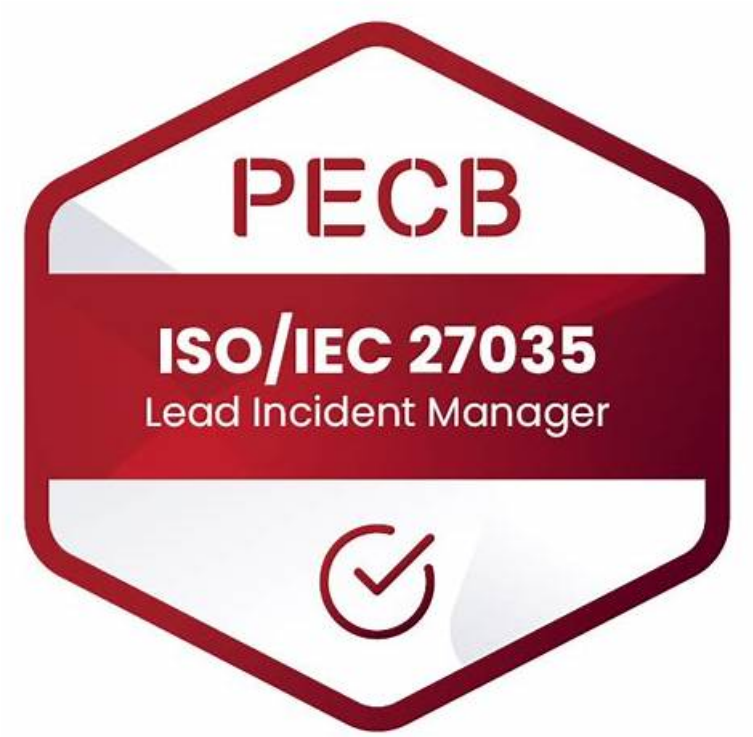
Quiz PECB - Updated ISO-IEC-27035-Lead-Incident-Manager - PECB Certified ISO/IEC 27035 Lead Incident Manager Latest Cram Materials



Exams-boost also presents desktop-based PECB ISO-IEC-27035-Lead-Incident-Manager practice test software which is usable without any internet connection after installation and only required license verification. PECB Certified ISO/IEC 27035 Lead Incident Manager (ISO-IEC-27035-Lead-Incident-Manager) practice test software is very helpful for all those who desire to practice in an actual PECB Certified ISO/IEC 27035 Lead Incident Manager (ISO-IEC-27035-Lead-Incident-Manager) exam-like environment. PECB Certified ISO/IEC 27035 Lead Incident Manager (ISO-IEC-27035-Lead-Incident-Manager) practice test software contains many PECB ISO-IEC-27035-Lead-Incident-Manager practice exam designs just like the real PECB Certified ISO/IEC 27035 Lead Incident Manager (ISO-IEC-27035-Lead-Incident-Manager) exam.

It is known to us that the ISO-IEC-27035-Lead-Incident-Manager exam braindumps have dominated the leading position in the global market with the decades of painstaking efforts of our experts and professors. There are many special functions about study materials to help a lot of people to reduce the heavy burdens when they are preparing for the exams. For example, the ISO-IEC-27035-Lead-Incident-Manager study practice question from our company can help all customers to make full use of their sporadic time. Just like the old saying goes, time is our product by a good at using sporadic time person, will make achievements. If you can learn to make full use of your sporadic time to preparing for your ISO-IEC-27035-Lead-Incident-Manager Exam, you will find that it will be very easy for you to achieve your goal on the exam. Using our study materials, your sporadic time will not be wasted, on the contrary, you will spend your all sporadic time on preparing for your ISO-IEC-27035-Lead-Incident-Manager exam.

>> ISO-IEC-27035-Lead-Incident-Manager Latest Cram Materials <<

Latest updated PECB ISO-IEC-27035-Lead-Incident-Manager: PECB Certified ISO/IEC 27035 Lead Incident Manager Latest Cram Materials - Reliable Exams-boost ISO-IEC-27035-Lead-Incident-Manager Test Price

The evergreen field of PECB is so attractive that it provides non-stop possibilities for the one who passes the PECB ISO-IEC-27035-Lead-Incident-Manager exam. So, to be there on top of the IT sector, earning the PECB Certified ISO/IEC 27035 Lead Incident Manager (ISO-IEC-27035-Lead-Incident-Manager) certification is essential. Because of using outdated ISO-IEC-27035-Lead-Incident-Manager Study Material, many candidates don't get success in the ISO-IEC-27035-Lead-Incident-Manager exam

and lose their resources. The ISO-IEC-27035-Lead-Incident-Manager PDF Questions of Exams-boost are authentic and real.

