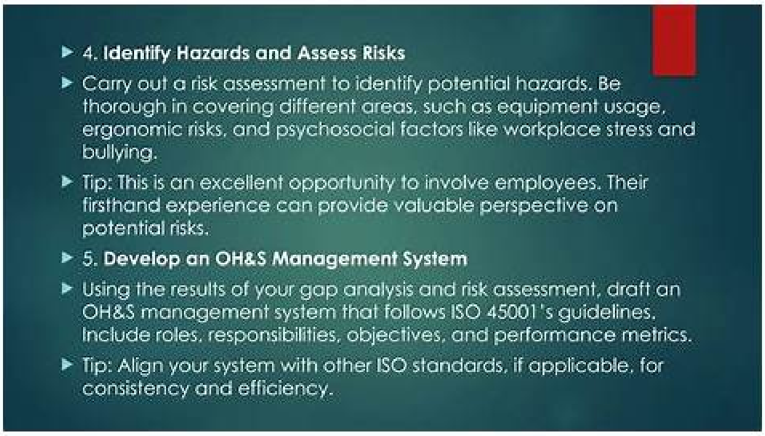
Study ISO-IEC-27035-Lead-Incident-Manager Plan | Test ISO-IEC-27035-Lead-Incident-Manager Questions Fee



- 4. **Identify Hazards and Assess Risks**
- Carry out a risk assessment to identify potential hazards. Be thorough in covering different areas, such as equipment usage, ergonomic risks, and psychosocial factors like workplace stress and bullying.
- Tip: This is an excellent opportunity to involve employees. Their firsthand experience can provide valuable perspective on potential risks.
- 5. **Develop an OH&S Management System**
- Using the results of your gap analysis and risk assessment, draft an OH&S management system that follows ISO 45001's guidelines. Include roles, responsibilities, objectives, and performance metrics.
- Tip: Align your system with other ISO standards, if applicable, for consistency and efficiency.

DOWNLOAD the newest TrainingQuiz ISO-IEC-27035-Lead-Incident-Manager PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1-qkY8lwTtgo5GRp5l_1uWkn7lB30W2Jg

The TrainingQuiz team regularly updates the ISO-IEC-27035-Lead-Incident-Manager exam pdf format to make sure that applicants receive the most up-to-date PECB ISO-IEC-27035-Lead-Incident-Manager exam questions. Additionally, our ISO-IEC-27035-Lead-Incident-Manager PDF is designed to be user-friendly and accessible on any smart device, which means that students can prepare for the ISO-IEC-27035-Lead-Incident-Manager from anywhere, at any time.

Our experts have worked hard for several years to formulate ISO-IEC-27035-Lead-Incident-Manager exam braindumps for all examiners. Our ISO-IEC-27035-Lead-Incident-Manager study materials not only target but also cover all knowledge points. And our practice materials also have a statistical analysis function to help you find out the deficiency in the learning process of ISO-IEC-27035-Lead-Incident-Manager practice materials, so that you can strengthen the training for weak links. In this way, you can more confident for your success since you have improved your ability.

>> Study ISO-IEC-27035-Lead-Incident-Manager Plan <<

Test ISO-IEC-27035-Lead-Incident-Manager Questions Fee & Exam ISO-IEC-27035-Lead-Incident-Manager Forum

One of features of us is that we are pass guaranteed and money back guaranteed if you fail to pass the exam after buying ISO-IEC-27035-Lead-Incident-Manager training materials of us. Or if you have other exam to attend, we can replace other 2 valid exam dumps to you, at the same time, you can get the update version for ISO-IEC-27035-Lead-Incident-Manager Training Materials. Besides, we offer you free update for 365 days after purchasing, and the update version will be sent to your email address automatically. The ISO-IEC-27035-Lead-Incident-Manager exam dumps include both the questions and answers, and it will help you to practice.

PECB Certified ISO/IEC 27035 Lead Incident Manager Sample Questions (Q77-Q82):

NEW QUESTION # 77
Which element should an organization consider when identifying the scope of their information security incident management?

- A. Hardcopy information
- B. Electronic information
- C. Both A and B

Answer: C

Explanation:
Comprehensive and Detailed Explanation:

According to ISO/IEC 27035-1:2016 and ISO/IEC 27001:2022, when defining the scope of an information security incident management system, organizations must consider all forms of information-whether digital or physical-that are relevant to the business. Incidents can affect hardcopy (e.g., paper-based records) and electronic data (e.g., emails, files), so both must be included in the scope assessment.
Reference:
ISO/IEC 27001:2022, Clause 4.3: "The scope shall consider interfaces and dependencies between activities performed by the organization and those that are outsourced." ISO/IEC 27035-1:2016, Clause 4.2.1: "Information in all formats-including printed or written-should be protected." Correct answer: C
-

NEW QUESTION # 78
What is the first step in planning the response to information security incidents?

