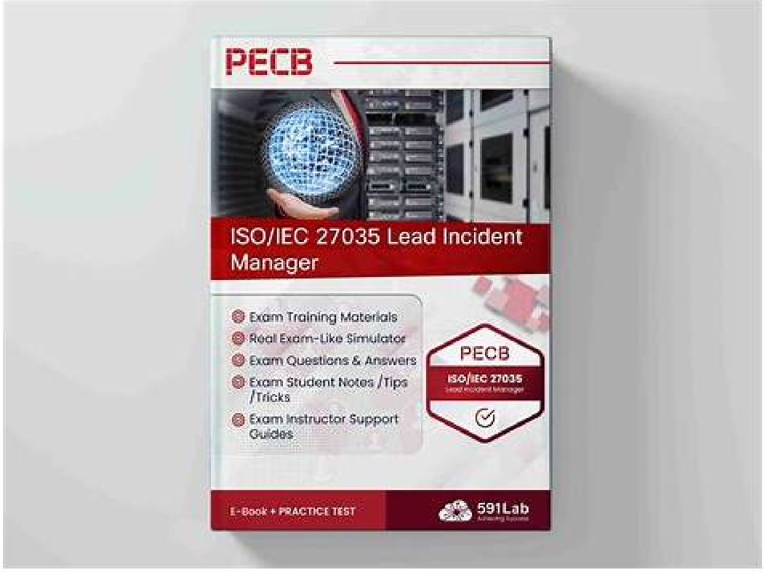
Exam ISO-IEC-27035-Lead-Incident-Manager Demo, Reliable ISO-IEC-27035-Lead-Incident-Manager Exam Online



BTW, DOWNLOAD part of ExamsLabs ISO-IEC-27035-Lead-Incident-Manager dumps from Cloud Storage: https://drive.google.com/open?id=1u7eokMTlK0Twgrg9aR3IUjB1yxhSKJLr

ISO-IEC-27035-Lead-Incident-Manager answers real questions can help candidates have correct directions and prevent useless effort. If you still lack of confidence in preparing your exam, choosing a good ISO-IEC-27035-Lead-Incident-Manager answers real questions will be a wise decision for you, it is also an economical method which is saving time, money and energy. Valid ISO-IEC-27035-Lead-Incident-Manager Answers Real Questions will help you clear exam at the first time, it will be fast for you to obtain certifications and achieve your dream.

Once you get the PECB ISO-IEC-27035-Lead-Incident-Manager certificate, you can quickly quit your current job and then change a desirable job. The PECB ISO-IEC-27035-Lead-Incident-Manager certificate can prove that you are a competent person. So it is easy for you to pass the interview and get the job. The assistance of our ISO-IEC-27035-Lead-Incident-Manager practice quiz will change your life a lot.

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

High Pass-Rate Exam ISO-IEC-27035-Lead-Incident-Manager Demo & Leading Provider in Qualification Exams & Fast Download Reliable ISO-IEC-27035-Lead-Incident-Manager Exam Online

Since our PECB Certified ISO/IEC 27035 Lead Incident Manager practice exam tracks your progress and reports results, you can review these results and strengthen your weaker concepts. We offer PECB ISO-IEC-27035-Lead-Incident-Manager desktop practice test software which works on Windows computers after installation. The web-based ISO-IEC-27035-Lead-Incident-Manager practice exam needs no plugins or software installation. Linux, iOS, Android, Windows, and Mac support the web-based PECB ISO-IEC-27035-Lead-Incident-Manager Practice Exam. Additionally, Chrome, Opera, Firefox, Safari, Internet Explorer support this PECB Certified ISO/IEC 27035 Lead Incident Manager ISO-IEC-27035-Lead-Incident-Manager web-based practice test.

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

Topic	Details

Topic 1	- 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 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	- 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.

PECB Certified ISO/IEC 27035 Lead Incident Manager Sample Questions (Q68-Q73):

NEW QUESTION # 68
Why is it important to identify all impacted hosts during the eradication phase?

- A. To enhance overall security
- B. To facilitate recovery efforts
- C. To optimize hardware performance

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
During the eradication phase of the information security incident management process, identifying all impacted hosts is essential to ensure that every element affected by the incident is addressed before proceeding to recovery. According to ISO/IEC 27035-2:2016, Clause 6.4.5, the eradication phase involves removing malware, disabling unauthorized access, and remediating vulnerabilities that led to the incident.
Identifying all impacted hosts ensures:
Comprehensive removal of malicious artifacts
Prevention of reinfection or further propagation
A smooth and complete transition into the recovery phase
This directly supports recovery planning because it helps teams understand which systems need to be restored, rebuilt, or validated.
Option B (optimizing hardware performance) is not a goal of incident management, and Option C (enhancing overall security) is a long-term objective but not the immediate goal of the eradication phase.
Reference:
ISO/IEC 27035-2:2016, Clause 6.4.5: "During eradication, it is important to identify all affected systems so that root causes and malicious components are removed prior to recovery." Correct answer: A
-

NEW QUESTION # 69
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. Collection
- B. Reporting
- C. Analysis

Answer: A

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 # 70

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.

