ISO-IEC-27035-Lead-Incident-Manager模擬練習 & ISO-IEC-27035-Lead-Incident-Manager模擬対策

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

簡単になりたい場合は、ISO-IEC-27035-Lead-Incident-Manager信頼性の高い試験ガイドのバージョンを選択するのが難しいと感じる場合、PDFバージョンが適している可能性があります。 PDFバージョンは通常のファイルです。 多くの受験者は、ISO-IEC-27035-Lead-Incident-Manager信頼できる試験ガイドを紙に印刷してから読み書きすることに慣れています。 はい、それは静かで明確です。 また、不明な点がある場合は、他の人に簡単に質問したり話したりできます。 他の人は、それが通常は練習資料だと考えるかもしれません。 また、PECB ISO-IEC-27035-Lead-Incident-Manager信頼できる試験ガイドの多くのコピーを印刷して、他の人と共有することもできます。

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	• 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 2	• 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 3	• 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。
トピック 4	• インシデント管理プロセスの実装と情報セキュリティインシデントの管理：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評価し、インシデント管理戦略の実践的な実装について学びます。継続的なインシデント追跡、危機発生時のコミュニケーション、そして確立されたプロトコルに従ったインシデント解決の確保について考察します。

PECB ISO-IEC-27035-Lead-Incident-Manager模擬練習: 無料ダウンロードPECB Certified ISO/IEC 27035 Lead Incident Manager

私たちのサービス理念は、クライアントが最高のユーザー体験を得て満足することです。調査、編集、制作から販売、アフターサービスまで、お客様に利便性を提供し、ISO-IEC-27035-Lead-Incident-Managerガイド資料を最大限に活用できるように最善を尽くします。エキスパートチームを編成してISO-IEC-27035-Lead-Incident-Manager実践ガイドを精巧にまとめ、常に更新しています。クライアントがISO-IEC-27035-Lead-Incident-Managerトレーニング資料を基本的に理解できるように、購入前にISO-IEC-27035-Lead-Incident-Manager試験問題の無料トライアルを提供しています。

PECB Certified ISO/IEC 27035 Lead Incident Manager 認定 ISO-IEC-27035-Lead-Incident-Manager 試験問題 (Q66-Q71):

質問 # 66
What is the primary function of a single type of IRT?

- A. Managing incidents within a specified organization
- B. Monitoring targets from remote locations
- C. Enhancing the reliability of incident response activities

正解：A

解説：
Comprehensive and Detailed Explanation From Exact Extract:
A single-type Incident Response Team (IRT), as defined in ISO/IEC 27035-1:2016, is responsible for managing and coordinating incident response within a specific organization or business unit. Its scope typically covers the entire lifecycle of incident handling-preparation, detection, containment, response, recovery, and lessons learned-focused solely on the needs of that particular entity. This contrasts with a coordinating or multi-party IRT, which may support multiple organizations or coordinate between units. While Option A is a byproduct of a well-functioning IRT, it is not its core function.
Option B (monitoring) may fall under a SOC, but not the primary function of a single IRT.
Reference Extracts:
ISO/IEC 27035-1:2016, Clause 6.5.1: "An organization may establish a single IRT responsible for handling all incidents affecting the organization." ISO/IEC 27035-2:2016, Clause 6.2.3: "Single IRTs typically manage incidents internally and directly support the organization's response processes." Correct answer: C
-

質問 # 67

Which of the following is NOT an example of technical control?

- A. Implementing surveillance cameras
- B. Installing a firewall to protect the network
- C. Implementing a policy for regular password changes

正解：C

解説：
Comprehensive and Detailed Explanation From Exact Extract:
According to ISO/IEC 27002:2022 (and earlier versions), information security controls can be broadly categorized into three types: technical (also called logical), physical, and administrative (or organizational) controls.
Technical controls (also known as logical controls) involve the use of software and hardware to protect assets.
Examples include:
Firewalls
Intrusion detection systems
Encryption
Access control mechanisms
Physical controls are designed to prevent physical access to IT systems and include things such as:
Surveillance cameras
Security guards
Biometric access systems
Administrative controls, also called management or procedural controls, include the policies, procedures, and guidelines that govern the organization's security practices. These include:
Security awareness training
Acceptable use policies
Password policies
Option A, "Implementing a policy for regular password changes," is an administrative control, not a technical one. It dictates user behavior through rules and policy enforcement, but does not technically enforce the change itself unless paired with technical enforcement (like system settings).
Option B, surveillance cameras, are physical controls, and option C, installing a firewall, is a classic example of a technical control.
Reference Extracts:
ISO/IEC 27002:2022, Clause 5.1 - "Information security controls can be administrative (policy-based), technical, or physical depending on their form and implementation." NIST SP 800-53, Control Families - Differentiates between management, operational, and technical controls.
Therefore, the correct answer is A: Implementing a policy for regular password changes.
-

