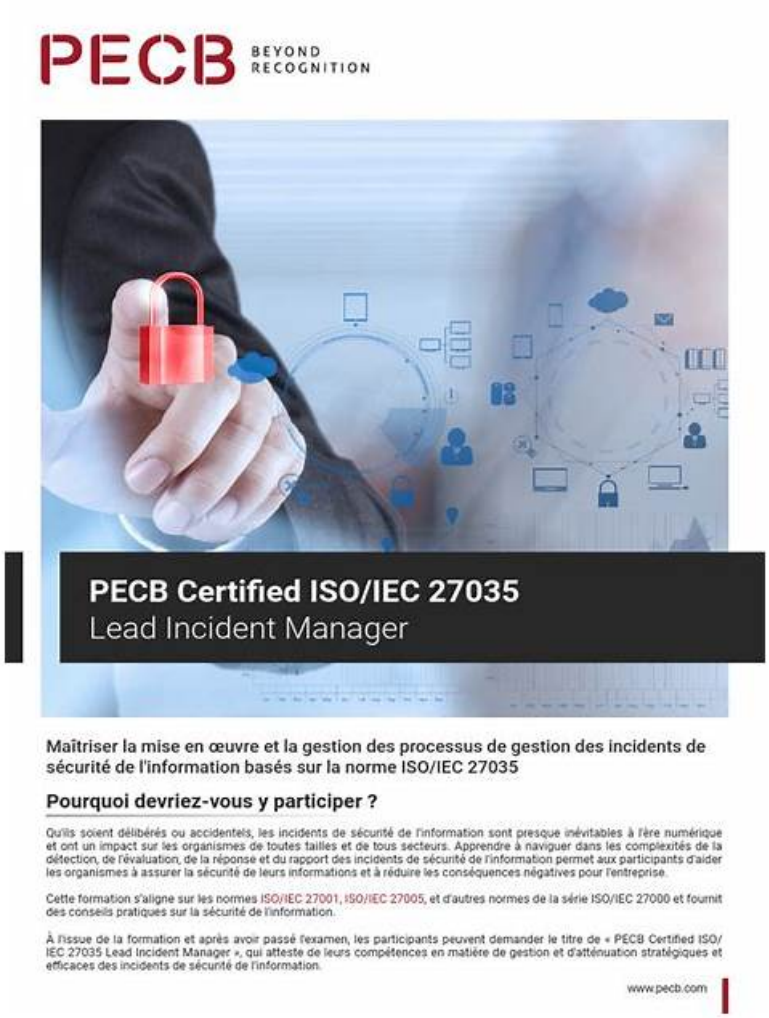
PDF ISO-IEC-27035-Lead-Incident-Manager Download & ISO-IEC-27035-Lead-Incident-Manager Valid Test Cost



The point of every question in our ISO-IEC-27035-Lead-Incident-Manager exam braindumps is set separately. Once you submit your exercises of the ISO-IEC-27035-Lead-Incident-Manager learning questions, the calculation system will soon start to work. The whole process only lasts no more than one minute. Then you will clearly know how many points you have got for your exercises of the ISO-IEC-27035-Lead-Incident-Manager study engine. And at the same time, our system will auto remember the wrong questions that you answered and give you more practice on them until you can master.

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	• 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 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	• 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.
Topic 5	• 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.

Updated PECB ISO-IEC-27035-Lead-Incident-Manager Exam Questions And Answer

Our windows software of the ISO-IEC-27035-Lead-Incident-Manager study materials are designed to simulate the real test environment. If you want to experience the real test environment, you must install our ISO-IEC-27035-Lead-Incident-Manager preparation questions on windows software. Also, it only support running on Java environment. If you do not install the system, the system of our ISO-IEC-27035-Lead-Incident-Manager Exam Braindumps will automatically download to ensure the normal operation.

PECB Certified ISO/IEC 27035 Lead Incident Manager Sample Questions (Q32-Q37):

NEW QUESTION # 32
What role does the incident coordinator play during the response phase?

- A. Coordinating the activities of IRTs and monitoring response time
- B. Assessing if the event is a potential or confirmed security incident
- C. Initiating the response actions immediately

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The incident coordinator plays a vital managerial and operational role in guiding and synchronizing the efforts of Incident Response Teams (IRTs). ISO/IEC 27035-2:2016, Clause 7.2.2 describes the role as one that involves coordination of resources, communication, and oversight to ensure that all phases of the response are executed according to procedure and within acceptable timelines.
Responsibilities include:
Assigning roles and responsibilities
Overseeing containment, eradication, and recovery efforts
Communicating with stakeholders
Tracking incident metrics and resolution progress
Initiating the response (Option B) is typically a decision taken collectively or by senior management or the IMT after classification.
Assessing the nature of an event (Option C) falls under the detection and classification phase, not the coordinator's primary role during response.
Reference:
ISO/IEC 27035-2:2016, Clause 7.2.2: "The incident coordinator is responsible for leading and coordinating the incident response

process, ensuring timely and efficient execution." Correct answer: A
-

NEW QUESTION # 33
According to ISO/IEC 27035-2, how should an organization plan the development of the incident response team capabilities?