- A. Defining the response classification
- B. Assigning the response class based on incident information
- C. Developing processes that support the response to information security incidents

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
In ISO/IEC 27035-2:2016, the planning phase of incident response starts with establishing a classification system. Response classification is essential to ensure that incidents are assessed and categorized in a consistent manner, allowing appropriate response measures to be applied. This classification forms the foundation for selecting the right procedures, team involvement, and communication protocols.
Assigning a response class (Option A) is a subsequent step that occurs once an incident is analyzed and matched to a pre-defined category. Developing response processes (Option B) is important but comes after the classification model is defined.
Reference Extracts:
ISO/IEC 27035-2:2016, Clause 6.3.2: "The response planning process begins with the classification of potential incidents to determine the required actions and responsibilities." Clause 7.2.2: "Defining response classes helps the organization decide how to handle specific categories of incidents." Correct answer: C
-

NEW QUESTION # 79
Based on ISO/IEC 27035-2, which of the following is an example of evaluation activities used to evaluate the effectiveness of the incident management team?

- A. Conducting information security testing, particularly vulnerability assessment
- B. Analyzing the lessons learned once an information security incident has been handled and closed
- C. Evaluating the capabilities and services once they become operational

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-2:2016 Clause 7.4.3 emphasizes the role of lessons learned reviews as key evaluation activities for assessing the performance of incident response teams. This activity involves post-incident debriefs to evaluate what went right or wrong and how response processes or team functions could improve.
While options A and C are related to broader security or deployment procedures, Option B directly reflects a formal evaluation mechanism used to gauge incident team effectiveness.
Reference:
ISO/IEC 27035-2:2016 Clause 7.4.3: "Lessons learned should be documented and used to evaluate the effectiveness of the incident management process." Correct answer: B
-

NEW QUESTION # 80
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 conducts continuous review of the incident management process to ensure the effectiveness of processes and procedures in place. Is this a good practice to follow?

- A. No, organizations should regularly assess the physical security measures to ensure they align with incident management protocols
- B. No, organizations should conduct quarterly performance reviews of individual employees to ensure they follow incident management protocols
- C. Yes, organizations should conduct continuous review of the incident management process to ensure the effectiveness of the processes and procedures in place

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-1:2016 stresses the importance of continual review and improvement of the incident management process. Clause 7.1 specifically advises that organizations regularly evaluate their policies, procedures, and tools to ensure they remain effective in the face of evolving threats and business changes.
Moneda Vivo's continuous review aligns perfectly with this guidance, reinforcing preparedness and adaptability. Options A and C, while related to broader security or HR practices, are not directly aligned with ISO/IEC 27035's core recommendation regarding process review.
Reference:
ISO/IEC 27035-1:2016, Clause 7.1: "The organization should review the effectiveness of the information security incident management process regularly and in response to incidents and significant changes."

NEW QUESTION # 81

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 the scenario above, answer the following question:
After identifying a suspicious state in ORingo's system, a member of the IRT initiated a company-wide system shutdown until the anomaly was investigated. Is this acceptable?

- A. No, the IRT should have determined the facts that enable detection of the event occurrence
- B. No, the IRT should have immediately informed all employees about the potential data breach
- C. Yes, the correct action is to initiate a company-wide system shutdown until the anomaly is investigated

Answer: A

Explanation:
Comprehensive and Detailed Explanation:
According to ISO/IEC 27035-1:2016, particularly in Clause 6.2.2 (Assess and Decide), the organization must first assess the reported event to determine whether it qualifies as a security incident before implementing disruptive responses such as a full system shutdown.
Initiating a shutdown without first determining the cause, impact, or whether it's a confirmed incident can lead to unnecessary operational disruption and loss of services. The proper approach is to collect evidence, analyze system behavior, and make informed decisions based on risk level and confirmed facts.
Option B best reflects the required approach: The IRT should first determine the facts that enable detection and validation of the event's occurrence and impact before initiating drastic action like shutting down critical systems.
Reference:
ISO/IEC 27035-1:2016, Clause 6.2.2 - "An analysis should be conducted to determine whether the event should be treated as an information security incident." Clause 6.2.3 - "Response should be proportionate to the impact and type of the incident." Therefore, the correct answer is B.
-

NEW QUESTION # 82
......

Pass Guaranteed Quiz PECB - High-quality Study ISO-IEC-27035-Lead-Incident-Manager Plan

100% Money Back Guarantee TrainingQuiz's dumps guarantee your success with a promise of returning back the amount you paid, Our ISO-IEC-27035-Lead-Incident-Manager test torrent not only help you to improve the efficiency of learning, but also help you to shorten the review time of up to even two or three days, so that you use the least time and effort to get the maximum improvement to achieve your ISO-IEC-27035-Lead-Incident-Manager certification.

Or you can adjust the content or some styles of ISO-IEC-27035-Lead-Incident-Manager exam torrent as you like, with PDF version.