質問 # 68
Scenario 1: RoLawyers is a prominent legal firm based in Guadalajara, Mexico. It specializes in a wide range of legal services tailored to meet the diverse needs of its clients. Committed to excellence and integrity, RoLawyers has a reputation for providing legal representation and consultancy to individuals, businesses, and organizations across various sectors.
Recognizing the critical importance of information security in today's digital landscape, RoLawyers has embarked on a journey to enhance its information security measures. This company is implementing an information security incident management system aligned with ISO/IEC 27035-1 and ISO/IEC 27035-2 guidelines. This initiative aims to strengthen RoLawyers' protections against possible cyber threats by implementing a structured incident response process to provide guidance on establishing and maintaining a competent incident response team.
After transitioning its database from physical to online infrastructure to facilitate seamless information sharing among its branches, RoLawyers encountered a significant security incident. A malicious attack targeted the online database, overloading it with traffic and causing a system crash, making it impossible for employees to access it for several hours.
In response to this critical incident, RoLawyers quickly implemented new measures to mitigate the risk of future occurrences. These measures included the deployment of a robust intrusion detection system (IDS) designed to proactively identify and alert the IT security team of potential intrusions or suspicious activities across the network infrastructure. This approach empowers RoLawyers to respond quickly to security threats, minimizing the impact on their operations and ensuring the continuity of its legal services.
By being proactive about information security and incident management, RoLawyers shows its dedication to protecting sensitive data, keeping client information confidential, and earning the trust of its stakeholders.
Using the latest practices and technologies, RoLawyers stays ahead in legal innovation and is ready to handle cybersecurity threats with resilience and careful attention.
Based on the scenario above, answer the following question:
Considering its industry and services, is the guidance provided in ISO/IEC 27035-1 applicable for RoLawyers?

- A. No, it is specific to organizations in the information security industry
- B. Yes, it applies to all organizations, regardless of their size, type, or nature
- C. No, it is specific to organizations providing incident management services

正解：B

解説：
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-1:2016 is titled "Information security incident management - Part 1: Principles of incident management". This standard provides a comprehensive framework for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving incident management within an organization.
The scope of ISO/IEC 27035-1 is explicitly broad and designed to be applicable to all organizations, regardless of their size, type, or nature, as stated in the standard's introduction and scope sections. The principles laid out in the document are intended to be flexible and scalable so that organizations from any sector can adopt and implement incident management processes suitable to their specific context.
The document clearly emphasizes that information security incidents can impact any organization that processes, stores, or transmits information digitally - including law firms like RoLawyers. The guidance addresses the creation of an incident response capability to detect, respond, and recover from information security incidents effectively.
Furthermore, the standard stresses that incident management is a vital part of maintaining information security resilience, minimizing damage, and protecting the confidentiality, integrity, and availability of information assets, which is crucial for organizations handling sensitive data, such as legal firms.
Hence, ISO/IEC 27035-1 is not limited to IT or information security service providers alone; instead, it supports any organization's need to manage information security incidents systematically. RoLawyers, given its reliance on digital data and the critical nature of its information, can and should apply the standard's principles to safeguard its assets and clients.
Reference Extracts from ISO/IEC 27035-1:2016:
* Scope (Section 1): "The principles provided in this document are intended to be applicable to all organizations, irrespective of type, size or nature."
* Introduction (Section 0.1): "Effective incident management helps organizations to reduce the consequences of incidents and limit the damage caused to information and information systems."
* General (Section 4): "This document provides guidance for establishing, implementing, operating, monitoring, reviewing, maintaining and improving incident management processes within an organization." Thus, based on ISO/IEC 27035-1, the guidance is fully applicable to RoLawyers, aligning with their objective to improve information security and incident management practices.

質問 # 69
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.
In scenario 3, which technique did L&K Associates use for its risk analysis process?

- A. Quantitative risk analysis
- B. Qualitative risk analysis
- C. Semi-quantitative risk analysis

正解：A

解説：
Comprehensive and Detailed Explanation From Exact Extract:
In the scenario, Leona used a methodology that estimates "practical values for consequences and their probabilities," which clearly points to a quantitative risk analysis approach.
Quantitative risk analysis, as defined in ISO/IEC 27005:2018, involves assigning numerical values (e.g., monetary impact, frequency rates) to both the probability and consequence of risks. This allows for risk prioritization based on actual or estimated figures, enabling data-driven decisions on mitigation strategies.
Qualitative analysis uses descriptive categories (e.g., high/medium/low), and semi-quantitative methods mix ranking scales with partial numeric estimations - neither of which are described in this scenario.
Reference:

ISO/IEC 27005:2018, Clause 8.3.3: "Quantitative risk analysis estimates the probability and impact of risk using numerical values to derive a risk level." Therefore, the correct answer is C: Quantitative risk analysis.
-

質問 # 70
Which team has a broader cybersecurity role, including incident response, monitoring, and overseeing general operations?

