Pass Guaranteed 2026 Reliable PECB ISO-IEC-27035-Lead-Incident-Manager: PECB Certified ISO/IEC 27035 Lead Incident Manager Online Exam

What's more, part of that Real4test ISO-IEC-27035-Lead-Incident-Manager dumps now are free: https://drive.google.com/open?id=11zMWlFWrrvnMzw7Jis5ux6us7PwYPAw2

Real4test is an experienced website with great reputation which offering PECB dumps torrent and professional explanations. Our ISO-IEC-27035-Lead-Incident-Manager test questions are created by our IT elites who pay great attention to the IT exam certification so we can ensure you the authority and reliability of our ISO-IEC-27035-Lead-Incident-Manager Practice Test.

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

Topic	Details
Topic 1	• 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.
Topic 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.
Topic 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.

>> ISO-IEC-27035-Lead-Incident-Manager Online Exam <<

High Pass-Rate ISO-IEC-27035-Lead-Incident-Manager Online Exam to Obtain PECB Certification

For the office worker, they are both busy in the job or their family; for the students, they possibly have to learn or do other things. But if they use our ISO-IEC-27035-Lead-Incident-Manager test prep, they won’t need so much time to prepare the exam and master exam content in a short time. What they need to do is just to spare 1-2 hours to learn and practice every day and then pass the exam with ISO-IEC-27035-Lead-Incident-Manager Test Prep easily. It costs them little time and energy.

PECB Certified ISO/IEC 27035 Lead Incident Manager Sample Questions (Q74-Q79):

NEW QUESTION # 74
Which team has a broader cybersecurity role, including incident response, monitoring, and overseeing general operations?

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

Answer: C

Explanation:
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)
-

NEW QUESTION # 75
What is the purpose of a gap analysis?

- A. To determine the steps to achieve a desired future state from the current state
- B. To assess risks associated with identified gaps in current practices compared to best practices
- C. To identify the differences between current processes and company policies

Answer: A

Explanation:
Comprehensive and Detailed Explanation:
Gap analysis is a structured method used to compare the current state of processes, capabilities, or systems against a desired or required state (such as compliance with ISO standards). The main goal is to determine what needs to change to achieve that future state. While identifying gaps (A) and assessing risks (C) may occur during the process, the primary purpose is strategic planning and improvement.
Reference:
ISO/IEC 27001 Implementation Guidelines, Clause 0.3: "Gap analysis is used to evaluate the difference between current practices and ISO requirements and to define actions to meet compliance." Correct answer: B
-

NEW QUESTION # 76
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 considering how often certain capabilities were needed in the past
- C. By focusing only on internal capabilities

Answer: B

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 # 77
Which action is NOT involved in the process of improving controls in incident management?

- A. Implementing new or updated controls
- B. Updating the incident management policy
- C. Documenting risk assessment results

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Improving controls in incident management is a proactive activity focused on directly adjusting and strengthening existing defenses. As per ISO/IEC 27035-2:2016, Clause 7.4, this process typically involves identifying deficiencies, updating or implementing new technical or procedural controls, and revising policies.
While risk assessments inform control decisions, simply documenting their results does not constitute direct improvement of controls. Hence, Option A is not part of the control improvement process itself.
Reference:
ISO/IEC 27035-2:2016 Clause 7.4: "Actions to improve controls include analyzing causes of incidents and updating procedures and policies accordingly." Correct answer: A
-

NEW QUESTION # 78
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 has recently upgraded its digital banking platform. In line with the continual improvement process, Moneda Vivo has decided to review the information security incident management process for accuracy immediately after the software update. Is this recommended?

- A. No, the incident management process should be evaluated after a significant technological overhaul to ensure the system is up-to-date
- B. No, the incident management process should be reviewed when the bank's annual audit is conducted
- C. Yes, the incident management process should be reviewed after any minor software update

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
According to ISO/IEC 27035-1:2016, Clause 7.1 and ISO/IEC 27035-2:2016, Clause 7.3.3, it is advised to review and revise the information security incident management process following major organizational or technical changes. These changes include upgrades, system overhauls, and structural IT shifts. While minor updates may not necessitate a full review, significant technological updates, such as those affecting core digital banking platforms, should trigger immediate evaluation to ensure continued relevance and effectiveness of incident response strategies.
In the scenario, Moneda Vivo recognized the need for a review but delayed it, which could pose risks. Option C accurately reflects ISO guidance.
Reference:
ISO/IEC 27035-1:2016 Clause 7.1: "Reviews should be performed after major changes or after information security incidents."
ISO/IEC 27035-2:2016 Clause 7.3.3 Correct answer: C
-

NEW QUESTION # 79
......

