New ISO-IEC-27035-Lead-Incident-Manager Exam Vce & New ISO-IEC-27035-Lead-Incident-Manager Exam Test

2026 Latest Getcertkey 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=1YzIGlz3WJL6_rIAL8WRZe0TAI7cKSdRM

Our ISO-IEC-27035-Lead-Incident-Manager guide torrent boosts 98-100% passing rate and high hit rate. Our PECB Certified ISO/IEC 27035 Lead Incident Manager test torrent use the certificated experts and our questions and answers are chosen elaborately and based on the real exam according to the past years' exam papers and the popular trend in the industry. The language of our ISO-IEC-27035-Lead-Incident-Manager study torrent is easy to be understood and the content has simplified the important information. Our product boosts the function to simulate the exam, the timing function and the self-learning and the self-assessment functions to make the learners master the ISO-IEC-27035-Lead-Incident-Manager Guide Torrent easily and in a convenient way. Based on the plenty advantages of our product, you have little possibility to fail in the exam.

With the best quality and high accuracy, our ISO-IEC-27035-Lead-Incident-Manager vce braindumps are the best study materials for the certification exam among the dumps vendors. Our experts constantly keep the pace of the current exam requirement for ISO-IEC-27035-Lead-Incident-Manager Actual Test to ensure the accuracy of our questions. The pass rate of our ISO-IEC-27035-Lead-Incident-Manager exam dumps almost reach to 98% because our questions and answers always updated according to the latest exam information.

>> New ISO-IEC-27035-Lead-Incident-Manager Exam Vce <<

High Pass-Rate New ISO-IEC-27035-Lead-Incident-Manager Exam Vce & Effective New ISO-IEC-27035-Lead-Incident-Manager Exam Test & Practical ISO-IEC-27035-Lead-Incident-Manager Latest Test Vce

According to the research of the past exams and answers, Getcertkey provide you the latest PECB ISO-IEC-27035-Lead-Incident-Manager exercises and answers, which have have a very close similarity with real exam. Getcertkey can promise that you can 100% pass your first time to attend PECB Certification ISO-IEC-27035-Lead-Incident-Manager Exam.

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	• 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 3	• 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 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	• 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.

PECB Certified ISO/IEC 27035 Lead Incident Manager Sample Questions (Q74-Q79):

NEW QUESTION # 74
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 # 75
Scenario 2: NoSpace, a forward-thinking e-commerce store based in London, is renowned for its diverse products and advanced technology. To enhance its information security, NoSpace implemented an ISMS according to ISO/IEC 27001 to better protect customer data and ensure business continuity. Additionally, the company adopted ISO/IEC 27035-1 and ISO/IEC 27035-2 guidelines. Mark, the incident manager at NoSpace, strategically led the entire implementation. He played a crucial role in aligning the company's ISMS with the requirements specified in ISO/IEC 27001, using ISO/IEC 27035-1 guidelines as the foundation.
During a routine internal audit, a minor anomaly was detected in the data traffic that could potentially indicate a security threat. Mark was immediately notified to assess the situation. Then, Mark and his team immediately escalated the incident to crisis management to handle the potential threat without further assessment. The decision was made to ensure a swift response.
After resolving the situation, Mark decided to update the incident management process. During the initial phase of incident management, Mark recognized the necessity of updating NoSpace's information security policies. This included revising policies related to risk management at the organizational level as well as for specific systems, services, or networks. The second phase of the updated incident management process included the assessment of the information associated with occurrences of information security events and the importance of classifying events and vulnerabilities as information security incidents. During this phase, he also introduced a "count down" process to expedite the evaluation and classification of occurrences, determining whether they should be recognized as information security incidents.
Mark developed a new incident management policy to enhance the organization's resilience and adaptability in handling information security incidents. Starting with a strategic review session with key stakeholders, the team prioritized critical focus areas over less impactful threats, choosing not to include all potential threats in the policy document. This decision was made to keep the policy streamlined and actionable, focusing on the most significant risks identified through a risk assessment. The policy was shaped by integrating feedback from various department heads to ensure it was realistic and enforceable. Training and awareness initiatives were tailored to focus only on critical response roles, optimizing resource allocation and focusing on essential capabilities.
Based on the scenario above, answer the following question:
Do the actions taken by the IRT of NoSpace upon detecting the anomaly align with the objectives of a structured approach to incident management?