- 100% Pass Rate PECB Study ISO-IEC-27035-Lead-Incident-Manager Plan - ISO-IEC-27035-Lead-Incident-Manager Free Download □ Easily obtain " ISO-IEC-27035-Lead-Incident-Manager " for free download through 【 www.testkingpass.com 】 □ISO-IEC-27035-Lead-Incident-Manager Exam Answers
- ISO-IEC-27035-Lead-Incident-Manager Latest Demo □ ISO-IEC-27035-Lead-Incident-Manager Exam Registration □ □ ISO-IEC-27035-Lead-Incident-Manager Standard Answers □ Open ➤ www.pdfvce.com □ enter { ISO-IEC-27035-Lead-Incident-Manager } and obtain a free download □ISO-IEC-27035-Lead-Incident-Manager Reliable Test Book
- Valid Dumps ISO-IEC-27035-Lead-Incident-Manager Ebook □ ISO-IEC-27035-Lead-Incident-Manager Standard Answers □ Reliable ISO-IEC-27035-Lead-Incident-Manager Test Camp □ Open ➡ www.testkingpass.com □ and search for ⇒ ISO-IEC-27035-Lead-Incident-Manager ⇐ to download exam materials for free □ISO-IEC-27035-Lead-Incident-Manager Reliable Test Book
- ISO-IEC-27035-Lead-Incident-Manager Reasonable Exam Price □ ISO-IEC-27035-Lead-Incident-Manager Exam Registration □ ISO-IEC-27035-Lead-Incident-Manager Latest Demo □ Easily obtain 《 ISO-IEC-27035-Lead-Incident-Manager 》 for free download through " www.pdfvce.com " □ISO-IEC-27035-Lead-Incident-Manager Reasonable Exam Price
- 100% Pass Rate PECB Study ISO-IEC-27035-Lead-Incident-Manager Plan - ISO-IEC-27035-Lead-Incident-Manager Free Download □ Search for ➡ ISO-IEC-27035-Lead-Incident-Manager □ and download it for free immediately on ⇒ www.dumpsmaterials.com ⇐ □Test ISO-IEC-27035-Lead-Incident-Manager Question
- ISO-IEC-27035-Lead-Incident-Manager Relevant Questions □ ISO-IEC-27035-Lead-Incident-Manager New Learning Materials □ Guaranteed ISO-IEC-27035-Lead-Incident-Manager Passing □ Enter ➡ www.pdfvce.com □ and search for □ ISO-IEC-27035-Lead-Incident-Manager □ to download for free □ISO-IEC-27035-Lead-Incident-Manager Relevant Questions
- Practical ISO-IEC-27035-Lead-Incident-Manager Information □ ISO-IEC-27035-Lead-Incident-Manager Valid Test Questions □ Valid Dumps ISO-IEC-27035-Lead-Incident-Manager Ebook □ Immediately open " www.testkingpass.com " and search for ➡ ISO-IEC-27035-Lead-Incident-Manager □ to obtain a free download □ □ISO-IEC-27035-Lead-Incident-Manager Standard Answers
- ISO-IEC-27035-Lead-Incident-Manager Relevant Questions □ ISO-IEC-27035-Lead-Incident-Manager New Learning Materials □ New ISO-IEC-27035-Lead-Incident-Manager Exam Practice □ ⇒ www.pdfvce.com ⇐ is best website to obtain " ISO-IEC-27035-Lead-Incident-Manager " for free download □ISO-IEC-27035-Lead-Incident-Manager Standard Answers
- ISO-IEC-27035-Lead-Incident-Manager Relevant Questions □ Reliable ISO-IEC-27035-Lead-Incident-Manager Test Camp □ Test ISO-IEC-27035-Lead-Incident-Manager Question □ Download （ ISO-IEC-27035-Lead-Incident-Manager ） for free by simply entering [www.prepawayexam.com] website □ISO-IEC-27035-Lead-Incident-Manager Reliable Test Book
- ISO-IEC-27035-Lead-Incident-Manager Relevant Questions □ ISO-IEC-27035-Lead-Incident-Manager Standard Answers □ ISO-IEC-27035-Lead-Incident-Manager Valid Exam Tips □ Open website { www.pdfvce.com } and search for " ISO-IEC-27035-Lead-Incident-Manager " for free download □ISO-IEC-27035-Lead-Incident-Manager Reliable Test Book
- Free ISO-IEC-27035-Lead-Incident-Manager Learning Cram □ Valid Dumps ISO-IEC-27035-Lead-Incident-Manager Ebook □ ISO-IEC-27035-Lead-Incident-Manager Standard Answers ℹ Download ✔ ISO-IEC-27035-Lead-Incident-Manager □✔□ for free by simply searching on 【 www.prepawayexam.com 】 □ISO-IEC-27035-Lead-Incident-Manager Exam Answers
- 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, learn.idealhomerealtor.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, ncon.edu.sa, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt,