Latest ISO-IEC-27035-Lead-Incident-Manager Exam Question - New ISO-IEC-27035-Lead-Incident-Manager Exam Bootcamp

DOWNLOAD the newest Exam4PDF ISO-IEC-27035-Lead-Incident-Manager PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1nUDvfuY_kthSwoLnTOFLEPj_mMZ9ekaU

The meaning of qualifying examinations is, in some ways, to prove the candidate's ability to obtain qualifications that show your ability in various fields of expertise. If you choose our ISO-IEC-27035-Lead-Incident-Manager learning guide materials, you can create more unlimited value in the limited study time, through qualifying examinations, this is our ISO-IEC-27035-Lead-Incident-Manager Real Questions and the common goal of every user, we are trustworthy helpers, so please don't miss such a good opportunity. The acquisition of ISO-IEC-27035-Lead-Incident-Manager qualification certificates can better meet the needs of users' career development.

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

Topic	Details
Topic 1	• 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 2	• 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 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.

>> Latest ISO-IEC-27035-Lead-Incident-Manager Exam Question <<

New ISO-IEC-27035-Lead-Incident-Manager Exam Bootcamp - Exam ISO-IEC-27035-Lead-Incident-Manager Actual Tests

If you purchase our study materials to prepare the ISO-IEC-27035-Lead-Incident-Manager Exam, your passing rate will be much higher than others. Also, the operation of our study material is smooth and flexible and the system is stable and powerful. You can install the ISO-IEC-27035-Lead-Incident-Manager exam guide on your computers, mobile phone and other electronic devices. There are no restrictions to the number equipment you install. In short, it depends on your own choice. We sincerely hope that you can enjoy the good service of our products.

PECB Certified ISO/IEC 27035 Lead Incident Manager Sample Questions (Q30-Q35):

NEW QUESTION # 30
What determines the frequency of reviewing an organization's information security incident management strategy?

- A. The number of employees in the organization
- B. The nature, scale, and complexity of the organization
- C. The frequency of audits conducted by external agencies

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-1:2016 Clause 7.1 explicitly states that the frequency and depth of reviewing the incident management strategy should be based on the organization's size, complexity, and threat environment. Larger or more complex environments may require more frequent reviews to remain agile and responsive.
Audit schedules (Option C) may influence timing, but they do not dictate the necessary frequency for strategic reviews. The number of employees (Option A) alone is not a sufficient factor.
Reference:
ISO/IEC 27035-1:2016 Clause 7.1: "The frequency and scope of reviews should be determined by the nature, scale, and complexity of the organization." Correct answer: B
-

NEW QUESTION # 31
Scenario 7: Located in central London, Konzolo has become a standout innovator in the cryptocurrency field.
By introducing its unique cryptocurrency, Konzolo has contributed to the variety of digital currencies and prioritized enhancing the security and reliability of its offerings.
Konzolo aimed to enhance its systems but faced challenges in monitoring the security of its own and third- party systems. These issues became especially evident during an incident that caused several hours of server downtime This downtime was primarily caused by a third-party service provider that failed to uphold strong security measures, allowing unauthorized access.
In response to this critical situation, Konzolo strengthened its information security infrastructure. The company initiated a comprehensive vulnerability scan of its cryptographic wallet software, a cornerstone of its digital currency offerings The scan revealed a critical vulnerability due to the software using outdated encryption algorithms that are susceptible to decryption by modern methods that posed a significant risk of asset exposure Noah, the IT manager, played a central role in this discovery With careful attention to detail, he documented the vulnerability and communicated the findings to the incident response team and management. Acknowledging the need for expertise in navigating the complexities of information security incident management. Konzolo welcomed Paulina to the team. After addressing the vulnerability and updating the cryptographic algorithms, they recognized the importance of conducting a thorough investigation to prevent future vulnerabilities. This marked the stage for Paulina s crucial involvement. She performed a detailed forensic analysis of the incident, employing automated and manual methods during the collection phase. Her analysis provided crucial insights into the security breach, enabling Konzolo to understand the depth of the vulnerability and the actions required to mitigate it.
Paulina also played a crucial role in the reporting phase, as her comprehensive approach extended beyond analysis. By defining clear and actionable steps for future prevention and response, she contributed significantly to developing a resilient information security incident management system based on ISO/IEC
27035-1 and 27035-2 guidelines. This strategic initiative marked a significant milestone in Konzolo's quest to strengthen its defenses against cyber threats Based on scenario 7, which phase of forensic analysis did Paulina fail to conduct correctly?

