PECB ISO-IEC-27035-Lead-Incident-Manager시험준비, ISO-IEC-27035-Lead-Incident-Manager퍼펙트덤프데모문제다운

그 외, ExamPassdump ISO-IEC-27035-Lead-Incident-Manager 시험 문제집 일부가 지금은 무료입니다: https://drive.google.com/open?id=1C-QgZsGRwayCgfF-gaMNqesqLJvSnsGC

ExamPassdump는 여러분의 요구를 만족시켜드리는 사이트입니다. 많은 분들이 우리사이트의 it인증덤프를 사용함으로 관련it시험을 안전하게 패스를 하였습니다. 이니 우리 ExamPassdump사이트의 단골이 되었죠. ExamPassdump에서는 최신의PECB ISO-IEC-27035-Lead-Incident-Manager자료를 제공하며 여러분의PECB ISO-IEC-27035-Lead-Incident-Manager인증시험에 많은 도움이 될 것입니다.

PECB ISO-IEC-27035-Lead-Incident-Manager 시험요강:

주제	소개
주제 1	• 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.
주제 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.
주제 3	• 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.
주제 4	• 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.

시험대비 ISO-IEC-27035-Lead-Incident-Manager시험준비 최신 공부자료

최신 ISO 27001 ISO-IEC-27035-Lead-Incident-Manager 무료샘플문제 (Q20-Q25):

질문 # 20

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. Because the implementation of a structured incident management process helps the company effectively address the need for skilled incident response
- B. No, because the structured incident management process should primarily focus on preventive measures rather than response capabilities
- C. 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

정답： A

설명：
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.

질문 # 21
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. Yes, IRT's responsibilities include identifying root causes, discovering hidden vulnerabilities, and resolving incidents quickly to minimize their impact
- C. No, the responsibilities of IRT also include assessing events and declaring incidents

정답： C

설명：
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.
-

질문 # 22
Which of the following statements regarding the principles for digital evidence gathering is correct?

- A. Reliability implies that all processes used in handling digital evidence should be unique and not necessarily reproducible
- B. 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
- C. Sufficiency means that only a minimal amount of material should be gathered to avoid unnecessary auditing and justification efforts

정답： B

설명:
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
-

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

정답： B

설명：
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
-

질문 # 24
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.
Based on scenario 3, did Leona follow all the ISO/IEC 27035-1 guidelines when communicating the information security incident management policy to interested parties?

- A. No, she should also communicate how often the information security incident policies are updated and revised
- B. Yes, she effectively communicated the outcomes of incidents and strategies to minimize recurrence, meeting the necessary communication requirements
- C. No, she should also communicate the incident reporting procedures and specify the appropriate contact for further information

정답： C

설명：
Comprehensive and Detailed Explanation:
According to ISO/IEC 27035-1:2016, effective communication of the incident management policy must include not only policy content, roles, and responsibilities but also specific procedural aspects-such as how to report an incident and who to contact. This ensures that all stakeholders clearly understand their responsibilities in the event of an incident and know how to respond.
In the scenario, Leona communicated the outcomes of incidents, mitigation strategies, personnel obligations, and policy content. However, she did not include the incident reporting procedures or contact points, which are essential components of incident communication as per ISO guidelines.
Reference:
ISO/IEC 27035-1:2016, Clause 6.1: "Communication of the incident management policy should include reporting channels, escalation contacts, and policy revision frequency." Therefore, the correct answer is B.
-

질문 # 25
......

ExamPassdump의 PECB인증 ISO-IEC-27035-Lead-Incident-Manager시험덤프는 실제시험의 기출문제와 예상문제를 묶어둔 공부자료로서 시험문제커버율이 상당히 높습니다.IT업계에 계속 종사하려는 IT인사들은 부단히 유력한 자격증을 취득하고 자신의 자리를 보존해야 합니다. ExamPassdump의 PECB인증 ISO-IEC-27035-Lead-Incident-Manager시험덤프로 어려운 PECB인증 ISO-IEC-27035-Lead-Incident-Manager시험을 쉽게 패스해보세요. IT자격증 취득이 여느때보다 여느일보다 쉬워져 자격증을 많이 따는 꿈을 실현해드립니다.

