ISO-IEC-27035-Lead-Incident-Manager Test Prep & ISO-IEC-27035-Lead-Incident-Manager Reliable Exam Registration

PECB

BEYOND RECOGNITION

Professional Evaluation and Certification Board

hereby attests that

Ernestas Lipnickas

is awarded the title

PECB Certified ISO/IEC 27035 Lead Incident Manager

having met all the certification requirements, including all examination requirements, professional experience and adoption of the PECB Code of Ethics

Certificate Number: ISIMLM1030239-2022-10
Issue Date: 2022-10-24
This certificate is valid for three years for the purpose of PECB certification

Carolina Cabezas
Chief Compliance Officer

DOWNLOAD the newest DumpsValid ISO-IEC-27035-Lead-Incident-Manager PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1rL9zt8DZwMRmOwWoikH0Q-G_tDYM3tI6

DumpsValid PECB ISO-IEC-27035-Lead-Incident-Manager exam dumps are the best reference materials. DumpsValid test questions and answers are the training materials you have been looking for. This is a special IT exam dumps for all candidates. DumpsValid pdf real questions and answers will help you prepare well enough for PECB ISO-IEC-27035-Lead-Incident-Manager test in the short period of time and pass your exam successfully. If you don't want to waste a lot of time and efforts on the exam, you had better select DumpsValid PECB ISO-IEC-27035-Lead-Incident-Manager Dumps. Using this certification training dumps can let you improve the efficiency of your studying so that it can help you save much more time.

What do you think of using DumpsValid PECB ISO-IEC-27035-Lead-Incident-Manager Exam Dumps? DumpsValid PECB ISO-IEC-27035-Lead-Incident-Manager certification training dumps, it may be said, is the most excellent reference materials among all exam-related reference materials. Why? There are four reasons in the following. Firstly, DumpsValid exam dumps are researched by IT experts who used their experience for years and can figure out accurately the scope of the examinations. Secondly, DumpsValid exam dumps conclude all questions that can appear in the real exam. Thirdly, DumpsValid exam dumps ensures the candidate will pass their exam at the first attempt. If the candidate fails the exam, DumpsValid will give him FULL REFUND. Fourthly, DumpsValid exam dumps have two versions: PDF and SOFT version. With the two versions, the candidates can pass their exam with ease.

>> ISO-IEC-27035-Lead-Incident-Manager Test Prep <<

ISO-IEC-27035-Lead-Incident-Manager Reliable Exam Registration, ISO-IEC-27035-Lead-Incident-Manager Exams Training

On each attempt, the PECB ISO-IEC-27035-Lead-Incident-Manager practice test questions taker will provide a score report. With this report, one can find mistakes and remove them for the final attempt. A situation that the web-based test creates is similar to the ISO-IEC-27035-Lead-Incident-Manager Real Exam Questions. Practicing in this situation will help you kill PECB Certified ISO/IEC 27035 Lead Incident Manager (ISO-IEC-27035-Lead-Incident-Manager) exam anxiety. The customizable feature of this format allows you to change the settings of the PECB Certified ISO/IEC 27035 Lead Incident Manager (ISO-IEC-27035-Lead-Incident-Manager) practice 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	• 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 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 (Q14-Q19):

NEW QUESTION # 14

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.
Scenario 6: EastCyber has established itself as a premier cybersecurity 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.
Based on the scenario above, answer the following question:
While implementing monitoring protocols, Mike ensured that every device within the company's purview was under constant surveillance. Is this a recommended practice?

- A. No, Mike should have focused on the essential components to reduce the clutter and noise in the data collected
- B. Yes. Mike defined the objective of network monitoring correctly
- C. No, Mike should have focused on new devices, as they are more likely to have undetected vulnerabilities

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
According to ISO/IEC 27035-2:2016, Clause 7.3.2, implementing continuous monitoring across all critical assets and endpoints is a key component of proactive incident detection. Organizations are encouraged to establish real-time detection mechanisms that allow prompt identification of unauthorized or abnormal behavior.
Mike's approach-ensuring all systems are under constant surveillance-is consistent with this recommendation. Comprehensive monitoring allows the early identification of security events that may otherwise go unnoticed, especially in environments where advanced persistent threats (APTs) or insider threats are concerns.
While focusing only on new devices or limiting monitoring to certain components may reduce noise, it creates gaps in coverage and increases the risk of missed threats.
Reference:
ISO/IEC 27035-2:2016, Clause 7.3.2: "Monitoring systems and activities should be established and maintained to detect deviations that may indicate a security incident." ISO/IEC 27001:2022, Control A.5.28: "Monitoring systems should cover all devices that process or store sensitive information." Correct answer: A
-

NEW QUESTION # 15
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.
Based on scenario 3, did Leona follow all the ISO/IEC 27035-1 guidelines when communicating the information security incident management policy to interested parties?