- A. Analysis
- B. Reporting

- C. Collection

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
As detailed in scenario 7 and reinforced in the previous question, Paulina began her forensic work after the system was restored-missing the critical Collection phase as defined in ISO/IEC 27043 and referenced in ISO/IEC 27035-2.
Forensic collection involves gathering volatile and non-volatile data (e.g., logs, RAM dumps, file artifacts) at the earliest possible moment in the incident lifecycle to avoid data loss. By waiting until after recovery, she likely compromised the chain of custody and the completeness of her evidence.
The scenario notes that her analysis and reporting were thorough, providing valuable insights and mitigation strategies. Thus, the failure lies in the timing and execution of the Collection phase.
Reference:
* ISO/IEC 27035-2:2016, Clause 6.4.2 and 7.2.3: "Collection activities should begin immediately upon identifying a potential incident and before recovery begins."
* ISO/IEC 27043:2015, Clause 8.2.1: "Forensic collection is critical to ensuring reliable analysis and admissible evidence." Correct answer: A
-
-

NEW QUESTION # 32
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.
Based on scenario 6, EastCyber's team established a procedure for documenting only the information security events that escalate into high-severity incidents. According to ISO/IEC 27035-1, is this approach acceptable?

- A. No, because documentation should only occur post-incident to avoid any interference with the response process
- B. The standard suggests that organizations document only events that classify as high-severity incidents
- C. No, they should use established guidelines to document events and subsequent actions when the event is classified as an information security incident

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-1:2016 clearly states that documentation is essential for all information security incidents, regardless of severity. While prioritization is necessary, the standard recommends that events meeting the threshold of an information security incident (based on classification and assessment) must be recorded, along with the corresponding actions taken.
The practice described-documenting only high-severity incidents-may result in overlooking patterns in lower-priority events that

could lead to significant issues if repeated or correlated.
Clause 6.4.5 of ISO/IEC 27035-1:2016 emphasizes that documentation should be thorough and begin from the detection phase through to response and lessons learned.
Option A is incorrect, as the standard does not permit selective documentation only for severe incidents.
Option C misrepresents the intent of documentation, which must be concurrent with or shortly after incident handling-not only post-event.
Reference:
ISO/IEC 27035-1:2016, Clause 6.4.5: "All incident information, decisions, and activities should be documented in a structured way to enable future review, learning, and audit." Clause 6.2.3: "When an event is assessed as an incident, it must be recorded along with all subsequent actions." Correct answer: B
-

NEW QUESTION # 33
Scenario 7: Located in central London, Konzolo has become a standout innovator in the cryptocurrency field.
By introducing its unique cryptocurrency, Konzolo has contributed to the variety of digital currencies and prioritized enhancing the security and reliability of its offerings.
Konzolo aimed to enhance its systems but faced challenges in monitoring the security of its own and third- party systems. These issues became especially evident during an incident that caused several hours of server downtime This downtime was primarily caused by a third-party service provider that failed to uphold strong security measures, allowing unauthorized access.
In response to this critical situation, Konzolo strengthened its information security infrastructure. The company initiated a comprehensive vulnerability scan of its cryptographic wallet software, a cornerstone of its digital currency offerings The scan revealed a critical vulnerability due to the software using outdated encryption algorithms that are susceptible to decryption by modern methods that posed a significant risk of asset exposure Noah, the IT manager, played a central role in this discovery With careful attention to detail, he documented the vulnerability and communicated the findings to the incident response team and management. Acknowledging the need for expertise in navigating the complexities of information security incident management. Konzolo welcomed Paulina to the team. After addressing the vulnerability and updating the cryptographic algorithms, they recognized the importance of conducting a thorough investigation to prevent future vulnerabilities. This marked the stage for Paulina s crucial involvement. She performed a detailed forensic analysis of the incident, employing automated and manual methods during the collection phase. Her analysis provided crucial insights into the security breach, enabling Konzolo to understand the depth of the vulnerability and the actions required to mitigate it.
Paulina also played a crucial role in the reporting phase, as her comprehensive approach extended beyond analysis. By defining clear and actionable steps for future prevention and response, she contributed significantly to developing a resilient information security incident management system based on ISO/IEC
27035-1 and 27035-2 guidelines. This strategic initiative marked a significant milestone in Konzolo's quest to strengthen its defenses against cyber threats Based on scenario 7, a vulnerability scan at Konzolo revealed a critical vulnerability in the cryptographic wallet software that could lead to asset exposure. Noah, the IT manager, documented the event and communicated it to the incident response team and management. Is this acceptable?