In scenario 3, which of the following risk identification approaches was used by L&K Associates?

- A. Both A and B
- B. Event-based approach
- C. Asset-based approach

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

L&K Associates employed two distinct approaches as described in ISO/IEC 27005:2018 and referenced in ISO/IEC 27035-2:

Strategic scenario identification, which involves analyzing sources of risk and their impact on stakeholders and objectives. This is aligned with the event-based approach, which focuses on risk sources and events that may lead to incidents.

Operational scenario identification, which involves a thorough assessment of assets, threats, and vulnerabilities - aligning with the

asset-based approach, where the focus is on critical assets and the threats that may exploit their weaknesses.
ISO/IEC 27005:2018, Clause 8.2.2, identifies multiple methods for risk identification, including:
Asset-based approach
Event-based (or threat-based) approach
Vulnerability-centered approach
In this scenario, both the asset- and event-based methods were clearly applied by Leona, which is encouraged in ISO risk management practices to provide a holistic view of risk.
Therefore, the correct answer is C: Both A and B.

NEW QUESTION # 71
When does the information security incident management plan come into effect?

- A. When a new security policy is drafted
- B. When a security vulnerability is reported
- C. After a security audit is completed

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
According to ISO/IEC 27035-1 and 27035-2, the incident management plan is activated upon the detection or reporting of a security event, particularly when a vulnerability, threat, or compromise has been identified. The plan ensures structured response and accountability from the very first signs of a potential incident.
Clause 6.4.2 in ISO/IEC 27035-2 explains that incident response activities-including logging, categorization, assessment, and escalation-should begin as soon as a security incident or vulnerability is reported. This proactive trigger allows early containment and mitigation.
Security audits and policy drafts (Options A and B) are part of preventive or governance mechanisms, not operational triggers for activating the plan.
Reference Extracts:
ISO/IEC 27035-2:2016, Clause 6.4.2: "The incident management plan should be activated once a security incident or significant vulnerability is identified and reported." Clause 5.1: "Detection and reporting are the initial steps in triggering the formal incident management lifecycle." Correct answer: C

NEW QUESTION # 72
What is a key responsibility of the incident response team?

- A. Performing vulnerability scans and penetration testing
- B. Maintaining physical security infrastructure
- C. Investigating and managing cybersecurity incidents

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The primary role of an incident response team, according to ISO/IEC 27035-2:2016, is to manage and respond to information security incidents effectively. This includes tasks such as identifying, analyzing, containing, mitigating, and recovering from incidents. The goal is to minimize the impact on the organization and restore normal operations as quickly as possible.
Key responsibilities include:
Incident detection and validation
Impact assessment
Coordination of containment and eradication efforts
Communication with stakeholders
Post-incident analysis and lessons learned
While vulnerability scanning and penetration testing (option C) are important security functions, they are typically assigned to the security operations team or dedicated assessment teams - not the incident response team per se. Likewise, maintaining physical infrastructure (option A) is the responsibility of facilities management or physical security teams, not the incident response team.
Reference Extracts:
ISO/IEC 27035-2:2016, Clause 5.2 - "The incident response team is responsible for analyzing, responding to, and resolving incidents." NIST SP 800-61r2 (Computer Security Incident Handling Guide) - "An incident response team handles the investigation

and resolution of security incidents." Therefore, the correct answer is B: Investigating and managing cybersecurity incidents.Question Certainly!

NEW QUESTION # 73

......

We check the updating of PECB exam dumps everyday to make sure customer to pass the exam with latest vce dumps. Once the latest version of ISO-IEC-27035-Lead-Incident-Manager exam pdf released, our system will send it to your mail immediately. You will be allowed to free update your ISO-IEC-27035-Lead-Incident-Manager Top Questions one-year after purchased. Please feel free to contact us if you have any questions about our dumps.