- A. No, she should also communicate the incident reporting procedures and specify the appropriate contact for further information
- B. Yes, she effectively communicated the outcomes of incidents and strategies to minimize recurrence, meeting the necessary communication requirements
- C. No, she should also communicate how often the information security incident policies are updated and revised

Answer: A

Explanation:
Comprehensive and Detailed Explanation:
According to ISO/IEC 27035-1:2016, effective communication of the incident management policy must include not only policy content, roles, and responsibilities but also specific procedural aspects-such as how to report an incident and who to contact. This ensures that all stakeholders clearly understand their responsibilities in the event of an incident and know how to respond.
In the scenario, Leona communicated the outcomes of incidents, mitigation strategies, personnel obligations, and policy content. However, she did not include the incident reporting procedures or contact points, which are essential components of incident communication as per ISO guidelines.
Reference:
ISO/IEC 27035-1:2016, Clause 6.1: "Communication of the incident management policy should include reporting channels, escalation contacts, and policy revision frequency." Therefore, the correct answer is B.
-

NEW QUESTION # 16
Which action is NOT involved in the process of improving controls in incident management?

- A. Updating the incident management policy
- B. Documenting risk assessment results
- C. Implementing new or updated controls

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Improving controls in incident management is a proactive activity focused on directly adjusting and strengthening existing defenses. As per ISO/IEC 27035-2:2016, Clause 7.4, this process typically involves identifying deficiencies, updating or implementing new technical or procedural controls, and revising policies.
While risk assessments inform control decisions, simply documenting their results does not constitute direct improvement of controls. Hence, Option A is not part of the control improvement process itself.
Reference:
ISO/IEC 27035-2:2016 Clause 7.4: "Actions to improve controls include analyzing causes of incidents and updating procedures and policies accordingly." Correct answer: A
-

NEW QUESTION # 17
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, did Mark follow the guidelines of ISO/IEC 27035 series regarding the incident management phases in the updated incident management process?

- A. Yes, all phases of the incident management process were established according to the ISO/IEC 27035-1 guidelines
- B. No, the second phase of the incident management process should include the collection of information associated with the occurrences of information security events
- C. No, the decision on whether to classify events as information security incidents should be assessed before initiating the incident management process

Answer: B

Explanation:
-
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-1:2016 outlines a structured five-phase approach to information security incident management, which includes:
1. Prepare
2. Identify (or detect and report)
3. Assess and Decide
4. Respond
5. Lessons Learned
According to the standard, the "Assess and Decide" phase must include the collection, review, and analysis of information associated with the occurrence of a potential incident. This phase ensures that the organization bases its classification decisions on factual data and contextual analysis, allowing the organization to determine whether the event should be categorized as a formal security incident.
In the scenario, Mark does introduce an accelerated "count down" process to evaluate and classify incidents, which is a commendable improvement in efficiency. However, there is no mention of gathering or documenting the actual event data prior to classification. This oversight fails to fully align with the standard.

Option A is incorrect because not all phases were implemented as defined-specifically, phase 3 ("Assess and Decide") lacks an essential component: the collection of evidence/information from the anomaly or event.
Option C is also incorrect. According to ISO/IEC 27035, assessment and classification take place within the formal incident management process-not before it. The initiation of the process includes the evaluation of whether a security event becomes an incident.
Reference Extracts:
* ISO/IEC 27035-1:2016, Clause 6.2.2: "The assessment and decision process involves analyzing the information associated with reported events to decide whether they should be treated as incidents."
* ISO/IEC 27035-2:2016, Clause 7.3: "This phase includes collecting information from available sources...
such as logs, reports, and alerts, to support classification and response decisions." Therefore, the correct answer is B: No, the second phase of the incident management process should include the collection of information associated with the occurrences of information security events.

NEW QUESTION # 18
What is the purpose of incident categorization within the incident management lifecycle?

- A. To sort incidents based on the disrupted IT or business domain
- B. To determine the priority of incidents
- C. To automatically assign incidents to technicians

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
According to ISO/IEC 27035-1:2016 and ISO/IEC 27035-2:2016, incident categorization is a vital step in the incident management lifecycle. Its primary purpose is to sort and group incidents based on specific criteria so that appropriate actions and escalation paths can be taken.
One of the core objectives of categorization is to sort incidents by the domain or system affected - whether it' s a database, email system, network, or physical server. This enables organizations to assign incidents to relevant subject matter experts and apply the right procedures, based on the affected business function or IT component.
While categorization can influence prioritization (option A), the main intent is classification based on nature and domain. Automatic technician assignment (option B) may be supported by some service management platforms but is not the foundational purpose of incident categorization under ISO 27035.
Reference Extracts:
ISO/IEC 27035-1:2016, Clause 6.1.2 - "Categorization should identify the domain or component affected to enable appropriate response and escalation." ISO/IEC 27035-2:2016, Clause 7.3 - "Incidents should be categorized based on the type of disruption they cause and the business or technical domain they impact." Therefore, the correct answer is C: To sort incidents based on the disrupted IT or business domain.
-

NEW QUESTION # 19
......