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

Answer: C

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 # 34
Scenario 1: RoLawyers is a prominent legal firm based in Guadalajara, Mexico. It specializes in a wide range of legal services tailored to meet the diverse needs of its clients. Committed to excellence and integrity, RoLawyers has a reputation for providing legal representation and consultancy to individuals, businesses, and organizations across various sectors.
Recognizing the critical importance of information security in today's digital landscape, RoLawyers has embarked on a journey to enhance its information security measures. This company is implementing an information security incident management system aligned with ISO/IEC 27035-1 and ISO/IEC 27035-2 guidelines. This initiative aims to strengthen RoLawyers' protections against possible cyber threats by implementing a structured incident response process to provide guidance on establishing and maintaining a competent incident response team.
After transitioning its database from physical to online infrastructure to facilitate seamless information sharing among its branches, RoLawyers encountered a significant security incident. A malicious attack targeted the online database, overloading it with traffic and causing a system crash, making it impossible for employees to access it for several hours.
In response to this critical incident, RoLawyers quickly implemented new measures to mitigate the risk of future occurrences. These measures included the deployment of a robust intrusion detection system (IDS) designed to proactively identify and alert the IT security team of potential intrusions or suspicious activities across the network infrastructure. This approach empowers RoLawyers to respond quickly to security threats, minimizing the impact on their operations and ensuring the continuity of its legal services.
By being proactive about information security and incident management, RoLawyers shows its dedication to protecting sensitive data, keeping client information confidential, and earning the trust of its stakeholders.
Using the latest practices and technologies, RoLawyers stays ahead in legal innovation and is ready to handle cybersecurity threats with resilience and careful attention.
According to scenario 1, what information security incident did RoLawyers face?

- A. Man-in-the-middle attack
- B. Malware attack
- C. Denial-of-service attack

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:

According to ISO/IEC 27035-1:2016, an information security incident is any event that compromises the confidentiality, integrity, or availability of information. In this scenario, RoLawyers experienced an attack where their online database was overloaded with excessive traffic, resulting in a system crash. This incident made it impossible for employees to access the database for several hours. This type of event is characteristic of a Denial-of-Service (DoS) attack. ISO/IEC 27035-1 Annex B provides examples of typical incidents, and one example includes "network-based attacks, including denial-of-service attacks." A DoS attack typically aims to make a service or resource unavailable to its intended users by overwhelming it with traffic.
There is no indication in the scenario that the attackers were intercepting communications (as would be seen in a Man-in-the-Middle attack) or installing malware to damage or steal data. The nature of the attack- excess traffic causing a crash-clearly aligns with the definition of a DoS attack.
Reference Extracts:
ISO/IEC 27035-1:2016, Clause B.2.1 (Examples of incident types): "Denial-of-service (DoS) attacks cause disruption or degradation of services." ISO/IEC 27035-1:2016, Clause 4.1: "An incident can result from deliberate attacks such as DoS, malicious code, or unauthorized access." Therefore, the incident faced by RoLawyers was a Denial-of-Service attack.
-

