# ISO-IEC-27035-Lead-Incident-Manager Deutsch Prüfung, ISO-IEC-27035-Lead-Incident-Manager Pruefungssimulationen


Die PECB ISO-IEC-27035-Lead-Incident-Manager Fragenkataloge von ZertPruefung werden von den IT-Experten konzipiert. Sein Design ist eng mit dem heutigen schnell verändernden IT-Markt verbunden. Die Ausbildung von ZertPruefung wird Ihnen helfen, mit der erneuerten Technik Ihre Fähigkeit zur Problemlösung zu fördern und Ihre Zufriedenheit am Arbeitsplatz zu verbessern. Die Deckung der PECB ISO-IEC-27035-Lead-Incident-Manager Zertifizierung von ZertPruefung ist um 100% als geplant gestiegen. Solange Sie unsere Prüfungsfragen und Antworten verwenden, garantieren wir Ihnen, dass Sie zum ersten Mal die PECB ISO-IEC-27035-Lead-Incident-Manager Prüfung mühlos bestehen können.

## PECB ISO-IEC-27035-Lead-Incident-Manager Prüfungsplan:

| Thema | Einzelheiten |
|---|---|
| Thema 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. |
| Thema 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. |
| Thema 3 | • 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. |

| | |
|---|---|
| Thema 4 | • Information security incident management process based on ISO<br>• IEC 27035: This section of the exam measures skills of Incident Response Managers and covers the standardized steps and processes outlined in ISO<br>• IEC 27035. It emphasizes how organizations should structure their incident response lifecycle from detection to closure in a consistent and effective manner. |
| Thema 5 | • 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. |



## PECB ISO-IEC-27035-Lead-Incident-Manager Pruefungssimulationen, ISO-IEC-27035-Lead-Incident-Manager Prüfungen

ZertPruefung aktualisiert ständig die Prüfungsfragen und Antworten. Das bedeutet, dass Sie jederzeit die neuesten Schulungsmaterialien zur ISO-IEC-27035-Lead-Incident-Manager Prüfung bekommen können. Solange das Prüfungsziel geändert wird, ändern wir unsere Lernmaterialien entsprechend. Unser ZertPruefung kennt die Bedürfnisse aller Kandidaten und hilft Ihnen mit dem günstigen Preis und guter Qualität, die ISO-IEC-27035-Lead-Incident-Manager Prüfung zu bestehen und das Zertifikat zu bekommen.

## PECB Certified ISO/IEC 27035 Lead Incident Manager ISO-IEC-27035-Lead-Incident-Manager Prüfungsfragen mit Lösungen (Q71-Q76):

**71. Frage**
How is the impact of an information security event assessed?

- A. By evaluating the effect on the confidentiality, integrity, and availability of information
- B. By identifying the assets affected by the event
- C. By determining if the event is an information security incident

**Antwort: A**

Begründung:
Comprehensive and Detailed Explanation From Exact Extract:
The impact of an information security event is assessed by evaluating how the event affects the CIA triad- Confidentiality, Integrity, and Availability-of information assets. This fundamental concept underpins all ISO/IEC 27000-series standards, including ISO/IEC 27035.
ISO/IEC 27035-1:2016, Clause 6.2.3 explicitly states that an event's severity and urgency are to be assessed by evaluating its actual or potential impact on the organization's information security objectives, namely:
Confidentiality: Protection from unauthorized disclosure
Integrity: Protection from unauthorized modification
Availability: Assurance of timely and reliable access
This approach ensures consistent and risk-based decision-making during incident assessment. Options A and B are important steps, but they are part of the broader process; they do not directly measure impact.
Reference:
ISO/IEC 27035-1:2016, Clause 6.2.3: "The impact should be assessed based on the effect on confidentiality, integrity, and availability of the information assets affected." Correct answer: C
-

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

**Antwort: C**

Begründung:
-
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.

**73. Frage**
What is the primary input for the information security risk treatment process?

- A. A prioritized set of risks to be treated based on risk criteria
- B. A prioritized list of all assets within the organization
- C. A prioritized list of IT systems for security upgrades

**Antwort: A**

Begründung:
Comprehensive and Detailed Explanation:
According to ISO/IEC 27005:2018, the risk treatment process begins after risk analysis and evaluation. The main input to this phase is a prioritized set of identified and assessed risks, chosen based on the organization's risk acceptance criteria. These risks are then assigned treatments such as mitigation, avoidance, or acceptance.
Reference:
ISO/IEC 27005:2018, Clause 8.4: "Risk treatment is based on a set of prioritized risks resulting from the risk assessment process."
Correct answer: B
-

**74. Frage**
What is a key activity in the response phase of information security incident management?

- A. Restoring systems to normal operation
- B. Logging all activities, results, and related decisions for later analysis
- C. Ensuring the change control regime covers information security incident tracking

