ISO-IEC-27035-Lead-Incident-Manager合格直結！至高のPECB PECB Certified ISO/IEC 27035 Lead Incident Manager学習法

BONUS！！！ CertShiken ISO-IEC-27035-Lead-Incident-Managerダンプの一部を無料でダウンロード：https://drive.google.com/open?id=1JrC4ol1w1yAt4hwnm_mjtRmMCidHMU5Q

私たちPECBは非常に人気があり、詳細で完璧なCertShiken顧客サービスシステムを持っています。 まず、ISO-IEC-27035-Lead-Incident-Managerの実際の試験の顧客によるオンライン支払いが成功してから5〜10分後に、顧客サービスから電子メールを受信し、すぐにPECB Certified ISO/IEC 27035 Lead Incident Manager学習を開始できます。 また、ISO-IEC-27035-Lead-Incident-Manager試験問題を毎日確認および更新する専任スタッフがいるため、ISO-IEC-27035-Lead-Incident-Manager試験教材の最新情報を購入するたびに入手できます。 第二に、24時間体制のサービスをお客様に提供します。 ISO-IEC-27035-Lead-Incident-Manager学習教材に関する問題は、いつでもどこでも必要に応じて解決できます。

PECB ISO-IEC-27035-Lead-Incident-Manager 認定試験の出題範囲：

トピック	出題範囲
トピック 1	• 情報セキュリティ インシデント管理の基本原則と概念: 試験のこのセクションでは、情報セキュリティ アナリストのスキルを測定し、セキュリティ インシデントを構成する要素の理解、タイムリーな対応が重要な理由、潜在的な脅威の初期兆候の特定方法など、インシデント管理の背後にある中核的な考え方を取り上げます。
トピック 2	• ISO • IEC 27035 に基づく組織のインシデント管理プロセスの設計と開発: 試験のこのセクションでは、情報セキュリティアナリストのスキルを測定し、ポリシー開発、ロール定義、インシデント処理のワークフローの確立など、組織の固有のニーズに合わせて ISO • IEC 27035 フレームワークをカスタマイズする方法を取り上げます。

トピック 3	• インシデント管理プロセスと活動の改善：この試験セクションでは、インシデント対応マネージャーのスキルを評価し、既存のインシデント管理プロセスのレビューと改善について学びます。インシデント後のレビュー、過去の事例からの学び、そして将来の対応活動を改善するためのツール、トレーニング、および手法の改善が含まれます。
トピック 4	• ISO • IEC 27035 に基づく情報セキュリティ インシデント管理プロセス:試験のこのセクションでは、インシデント対応マネージャーのスキルを測定し、ISO • IEC 27035 に概説されている標準化された手順とプロセスをカバーします。組織が、検出から終了までのインシデント対応ライフサイクルを一貫性と効率性をもって構築する方法に重点を置いています。
トピック 5	• 情報セキュリティインシデントに対するインシデント対応計画の策定と実行：この試験セクションでは、インシデント対応マネージャーのスキルを評価し、インシデント対応計画の策定と実行について扱います。チームトレーニング、リソース割り当て、シミュレーション演習といった準備活動に加え、インシデント発生時の実際の対応実行にも重点が置かれます。

ISO-IEC-27035-Lead-Incident-Manager模擬試験最新版 & ISO-IEC-27035-Lead-Incident-Manager受験内容

ISO-IEC-27035-Lead-Incident-Managerの認定を取得するのが簡単ではないことが心配な場合。 ISO-IEC-27035-Lead-Incident-Manager試験の質問は、お客様のニーズを満たすことができます。一度ISO-IEC-27035-Lead-Incident-Manager試験資料を使用すれば、時間の浪費を心配する必要はありません。高い効率が私たちの大きな利点です。 ISO-IEC-27035-Lead-Incident-Manager学習教材の練習と統合に20〜30時間を費やすだけで、良い結果が得られます。長年の開発プラクティスの後、ISO-IEC-27035-Lead-Incident-Managerテストトレントは絶対に最高です。 ISO-IEC-27035-Lead-Incident-Manager試験の資料を選択すると、より良い未来を受け入れることができます。

PECB Certified ISO/IEC 27035 Lead Incident Manager 認定 ISO-IEC-27035-Lead-Incident-Manager 試験問題 (Q44-Q49):

質問 # 44
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, what mechanisms for detecting security incidents did EastCyber implement?