The candidates all enjoy learning on our ISO-IEC-27035-Lead-Incident-Manager practice exam study materials. Also, we have picked out the most important knowledge for you to learn. The difficult questions of the ISO-IEC-27035-Lead-Incident-Manager study materials have detailed explanations such as charts, illustrations and so on. We have invested a lot of efforts to develop the ISO-IEC-27035-Lead-Incident-Manager Training Questions. Please trust us. You absolutely can understand them after careful learning.

ISO-IEC-27035-Lead-Incident-Manager Reliable Exam Registration: https://www.dumpsvalid.com/ISO-IEC-27035-Lead-Incident-Manager-still-valid-exam.html

- How to Obtain Excellent Results Here on PECB ISO-IEC-27035-Lead-Incident-Manager Exam □ Simply search for [ISO-IEC-27035-Lead-Incident-Manager] for free download on ➤ www.examcollectionpass.com □ □ISO-IEC-27035-Lead-Incident-Manager Valid Exam Preparation
- Valid ISO-IEC-27035-Lead-Incident-Manager Test Prep - Pass ISO-IEC-27035-Lead-Incident-Manager Exam □ Enter ⇛ www.pdfvce.com ⇚ and search for □ ISO-IEC-27035-Lead-Incident-Manager □ to download for free □Study ISO-IEC-27035-Lead-Incident-Manager Tool
- Free PDF PECB ISO-IEC-27035-Lead-Incident-Manager First-grade PECB Certified ISO/IEC 27035 Lead Incident

Manager Test Prep □ Download “ ISO-IEC-27035-Lead-Incident-Manager ” for free by simply searching on ➠ www.prep4sures.top □ □New ISO-IEC-27035-Lead-Incident-Manager Exam Test

- Quiz Professional PECB - ISO-IEC-27035-Lead-Incident-Manager - PECB Certified ISO/IEC 27035 Lead Incident Manager Test Prep □ Easily obtain free download of [ISO-IEC-27035-Lead-Incident-Manager] by searching on □ www.pdfvce.com □ □New Exam ISO-IEC-27035-Lead-Incident-Manager Materials
- Quiz Professional PECB - ISO-IEC-27035-Lead-Incident-Manager - PECB Certified ISO/IEC 27035 Lead Incident Manager Test Prep □ Search for ▹ ISO-IEC-27035-Lead-Incident-Manager ◃ and download it for free on ➠ www.prepawayete.com □ website □ISO-IEC-27035-Lead-Incident-Manager Online Exam
- How to Obtain Excellent Results Here on PECB ISO-IEC-27035-Lead-Incident-Manager Exam □ 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 Actual Dump
- Pass Guaranteed Quiz 2026 Unparalleled ISO-IEC-27035-Lead-Incident-Manager: PECB Certified ISO/IEC 27035 Lead Incident Manager Test Prep □ Go to website ⇛ www.vce4dumps.com ⇚ open and search for ➠ ISO-IEC-27035-Lead-Incident-Manager □ to download for free □ISO-IEC-27035-Lead-Incident-Manager Actual Dump
- ISO-IEC-27035-Lead-Incident-Manager Book Free □ Dumps ISO-IEC-27035-Lead-Incident-Manager Questions □ New Exam ISO-IEC-27035-Lead-Incident-Manager Materials □ Download 《 ISO-IEC-27035-Lead-Incident-Manager 》 for free by simply searching on 《 www.pdfvce.com 》 □ISO-IEC-27035-Lead-Incident-Manager Valid Exam Preparation
- New ISO-IEC-27035-Lead-Incident-Manager Exam Question □ New ISO-IEC-27035-Lead-Incident-Manager Dumps Ppt □ ISO-IEC-27035-Lead-Incident-Manager Latest Exam Question □ Open “ www.pdfdumps.com ” enter “ ISO-IEC-27035-Lead-Incident-Manager ” and obtain a free download □New ISO-IEC-27035-Lead-Incident-Manager Dumps Ppt
- Pass Guaranteed Quiz 2026 Unparalleled ISO-IEC-27035-Lead-Incident-Manager: PECB Certified ISO/IEC 27035 Lead Incident Manager Test Prep □ Open [www.pdfvce.com] and search for ➠ ISO-IEC-27035-Lead-Incident-Manager □ □ to download exam materials for free □ISO-IEC-27035-Lead-Incident-Manager Actual Dump
- PECB ISO-IEC-27035-Lead-Incident-Manager Test Prep - www.verifieddumps.com - Leading Offer in Certification Exams Products □ Search for ✔ ISO-IEC-27035-Lead-Incident-Manager □✔□ and download it for free on ➡ www.verifieddumps.com □□□ website □ISO-IEC-27035-Lead-Incident-Manager Online Exam
- eishkul.com, winningmadness.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes

DOWNLOAD the newest DumpsValid ISO-IEC-27035-Lead-Incident-Manager PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1rL9zt8DZwMRmOwWoikH0Q-G_tDYM3tI6