with ISO/IEC 27035's core recommendation regarding process review.

Reference:
ISO/IEC 27035-1:2016, Clause 7.1: "The organization should review the effectiveness of the information security incident management process regularly and in response to incidents and significant changes."

問題 #38
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. No, it is specific to organizations providing incident management services
- B. No, it is specific to organizations in the information security industry
- C. Yes, it applies to all organizations, regardless of their size, type, or nature

答案：C

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 #39
Which document provides guidelines for planning and preparing for incident response and for learning lessons from the incident response process?

- A. ISO/IEC 27035-1
- B. ISO/IEC 27035-2
- C. ISO/IEC 27037

答案：B

解題說明：
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-2:2016 is titled "Information security incident management - Part 2: Guidelines to plan and prepare for incident response." This document provides detailed guidance on establishing an incident response capability, planning for incident response, and implementing effective response actions. It also emphasizes the importance of post-incident analysis and lessons learned to improve future incident handling.
Key activities covered in ISO/IEC 27035-2 include:
* Planning and preparing for incident handling (e.g., policy development, roles and responsibilities)
* Establishing and training the incident response team (IRT)
* Developing communication strategies and escalation procedures
* Conducting root cause analysis and collecting lessons learned
* Applying improvements to prevent recurrence
By contrast:
* ISO/IEC 27035-1 provides high-level principles of incident management (Part 1: Principles).
* ISO/IEC 27037 relates to the handling of digital evidence and is focused more on forensic practices than incident response preparation.
Reference Extracts:
* ISO/IEC 27035-2:2016, Introduction: "This part provides guidance on the planning and preparation necessary for effective incident response and for learning lessons from incidents."
* ISO/IEC 27035-2:2016, Clause 6.5: "Lessons learned and reporting can help improve future incident response and provide input to risk assessments and control improvements."

問題 #40
.....

Incident-Manager測試

- 值得信賴的ISO-IEC-27035-Lead-Incident-Manager權威認證 |高通過率的考試材料|授權的ISO-IEC-27035-Lead-Incident-Manager學習資料 □ 到□ tw.fast2test.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認證考試
- ISO-IEC-27035-Lead-Incident-Manager考古題：最新的PECB ISO-IEC-27035-Lead-Incident-Manager認證考試題庫 □ 在☀ www.newdumpspdf.com □☀□搜索最新的【 ISO-IEC-27035-Lead-Incident-Manager 】題庫ISO-IEC-27035-Lead-Incident-Manager權威認證
- ISO-IEC-27035-Lead-Incident-Manager真題 □ ISO-IEC-27035-Lead-Incident-Manager題庫下載 □ ISO-IEC-27035-Lead-Incident-Manager信息資訊 □ 透過➽ tw.fast2test.com □輕鬆獲取➠ ISO-IEC-27035-Lead-Incident-Manager □免費下載ISO-IEC-27035-Lead-Incident-Manager考題
- 綜合全面ISO-IEC-27035-Lead-Incident-Manager權威認證，最好的考試題庫幫助妳壹次性通過ISO-IEC-27035-Lead-Incident-Manager考試 □ 在➥ www.newdumpspdf.com □網站下載免費➤ ISO-IEC-27035-Lead-Incident-Manager □題庫收集ISO-IEC-27035-Lead-Incident-Manager考題
- ISO-IEC-27035-Lead-Incident-Manager考題免費下載 □ ISO-IEC-27035-Lead-Incident-Manager熱門證照 □ ISO-IEC-27035-Lead-Incident-Manager權威認證 □ 透過（ tw.fast2test.com ）輕鬆獲取（ ISO-IEC-27035-Lead-Incident-Manager ）免費下載新版ISO-IEC-27035-Lead-Incident-Manager題庫
- www.stes.tyc.edu.tw, www.notebook.ai, backloggd.com, www.fuxinwang.com, launchpadlms.com, divisionmidway.org, tooter.in, p.me-page.com, learn.csisafety.com.au, forum.phuongnamedu.vn, Disposable vapes

BONUS!!! 免費下載PDFExamDumps ISO-IEC-27035-Lead-Incident-Manager考試題庫的完整版：https://drive.google.com/open?id=1nai3xcJOptIQuBBb5Fsp47l3Dwtgg9Zc