PECB ISO-IEC-27035-Lead-Incident-Manager Exam Syllabus Topics:

Topic	Details
Topic 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.
Topic 2	• 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.
Topic 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.
Topic 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.

PECB Certified ISO/IEC 27035 Lead Incident Manager Sample Questions (Q59-Q64):

NEW QUESTION # 59
Which of the following statements regarding the principles for digital evidence gathering is correct?

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

Answer: B

Explanation:
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
-

NEW QUESTION # 60
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.
According to scenario 6, Nate compiled a detailed incident report that analyzed the problem and its cause but did not evaluate the incident's severity and response urgency. Does this align with the ISO/IEC 27035-1 guidelines?

- A. No, as the report did not include a comprehensive list of all employees who accessed the system within 24 hours before the incident
- B. Yes. Nate included all the elements required by ISO/IEC 27035-1
- C. No, Nate overlooked the necessity of assessing the seriousness and the urgency of the response

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-1:2016 emphasizes that part of the incident handling process-particularly during assessment and documentation-must include evaluation of both the seriousness (severity) and urgency (criticality) of the incident.
Clause 6.4.2 requires that an incident's potential impact and required response timelines be assessed promptly to determine appropriate action. Nate's omission of this evaluation, despite creating a technically sound report, means that the organization could misjudge the incident's risk, delay appropriate response, or fail to meet notification obligations.
Option A is incorrect because ISO/IEC 27035 explicitly lists impact and urgency as required analysis elements. Option C, while possibly helpful in forensic analysis, is not a required component per the standard.
Reference:
ISO/IEC 27035-1:2016, Clause 6.4.2: "Assess the impact, severity, and urgency of the incident to determine the necessary response and escalation procedures." Clause 6.5.4: "An incident report should include an evaluation of incident criticality to inform decision- making." Correct answer: B Each includes the correct answer, detailed justification, and citation from ISO/IEC 27035 standards.
-

NEW QUESTION # 61
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. Event-based approach
- B. Both A and B
- C. Asset-based approach

Answer: B

Explanation:
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.

NEW QUESTION # 62
According to ISO/IEC 27035-2, how should an organization plan the development of the incident response team capabilities?

- A. By discontinuing any capabilities that have not been used recently
- B. By focusing only on internal capabilities
- C. By considering how often certain capabilities were needed in the past

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-2:2016 recommends that organizations should assess the necessary capabilities of the Incident Response Team (IRT) based on risk exposure and the frequency of past incidents requiring specific skills or tools. This ensures a balanced and realistic approach to resource allocation while preparing for probable future events.
Section 7.2.1 of ISO/IEC 27035-2 outlines that capability planning should consider:
Lessons learned from prior incidents
Incident history and trends
Anticipated threat landscape
Option A is incorrect because relying solely on internal capabilities may leave organizations vulnerable when specialized expertise is required. Option C contradicts ISO guidance because a lack of recent use does not mean a capability is no longer critical; it may still be required during high-impact, low-frequency incidents.
Reference:
ISO/IEC 27035-2:2016, Clause 7.2.1: "Incident response capabilities should be planned and developed based on the history of incidents, business requirements, and likely future needs." Correct answer: B
-

NEW QUESTION # 63
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.
In scenario 4, during a routine check, the IT manager discovered that multiple employees were unaware of the proper procedures following the detection of a phishing email and scheduled immediate training for all employees on information security policies and incident response. Is this recommended?

- A. No, providing training is unnecessary; the employees' ignorance of proper procedures regarding phishing emails is a minor issue
- B. No, the IT manager should handle the incident without involving other employees
- C. Yes, it is recommended that immediate training on these topics be provided to ensure employees know how to respond correctly to phishing emails

Answer: C

Explanation:
Comprehensive and Detailed Explanation:
Phishing is one of the most common entry points for cybersecurity incidents. ISO/IEC 27035 and ISO/IEC 27002 both recommend security awareness training as a key preventive control. When users do not understand proper response procedures, the risk of successful attacks increases significantly.
Providing immediate training, especially following the identification of a knowledge gap, is considered best practice. This aligns with ISO/IEC 27001:2022 Annex A.6.3 and A.5.36, which emphasize the need for education and continuous awareness on security topics, including how to handle phishing attempts.
Reference:
ISO/IEC 27035-1:2016, Clause 6.1 - "Preparation includes awareness training to reduce the likelihood and impact of incidents."
ISO/IEC 27002:2022, Control A.6.3 - "Personnel should receive appropriate awareness education and training to carry out their information security responsibilities." Therefore, the correct answer is A.

