ISO-IEC-27035-Lead-Incident-Manager考試證照 & ISO-IEC-27035-Lead-Incident-Manager新版題庫上線


PECB

BEYOND RECOGNITION

Professional Evaluation and Certification Board

hereby attests that

Ernestas Lipnickas

is awarded the title

PECB Certified ISO/IEC 27035 Lead Incident Manager

having met all the certification requirements, including all examination requirements, professional experience and adoption of the PECB Code of Ethics

Certificate Number: ISIMLM1030239-2022-10
Issue Date: 2022-10-24
This certificate is valid for three years for the purpose of PECB certification

Carolina Cabezas
Chief Compliance Officer

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=1U1mNnJqg-6JoYO03kLgMd_W-U7kIRU3m

PECB的ISO-IEC-27035-Lead-Incident-Manager考試認證是業界廣泛認可的IT認證，世界各地的人都喜歡PECB的ISO-IEC-27035-Lead-Incident-Manager考試認證，這項認證可以強化自己的職業生涯，使自己更靠近成功。談到PECB的ISO-IEC-27035-Lead-Incident-Manager考試,PDFExamDumps PECB的ISO-IEC-27035-Lead-Incident-Manager的考試培訓資料一直領先於其他的網站，因為PDFExamDumps有一支強大的IT精英團隊，他們時刻跟蹤著最新的 PECB的ISO-IEC-27035-Lead-Incident-Manager的考試培訓資料，用他們專業的頭腦來專注於 PECB的ISO-IEC-27035-Lead-Incident-Manager的考試培訓資料。

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	• 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	• 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.

>> ISO-IEC-27035-Lead-Incident-Manager考試證照 <<

PECB ISO-IEC-27035-Lead-Incident-Manager考試證照和PDFExamDumps - 保證認證成功，簡便的培訓方式

如果你擁有了PDFExamDumps PECB的ISO-IEC-27035-Lead-Incident-Manager考試培訓資料，我們將免費為你提供一年的更新，這意味著你總是得到最新的考試認證資料，只要考試目標有所變化，以及我們的學習材料有所變化，我們將在第一時間為你更新。我們知道你的需求，我們將幫助得到 PECB的ISO-IEC-27035-Lead-Incident-Manager考試認證的信心，讓你可以安然無憂的去參加考試，並順利通過獲得認證。

最新的 ISO 27001 ISO-IEC-27035-Lead-Incident-Manager 免費考試真題 (Q23-Q28):

問題 #23
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.
Based on scenario 6, EastCyber's team established a procedure for documenting only the information security events that escalate into high-severity incidents. According to ISO/IEC 27035-1, is this approach acceptable?

- A. The standard suggests that organizations document only events that classify as high-severity incidents
- B. No, because documentation should only occur post-incident to avoid any interference with the response process
- C. No, they should use established guidelines to document events and subsequent actions when the event is classified as an information security incident

答案：C

解題說明：
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-1:2016 clearly states that documentation is essential for all information security incidents, regardless of severity. While prioritization is necessary, the standard recommends that events meeting the threshold of an information security incident (based on classification and assessment) must be recorded, along with the corresponding actions taken.
The practice described-documenting only high-severity incidents-may result in overlooking patterns in lower-priority events that could lead to significant issues if repeated or correlated.
Clause 6.4.5 of ISO/IEC 27035-1:2016 emphasizes that documentation should be thorough and begin from the detection phase through to response and lessons learned.
Option A is incorrect, as the standard does not permit selective documentation only for severe incidents.
Option C misrepresents the intent of documentation, which must be concurrent with or shortly after incident handling-not only post-event.
Reference:
ISO/IEC 27035-1:2016, Clause 6.4.5: "All incident information, decisions, and activities should be documented in a structured way to enable future review, learning, and audit." Clause 6.2.3: "When an event is assessed as an incident, it must be recorded along with all subsequent actions." Correct answer: B
-

問題 #24
Which team has a broader cybersecurity role, including incident response, monitoring, and overseeing general operations?