- A. No, escalating a minor anomaly directly to crisis management without further assessment deviates from the objectives of a structured incident management approach, which typically reserves crisis management for more severe, crisis-level situations
- B. No, the actions taken by the IRT do not align with structured incident management objectives because they failed to utilize external resources immediately
- C. Yes, escalating all incidents to crisis management regardless of severity and focusing solely on the crisis management process aligns with the objectives

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
According to ISO/IEC 27035-1:2016, a structured approach to incident management involves a phased and deliberate process: detect and report, assess and decide, respond, and learn lessons. Each phase has specific objectives, especially the "Assess and Decide" phase, which is critical in determining whether an event is a real security incident and what level of response it necessitates. The decision by NoSpace's IRT to escalate a minor anomaly directly to crisis management without performing a structured assessment contradicts this methodology. Crisis management is typically reserved for severe incidents that have already been assessed and confirmed to be of high impact.
Escalating prematurely not only bypasses the formal classification and analysis phase but also risks wasting resources and causing unnecessary alarm. ISO/IEC 27035-1, Clause 6.2.3, specifically outlines that incidents must first be categorized and assessed to determine their significance before involving higher-level response mechanisms such as crisis management.
Reference Extracts:
ISO/IEC 27035-1:2016, Clause 6.2.2: "Assess and decide involves analyzing reported events to determine whether they are to be classified as incidents, and how they should be handled." ISO/IEC 27035-2:2016, Clause 6.4: "Crisis management should be triggered only in cases of major incidents where organizational impact is high." Therefore, the correct answer is A: No, escalating a minor anomaly directly to crisis management without further assessment deviates from the objectives of a structured incident management approach.
-

NEW QUESTION # 76
Which team has a broader cybersecurity role, including incident response, monitoring, and overseeing general operations?

- A. Security Operations Center (SOC)
- B. Computer Emergency Response Team (CERT)
- C. Computer Security Incident Response Team (CSIRT)

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
According to ISO/IEC 27035 and industry best practices, a Security Operations Center (SOC) is the central hub for an organization's cybersecurity operations. Its responsibilities go beyond pure incident response.
SOCs continuously monitor the organization's network and systems for suspicious activity and threats, providing real-time threat detection, incident response coordination, vulnerability management, and overall security infrastructure oversight.
While CSIRTs and CERTs specialize in handling and managing security incidents, their roles are generally more narrowly focused on the detection, reporting, and resolution of security events. SOCs, on the other hand, manage the broader spectrum of operations, including:
Real-time monitoring and logging
Threat hunting and intelligence
Security incident analysis and triage
Coordinating CSIRT activities
Supporting policy compliance and auditing
Integration with vulnerability management and security infrastructure
Reference Extracts:
ISO/IEC 27035-2:2016, Clause 7.3.1: "Monitoring systems and activities should be established, operated and maintained to identify deviations from normal behavior." NIST SP 800-61 Revision 2 and industry alignment with ISO/IEC 27035 recognize the SOC as the broader operational environment that houses or interacts with the CSIRT/CERT.
Therefore, the correct answer is: B - Security Operations Center (SOC)
-

NEW QUESTION # 77
According to scenario 4, what is the next action ORingo should take to prevent escalation when conducting exercises?

- A. Wait until the exercise is completed to clarify the situation with all parties involved
- B. Inform all participants and external entities involved that this was a simulated scenario and not a real threat immediately
- C. Proceed with the exercise as planned, considering this as a part of the learning process

Answer: B

Explanation:
Comprehensive and Detailed Explanation:
According to ISO/IEC 27035-2:2016, incident response exercises (including simulations such as phishing campaigns) must be carefully controlled to avoid confusion, escalation, or reputational damage. If an exercise is misunderstood by employees or external parties, it could lead to unintended consequences including external escalation, customer concern, or media involvement.
The best practice is to ensure that all involved-especially external stakeholders-are informed as soon as possible if they are exposed to simulated elements. Transparency ensures the organization maintains trust and mitigates potential fallout. This is part of effective communication during planned exercises.
Reference:
ISO/IEC 27035-2:2016, Clause 7.5 - "Exercises should be clearly identified, controlled, and followed by communication plans that inform affected parties of their simulated nature." Correct answer: C
-

