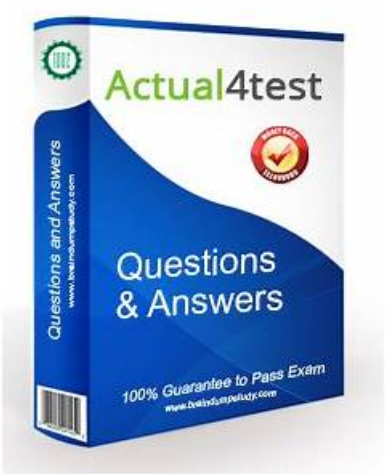
Sample ISO-IEC-27035-Lead-Incident-Manager Test Online & ISO-IEC-27035-Lead-Incident-Manager Latest Exam Labs



P.S. Free & New ISO-IEC-27035-Lead-Incident-Manager dumps are available on Google Drive shared by Real4exams: https://drive.google.com/open?id=1O7HBitBK9dY9m-PMvig69IY9Wa8BCI_2

For all of you, it is necessary to get the PECB certification to enhance your career path. Real4exams is the leading provider of its practice exams, study guides and online learning courses, which may can help you. For example, the ISO-IEC-27035-Lead-Incident-Manager practice dumps contain the comprehensive contents which relevant to the actual test, with which you can pass your ISO-IEC-27035-Lead-Incident-Manager Actual Test with high score. Besides, you can print the ISO-IEC-27035-Lead-Incident-Manager study torrent into papers, which can give a best way to remember the questions. We guarantee full refund for any reason in case of your failure of ISO-IEC-27035-Lead-Incident-Manager test.

Quality of ISO-IEC-27035-Lead-Incident-Manager practice materials you purchased is of prior importance for consumers. Our ISO-IEC-27035-Lead-Incident-Manager practice materials make it easier to prepare exam with a variety of high quality functions. Their quality function is observably clear once you download them. We have three kinds of ISO-IEC-27035-Lead-Incident-Manager practice materials moderately priced for your reference. All these three types of ISO-IEC-27035-Lead-Incident-Manager practice materials win great support around the world and all popular according to their availability of goods, prices and other term you can think of.

>> Sample ISO-IEC-27035-Lead-Incident-Manager Test Online <<

Master The ISO-IEC-27035-Lead-Incident-Manager Content for ISO-IEC-27035-Lead-Incident-Manager exam success

This is the reason why the experts suggest taking the ISO-IEC-27035-Lead-Incident-Manager practice test with all your concentration and effort. The more you can clear your doubts, the more easily you can pass the ISO-IEC-27035-Lead-Incident-Manager exam. Real4exams PECB Certified ISO/IEC 27035 Lead Incident Manager (ISO-IEC-27035-Lead-Incident-Manager) practice test works amazingly to help you understand the PECB ISO-IEC-27035-Lead-Incident-Manager Exam Pattern and how you can attempt the real PECB Exam Questions. It is just like the final ISO-IEC-27035-Lead-Incident-Manager exam pattern and you can change its settings.

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

Topic	Details
Topic 1	• 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.
Topic 2	• 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.
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 (Q35-Q40):

NEW QUESTION # 35
When does the information security incident management plan come into effect?

- A. When a new security policy is drafted
- B. When a security vulnerability is reported
- C. After a security audit is completed

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
According to ISO/IEC 27035-1 and 27035-2, the incident management plan is activated upon the detection or reporting of a security event, particularly when a vulnerability, threat, or compromise has been identified. The plan ensures structured response and accountability from the very first signs of a potential incident.
Clause 6.4.2 in ISO/IEC 27035-2 explains that incident response activities-including logging, categorization, assessment, and escalation-should begin as soon as a security incident or vulnerability is reported. This proactive trigger allows early containment and mitigation.
Security audits and policy drafts (Options A and B) are part of preventive or governance mechanisms, not operational triggers for activating the plan.
Reference Extracts:
ISO/IEC 27035-2:2016, Clause 6.4.2: "The incident management plan should be activated once a security incident or significant vulnerability is identified and reported." Clause 5.1: "Detection and reporting are the initial steps in triggering the formal incident

management lifecycle." Correct answer: C

NEW QUESTION # 36
According to ISO/IEC 27035-2, how should an organization plan the development of the incident response team capabilities?