The Internet is increasingly becoming a platform for us to work and learn, while many products are unreasonable in web design, and too much information is not properly classified. Our ISO-IEC-27035-Lead-Incident-Manager exam materials draw lessons from the experience of failure, will all kinds of ISO-IEC-27035-Lead-Incident-Manager qualification examination has carried on the classification of clear layout, at the same time the user when they entered the ISO-IEC-27035-Lead-Incident-Manager Study Guide materials page in the test module classification of clear, convenient to use a very short time to find what they want to study for the ISO-IEC-27035-Lead-Incident-Manager exam.

Review □ Valid ISO-IEC-27035-Lead-Incident-Manager Test Practice □ Search for ✔ ISO-IEC-27035-Lead-Incident-Manager □✔□ and download exam materials for free through ➡ www.practicevce.com □□□ □ISO-IEC-27035-Lead-Incident-Manager Valid Test Review

- Practice Exam Software PECB ISO-IEC-27035-Lead-Incident-Manager Exam Questions □ Download □ ISO-IEC-27035-Lead-Incident-Manager □ for free by simply searching on ▹ www.pdfvce.com ◃ □ISO-IEC-27035-Lead-Incident-Manager Valid Exam Materials
- Latest ISO-IEC-27035-Lead-Incident-Manager Exam Dumps □ ISO-IEC-27035-Lead-Incident-Manager Valid Test Review □ ISO-IEC-27035-Lead-Incident-Manager Reliable Exam Questions □ Search for ➤ ISO-IEC-27035-Lead-Incident-Manager □ and easily obtain a free download on ⇛ www.prep4away.com ⇚ □Reliable ISO-IEC-27035-Lead-Incident-Manager Exam Guide
- Pass Guaranteed Quiz PECB - ISO-IEC-27035-Lead-Incident-Manager Fantastic Online Exam □ Go to website ▸ www.pdfvce.com ◂ open and search for 【 ISO-IEC-27035-Lead-Incident-Manager 】 to download for free ❇Valid ISO-IEC-27035-Lead-Incident-Manager Mock Exam
- ISO-IEC-27035-Lead-Incident-Manager Materials □ New ISO-IEC-27035-Lead-Incident-Manager Braindumps Files □ Reliable ISO-IEC-27035-Lead-Incident-Manager Exam Guide □ Open " www.vce4dumps.com " and search for [ISO-IEC-27035-Lead-Incident-Manager] to download exam materials for free □Reliable ISO-IEC-27035-Lead-Incident-Manager Exam Questions
- Valid ISO-IEC-27035-Lead-Incident-Manager Mock Exam □ Valid ISO-IEC-27035-Lead-Incident-Manager Mock Exam □ ISO-IEC-27035-Lead-Incident-Manager Valid Test Pattern □ Open website ➥ www.pdfvce.com □ and search for ➡ ISO-IEC-27035-Lead-Incident-Manager □□□ for free download ☢Reliable ISO-IEC-27035-Lead-Incident-Manager Exam Guide
- Famous ISO-IEC-27035-Lead-Incident-Manager Training Quiz Bring You the Topping Exam Questions - www.prepawaypdf.com □ Search for ➤ ISO-IEC-27035-Lead-Incident-Manager □ and obtain a free download on ➽ www.prepawaypdf.com □ □ISO-IEC-27035-Lead-Incident-Manager Reliable Exam Questions
- summerschool.entrehubs.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, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, thecodingtracker.com, github.com, www.stes.tyc.edu.tw, k12.instructure.com, hashnode.com, bbs.t-firefly.com, Disposable vapes

What's more, part of that Real4test ISO-IEC-27035-Lead-Incident-Manager dumps now are free: https://drive.google.com/open?id=11zMWlFWrrvnMzw7Jis5ux6us7PwYPAw2