ISO-IEC-27035-Lead-Incident-Manager Reliable Test Materials | ISO-IEC-27035-Lead-Incident-Manager Pdf Exam Dump

DOWNLOAD the newest Actual4Cert ISO-IEC-27035-Lead-Incident-Manager PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=19hGKP_PTRXZ-bbzBGQPBX4c_bZzvjmF4

If you prepare for the ISO-IEC-27035-Lead-Incident-Manager exam using our Actual4Cert testing engine, it is easy and convenient to buy. Just two steps to complete your purchase, we will send the ISO-IEC-27035-Lead-Incident-Manager product to your mailbox quickly. And you only need to download e-mail attachments to get your products.

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	• 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 3	• 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 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.

PECB ISO-IEC-27035-Lead-Incident-Manager Pdf Exam Dump - ISO-IEC-27035-Lead-Incident-Manager Study Group

Different from general education training software, our ISO-IEC-27035-Lead-Incident-Manager exam questions just need students to spend 20 to 30 hours practicing on the platform which provides simulation problems, can let them have the confidence to pass the ISO-IEC-27035-Lead-Incident-Manager exam, so little time great convenience for some workers, how efficiency it is. Time is money, in today's increasingly pay attention to efficiency, we should use time in the right place, with low time get high scores in return, the ISO-IEC-27035-Lead-Incident-Manager Latest Exam torrents are very good to do this.

PECB Certified ISO/IEC 27035 Lead Incident Manager Sample Questions (Q11-Q16):

NEW QUESTION # 11
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. Yes, it is recommended that immediate training on these topics be provided to ensure employees know how to respond correctly to phishing emails
- B. No, providing training is unnecessary; the employees' ignorance of proper procedures regarding phishing emails is a minor issue

- C. No, the IT manager should handle the incident without involving other employees

Answer: A

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 # 12
What can documenting recovery options and associated data loss/recovery timeframes assist with during incident response?

- A. Minimizing the impact on system performance
- B. Making informed decisions about containment and recovery
- C. Accelerating the incident response process

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Documenting recovery options and estimating recovery time objectives (RTOs) and data loss tolerances (Recovery Point Objectives - RPOs) is a crucial planning activity that supports decision-making during the containment and recovery phases. ISO/IEC 27035-2:2016, Clause 6.4.6 emphasizes that such documentation allows teams to:
Evaluate trade-offs between containment scope and data loss
Determine acceptable downtime for critical services
Select the most appropriate recovery strategy based on business impact
This documentation supports strategic thinking rather than rushed action, reducing the likelihood of costly decisions. It does not necessarily accelerate the process (Option C), nor is it designed to optimize performance (Option A).
Reference:
ISO/IEC 27035-2:2016, Clause 6.4.6: "Recovery planning should consider documented recovery procedures, acceptable data loss, and system downtime to support business continuity." Correct answer: B

NEW QUESTION # 13
Which document provides guidelines for planning and preparing for incident response and for learning lessons from the incident response process?

- A. ISO/IEC 27035-1
- B. ISO/IEC 27035-2
- C. ISO/IEC 27037

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-2:2016 is titled "Information security incident management - Part 2: Guidelines to plan and prepare for incident response." This document provides detailed guidance on establishing an incident response capability, planning for incident response, and implementing effective response actions. It also emphasizes the importance of post-incident analysis and lessons learned to improve future incident handling.
Key activities covered in ISO/IEC 27035-2 include:
* Planning and preparing for incident handling (e.g., policy development, roles and responsibilities)
* Establishing and training the incident response team (IRT)

* Developing communication strategies and escalation procedures
* Conducting root cause analysis and collecting lessons learned
* Applying improvements to prevent recurrence
By contrast:
* ISO/IEC 27035-1 provides high-level principles of incident management (Part 1: Principles).
* ISO/IEC 27037 relates to the handling of digital evidence and is focused more on forensic practices than incident response preparation.
Reference Extracts:
* ISO/IEC 27035-2:2016, Introduction: "This part provides guidance on the planning and preparation necessary for effective incident response and for learning lessons from incidents."
* ISO/IEC 27035-2:2016, Clause 6.5: "Lessons learned and reporting can help improve future incident response and provide input to risk assessments and control improvements."

NEW QUESTION # 14
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.
According to scenario 3, Leona decided to initially include only the elements provided in Clause 4.3 of ISO /IEC 27035-2, Information security incident management policy content, in the incident management policy.
Is this acceptable?