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

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 # 37
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 also include assessing events and declaring incidents
- B. No, the responsibilities of IRT do not include resolving incidents

- C. Yes, IRT's responsibilities include identifying root causes, discovering hidden vulnerabilities, and resolving incidents quickly to minimize their impact

Answer: A

Explanation:
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.
-

NEW QUESTION # 38
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 ignored the trend and continued regular operations when the mean time between the same types of incidents decreased after a few occurrences. Is this acceptable?

- A. No, when the mean time between the same types of incidents decreases, a study should be necessary to confirm that the incidents are unrelated
- B. No, when the mean time between the same types of incidents decreases, a study should be conducted to discover why
- C. When the mean time between the same types of incidents decreases after a few occurrences, it shows that the incidents are becoming less significant

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-1 encourages organizations to monitor metrics, such as the frequency of incident types, as part of continual improvement (Clause 7.3). A decreasing mean time between incidents (MTBI) may indicate increased threat frequency, weakened controls, or emerging vulnerabilities. Ignoring such trends can prevent timely corrective actions and weaken overall resilience.
Instead of assuming the incidents are less significant, ISO guidance suggests conducting root cause analysis and trend evaluations when patterns like this emerge.
Reference:

ISO/IEC 27035-1:2016, Clause 7.3: "Monitoring and measurement of the incident management process should include trend analysis to identify recurring issues or new patterns." Correct answer: C
-

NEW QUESTION # 39
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, what mechanisms for detecting security incidents did EastCyber implement?

- A. Intrusion detection systems
- B. Security information and event management systems
- C. Intrusion prevention systems

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
In the scenario, EastCyber implemented an "advanced network traffic monitoring system" that "spots and alerts the security team to unauthorized actions." This aligns closely with the functional characteristics of an Intrusion Detection System (IDS), which monitors traffic or systems for malicious activities and policy violations and sends alerts for review.
While Security Information and Event Management (SIEM) tools and Intrusion Prevention Systems (IPS) offer valuable detection and response capabilities, the scenario specifically describes a system focused on monitoring and alerting-not automatically blocking traffic, which would indicate an IPS.
SIEM platforms correlate and analyze logs from various sources, which wasn't described. Therefore, IDS is the most accurate interpretation.
Reference:
ISO/IEC 27035-2:2016, Clause 7.4.2: "Detection mechanisms can include intrusion detection systems, log analysis tools, and traffic monitoring systems to detect potential security events." Correct answer: B
-

NEW QUESTION # 40
.....

windfall.

ISO-IEC-27035-Lead-Incident-Manager Latest Exam Labs: https://www.real4exams.com/ISO-IEC-27035-Lead-Incident-Manager_braindumps.html