**Antwort: B**

Begründung:
Comprehensive and Detailed Explanation From Exact Extract:
During the response phase, one of the most critical activities-according to ISO/IEC 27035-1 and 27035-2- is the documentation of actions, decisions, and results. Clause 6.4.6 of ISO/IEC 27035-1 emphasizes that all activities must be logged to support post-incident analysis, audit trails, and lessons learned. This ensures that:
Accountability is maintained
Decisions can be reviewed
Investigations are legally sound (especially in regulated environments) While restoring systems (Option C) typically occurs in the recovery phase, logging activities and outcomes is essential during the actual response. Change control processes (Option B) are supporting functions but are not core to the immediate response phase.
Reference:
ISO/IEC 27035-1:2016, Clause 6.4.6: "All incident response actions and decisions should be recorded to enable traceability and facilitate future improvement." Correct answer: A
-

**75. Frage**
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.
According to scenario 6, Nate compiled a detailed incident report that analyzed the problem and its cause but did not evaluate the incident's severity and response urgency. Does this align with the ISO/IEC 27035-1 guidelines?

- A. Yes. Nate included all the elements required by ISO/IEC 27035-1
- B. No, Nate overlooked the necessity of assessing the seriousness and the urgency of the response
- C. No, as the report did not include a comprehensive list of all employees who accessed the system within 24 hours before the incident

**Antwort: B**

Begründung:
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-1:2016 emphasizes that part of the incident handling process-particularly during assessment and documentation-must include evaluation of both the seriousness (severity) and urgency (criticality) of the incident.
Clause 6.4.2 requires that an incident's potential impact and required response timelines be assessed promptly to determine appropriate action. Nate's omission of this evaluation, despite creating a technically sound report, means that the organization could misjudge the incident's risk, delay appropriate response, or fail to meet notification obligations.
Option A is incorrect because ISO/IEC 27035 explicitly lists impact and urgency as required analysis elements. Option C, while possibly helpful in forensic analysis, is not a required component per the standard.
Reference:
ISO/IEC 27035-1:2016, Clause 6.4.2: "Assess the impact, severity, and urgency of the incident to determine the necessary response and escalation procedures." Clause 6.5.4: "An incident report should include an evaluation of incident criticality to inform decision- making." Correct answer: B Each includes the correct answer, detailed justification, and citation from ISO/IEC 27035 standards.
-

**76. Frage**
.....

exams4sure pdf - PECB ISO-IEC-27035-Lead-Incident-Manager pdf vce □ Geben Sie ✔ www.itzert.com □✔□ ein und suchen Sie nach kostenloser Download von ✔ ISO-IEC-27035-Lead-Incident-Manager □✔□ □ISO-IEC-27035-Lead-Incident-Manager Testking

- ISO-IEC-27035-Lead-Incident-Manager Prüfungsressourcen: PECB Certified ISO/IEC 27035 Lead Incident Manager - ISO-IEC-27035-Lead-Incident-Manager Reale Fragen □ Suchen Sie einfach auf ➠ www.zertpruefung.de □ nach kostenloser Download von 【 ISO-IEC-27035-Lead-Incident-Manager 】 □ISO-IEC-27035-Lead-Incident-Manager Online Tests
- Kostenlos ISO-IEC-27035-Lead-Incident-Manager Dumps Torrent - ISO-IEC-27035-Lead-Incident-Manager exams4sure pdf - PECB ISO-IEC-27035-Lead-Incident-Manager pdf vce □ Sie müssen nur zu ✔ www.itzert.com □✔□ gehen um nach kostenloser Download von ✔ ISO-IEC-27035-Lead-Incident-Manager □✔□ zu suchen □ISO-IEC-27035-Lead-Incident-Manager Demotesten
- Die neuesten ISO-IEC-27035-Lead-Incident-Manager echte Prüfungsfragen, PECB ISO-IEC-27035-Lead-Incident-Manager originale fragen □ Sie müssen nur zu 「 www.zertfragen.com 」 gehen um nach kostenloser Download von ➠ ISO-IEC-27035-Lead-Incident-Manager □ zu suchen □ISO-IEC-27035-Lead-Incident-Manager Trainingsunterlagen
- ISO-IEC-27035-Lead-Incident-Manager Prüfungsressourcen: PECB Certified ISO/IEC 27035 Lead Incident Manager - ISO-IEC-27035-Lead-Incident-Manager Reale Fragen □ Sie müssen nur zu □ www.itzert.com □ gehen um nach kostenloser Download von ▹ ISO-IEC-27035-Lead-Incident-Manager ◃ zu suchen □ISO-IEC-27035-Lead-Incident-Manager PDF
- ISO-IEC-27035-Lead-Incident-Manager Übungsfragen: PECB Certified ISO/IEC 27035 Lead Incident Manager - ISO-IEC-27035-Lead-Incident-Manager Dateien Prüfungsunterlagen □ Öffnen Sie die Webseite { www.zertfragen.com } und suchen Sie nach kostenloser Download von ➥ ISO-IEC-27035-Lead-Incident-Manager □ □ISO-IEC-27035-Lead-Incident-Manager Prüfungs
- www.stes.tyc.edu.tw, lms.ait.edu.za, www.stes.tyc.edu.tw, marciealfredo.blogofoto.com, askfraternity.com, lt.dananxun.cn, www.wcs.edu.eu, motionentrance.edu.np, 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, Disposable vapes