KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **ISO-IEC-27035 Lead Incident Manager**

Title : PECB Certified ISO/IEC 27035 Lead Incident Manager

Version : DEMO

1.Scenario 4: ORingo is a company based in Krakow, Poland, specializing in developing and distributing electronic products for health monitoring and heart rate measurement applications. With a strong emphasis on innovation and technological advancement, ORingo has established itself as a trusted provider of high-quality, reliable devices that enhance the well being and healthcare capabilities of individuals and healthcare professionals alike.
As part of its commitment to maintaining the highest standards of information security, ORingo has established an information security incident management process This process aims to ensure that any potential threats are swiftly identified, assessed, and addressed to protect systems and information. However, despite these measures, an incident response team member at ORingo recently detected a suspicious state in their systems operational data, leading to the decision to shut down the company-wide system until the anomaly could be thoroughly investigated Upon detecting the threat, the company promptly established an incident response team to respond to the incident effectively. The team's responsibilities encompassed identifying root causes, uncovering hidden vulnerabilities, and implementing timely resolutions to mitigate the impact of the incident on ORingo's operations and customer trust.
In response to the threat detected across its cloud environments. ORingo employed a sophisticated security tool that broadened the scope of incident detection and mitigation This tool covers network traffic, doud environments, and potential attack vectors beyond traditional endpoints, enabling ORingo to proactively defend against evolving cybersecurity threats
During a routine check, the IT manager at ORingo discovered that multiple employees lacked awareness of proper procedures following the detection of a phishing email. In response, immediate training sessions on information security policies and incident response were scheduled for all employees, emphasizing the importance of vigilance and adherence to established protocols in safeguarding ORingo's sensitive data and assets.
As part of the training initiative. ORingo conducted a simulated phishing attack exercise to assess employee response and knowledge. However, an employee inadvertently informed an external partner about the 'attack'' during the exercise, highlighting the importance of ongoing education and reinforcement of security awareness principles within the organization.
Through its proactive approach to incident management and commitment to fostering a culture of security awareness and readiness. ORingo reaffirms its dedication to safeguarding the integrity and confidentiality of its electronic products and ensuring the trust and confidence of its customers and stakeholders worldwide.
Based on the scenario above, answer the following question:
After identifying a suspicious state in ORingo's system, a member of the IRT initiated a company-wide system shutdown until the anomaly was investigated. Is this acceptable?
A. No, the IRT should have immediately informed all employees about the potential data breach
B. No, the IRT should have determined the facts that enable detection of the event occurrence
C. Yes, the correct action is to initiate a company-wide system shutdown until the anomaly is investigated
Answer: B
Explanation:
Comprehensive and Detailed Explanation
According to ISO/IEC 27035-1:2016, particularly in Clause 6.2.2 (Assess and Decide), the organization must first assess the reported event to determine whether it qualifies as a security incident before

implementing disruptive responses such as a full system shutdown.
Initiating a shutdown without first determining the cause, impact, or whether it’s a confirmed incident can lead to unnecessary operational disruption and loss of services. The proper approach is to collect evidence, analyze system behavior, and make informed decisions based on risk level and confirmed facts.
Option B best reflects the required approach: The IRT should first determine the facts that enable detection and validation of the event's occurrence and impact before initiating drastic action like shutting down critical systems.
Reference: ISO/IEC 27035-1:2016, Clause 6.2.2 – “An analysis should be conducted to determine whether the event should be treated as an information security incident.”
Clause 6.2.3 – “Response should be proportionate to the impact and type of the incident.”
Therefore, the correct answer is B.