NEW QUESTION # 78
Scenario 2: NoSpace, a forward-thinking e-commerce store based in London, is renowned for its diverse products and advanced technology. To enhance its information security, NoSpace implemented an ISMS according to ISO/IEC 27001 to better protect customer data and ensure business continuity. Additionally, the company adopted ISO/IEC 27035-1 and ISO/IEC 27035-2 guidelines. Mark, the incident manager at NoSpace, strategically led the entire implementation. He played a crucial role in aligning the company's ISMS with the requirements specified in ISO/IEC 27001, using ISO/IEC 27035-1 guidelines as the foundation.
During a routine internal audit, a minor anomaly was detected in the data traffic that could potentially indicate a security threat. Mark was immediately notified to assess the situation. Then, Mark and his team immediately escalated the incident to crisis management to handle the potential threat without further assessment. The decision was made to ensure a swift response.
After resolving the situation, Mark decided to update the incident management process. During the initial phase of incident management, Mark recognized the necessity of updating NoSpace's information security policies. This included revising policies related to risk management at the organizational level as well as for specific systems, services, or networks. The second phase of the

updated incident management process included the assessment of the information associated with occurrences of information security events and the importance of classifying events and vulnerabilities as information security incidents. During this phase, he also introduced a 'count down' process to expedite the evaluation and classification of occurrences, determining whether they should be recognized as information security incidents.
Mark developed a new incident management policy to enhance the organization's resilience and adaptability in handling information security incidents. Starting with a strategic review session with key stakeholders, the team prioritized critical focus areas over less impactful threats, choosing not to include all potential threats in the policy document. This decision was made to keep the policy streamlined and actionable, focusing on the most significant risks identified through a risk assessment. The policy was shaped by integrating feedback from various department heads to ensure it was realistic and enforceable. Training and awareness initiatives were tailored to focus only on critical response roles, optimizing resource allocation and focusing on essential capabilities.
Based on scenario 2, was Mark's information security incident management policy appropriately developed?

- A. Yes, the information security incident management policy was appropriately developed
- B. No, the purpose of the information security incident management policy was not appropriately defined, as it failed to address all potential threats
- C. No, he should have outlined any awareness and training initiatives within the organization that are related to incident management

Answer: A

Explanation:
-
Comprehensive and Detailed Explanation From Exact Extract:
Yes, Mark's approach to developing NoSpace's information security incident management policy was aligned with the structured guidelines outlined in ISO/IEC 27035-1 and ISO/IEC 27035-2. These standards emphasize the importance of establishing an effective and realistic policy framework that supports the identification, management, and learning from information security incidents.
ISO/IEC 27035-1:2016, Clause 6.1, outlines the core components of the "Prepare" phase of the incident management lifecycle. A well-developed incident management policy should:
* Define the purpose, scope, and applicability of the policy
* Focus on critical assets and threats identified through a formal risk assessment
* Be shaped by stakeholder input
* Be realistic, enforceable, and capable of being integrated across departments
* Include training and awareness tailored to relevant personnel
In this scenario, Mark held a strategic session with stakeholders, ensured the policy was risk-based, and tailored training initiatives to critical roles only - which aligns precisely with ISO guidance on optimizing resource allocation and ensuring enforceability.
Option A is incorrect because the scenario clearly states that Mark implemented training and awareness initiatives tailored to critical response roles, which meets ISO/IEC 27035-1 expectations.
Option B is incorrect because ISO/IEC 27035-1 emphasizes prioritization of high-risk threats rather than attempting to address all potential threats equally. A focused and actionable policy that targets the most significant risks is more practical and aligns with international best practices.
Reference Extracts:
* ISO/IEC 27035-1:2016, Clause 6.1: "The preparation phase should include the definition of incident management policy, development of procedures, and awareness/training initiatives."
* ISO/IEC 27035-2:2016, Clause 5.1: "The policy should be concise, focused on relevant threats, and shaped by organizational structure and risk appetite."
* ISO/IEC 27001:2022, Annex A.5.25 & A.5.27: "Clear roles, responsibilities, and awareness should be assigned and supported through training."
Therefore, the correct answer is: C. Yes, the information security incident management policy was appropriately developed.

NEW QUESTION # 79
.....