- A. Yes, because Leona has conducted a thorough risk assessment to identify potential gaps in the incident management policy beyond the scope of clause 4.3 of ISO/IEC 27035-2
- B. Yes, because as a minimum, the policy must cover the elements provided in clause 4.3 of ISO/IEC 27035-2
- C. No, clause 4.3 of ISO/IEC 27035-2 does not cover elements for an effective incident management policy

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Clause 4.3 of ISO/IEC 27035-2:2016 outlines the minimum content requirements for an effective incident management policy. These include:
Purpose and objectives of the policy
Scope and applicability
Roles and responsibilities
Key terminology and definitions
High-level processes for incident detection, reporting, response, and learning Obligations of internal stakeholders Leona's decision to base the initial policy draft on Clause 4.3 is fully compliant and appropriate, as it ensures foundational consistency. ISO/IEC 27035-2 explicitly states that these elements form the minimum baseline for effective policy creation, and the document can be expanded later as needed.
Reference:
ISO/IEC 27035-2:2016, Clause 4.3: "The information security incident management policy should, at a minimum, contain the following elements..." Therefore, the correct answer is B: Yes, because as a minimum, the policy must cover the elements provided in clause 4.3 of ISO/IEC 27035-2.
-

NEW QUESTION # 15
During the 'detect and report' phase of incident management at TechFlow, the incident response team began collecting detailed threat intelligence and conducting vulnerability assessments related to these login attempts.
Additionally, the incident response team classified a series of unusual login attempts as a potential security incident and distributed initial reports to the incident coordinator. Is this approach correct?

- A. No, because collecting detailed information about threats and vulnerabilities should occur in later phases
- B. No, because information security incidents cannot yet be classified as information security incidents in this phase
- C. Yes, because classifying events as information security incidents is essential during this phase

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The 'detect and report' phase, as defined in ISO/IEC 27035-1:2016 (Clause 6.2), includes the identification, classification, and initial reporting of information security events. If events meet certain thresholds-such as multiple failed login attempts from unknown IP addresses or matching threat indicators-they can and should be classified as potential incidents.
It is also appropriate to begin collecting supporting information during this phase. Gathering threat intelligence and performing basic vulnerability assessments help in confirming the scope and nature of the threat, allowing faster escalation and response.
Option B is incorrect because while deep forensic collection occurs later, preliminary data collection should begin during detection.
Option C is incorrect as incident classification is explicitly allowed and encouraged in this phase.
Reference:
ISO/IEC 27035-1:2016, Clause 6.2.2: "Events should be assessed and classified to determine whether they qualify as information security incidents." Clause 6.2.3: "All relevant details should be collected to support early classification and reporting." Correct answer: A

NEW QUESTION # 16
.....

ISO-IEC-27035-Lead-Incident-Manager study material has a high quality service team. First of all, the authors of study materials are experts in the field. They have been engaged in research on the development of the industry for many years, and have a keen sense of smell for changes in the examination direction. During your installation, ISO-IEC-27035-Lead-Incident-Manager exam questions hired dedicated experts to provide you with free remote online guidance. During your studies, ISO-IEC-27035-Lead-Incident-Manager Exam Torrent also provides you with free online services for 24 hours, regardless of where and when you are, as long as an email, we will solve all the problems for you. At the same time, if you fail to pass the exam after you have purchased ISO-IEC-27035-Lead-Incident-Manager training materials, you just need to submit your transcript to our customer service staff and you will receive a full refund.

ISO-IEC-27035-Lead-Incident-Manager □ by searching on ➠ www.practicevce.com □ □ISO-IEC-27035-Lead-Incident-Manager Valid Test Syllabus

- ISO-IEC-27035-Lead-Incident-Manager Related Exams □ ISO-IEC-27035-Lead-Incident-Manager Reliable Exam Guide □ Valid ISO-IEC-27035-Lead-Incident-Manager Exam Syllabus □ Immediately open □ www.pdfvce.com □ and search for ➽ ISO-IEC-27035-Lead-Incident-Manager □ to obtain a free download □ISO-IEC-27035-Lead-Incident-Manager Download Demo
- Why Do You Need to Trust on {PECB} PECB ISO-IEC-27035-Lead-Incident-Manager Exam Questions? □ Search for ➤ ISO-IEC-27035-Lead-Incident-Manager □ and download it for free on ☀ www.testkingpass.com □☀□ website □ □Reliable ISO-IEC-27035-Lead-Incident-Manager Exam Tips
- ISO-IEC-27035-Lead-Incident-Manager Certification Dumps - ISO-IEC-27035-Lead-Incident-Manager Study Guide Files - ISO-IEC-27035-Lead-Incident-Manager Practice Test Questions ☃ Search for 【 ISO-IEC-27035-Lead-Incident-Manager 】 on ➥ www.pdfvce.com □ immediately to obtain a free download □ISO-IEC-27035-Lead-Incident-Manager Reliable Exam Guide
- Intereactive ISO-IEC-27035-Lead-Incident-Manager Testing Engine □ ISO-IEC-27035-Lead-Incident-Manager Test Sample Online □ Valid Braindumps ISO-IEC-27035-Lead-Incident-Manager Book □ Easily obtain 【 ISO-IEC-27035-Lead-Incident-Manager 】 for free download through ▸ www.exam4labs.com ◂ □ISO-IEC-27035-Lead-Incident-Manager Test Sample Online
- willysforsale.com, building.lv, notefolio.net, 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

DOWNLOAD the newest Actual4Cert ISO-IEC-27035-Lead-Incident-Manager PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=19hGKP_PTRXZ-bbzBGQPBX4c_bZzvjmF4