ISO-IEC-27035-Lead-Incident-Manager퍼펙트 덤프데모문제 다운: https://www.exampassdump.com/ISO-IEC-27035-Lead-Incident-Manager_valid-braindumps.html

- 최신 업데이트버전 ISO-IEC-27035-Lead-Incident-Manager시험준비 덤프문제 □ ➽ www.koreadumps.com □에서➥ ISO-IEC-27035-Lead-Incident-Manager □를 검색하고 무료로 다운로드하세요ISO-IEC-27035-Lead-Incident-Manager최신 시험대비 공부자료
- ISO-IEC-27035-Lead-Incident-Manager시험준비 덤프로 시험패스하여 자격증을 취득 □ 무료로 쉽게 다운로드하려면□ www.itdumpskr.com □에서{ ISO-IEC-27035-Lead-Incident-Manager }를 검색하세요ISO-IEC-27035-Lead-Incident-Manager시험패스 가능한 인증공부
- ISO-IEC-27035-Lead-Incident-Manager최신버전 덤프데모문제 □ ISO-IEC-27035-Lead-Incident-Manager시험덤프데모 □ ISO-IEC-27035-Lead-Incident-Manager최신버전 덤프문제 □ 지금➠ www.pass4test.net □에서【 ISO-IEC-27035-Lead-Incident-Manager 】를 검색하고 무료로 다운로드하세요ISO-IEC-27035-Lead-Incident-Manager최신버전 덤프데모문제
- ISO-IEC-27035-Lead-Incident-Manager최신버전 덤프데모문제 □ ISO-IEC-27035-Lead-Incident-Manager시험덤프문제 □ ISO-IEC-27035-Lead-Incident-Manager덤프문제집 □ 【 www.itdumpskr.com 】에서「 ISO-IEC-27035-Lead-Incident-Manager 」를 검색하고 무료로 다운로드하세요ISO-IEC-27035-Lead-Incident-Manager시험패스 가능한 인증공부
- ISO-IEC-27035-Lead-Incident-Manager시험준비 기출자료 □ 【 www.passtip.net 】웹사이트에서“ ISO-IEC-27035-Lead-Incident-Manager ”를 열고 검색하여 무료 다운로드ISO-IEC-27035-Lead-Incident-Manager최신기출자료
- ISO-IEC-27035-Lead-Incident-Manager시험준비 기출자료 □ ⇛ www.itdumpskr.com ⇚에서▷ ISO-IEC-27035-Lead-Incident-Manager ◁를 검색하고 무료 다운로드 받기ISO-IEC-27035-Lead-Incident-Manager인증시험 덤프문제
- ISO-IEC-27035-Lead-Incident-Manager시험준비 100% 유효한 시험공부자료 □ 검색만 하면▷ www.koreadumps.com ◁에서✔ ISO-IEC-27035-Lead-Incident-Manager □✔□무료 다운로드ISO-IEC-27035-Lead-Incident-Manager완벽한 시험덤프
- ISO-IEC-27035-Lead-Incident-Manager인증시험 인기 덤프문제 □ ISO-IEC-27035-Lead-Incident-Manager최신버전 덤프문제 □ ISO-IEC-27035-Lead-Incident-Manager완벽한 시험덤프 □ ➤ www.itdumpskr.com □을(를) 열고{ ISO-IEC-27035-Lead-Incident-Manager }를 입력하고 무료 다운로드를 받으십시오ISO-IEC-27035-Lead-Incident-Manager덤프문제집
- ISO-IEC-27035-Lead-Incident-Manager시험준비 인기 인증시험은 덤프로 고고싱 □ 오픈 웹 사이트➠ www.pass4test.net □검색□ ISO-IEC-27035-Lead-Incident-Manager □무료 다운로드ISO-IEC-27035-Lead-Incident-Manager최신 덤프문제보기
- ISO-IEC-27035-Lead-Incident-Manager최신 시험대비 공부자료 □ ISO-IEC-27035-Lead-Incident-Manager최신버전 덤프문제 □ ISO-IEC-27035-Lead-Incident-Manager최신기출자료 □ ✔ www.itdumpskr.com □✔□에서□ ISO-IEC-27035-Lead-Incident-Manager □를 검색하고 무료 다운로드 받기ISO-IEC-27035-Lead-Incident-Manager높은 통과율 공부문제
- ISO-IEC-27035-Lead-Incident-Manager시험준비 인기 인증시험은 덤프로 고고싱 □ 《 www.passtip.net 》은➠ ISO-IEC-27035-Lead-Incident-Manager □무료 다운로드를 받을 수 있는 최고의 사이트입니다ISO-IEC-27035-Lead-Incident-Manager인증시험 인기 덤프문제
- 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, seldomlexx.alboompro.com, connect.garmin.com, www.stes.tyc.edu.tw, bbs.t-firefly.com, www.stes.tyc.edu.tw, building.lv, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, yqc-future.com, Disposable vapes

BONUS!!! ExamPassdump ISO-IEC-27035-Lead-Incident-Manager 시험 문제집 전체 버전을 무료로 다운로드하세요: https://drive.google.com/open?id=1C-QgZsGRwayCgfF-gaMNqesqLJvSnsGC