- A. Computer Security Incident Response Team (CSIRT)
- B. Security Operations Center (SOC)
- C. Computer Emergency Response Team (CERT)

答案：B

解題說明：
Comprehensive and Detailed Explanation From Exact Extract:
According to ISO/IEC 27035 and industry best practices, a Security Operations Center (SOC) is the central hub for an organization's cybersecurity operations. Its responsibilities go beyond pure incident response.
SOCs continuously monitor the organization's network and systems for suspicious activity and threats, providing real-time threat detection, incident response coordination, vulnerability management, and overall security infrastructure oversight.
While CSIRTs and CERTs specialize in handling and managing security incidents, their roles are generally more narrowly focused on the detection, reporting, and resolution of security events. SOCs, on the other hand, manage the broader spectrum of operations, including:
Real-time monitoring and logging
Threat hunting and intelligence
Security incident analysis and triage
Coordinating CSIRT activities
Supporting policy compliance and auditing
Integration with vulnerability management and security infrastructure
Reference Extracts:
ISO/IEC 27035-2:2016, Clause 7.3.1: "Monitoring systems and activities should be established, operated and maintained to identify deviations from normal behavior." NIST SP 800-61 Revision 2 and industry alignment with ISO/IEC 27035 recognize the SOC as the broader operational environment that houses or interacts with the CSIRT/CERT.
Therefore, the correct answer is: B - Security Operations Center (SOC)
-

問題 #25
Which of the following statements regarding the principles for digital evidence gathering is correct?

- A. Relevance means that the DEFR should be able to describe the procedures followed and justify the decision to acquire each item based on its value to the investigation
- B. Reliability implies that all processes used in handling digital evidence should be unique and not necessarily reproducible
- C. Sufficiency means that only a minimal amount of material should be gathered to avoid unnecessary auditing and justification efforts

答案：A

解題說明：
Comprehensive and Detailed Explanation From Exact Extract:
Digital evidence gathering, as outlined in ISO/IEC 27037 and referenced in ISO/IEC 27035-2, must adhere to several core principles-reliability, sufficiency, relevance, and integrity. Relevance, in particular, means that the Digital Evidence First Responder (DEFR) must ensure that any item collected has direct or potential bearing on the investigation.
Relevance also requires:
Clear justification for why an item was acquired
Ability to trace the decision-making process
Alignment with investigation objectives
Option A misrepresents "sufficiency," which does not mean minimal collection but rather collecting enough evidence to support conclusions without overburdening the investigation. Option B contradicts the principle of reliability, which requires that processes be standardized and reproducible.
Reference:
ISO/IEC 27037:2012, Clause 6.2.2.4: "Relevance is determined by the value of the digital evidence in addressing the objectives of the investigation." ISO/IEC 27035-2:2016 references this standard in Clause 7.4.4 regarding forensic evidence handling.
Correct answer: C
-

問題 #26
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.
According to scenario 1, RoLawyers incorporated a structured incident management process to provide guidance on establishing and maintaining a competent incident response team. Is this acceptable?

- A. No, because the implementation of a structured approach helps the RoLawyers to ensure consistency in incident handling across the organization, rather than focusing only on guidance for establishing and maintaining a competent incident response team
- B. No, because the structured incident management process should primarily focus on preventive measures rather than response capabilities
- C. Because the implementation of a structured incident management process helps the company effectively address the need for skilled incident response

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 provide comprehensive guidance on managing information security incidents through a structured incident management process. These documents emphasize the importance of establishing, maintaining, and continually improving an incident response capability, which includes forming a competent incident response team.
The structured incident management process is designed to ensure that organizations can respond effectively and efficiently to incidents, minimizing damage and impact. Specifically, ISO/IEC 27035-2 addresses the practical aspects of incident response, including the formation of an incident response team, their roles, responsibilities, and the need for appropriate skills and training.
The standard explicitly states that a competent incident response team is critical to the incident management lifecycle, which involves preparation, detection and reporting, assessment and decision, responses, and lessons learned. The establishment and maintenance of such a team ensure that the organization is capable of managing incidents with professionalism and consistency.
Furthermore, the structured process helps organizations not only to react to incidents but also to improve resilience through continual learning and process refinement. Preventive measures are part of a broader information security management system (ISMS), but incident management focuses primarily on effective response and recovery, supported by trained personnel.
In the scenario, RoLawyers' approach aligns fully with the ISO/IEC 27035 guidelines. By implementing a structured incident management process and forming a competent incident response team, the firm enhances its ability to deal with threats proactively and respond to incidents efficiently.
Reference Extracts from ISO/IEC 27035-1:2016 and ISO/IEC 27035-2:2016:
* ISO/IEC 27035-1, Section 4.2 (Incident Management Process): "An effective incident management process requires the establishment and maintenance of an incident response capability including a competent incident response team."
* ISO/IEC 27035-2, Section 5.2 (Incident Response Team): "The incident response team should have clearly defined roles and responsibilities and possess the necessary skills and training to manage information security incidents."
* ISO/IEC 27035-2, Introduction: "Incident management activities primarily focus on preparing, detecting, responding, and learning from incidents, rather than solely on prevention." Thus, the correct interpretation confirms that option A is the appropriate answer: implementing a structured incident management process with a competent incident response team is acceptable and strongly recommended.

