Web-based PECB ISO-IEC-27035-Lead-Incident-Manager Practice Exam Software - Solution for Online Self-Assessment

2026 Latest VCEDumps ISO-IEC-27035-Lead-Incident-Manager PDF Dumps and ISO-IEC-27035-Lead-Incident-Manager Exam Engine Free Share: https://drive.google.com/open?id=1cWSH8fsEcbjmkYg0smH9o1bkWIC_SZtJ

With the rapid development of the economy, the demands of society on us are getting higher and higher. If you can have ISO-IEC-27035-Lead-Incident-Manager certification, then you will be more competitive in society. Our ISO-IEC-27035-Lead-Incident-Manager study materials will help you get the according certification. Believe me, after using our ISO-IEC-27035-Lead-Incident-Manager Study Materials, you will improve your work efficiency. Our ISO-IEC-27035-Lead-Incident-Manager free training materials will make you more prominent in the labor market than others, and more opportunities will take the initiative to find you.

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	• 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 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.

>> ISO-IEC-27035-Lead-Incident-Manager Study Tool <<

ISO-IEC-27035-Lead-Incident-Manager Study Tool Exam Pass For Sure | ISO-IEC-27035-Lead-Incident-Manager: PECB Certified ISO/IEC 27035 Lead Incident Manager

Just as I have just mentioned, almost all of our customers have passed the exam as well as getting the related certification easily with the help of our ISO-IEC-27035-Lead-Incident-Manager Exam Torrent, we strongly believe that it is impossible for you to be the exception. So choosing our PECB Certified ISO/IEC 27035 Lead Incident Manager exam question actually means that you will have more opportunities to get promotion in the near future, at the same time, needless to say that you will get a raise in pay accompanied with the promotion. What's more, when you have shown your talent with PECB Certified ISO/IEC 27035 Lead Incident Manager certification in relating field, naturally, you will have the chance to enlarge your friends circle with a lot of distinguished persons who may influence you career life profoundly.

PECB Certified ISO/IEC 27035 Lead Incident Manager Sample Questions (Q65-Q70):

NEW QUESTION # 65
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 as a minimum, the policy must cover the elements provided in clause 4.3 of ISO/IEC 27035-2
- B. No, clause 4.3 of ISO/IEC 27035-2 does not cover elements for an effective incident management policy
- C. 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

Answer: A

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 # 66

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.
Based on the scenario above, answer the following question:
Considering its industry and services, is the guidance provided in ISO/IEC 27035-1 applicable for RoLawyers?

- A. No, it is specific to organizations providing incident management services
- B. No, it is specific to organizations in the information security industry
- C. Yes, it applies to all organizations, regardless of their size, type, or nature

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-1:2016 is titled "Information security incident management - Part 1: Principles of incident management". This standard provides a comprehensive framework for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving incident management within an organization.
The scope of ISO/IEC 27035-1 is explicitly broad and designed to be applicable to all organizations, regardless of their size, type, or nature, as stated in the standard's introduction and scope sections. The principles laid out in the document are intended to be flexible and scalable so that organizations from any sector can adopt and implement incident management processes suitable to their specific context.
The document clearly emphasizes that information security incidents can impact any organization that processes, stores, or transmits information digitally - including law firms like RoLawyers. The guidance addresses the creation of an incident response capability to detect, respond, and recover from information security incidents effectively.
Furthermore, the standard stresses that incident management is a vital part of maintaining information security resilience, minimizing damage, and protecting the confidentiality, integrity, and availability of information assets, which is crucial for organizations handling sensitive data, such as legal firms.
Hence, ISO/IEC 27035-1 is not limited to IT or information security service providers alone; instead, it supports any organization's need to manage information security incidents systematically. RoLawyers, given its reliance on digital data and the critical nature of its information, can and should apply the standard's principles to safeguard its assets and clients.
Reference Extracts from ISO/IEC 27035-1:2016:
* Scope (Section 1): "The principles provided in this document are intended to be applicable to all organizations, irrespective of type, size or nature."

* Introduction (Section 0.1): "Effective incident management helps organizations to reduce the consequences of incidents and limit the damage caused to information and information systems."
* General (Section 4): "This document provides guidance for establishing, implementing, operating, monitoring, reviewing, maintaining and improving incident management processes within an organization." Thus, based on ISO/IEC 27035-1, the guidance is fully applicable to RoLawyers, aligning with their objective to improve information security and incident management practices.

NEW QUESTION # 67

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.

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. 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.

Based on scenario 6, answer the following:

EastCyber decided to address vulnerabilities exploited during an incident as part of the eradication phase, to eradicate the elements of the incident. Is this approach acceptable?