NEW QUESTION # 35
Scenario 5: Located in Istanbul. Turkey. Alura Hospital is a leading medical institution specializing in advanced eye surgery and vision care. Renowned for its modern facilities, cutting edge technology, and highly skilled staff, Alura Hospital is committed to delivering exceptional patient care. Additionally, Alura Hospital has implemented the ISO/IEC 27035 standards to enhance its information security incident management practices.
At Alura Hospital, the information security incident management plan is a critical component of safeguarding patient data and maintaining the integrity of its medical services This comprehensive plan includes instructions for handling vulnerabilities discovered during incident management According to this plan, when new vulnerabilities are discovered, Mehmet is appointed as the incident handler and is authorized to patch the vulnerabilities without assessing their potential impact on the current incident, prioritizing patient data security above all else Recognizing the importance of a structured approach to incident management. Alura Hospital has established four teams dedicated to various aspects of incident response The planning team focuses on implementing security processes and communicating with external organizations The monitoring team is responsible for security patches, upgrades, and security policy implementation The analysis team adjusts risk priorities and manages vulnerability reports, while the test and evaluation team organizes and performs incident response tests to ensure preparedness During an incident management training session, staff members at Alura Hospital were provided with clear roles and responsibilities. However, a technician expressed uncertainty about their role during a data integrity incident as the manager assigned them a role unrelated to their expertise. This decision was made to ensure that all staff members possess versatile skills and are prepared to handle various scenarios effectively.
Additionally. Alura Hospital realized it needed to communicate better with stakeholders during security incidents. The hospital discovered it was not adequately informing stakeholders and that relevant information must be provided using formats, language, and media that meet their needs. This would enable them to participate fully in the incident response process and stay informed about potential risks and mitigation strategies.
Also, the hospital has experienced frequent network performance issues affecting critical hospital systems and increased sophisticated cyber attacks designed to bypass traditional security measures. So, it has deployed an external firewall. This action is intended to strengthen the hospital s network security by helping detect threats that have already breached the perimeter defenses. The firewall's implementation is a part of the hospital's broader strategy to maintain a robust and secure IT infrastructure, which is crucial for protecting sensitive patient data and ensuring the reliability of critical hospital systems. Alura Hospital remains committed to integrating state-of-the-art technology solutions to uphold the highest patient care and data security standards.
When vulnerabilities are discovered during incident management, Mehmet takes action to patch the vulnerabilities without assessing their potential impact on the current incident. Is this action in accordance with ISO/IEC 27035-2 recommendations?

- A. No, he should report the vulnerability to the incident coordinator, who will redirect the issue to the team responsible for the vulnerability
- B. Yes, vulnerabilities should be patched without assessing their potential impact on the current incident
- C. No, he should wait for a scheduled vulnerability assessment instead

Answer: A

Explanation:
Comprehensive and Detailed Explanation:
According to ISO/IEC 27035-2:2016, vulnerabilities identified during incident handling must be assessed and documented before remediation. Immediate patching without evaluating its impact could compromise incident evidence, interfere with ongoing investigations, or unintentionally trigger additional issues.
ISO/IEC 27035-2 recommends that the incident coordinator (or an equivalent role) be responsible for directing how such vulnerabilities are managed and coordinated across relevant teams. This maintains process integrity and avoids uncoordinated actions.

Reference:
ISO/IEC 27035-2:2016, Clause 6.4.2: "Detected vulnerabilities should be communicated to appropriate stakeholders for evaluation. Unauthorized immediate actions could affect incident containment or recovery efforts." Correct answer: C
-

NEW QUESTION # 36
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 According to scenario 7, what type of incident has occurred at Konzolo?

- A. High severity incident
- B. Critical severity incident
- C. Medium severity incident

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Severity classification of an incident under ISO/IEC 27035-2:2016 is determined by factors such as potential data exposure, business disruption, and impact on critical services. In this scenario, the server downtime caused by a third-party breach and a vulnerability in cryptographic wallet software-capable of leading to asset exposure-signifies serious business and operational risks. Although the vulnerability was critical, no actual asset theft or breach was confirmed. Therefore, while serious, the incident does not reach the "critical" threshold (which would typically involve data exfiltration, irreversible loss, or public impact). The appropriate classification is "High Severity." Reference:
* ISO/IEC 27035-2:2016, Clause 6.3.1: "Severity is determined by the actual or potential impact on business operations, data, reputation, and legal obligations."
* Annex A (Example Severity Levels): "High-severity incidents involve confirmed vulnerabilities with significant potential for impact, such as financial loss or regulatory violations." Correct answer: B
-

NEW QUESTION # 37
.....

Are you finding it challenging to take the PECB Certified ISO/IEC 27035 Lead Incident Manager (ISO-IEC-27035-Lead-Incident-Manager) Certification Exam due to your busy schedule? Well, worry no more! Preparing for your ISO-IEC-27035-Lead-Incident-Manager exam has become convenient and hassle-free. You can now study from the comfort of your home, without needing to attend any classes or disrupt your existing schedule. With Exam-Killer, you have access to a reliable and comprehensive source of ISO-IEC-27035-Lead-Incident-Manager Exam Questions for your PECB Certified ISO/IEC 27035 Lead Incident Manager (ISO-IEC-27035-Lead-Incident-Manager) exam, ensuring your success in the test. Let's explore how Exam-Killer can

assist you in acing your real PECB Certified ISO/IEC 27035 Lead Incident Manager (ISO-IEC-27035-Lead-Incident-Manager) quiz quickly and smoothly.

ISO-IEC-27035-Lead-Incident-Manager Valid Test Cost: https://www.exam-killer.com/ISO-IEC-27035-Lead-Incident-Manager-valid-questions.html