Reliable ISO-IEC-27035-Lead-Incident-Manager Exam Online: https://www.examslabs.com/PECB/ISO-27001/best-ISO-IEC-27035-Lead-Incident-Manager-exam-dumps.html

- The Best Accurate Exam ISO-IEC-27035-Lead-Incident-Manager Demo, Ensure to pass the ISO-IEC-27035-Lead-Incident-Manager Exam □ Simply search for ➠ ISO-IEC-27035-Lead-Incident-Manager □ for free download on □ www.easy4engine.com □ 🈵Valid ISO-IEC-27035-Lead-Incident-Manager Test Book
- 100% Pass 2026 Fantastic ISO-IEC-27035-Lead-Incident-Manager: Exam PECB Certified ISO/IEC 27035 Lead Incident Manager Demo □ Easily obtain （ ISO-IEC-27035-Lead-Incident-Manager ） for free download through ⇛ www.pdfvce.com ⇚ □ISO-IEC-27035-Lead-Incident-Manager Actual Exams
- ISO-IEC-27035-Lead-Incident-Manager EXAM DUMPS WITH GUARANTEED SUCCESS □ Simply search for 【 ISO-IEC-27035-Lead-Incident-Manager 】 for free download on 《 www.pdfdumps.com 》 □ISO-IEC-27035-Lead-Incident-Manager Latest Dumps Book
- 2026 PECB ISO-IEC-27035-Lead-Incident-Manager –High-quality Exam Demo □ Download ✔ ISO-IEC-27035-Lead-Incident-Manager □✔□ for free by simply entering ▶ www.pdfvce.com ◀ website □ISO-IEC-27035-Lead-Incident-Manager Reliable Exam Vce
- Reliable ISO-IEC-27035-Lead-Incident-Manager Braindumps Book □ Latest ISO-IEC-27035-Lead-Incident-Manager Practice Questions □ Real ISO-IEC-27035-Lead-Incident-Manager Testing Environment □ Easily obtain free download of [ISO-IEC-27035-Lead-Incident-Manager] by searching on □ www.easy4engine.com □ □ISO-IEC-27035-Lead-Incident-Manager Actual Exams
- Real ISO-IEC-27035-Lead-Incident-Manager Testing Environment □ ISO-IEC-27035-Lead-Incident-Manager Actual Exams □ ISO-IEC-27035-Lead-Incident-Manager Actual Exams □ □ www.pdfvce.com □ is best website to obtain [ISO-IEC-27035-Lead-Incident-Manager] for free download □Reliable ISO-IEC-27035-Lead-Incident-Manager Braindumps Book
- Don't Fail ISO-IEC-27035-Lead-Incident-Manager Exam - Verified By www.vceengine.com ↩ Search on ⇛ www.vceengine.com ⇚ for □ ISO-IEC-27035-Lead-Incident-Manager □ to obtain exam materials for free download □ □Valid ISO-IEC-27035-Lead-Incident-Manager Test Book
- ISO-IEC-27035-Lead-Incident-Manager Latest Dumps Book □ Valid ISO-IEC-27035-Lead-Incident-Manager Test Book □ Latest ISO-IEC-27035-Lead-Incident-Manager Practice Questions □ 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 Latest Dumps Book
- Pass Guaranteed Quiz 2026 Newest ISO-IEC-27035-Lead-Incident-Manager: Exam PECB Certified ISO/IEC 27035 Lead Incident Manager Demo □ Simply search for ▹ ISO-IEC-27035-Lead-Incident-Manager ◃ for free download on ⇛ www.torrentvce.com ⇚ □ISO-IEC-27035-Lead-Incident-Manager Reliable Exam Vce
- Don't Fail ISO-IEC-27035-Lead-Incident-Manager Exam - Verified By Pdfvce □ Search for 「 ISO-IEC-27035-Lead-Incident-Manager 」 and easily obtain a free download on ⇛ www.pdfvce.com ⇚ □Composite Test ISO-IEC-27035-Lead-Incident-Manager Price
- Composite Test ISO-IEC-27035-Lead-Incident-Manager Price □ ISO-IEC-27035-Lead-Incident-Manager Prep Guide □ ISO-IEC-27035-Lead-Incident-Manager Exams Dumps □ Copy URL “ www.troytecdumps.com ” open and search for □ ISO-IEC-27035-Lead-Incident-Manager □ to download for free □ISO-IEC-27035-Lead-Incident-Manager Reliable Exam Vce
- 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.zazzle.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, pct.edu.pk, shortcourses.russellcollege.edu.au, Disposable vapes

P.S. Free & New ISO-IEC-27035-Lead-Incident-Manager dumps are available on Google Drive shared by ExamsLabs:

https://drive.google.com/open?id=1u7eokMTlK0Twgrg9aR3IUjB1yxhSKJLr