- Pass Guaranteed PECB ISO-IEC-27035-Lead-Incident-Manager - PECB Certified ISO/IEC 27035 Lead Incident Manager Marvelous New Exam Vce □ Easily obtain ▸ ISO-IEC-27035-Lead-Incident-Manager ◂ for free download through ➡ www.practicevce.com □□□ □ISO-IEC-27035-Lead-Incident-Manager Latest Test Simulations
- Pass Guaranteed PECB ISO-IEC-27035-Lead-Incident-Manager - PECB Certified ISO/IEC 27035 Lead Incident Manager Marvelous New Exam Vce □ Search for ✔ ISO-IEC-27035-Lead-Incident-Manager □✔□ and easily obtain a free download on （ www.pdfvce.com ） □Free ISO-IEC-27035-Lead-Incident-Manager Sample
- Selecting New ISO-IEC-27035-Lead-Incident-Manager Exam Vce - Say Goodbye to PECB Certified ISO/IEC 27035 Lead Incident Manager □ Enter 《 www.prepawaypdf.com 》 and search for ▹ ISO-IEC-27035-Lead-Incident-Manager ◃ to download for free □ISO-IEC-27035-Lead-Incident-Manager Test Pdf
- Dumps ISO-IEC-27035-Lead-Incident-Manager Guide □ ISO-IEC-27035-Lead-Incident-Manager Latest Test Simulations □ ISO-IEC-27035-Lead-Incident-Manager Certification Exam Cost □ Download ☀ ISO-IEC-27035-Lead-Incident-Manager □☀□ for free by simply entering 《 www.pdfvce.com 》 website □Online ISO-IEC-27035-Lead-Incident-Manager Version
- Free ISO-IEC-27035-Lead-Incident-Manager Sample □ ISO-IEC-27035-Lead-Incident-Manager Test Pdf □ ISO-IEC-27035-Lead-Incident-Manager Free Braindumps □ Simply search for 《 ISO-IEC-27035-Lead-Incident-Manager 》 for free download on 【 www.examdiscuss.com 】 □ISO-IEC-27035-Lead-Incident-Manager Certification Practice
- Pass Guaranteed PECB ISO-IEC-27035-Lead-Incident-Manager - PECB Certified ISO/IEC 27035 Lead Incident Manager Marvelous New Exam Vce □ Search for □ ISO-IEC-27035-Lead-Incident-Manager □ and download it for free on [www.pdfvce.com] website □Latest ISO-IEC-27035-Lead-Incident-Manager Exam Fee
- Selecting New ISO-IEC-27035-Lead-Incident-Manager Exam Vce - Say Goodbye to PECB Certified ISO/IEC 27035 Lead Incident Manager □ Search for 【 ISO-IEC-27035-Lead-Incident-Manager 】 and download it for free on ➥ www.pdfdumps.com □ website □ISO-IEC-27035-Lead-Incident-Manager Certification Practice
- Test ISO-IEC-27035-Lead-Incident-Manager Dumps Demo □ ISO-IEC-27035-Lead-Incident-Manager Certification Practice □ ISO-IEC-27035-Lead-Incident-Manager Passed □ Copy URL ➡ www.pdfvce.com □□□ open and search for ▹ ISO-IEC-27035-Lead-Incident-Manager ◃ to download for free □ISO-IEC-27035-Lead-Incident-Manager Passed
- You Can Never Think About Failure With PECB ISO-IEC-27035-Lead-Incident-Manager Exam Dumps □ Simply search for " ISO-IEC-27035-Lead-Incident-Manager " for free download on ✔ www.testkingpass.com □✔□ □ISO-IEC-27035-Lead-Incident-Manager Exam Questions Vce
- Free ISO-IEC-27035-Lead-Incident-Manager Sample □ ISO-IEC-27035-Lead-Incident-Manager Reliable Test Book □ ISO-IEC-27035-Lead-Incident-Manager Test Pdf □ Easily obtain ⇛ ISO-IEC-27035-Lead-Incident-Manager ⇚ for free download through （ www.pdfvce.com ） ♣ISO-IEC-27035-Lead-Incident-Manager Certification Exam Cost
- Online ISO-IEC-27035-Lead-Incident-Manager Version □ Dumps ISO-IEC-27035-Lead-Incident-Manager Guide □ ISO-IEC-27035-Lead-Incident-Manager Free Braindumps □ Search for ➽ ISO-IEC-27035-Lead-Incident-Manager □ □ and download it for free on □ www.prepawaypdf.com □ website □ISO-IEC-27035-Lead-Incident-Manager Exam Simulations
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, lms.ait.edu.za, www.stes.tyc.edu.tw, study.stcs.edu.np, lms.ait.edu.za, www.thingstogetme.com, www.4shared.com, www.stes.tyc.edu.tw, Disposable vapes

2026 Latest Getcertkey 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=1YzIGlz3WJL6_rIAL8WRZe0TAI7cKSdRM