- A. Addressing vulnerabilities exploited during an incident is appropriate during the eradication phase
- B. No, vulnerabilities exploited during an incident should be addressed during the containment phase
- C. No, vulnerabilities exploited during an incident should be addressed during the recovery phase

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

According to ISO/IEC 27035-1:2016 and ISO/IEC 27035-2:2016, the eradication phase of incident management is defined as the stage in which the causes and components of the incident-such as malware, unauthorized access points, or system vulnerabilities-are completely removed or neutralized.

Clause 6.4.5 of ISO/IEC 27035-2 clearly outlines that the eradication phase includes actions to eliminate the root causes of incidents, which may include fixing exploited vulnerabilities and removing malicious code.

This ensures that the underlying issues that allowed the incident to occur are effectively resolved, reducing the risk of recurrence.

While containment aims to limit the damage and prevent the spread of an incident, it is not intended for remediation of vulnerabilities.

Similarly, the recovery phase focuses on restoring services and returning systems to normal operations after the threat has been eradicated.

Reference Extracts:

ISO/IEC 27035-2:2016, Clause 6.4.5: "The eradication phase includes removing the root cause of the incident (e.g., patching vulnerabilities, deleting malware, and closing open ports)." Clause 6.4.3: "Containment is primarily focused on limiting the scope and impact, not resolving root causes." Correct answer: A

NEW QUESTION # 68

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 identify the differences between current processes and company policies
- C. To assess risks associated with identified gaps in current practices compared to best practices

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 # 69
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 information security incidents cannot yet be classified as information security incidents in this phase
- B. No, because collecting detailed information about threats and vulnerabilities should occur in later phases
- 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 # 70
......

Forum □ New ISO-IEC-27035-Lead-Incident-Manager Exam Pass4sure □ Search for ☀ ISO-IEC-27035-Lead-Incident-Manager □☀□ and download exam materials for free through ✔ www.prep4sures.top □✔□ □New ISO-IEC-27035-Lead-Incident-Manager Exam Pass4sure

- Quiz 2026 High-quality ISO-IEC-27035-Lead-Incident-Manager: PECB Certified ISO/IEC 27035 Lead Incident Manager Study Tool □ Search for ⇛ ISO-IEC-27035-Lead-Incident-Manager ⇚ and download it for free on （ www.pdfvce.com ） website □Study ISO-IEC-27035-Lead-Incident-Manager Dumps
- Quiz 2026 Useful PECB ISO-IEC-27035-Lead-Incident-Manager: PECB Certified ISO/IEC 27035 Lead Incident Manager Study Tool □ Immediately open ⇛ www.prepawaypdf.com ⇚ and search for ➤ ISO-IEC-27035-Lead-Incident-Manager □ to obtain a free download ⌛Reliable ISO-IEC-27035-Lead-Incident-Manager Test Question
- Exam ISO-IEC-27035-Lead-Incident-Manager Voucher □ ISO-IEC-27035-Lead-Incident-Manager Exam Consultant □ Exam ISO-IEC-27035-Lead-Incident-Manager Voucher ⌚ Immediately open （ www.pdfvce.com ） and search for { ISO-IEC-27035-Lead-Incident-Manager } to obtain a free download □Reliable ISO-IEC-27035-Lead-Incident-Manager Test Question
- Pass Guaranteed 2026 PECB Accurate ISO-IEC-27035-Lead-Incident-Manager: PECB Certified ISO/IEC 27035 Lead Incident Manager Study Tool □ Go to website ➽ www.practicevce.com □ open and search for ➥ ISO-IEC-27035-Lead-Incident-Manager □ to download for free □ISO-IEC-27035-Lead-Incident-Manager Test Braindumps
- 100% Pass Quiz Unparalleled PECB - ISO-IEC-27035-Lead-Incident-Manager Study Tool □ Open website ➥ www.pdfvce.com □ and search for ⇛ ISO-IEC-27035-Lead-Incident-Manager ⇚ for free download □Reliable ISO-IEC-27035-Lead-Incident-Manager Test Question
- PECB - Useful ISO-IEC-27035-Lead-Incident-Manager Study Tool □ Copy URL □ www.testkingpass.com □ open and search for 《 ISO-IEC-27035-Lead-Incident-Manager 》 to download for free □Download ISO-IEC-27035-Lead-Incident-Manager Demo
- interviewmeclasses.com, rhinotech.cc:88, www.stes.tyc.edu.tw, tinnitusheal.com, blogfreely.net, bbs.t-firefly.com, studyzonebd.com, 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, bbs.t-firefly.com, getitedu.com, Disposable vapes

2026 Latest VCEDumps ISO-IEC-27035-Lead-Incident-Manager PDF Dumps and ISO-IEC-27035-Lead-Incident-Manager Exam Engine Free Share: https://drive.google.com/open?id=1cWSH8fsEcbjmkYg0smH9o1bkWlC_SZtJ