- New ISO-IEC-27035-Lead-Incident-Manager Exam Question □ ISO-IEC-27035-Lead-Incident-Manager Exams Dumps □ Reliable ISO-IEC-27035-Lead-Incident-Manager Dumps Free □ Search for ▹ ISO-IEC-27035-Lead-Incident-Manager ◃ and download it for free immediately on " www.examcollectionpass.com " □ISO-IEC-27035-Lead-Incident-Manager New Exam Camp
- Free PDF Quiz 2026 High-quality ISO-IEC-27035-Lead-Incident-Manager: Sample PECB Certified ISO/IEC 27035 Lead Incident Manager Test Online □ Easily obtain ➡ ISO-IEC-27035-Lead-Incident-Manager □□□ for free download through ⇛ www.pdfvce.com ⇚ □ISO-IEC-27035-Lead-Incident-Manager Books PDF
- ISO-IEC-27035-Lead-Incident-Manager Instant Discount □ Real ISO-IEC-27035-Lead-Incident-Manager Dumps □ ISO-IEC-27035-Lead-Incident-Manager Latest Test Questions □ Search for ➽ ISO-IEC-27035-Lead-Incident-Manager □ and download it for free on ▹ www.torrentvce.com ◃ website □ISO-IEC-27035-Lead-Incident-Manager Valid Exam Materials
- Free PDF 2026 PECB ISO-IEC-27035-Lead-Incident-Manager: PECB Certified ISO/IEC 27035 Lead Incident Manager Fantastic Sample Test Online □ Easily obtain ☀ ISO-IEC-27035-Lead-Incident-Manager □☀□ for free download through ➥ www.pdfvce.com □ □ISO-IEC-27035-Lead-Incident-Manager Test Preparation
- Free PDF Quiz 2026 High-quality ISO-IEC-27035-Lead-Incident-Manager: Sample PECB Certified ISO/IEC 27035 Lead Incident Manager Test Online □ Search for □ ISO-IEC-27035-Lead-Incident-Manager □ on ➥ www.prepawaypdf.com □ immediately to obtain a free download ⏲Guaranteed ISO-IEC-27035-Lead-Incident-Manager Passing
- ISO-IEC-27035-Lead-Incident-Manager Reliable Exam Answers ♣ New ISO-IEC-27035-Lead-Incident-Manager Braindumps Free □ ISO-IEC-27035-Lead-Incident-Manager Instant Discount □ ☀ www.pdfvce.com □☀□ is best website to obtain ➥ ISO-IEC-27035-Lead-Incident-Manager □ for free download □Reliable ISO-IEC-27035-Lead-Incident-Manager Dumps Free
- Free PDF 2026 PECB ISO-IEC-27035-Lead-Incident-Manager: PECB Certified ISO/IEC 27035 Lead Incident Manager Fantastic Sample Test Online □ Search on [www.prepawayexam.com] for ⇛ ISO-IEC-27035-Lead-Incident-Manager ⇚ to obtain exam materials for free download □ISO-IEC-27035-Lead-Incident-Manager Passguide
- ISO-IEC-27035-Lead-Incident-Manager Latest Test Questions ❤□ ISO-IEC-27035-Lead-Incident-Manager Books PDF □ ISO-IEC-27035-Lead-Incident-Manager Exam Test □ Search on □ www.pdfvce.com □ for 【 ISO-IEC-27035-Lead-Incident-Manager 】 to obtain exam materials for free download □ISO-IEC-27035-Lead-Incident-Manager Valid Exam Materials
- ISO-IEC-27035-Lead-Incident-Manager Latest Test Questions □ ISO-IEC-27035-Lead-Incident-Manager Reliable Exam Answers □ ISO-IEC-27035-Lead-Incident-Manager Reliable Exam Answers □ Go to website ➠ www.vce4dumps.com □ open and search for [ISO-IEC-27035-Lead-Incident-Manager] to download for free □New ISO-IEC-27035-Lead-Incident-Manager Braindumps Free
- Free PDF Quiz 2026 High-quality ISO-IEC-27035-Lead-Incident-Manager: Sample PECB Certified ISO/IEC 27035 Lead Incident Manager Test Online □ Easily obtain free download of □ ISO-IEC-27035-Lead-Incident-Manager □ by searching on ⇛ www.pdfvce.com ⇚ □ISO-IEC-27035-Lead-Incident-Manager Exams Dumps
- Real ISO-IEC-27035-Lead-Incident-Manager Dumps □ ISO-IEC-27035-Lead-Incident-Manager Valid Exam Materials □ ISO-IEC-27035-Lead-Incident-Manager Valid Exam Materials □ Search for 「 ISO-IEC-27035-Lead-Incident-Manager 」 and download it for free immediately on □ www.prepawaypdf.com □ 👆 ISO-IEC-27035-Lead-Incident-Manager Instant Discount
- 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, myportal.utt.edu.tt, 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, 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, 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, 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, Disposable vapes

What's more, part of that Real4exams ISO-IEC-27035-Lead-Incident-Manager dumps now are free: https://drive.google.com/open?id=1O7HBitBK9dY9m-PMvig69IY9Wa8BCI_2