ISO-IEC-27035-Lead-Incident-Manager Exam Training | ISO-IEC-27035-Lead-Incident-Manager New Exam Braindumps

The ISO-IEC-27035-Lead-Incident-Manager study guide to good meet user demand, will be a little bit of knowledge to separate memory, but when you add them together will be surprised to find a day we can make use of the time is so much debris. The ISO-IEC-27035-Lead-Incident-Manager exam prep can allow users to use the time of debris anytime and anywhere to study and make more reasonable arrangements for their study and life. Choosing our ISO-IEC-27035-Lead-Incident-Manager simulating materials is a good choice for you, and follow our step, just believe in yourself, you can do it perfectly!

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

Topic	Details
Topic 1	- 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 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	- 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 4	- 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 5	- 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.

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

ISO-IEC-27035-Lead-Incident-Manager New Exam Braindumps - ISO-IEC-27035-Lead-Incident-Manager Dumps PDF

Exam-Killer ISO-IEC-27035-Lead-Incident-Manager desktop and web-based practice exams are distinguished by their excellent features. The ISO-IEC-27035-Lead-Incident-Manager web-based practice exam is supported by all operating systems and can be taken through popular browsers including Chrome, MS Edge, Internet Explorer, Opera, Firefox, and Safari. Windows computers can run the desktop PECB ISO-IEC-27035-Lead-Incident-Manager Practice Test software. You won't require a live internet connection to use the desktop PECB exam simulation software once you've verified the product's license.

PECB Certified ISO/IEC 27035 Lead Incident Manager Sample Questions (Q40-Q45):

NEW QUESTION # 40
According to scenario 4, what is the next action ORingo should take to prevent escalation when conducting exercises?

- A. Wait until the exercise is completed to clarify the situation with all parties involved
- B. Proceed with the exercise as planned, considering this as a part of the learning process
- C. Inform all participants and external entities involved that this was a simulated scenario and not a real threat immediately

Answer: C

Explanation:
Comprehensive and Detailed Explanation:
According to ISO/IEC 27035-2:2016, incident response exercises (including simulations such as phishing campaigns) must be carefully controlled to avoid confusion, escalation, or reputational damage. If an exercise is misunderstood by employees or external parties, it could lead to unintended consequences including external escalation, customer concern, or media involvement.
The best practice is to ensure that all involved-especially external stakeholders-are informed as soon as possible if they are exposed to simulated elements. Transparency ensures the organization maintains trust and mitigates potential fallout. This is part of effective communication during planned exercises.
Reference:
ISO/IEC 27035-2:2016, Clause 7.5 - "Exercises should be clearly identified, controlled, and followed by communication plans that inform affected parties of their simulated nature." Correct answer: C
-

NEW QUESTION # 41
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 # 42
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 # 43
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 immediately informed all employees about the potential data breach
- B. No, the IRT should have determined the facts that enable detection of the event occurrence
- C. Yes, the correct action is to initiate a company-wide system shutdown until the anomaly is investigated

Answer: B

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 # 44

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. Yes. Nate included all the elements required by ISO/IEC 27035-1
- B. No, as the report did not include a comprehensive list of all employees who accessed the system within 24 hours before the incident
- 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 # 45
......

Notes

- ISO-IEC-27035-Lead-Incident-Manager Online Tests ☀ ISO-IEC-27035-Lead-Incident-Manager Study Group ⌨ Real ISO-IEC-27035-Lead-Incident-Manager Exam Answers □ Go to website ➡ www.pdfvce.com □□□ open and search for □ ISO-IEC-27035-Lead-Incident-Manager □ to download for free □ISO-IEC-27035-Lead-Incident-Manager Dumps Questions
- Pass Guaranteed Quiz Authoritative PECB - ISO-IEC-27035-Lead-Incident-Manager - PECB Certified ISO/IEC 27035 Lead Incident Manager Exam Training □ Search on ➠ www.troytecdumps.com □ for □ ISO-IEC-27035-Lead-Incident-Manager □ to obtain exam materials for free download □ISO-IEC-27035-Lead-Incident-Manager Valid Real Test
- Get High Pass-Rate ISO-IEC-27035-Lead-Incident-Manager Exam Training and Pass Exam in First Attempt □ Search for □ ISO-IEC-27035-Lead-Incident-Manager □ and easily obtain a free download on ✔ www.pdfvce.com □✔□ □ □ISO-IEC-27035-Lead-Incident-Manager Unlimited Exam Practice
- ISO-IEC-27035-Lead-Incident-Manager Latest Braindumps Sheet □ ISO-IEC-27035-Lead-Incident-Manager Dumps Collection □ ISO-IEC-27035-Lead-Incident-Manager Exam Blueprint □ Search for ☀ ISO-IEC-27035-Lead-Incident-Manager □☀□ and obtain a free download on ✔ www.prepawaypdf.com □✔□ □New ISO-IEC-27035-Lead-Incident-Manager Test Tutorial
- Pass Guaranteed Quiz Authoritative PECB - ISO-IEC-27035-Lead-Incident-Manager - PECB Certified ISO/IEC 27035 Lead Incident Manager Exam Training □ The page for free download of { ISO-IEC-27035-Lead-Incident-Manager } on 「 www.pdfvce.com 」 will open immediately □ISO-IEC-27035-Lead-Incident-Manager Online Tests
- ISO-IEC-27035-Lead-Incident-Manager Latest Braindumps Sheet □ ISO-IEC-27035-Lead-Incident-Manager Latest Dumps Ebook □ ISO-IEC-27035-Lead-Incident-Manager Study Group □ Easily obtain free download of □ ISO-IEC-27035-Lead-Incident-Manager □ by searching on ▹ www.pdfdumps.com ◃ □ISO-IEC-27035-Lead-Incident-Manager Latest Study Notes
- ISO-IEC-27035-Lead-Incident-Manager Exam Blueprint □ ISO-IEC-27035-Lead-Incident-Manager Latest Braindumps Sheet □ ISO-IEC-27035-Lead-Incident-Manager Latest Study Notes □ Simply search for ➥ ISO-IEC-27035-Lead-Incident-Manager □ for free download on [www.pdfvce.com] □ISO-IEC-27035-Lead-Incident-Manager Dumps Questions
- Pass Guaranteed Quiz Authoritative PECB - ISO-IEC-27035-Lead-Incident-Manager - PECB Certified ISO/IEC 27035 Lead Incident Manager Exam Training □ Download “ ISO-IEC-27035-Lead-Incident-Manager ” for free by simply searching on ☀ www.practicevce.com □☀□ □Exam ISO-IEC-27035-Lead-Incident-Manager Labs
- 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, 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, 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, Disposable vapes