2.What is the first step in planning the response to information security incidents?
A. Assigning the response class based on incident information
B. Developing processes that support the response to information security incidents
C. Defining the response classification
Answer: C
Explanation:
Comprehensive and Detailed Explanation
From Exact Extract:
In ISO/IEC 27035-2:2016, the planning phase of incident response starts with establishing a classification system. Response classification is essential to ensure that incidents are assessed and categorized in a consistent manner, allowing appropriate response measures to be applied. This classification forms the foundation for selecting the right procedures, team involvement, and communication protocols.
Assigning a response class (Option A) is a subsequent step that occurs once an incident is analyzed and matched to a pre-defined category. Developing response processes (Option B) is important but comes after the classification model is defined.
Reference Extracts:
ISO/IEC 27035-2:2016, Clause 6.3.2: “The response planning process begins with the classification of potential incidents to determine the required actions and responsibilities.”
Clause 7.2.2: “Defining response classes helps the organization decide how to handle specific categories of incidents.”
Correct answer: C

3.Scenario 5: Located in Istanbul, Turkey, Alura Hospital is a leading medical institution specializing in advanced eye surgery and vision care. Renowned for its modern facilities, cutting-edge technology, and highly skilled staff, Alura Hospital is committed to delivering exceptional patient care. Additionally, Alura Hospital has implemented the ISO/IEC 27035 standards to enhance its information security incident management practices.
At Alura Hospital, the information security incident management plan is a critical component of safeguarding patient data and maintaining the integrity of its medical services. This comprehensive plan includes instructions for handling vulnerabilities discovered during incident management. According to

this plan, when new vulnerabilities are discovered, Mehmet is appointed as the incident handler and is authorized to patch the vulnerabilities without assessing their potential impact on the current incident, prioritizing patient data security above all else.
Recognizing the importance of a structured approach to incident management, Alura Hospital has established four teams dedicated to various aspects of incident response. The planning team focuses on implementing security processes and communicating with external organizations. The monitoring team is responsible for security patches, upgrades, and security policy implementation. The analysis team adjusts risk priorities and manages vulnerability reports, while the test and evaluation team organizes and performs incident response tests to ensure preparedness.
During an incident management training session, staff members at Alura Hospital were provided with clear roles and responsibilities. However, a technician expressed uncertainty about their role during a data integrity incident, as the manager assigned them a role unrelated to their expertise. This decision was made to ensure that all staff members possess versatile skills and are prepared to handle various scenarios effectively.
Additionally, Alura Hospital realized it needed to communicate better with stakeholders during security incidents. The hospital discovered it was not adequately informing stakeholders and that relevant information must be provided using formats, language, and media that meet their needs. This would enable them to participate fully in the incident response process and stay informed about potential risks and mitigation strategies.
Also, the hospital has experienced frequent network performance issues affecting critical hospital systems and increased sophisticated cyberattacks designed to bypass traditional security measures. So, it has deployed an external firewall. This action is intended to strengthen the hospital’s network security by helping detect threats that have already breached the perimeter defenses. The firewall's implementation is a part of the hospital's broader strategy to maintain a robust and secure IT infrastructure, which is crucial for protecting sensitive patient data and ensuring the reliability of critical hospital systems. Alura Hospital remains committed to integrating state-of-the-art technology solutions to uphold the highest patient care and data security standards.
According to scenario 5, which of the following principles of efficient communication did Alura Hospital NOT adhere to?
A. Credibility
B. Responsiveness
C. Appropriateness
Answer: C
Explanation:
Comprehensive and Detailed Explanation
From Exact Extract:
According to ISO/IEC 27035-1:2016 (Information Security Incident Management – Part 1: Principles of Incident Management), one of the core principles of effective communication in incident management is “appropriateness.” This refers to ensuring that the right information is shared with the right stakeholders using the appropriate channels, language, format, and timing. The objective is to guarantee that communication is both understandable and actionable by its recipients.
In the scenario, Alura Hospital recognized that they were not adequately informing stakeholders during security incidents. They identified a gap in providing relevant information using suitable formats, media, or language. This failure points directly to a lack of “appropriateness” in their communication strategy.

According to ISO/IEC 27035-1, Section 6.4 (Communication), it is essential to tailor incident communication to stakeholder needs to ensure informed decision-making and engagement.
The other options—credibility and responsiveness—are not indicated as the failing areas. There is no mention that the information provided lacked credibility or that the hospital failed to respond to incidents or communicate in a timely manner. Rather, the issue lies with the medium, clarity, and stakeholder alignment— hallmarks of appropriateness.
Reference Extracts from ISO/IEC 27035-1:2016:
Clause 6.4: “Communication must be timely, relevant, accurate, and appropriate for the target audience.”
Clause 7.2.4: “Stakeholders should be informed using formats and channels that they can easily access and understand.”
Therefore, the principle not adhered to by Alura Hospital is clearly: Appropriateness (C).