- A. Security information and event management systems
- B. Intrusion detection systems
- C. Intrusion prevention systems

正解：B

解説：
Comprehensive and Detailed Explanation From Exact Extract:
In the scenario, EastCyber implemented an "advanced network traffic monitoring system" that "spots and alerts the security team to unauthorized actions." This aligns closely with the functional characteristics of an Intrusion Detection System (IDS), which monitors traffic or systems for malicious activities and policy violations and sends alerts for review.
While Security Information and Event Management (SIEM) tools and Intrusion Prevention Systems (IPS) offer valuable detection and response capabilities, the scenario specifically describes a system focused on monitoring and alerting-not automatically blocking traffic, which would indicate an IPS.
SIEM platforms correlate and analyze logs from various sources, which wasn't described. Therefore, IDS is the most accurate interpretation.
Reference:
ISO/IEC 27035-2:2016, Clause 7.4.2: "Detection mechanisms can include intrusion detection systems, log analysis tools, and traffic monitoring systems to detect potential security events." Correct answer: B
-

質問 # 45
According to ISO/IEC 27035-2, how should an organization plan the development of the incident response team capabilities?

- A. By considering how often certain capabilities were needed in the past
- B. By focusing only on internal capabilities
- C. By discontinuing any capabilities that have not been used recently

正解：A

解説：
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-2:2016 recommends that organizations should assess the necessary capabilities of the Incident Response Team (IRT) based on risk exposure and the frequency of past incidents requiring specific skills or tools. This ensures a balanced and realistic approach to resource allocation while preparing for probable future events.
Section 7.2.1 of ISO/IEC 27035-2 outlines that capability planning should consider:
Lessons learned from prior incidents
Incident history and trends
Anticipated threat landscape
Option A is incorrect because relying solely on internal capabilities may leave organizations vulnerable when specialized expertise is required. Option C contradicts ISO guidance because a lack of recent use does not mean a capability is no longer critical; it may still be required during high-impact, low-frequency incidents.
Reference:
ISO/IEC 27035-2:2016, Clause 7.2.1: "Incident response capabilities should be planned and developed based on the history of incidents, business requirements, and likely future needs." Correct answer: B
-

質問 # 46
What is a key responsibility of the incident response team?

- A. Performing vulnerability scans and penetration testing
- B. Maintaining physical security infrastructure
- C. Investigating and managing cybersecurity incidents

正解：C

解説：
Comprehensive and Detailed Explanation From Exact Extract:
The primary role of an incident response team, according to ISO/IEC 27035-2:2016, is to manage and respond to information security incidents effectively. This includes tasks such as identifying, analyzing, containing, mitigating, and recovering from incidents. The goal is to minimize the impact on the organization and restore normal operations as quickly as possible.
Key responsibilities include:
Incident detection and validation
Impact assessment
Coordination of containment and eradication efforts
Communication with stakeholders
Post-incident analysis and lessons learned
While vulnerability scanning and penetration testing (option C) are important security functions, they are typically assigned to the security operations team or dedicated assessment teams - not the incident response team per se. Likewise, maintaining physical infrastructure (option A) is the responsibility of facilities management or physical security teams, not the incident response team.
Reference Extracts:
ISO/IEC 27035-2:2016, Clause 5.2 - "The incident response team is responsible for analyzing, responding to, and resolving incidents." NIST SP 800-61r2 (Computer Security Incident Handling Guide) - "An incident response team handles the investigation and resolution of security incidents." Therefore, the correct answer is B: Investigating and managing cybersecurity incidents.Question
Certainly!

質問 # 47
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 decision on whether to classify events as information security incidents should be assessed before initiating the incident management process
- C. No, the second phase of the incident management process should include the collection of information associated with the occurrences of information security events

正解：C

解説：
-
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.

質問 # 48
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. Responsiveness
- B. Appropriateness
- C. Credibility

正解：B

解説：
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).
-

質問 # 49
.....

弊社のCertShikenはIT認定試験のソフトの一番信頼たるバンドになるという目標を達成するために、弊社はあなたに最新版のPECBのISO-IEC-27035-Lead-Incident-Manager試験問題集を提供いたします。弊社のソフトを使用して、ほとんどのお客様は難しいと思われているPECBのISO-IEC-27035-Lead-Incident-Manager試験に順調に剛角しました。これも弊社が自信的にあなたに商品を薦める原因です。もし弊社のソフトを使ってあなたは残念で試験に失敗したら、弊社は全額で返金することを保証いたします。すべてのことの目的はあなたに安心に試験に準備さされるということです。

ISO-IEC-27035-Lead-Incident-Manager模擬試験最新版: https://www.certshiken.com/ISO-IEC-27035-Lead-Incident-Manager-shiken.html