- A. Yes, he should document the event and communicate it to the incident response team and management
- B. No, he should have waited for confirmation of an actual asset exposure before documenting and communicating the vulnerability
- C. No, he should have postponed the documentation process until a full investigation is completed

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
According to ISO/IEC 27035-1:2016, an information security event should be documented and communicated as soon as it is identified-particularly if it has the potential to escalate into an incident. Timely documentation and escalation enable the organization to take immediate and coordinated actions, which are essential to managing risk effectively.
Clause 6.2.1 of ISO/IEC 27035-1 states that events, even before confirmation as incidents, must be logged and assessed to determine appropriate response measures. Waiting until after a breach occurs or delaying documentation may violate both internal policies and regulatory requirements, especially in high-risk domains like cryptocurrency.
Therefore, Noah's actions align fully with the recommended practices outlined in ISO/IEC 27035.
Reference:
* ISO/IEC 27035-1:2016, Clause 6.2.1: "All identified information security events should be recorded and communicated to ensure appropriate assessment and response."
* Clause 6.2.2: "Early communication and documentation are crucial to managing potential incidents effectively." Correct answer: C
-

NEW QUESTION # 34
Who is responsible for providing threat intelligence and supporting the lead investigator within an incident response team?

- A. Analysts and researchers
- B. Team leader
- C. IT support staff

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
In an Incident Response Team (IRT), analysts and researchers are responsible for threat intelligence, data analysis, malware investigation, and providing in-depth technical insights. Their work directly supports the lead investigator by identifying root causes, attack vectors, indicators of compromise (IOCs), and evaluating threat actor tactics.
According to ISO/IEC 27035-2:2016, these roles are part of the broader support functions within an IRT and are crucial for technical depth and timely resolution of incidents.
Option A (IT support staff) may provide infrastructure-level assistance but typically lacks threat analysis capabilities. Option C (team leader) oversees coordination and communication but is not the primary intelligence resource.
Reference Extracts:
ISO/IEC 27035-2:2016, Clause 7.2.3: "Support roles may include malware analysts, forensic experts, and threat intelligence researchers." ENISA CSIRT Training Guide: "Analysts contribute to ongoing investigations by identifying attack patterns and supporting mitigation decisions." Correct answer: B
-

NEW QUESTION # 35
.....

To some extent, to pass the ISO-IEC-27035-Lead-Incident-Manager exam means that you can get a good job. The ISO-IEC-27035-Lead-Incident-Manager exam materials you master will be applied to your job. The possibility to enter in big and famous companies is also raised because they need outstanding talents to serve for them. Our ISO-IEC-27035-Lead-Incident-Manager Test Prep is compiled elaborately and will help the client a lot. Our product is of high quality and the passing rate and the hit rate are both high.

- ISO-IEC-27035-Lead-Incident-Manager Exam Assessment □ Reliable ISO-IEC-27035-Lead-Incident-Manager Dumps □ Latest ISO-IEC-27035-Lead-Incident-Manager Practice Questions □ Enter ▸ www.prepawayexam.com ◂ and search for ➠ ISO-IEC-27035-Lead-Incident-Manager □ to download for free ↗ISO-IEC-27035-Lead-Incident-Manager Certification Exam Infor
- ISO-IEC-27035-Lead-Incident-Manager Exam Assessment □ ISO-IEC-27035-Lead-Incident-Manager Real Brain Dumps □ ISO-IEC-27035-Lead-Incident-Manager Real Brain Dumps □ Immediately open ▸ www.pdfvce.com ◂ and search for [ISO-IEC-27035-Lead-Incident-Manager] to obtain a free download ➡□Latest ISO-IEC-27035-Lead-Incident-Manager Exam Vce
- ISO-IEC-27035-Lead-Incident-Manager Torrent □ Reliable ISO-IEC-27035-Lead-Incident-Manager Exam Cram □ ISO-IEC-27035-Lead-Incident-Manager Certification Exam Infor □ Go to website ⇛ www.torrentvce.com ⇚ open and search for □ ISO-IEC-27035-Lead-Incident-Manager □ to download for free □New ISO-IEC-27035-Lead-Incident-Manager Test Vce Free
- ISO-IEC-27035-Lead-Incident-Manager Real Exam Questions in Three Formats □ Download ☀ ISO-IEC-27035-Lead-Incident-Manager □☀□ for free by simply entering 【 www.pdfvce.com 】 website □Latest ISO-IEC-27035-Lead-Incident-Manager Practice Questions
- Latest ISO-IEC-27035-Lead-Incident-Manager Exam Online □ ISO-IEC-27035-Lead-Incident-Manager New Cram Materials □ Reliable ISO-IEC-27035-Lead-Incident-Manager Test Cram □ Easily obtain free download of 【 ISO-IEC-27035-Lead-Incident-Manager 】 by searching on ▹ www.torrentvce.com ◃ □Exam ISO-IEC-27035-Lead-Incident-Manager Material
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, bbs.t-firefly.com, www.stes.tyc.edu.tw, Disposable vapes

What's more, part of that Exam4PDF ISO-IEC-27035-Lead-Incident-Manager dumps now are free: https://drive.google.com/open?id=1nUDvfuY_kthSwoLnTOFLEPj_mMZ9ekaU