NEW QUESTION # 64
.....

□ ISO-IEC-27035-Lead-Incident-Manager Test Sample Online □ Easily obtain free download of □ ISO-IEC-27035-Lead-Incident-Manager □ by searching on 【 www.free4dump.com 】 □New ISO-IEC-27035-Lead-Incident-Manager Test Topics

- Best ISO-IEC-27035-Lead-Incident-Manager Study Material □ ISO-IEC-27035-Lead-Incident-Manager Lab Questions ☣ ISO-IEC-27035-Lead-Incident-Manager Exam Questions And Answers □ （ www.pdfvce.com ） is best website to obtain □ ISO-IEC-27035-Lead-Incident-Manager □ for free download □ISO-IEC-27035-Lead-Incident-Manager Exam Quick Prep
- Pass Guaranteed 2025 ISO-IEC-27035-Lead-Incident-Manager: PECB Certified ISO/IEC 27035 Lead Incident Manager –High Pass-Rate Latest Cram Materials □ Search for [ISO-IEC-27035-Lead-Incident-Manager] on ▹ www.getvalidtest.com ◃ immediately to obtain a free download ♣ISO-IEC-27035-Lead-Incident-Manager Test Sample Online
- Exam ISO-IEC-27035-Lead-Incident-Manager Dumps □ Exam ISO-IEC-27035-Lead-Incident-Manager Collection Pdf □ Dumps ISO-IEC-27035-Lead-Incident-Manager PDF □ Enter ➡ www.pdfvce.com □□□ and search for ➥ ISO-IEC-27035-Lead-Incident-Manager □ to download for free ❣ Dumps ISO-IEC-27035-Lead-Incident-Manager PDF
- ISO-IEC-27035-Lead-Incident-Manager Exam Questions And Answers □ ISO-IEC-27035-Lead-Incident-Manager Lab Questions □ New ISO-IEC-27035-Lead-Incident-Manager Exam Fee □ Go to website ▹ www.real4dumps.com ◃ open and search for □ ISO-IEC-27035-Lead-Incident-Manager □ to download for free □ISO-IEC-27035-Lead-Incident-Manager Exam Questions And Answers
- Best ISO-IEC-27035-Lead-Incident-Manager Study Material □ ISO-IEC-27035-Lead-Incident-Manager Test Engine □ □ Exam ISO-IEC-27035-Lead-Incident-Manager Dumps □ Open website ▹ www.pdfvce.com ◃ and search for { ISO-IEC-27035-Lead-Incident-Manager } for free download □Valid Dumps ISO-IEC-27035-Lead-Incident-Manager Ebook
- ISO-IEC-27035-Lead-Incident-Manager Exam Quick Prep □ ISO-IEC-27035-Lead-Incident-Manager Exam Quick Prep □ Exam ISO-IEC-27035-Lead-Incident-Manager Collection Pdf □ Easily obtain free download of 「 ISO-IEC-27035-Lead-Incident-Manager 」 by searching on { www.prep4pass.com } □ISO-IEC-27035-Lead-Incident-Manager Exam Quick Prep
- ISO-IEC-27035-Lead-Incident-Manager Cost Effective Dumps □ Best ISO-IEC-27035-Lead-Incident-Manager Study Material □ ISO-IEC-27035-Lead-Incident-Manager Test Engine □ Search for { ISO-IEC-27035-Lead-Incident-Manager } and easily obtain a free download on 《 www.pdfvce.com 》 □ISO-IEC-27035-Lead-Incident-Manager Lab Questions
- Valid Dumps ISO-IEC-27035-Lead-Incident-Manager Ebook □ ISO-IEC-27035-Lead-Incident-Manager Exam Quick Prep □ ISO-IEC-27035-Lead-Incident-Manager Test Engine ⧗ Enter □ www.actual4labs.com □ and search for ▹ ISO-IEC-27035-Lead-Incident-Manager ◃ to download for free □Reliable ISO-IEC-27035-Lead-Incident-Manager Exam Price
- shortcourses.russellcollege.edu.au, tutulszone.com, daotao.wisebusiness.edu.vn, www.wcs.edu.eu, sudacad.net, ennglish.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, daotao.wisebusiness.edu.vn, 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, jimbell680.blogolize.com, Disposable vapes