- ISO-IEC-27035-Lead-Incident-Manager関連資料 ✡ ISO-IEC-27035-Lead-Incident-Manager試験対応 □ ISO-IEC-27035-Lead-Incident-Manager赤本勉強 □ ⇒ jp.fast2test.com ⇐にて限定無料の➠ ISO-IEC-27035-Lead-Incident-Manager □問題集をダウンロードせよISO-IEC-27035-Lead-Incident-Manager関連資料
- 試験の準備方法-認定するISO-IEC-27035-Lead-Incident-Manager復習解答例試験-完璧なISO-IEC-27035-Lead-Incident-Manager模擬試験最新版 □ ▹ www.goshiken.com ◃を開き、□ ISO-IEC-27035-Lead-Incident-Manager □を入力して、無料でダウンロードしてくださいISO-IEC-27035-Lead-Incident-Manager日本語独学書籍
- ISO-IEC-27035-Lead-Incident-Manager試験対策書 □ ISO-IEC-27035-Lead-Incident-Manager赤本勉強 □ ISO-IEC-27035-Lead-Incident-Manager赤本勉強 □ 検索するだけで{ www.shikenpass.com }から➽ ISO-IEC-27035-Lead-Incident-Manager □を無料でダウンロードISO-IEC-27035-Lead-Incident-Managerキャリアパス
- ISO-IEC-27035-Lead-Incident-Manager試験対策書 □ ISO-IEC-27035-Lead-Incident-Managerシュミレーション問題集 □ ISO-IEC-27035-Lead-Incident-Manager試験対応 🐱 サイト「 www.goshiken.com 」で✔ ISO-IEC-27035-Lead-Incident-Manager □✔□問題集をダウンロードISO-IEC-27035-Lead-Incident-Manager最速合格
- 素敵なISO-IEC-27035-Lead-Incident-Manager復習解答例 - 合格スムーズISO-IEC-27035-Lead-Incident-Manager模擬試験最新版 | 更新するISO-IEC-27035-Lead-Incident-Manager受験内容 □ ➡ www.goshiken.com □□□サイトで□ ISO-IEC-27035-Lead-Incident-Manager □の最新問題が使えるISO-IEC-27035-Lead-Incident-Manager科目対策
- 効率的なISO-IEC-27035-Lead-Incident-Manager復習解答例一回合格-素晴らしいISO-IEC-27035-Lead-Incident-Manager模擬試験最新版 □ ⇒ www.goshiken.com ⇐にて限定無料の▸ ISO-IEC-27035-Lead-Incident-Manager ◂問題集をダウンロードせよISO-IEC-27035-Lead-Incident-Manager試験対応
- 素晴らしいISO-IEC-27035-Lead-Incident-Manager復習解答例と権威のあるISO-IEC-27035-Lead-Incident-Manager模擬試験最新版 □ □ www.shikenpass.com □で「 ISO-IEC-27035-Lead-Incident-Manager 」を検索して、無料でダウンロードしてくださいISO-IEC-27035-Lead-Incident-Manager関連資料
- 完璧なISO-IEC-27035-Lead-Incident-Manager復習解答例試験-試験の準備方法-最高のISO-IEC-27035-Lead-Incident-Manager模擬試験最新版 □ Open Webサイト[www.goshiken.com]検索➽ ISO-IEC-27035-Lead-Incident-Manager □無料ダウンロードISO-IEC-27035-Lead-Incident-Manager資格練習
- 効率的なISO-IEC-27035-Lead-Incident-Manager復習解答例一回合格-素晴らしいISO-IEC-27035-Lead-Incident-Manager模擬試験最新版 □ ☀ www.japancert.com □☀□を開き、“ ISO-IEC-27035-Lead-Incident-Manager ”を入力して、無料でダウンロードしてくださいISO-IEC-27035-Lead-Incident-Manager関連資格試験対応

- 試験の準備方法-認定するISO-IEC-27035-Lead-Incident-Manager復習解答例試験-完璧なISO-IEC-27035-Lead-Incident-Manager模擬試験最新版 □ □ ISO-IEC-27035-Lead-Incident-Manager □を無料でダウンロード“ www.goshiken.com ”で検索するだけISO-IEC-27035-Lead-Incident-Manager試験勉強過去問
- 素敵なISO-IEC-27035-Lead-Incident-Manager復習解答例 - 合格スムーズISO-IEC-27035-Lead-Incident-Manager模擬試験最新版 | 更新するISO-IEC-27035-Lead-Incident-Manager受験内容◂今すぐ☀ www.shikenpass.com □☀□で▸ ISO-IEC-27035-Lead-Incident-Manager◂を検索して、無料でダウンロードしてくださいISO-IEC-27035-Lead-Incident-Managerテスト参考書
- www.stes.tyc.edu.tw, 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, www.dkcomposite.com, shortcourses.russellcollege.edu.au, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, himanshugaurandroid.in, www.stes.tyc.edu.tw, motionentrance.edu.np, Disposable vapes

P.S.CertShikenがGoogle Driveで共有している無料の2025 PECB ISO-IEC-27035-Lead-Incident-Managerダンプ：https://drive.google.com/open?id=1JrC4o1lw1yAt4hwnm_mjtRmMCidHMU5Q