4.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, NoSpace used the ISO/IEC 27035-1 guidelines to meet the ISMS requirements specified in ISO/IEC 27001. Is this acceptable?
A. Yes, another objective associated with ISO/IEC 27035-1 is to provide guidance on meeting the ISMS requirements specified in ISO/IEC 27001

B. No, guidelines provided in ISO/IEC 27035-1 do not apply to ISMS requirements specified in ISO/IEC 27001
C. No, ISO/IEC 27035-1 is designed for incident management and response and does not address the broader scope of ISMS requirements specified in ISO/IEC 27001
Answer: A
Explanation:
Comprehensive and Detailed Explanation
From Exact Extract:
Yes, the use of ISO/IEC 27035-1 to support compliance with ISO/IEC 27001 ISMS requirements is fully acceptable and encouraged. ISO/IEC 27035-1:2016 is explicitly designed to support organizations in establishing and maintaining effective information security incident management processes. These processes are a crucial component of a well-functioning Information Security Management System (ISMS), which is governed by ISO/IEC 27001.
Clause 6.1.3 and Clause A.16.1 of ISO/IEC 27001:2022 (formerly 2013) require that organizations establish and respond to information security incidents, including detection, response, and learning from such events. ISO/IEC 27035-1 directly supports these controls by providing specific guidance on how to identify, manage, and learn from information security incidents in a structured and repeatable way.
Moreover, ISO/IEC 27035-1 is referenced by ISO/IEC 27001 Annex A (specifically A.5.24 to A.5.27 and A. 5.31 in the 2022 version), supporting requirements related to incident management, monitoring, and improvement. The ISO 27035 series acts as a detailed implementation guide for these controls, helping organizations meet both the management and operational requirements of the ISMS.
Therefore, Mark's decision to use ISO/IEC 27035-1 guidelines to align and enhance the incident management aspects of the ISMS is both appropriate and aligned with international best practices.
Reference Extracts:
* ISO/IEC 27035-1:2016, Clause 0.2: "This document also supports the information security requirements defined in ISO/IEC 27001 and provides detailed guidance on incident management activities relevant to an ISMS."
* ISO/IEC 27001:2022, Annex A (A.5.24–A.5.27): "Information security incident management should be based on established processes for detection, response, and learning."
* ISO/IEC 27001:2022, Clause 6.1.3: "Information security risks must be identified and treated as part of the ISMS."
Therefore, the correct answer is A: Yes, another objective associated with ISO/IEC 27035-1 is to provide guidance on meeting the ISMS requirements specified in ISO/IEC 27001.
Certainly! Below is your requested content in the structured ISO/IEC format for:
#
15.Including: full scenario, correct answer option, and a comprehensive explanation based on ISO/IEC 27035-1, 27035-2, and related ISO/IEC standards.

5.Based on ISO/IEC 27035-2, which of the following is an example of evaluation activities used to evaluate the effectiveness of the incident management team?
A. Conducting information security testing, particularly vulnerability assessment
B. Analyzing the lessons learned once an information security incident has been handled and closed
C. Evaluating the capabilities and services once they become operational
Answer: B

Explanation:
Comprehensive and Detailed Explanation
From Exact Extract:
ISO/IEC 27035-2:2016 Clause 7.4.3 emphasizes the role of lessons learned reviews as key evaluation activities for assessing the performance of incident response teams. This activity involves post-incident debriefs to evaluate what went right or wrong and how response processes or team functions could improve.
While options A and C are related to broader security or deployment procedures, Option B directly reflects a formal evaluation mechanism used to gauge incident team effectiveness.
Reference: ISO/IEC 27035-2:2016 Clause 7.4.3: “Lessons learned should be documented and used to evaluate the effectiveness of the incident management process.”
Correct answer: B