問題 #27
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.
According to scenario 1, what information security incident did RoLawyers face?

- A. Malware attack
- B. Denial-of-service attack
- C. Man-in-the-middle attack

答案：B

解題說明：
Comprehensive and Detailed Explanation From Exact Extract:
According to ISO/IEC 27035-1:2016, an information security incident is any event that compromises the confidentiality, integrity, or availability of information. In this scenario, RoLawyers experienced an attack where their online database was overloaded with excessive traffic, resulting in a system crash. This incident made it impossible for employees to access the database for several hours. This type of event is characteristic of a Denial-of-Service (DoS) attack. ISO/IEC 27035-1 Annex B provides examples of typical incidents, and one example includes "network-based attacks, including denial-of-service attacks." A DoS attack typically aims to make a service or resource unavailable to its intended users by overwhelming it with traffic.
There is no indication in the scenario that the attackers were intercepting communications (as would be seen in a Man-in-the-Middle attack) or installing malware to damage or steal data. The nature of the attack- excess traffic causing a crash-clearly aligns with the definition of a DoS attack.
Reference Extracts:
ISO/IEC 27035-1:2016, Clause B.2.1 (Examples of incident types): "Denial-of-service (DoS) attacks cause disruption or degradation of services." ISO/IEC 27035-1:2016, Clause 4.1: "An incident can result from deliberate attacks such as DoS, malicious code, or unauthorized access." Therefore, the incident faced by RoLawyers was a Denial-of-Service attack.
-

問題 #28
.....

www.newdumpspdf.com]上搜索ISO-IEC-27035-Lead-Incident-Manager更新

- ISO-IEC-27035-Lead-Incident-Manager下載 □ ISO-IEC-27035-Lead-Incident-Manager認證資料 □ ISO-IEC-27035-Lead-Incident-Manager考試重點 □ 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考題套裝
- 最新版的ISO-IEC-27035-Lead-Incident-Manager考試證照，免費下載ISO-IEC-27035-Lead-Incident-Manager考試題庫幫助妳通過ISO-IEC-27035-Lead-Incident-Manager考試 □ 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下載
- PECB ISO-IEC-27035-Lead-Incident-Manager考試證照：PECB Certified ISO/IEC 27035 Lead Incident Manager考試|PECB ISO-IEC-27035-Lead-Incident-Manager最佳捷徑 □ 打開網站[www.newdumpspdf.com]搜索➤ ISO-IEC-27035-Lead-Incident-Manager □免費下載ISO-IEC-27035-Lead-Incident-Manager下載
- 最新的ISO-IEC-27035-Lead-Incident-Manager認證考試考古題 □ 在□ www.newdumpspdf.com □上搜索⇛ ISO-IEC-27035-Lead-Incident-Manager ⇚並獲取免費下載ISO-IEC-27035-Lead-Incident-Manager考古題推薦
- 最新版的ISO-IEC-27035-Lead-Incident-Manager考試證照，免費下載ISO-IEC-27035-Lead-Incident-Manager考試題庫幫助妳通過ISO-IEC-27035-Lead-Incident-Manager考試 □ 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考題
- 最好的ISO-IEC-27035-Lead-Incident-Manager考試證照，由PECB權威專家撰寫 □“ www.newdumpspdf.com ”上的➥ ISO-IEC-27035-Lead-Incident-Manager □免費下載只需搜尋ISO-IEC-27035-Lead-Incident-Manager更新
- PECB ISO-IEC-27035-Lead-Incident-Manager考試證照：PECB Certified ISO/IEC 27035 Lead Incident Manager考試|PECB ISO-IEC-27035-Lead-Incident-Manager最佳捷徑 □ □ www.pdfexamdumps.com □最新【 ISO-IEC-27035-Lead-Incident-Manager 】問題集合ISO-IEC-27035-Lead-Incident-Manager考古題推薦
- ISO-IEC-27035-Lead-Incident-Manager測試題庫 □ ISO-IEC-27035-Lead-Incident-Manager證照考試 □ ISO-IEC-27035-Lead-Incident-Manager認證 □ 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考古題推薦
- ISO-IEC-27035-Lead-Incident-Manager熱門題庫 □ ISO-IEC-27035-Lead-Incident-Manager熱門題庫 ☂ ISO-IEC-27035-Lead-Incident-Manager考古題推薦 □ 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考古題
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, wjhsd.instructure.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, bbs.t-firefly.com, bbs.t-firefly.com, www.stes.tyc.edu.tw, 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=1U1mNnJqg-6JoYO03kLgMd_W-U7kIRU3m