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

正解：A

解説：
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)
-

質問 # 71
.....

PECB製品を購入する前に、無料でダウンロードして試用できるため、ISO-IEC-27035-Lead-Incident-Managerテスト準備を十分に理解できます。このように、クライアントは、ウェブサイト上で私たちのPECB Certified ISO/IEC 27035 Lead Incident Manager試験問題のページを訪問することができます。したがって、クライアントはISO-IEC-27035-Lead-Incident-Manager試験問題をよく理解し、ISO-IEC-27035-Lead-Incident-Manager試験問題の品質を確認したので、ISO-IEC-27035-Lead-Incident-Managerトレーニングガイドを購入するかどうかを決定できます。CertShikenお客様に最高のISO-IEC-27035-Lead-Incident-Manager学習ガイドを提供し、お客様に満足していただけるようにします。

ISO-IEC-27035-Lead-Incident-Manager模擬対策: https://www.certshiken.com/ISO-IEC-27035-Lead-Incident-Manager-shiken.html

- ISO-IEC-27035-Lead-Incident-Manager模擬資料 👆 ISO-IEC-27035-Lead-Incident-Manager模擬資料 □ ISO-IEC-27035-Lead-Incident-Manager受験対策解説集 □ □ www.jpshiken.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関連試験
- ISO-IEC-27035-Lead-Incident-Manager一発合格 □ ISO-IEC-27035-Lead-Incident-Manager日本語版試験解答 □ □ ISO-IEC-27035-Lead-Incident-Manager模擬資料 □ ☀ www.goshiken.com □☀□で【 ISO-IEC-27035-Lead-Incident-Manager 】を検索して、無料で簡単にダウンロードできますISO-IEC-27035-Lead-Incident-Manager的中合格問題集
- ISO-IEC-27035-Lead-Incident-Manager日本語版試験勉強法 ✴ ISO-IEC-27035-Lead-Incident-Manager過去問無料 □ ISO-IEC-27035-Lead-Incident-Manager受験対策解説集 □ ウェブサイト▸ www.mogiexam.com ◂を開き、「 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過去問無料

- ISO-IEC-27035-Lead-Incident-Manager資料的中率 □ ISO-IEC-27035-Lead-Incident-Managerテスト資料 □ ISO-IEC-27035-Lead-Incident-Manager日本語版試験解答 □ ▸ www.goshiken.com ◂サイトにて《 ISO-IEC-27035-Lead-Incident-Manager 》問題集を無料で使おうISO-IEC-27035-Lead-Incident-Manager真実試験
- PECB ISO-IEC-27035-Lead-Incident-Manager模擬練習 - www.passtest.jp - 認証の成功を保証, 簡単なトレーニング方法 □ ➽ www.passtest.jp □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受験対策解説集
- ISO-IEC-27035-Lead-Incident-Manager関連試験 □ ISO-IEC-27035-Lead-Incident-Manager認定デベロッパー □ □ ISO-IEC-27035-Lead-Incident-Manager関連合格問題 □ 今すぐ➽ www.goshiken.com □を開き、《 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認定試験トレーリング
- PECB ISO-IEC-27035-Lead-Incident-Manager模擬練習 - www.passtest.jp - 認証の成功を保証, 簡単なトレーニング方法 □ 最新[ISO-IEC-27035-Lead-Incident-Manager]問題集ファイルは【 www.passtest.jp 】にて検索ISO-IEC-27035-Lead-Incident-Manager試験問題
- 実際的なISO-IEC-27035-Lead-Incident-Manager模擬練習 - 合格スムーズISO-IEC-27035-Lead-Incident-Manager模擬対策 | 検証するISO-IEC-27035-Lead-Incident-Manager練習問題集 PECB Certified ISO/IEC 27035 Lead Incident Manager □ ▸ ISO-IEC-27035-Lead-Incident-Manager ◂を無料でダウンロード《 www.goshiken.com 》ウェブサイトを入力するだけISO-IEC-27035-Lead-Incident-Manager模擬資料
- PECB ISO-IEC-27035-Lead-Incident-Manager模擬練習 - www.goshiken.com - 認証の成功を保証, 簡単なトレーニング方法 □ 今すぐ➡ www.goshiken.com □□□を開き、{ 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関連試験
- ISO-IEC-27035-Lead-Incident-Manager認定デベロッパー □ ISO-IEC-27035-Lead-Incident-Manager日本語版試験勉強法 □ ISO-IEC-27035-Lead-Incident-Manager資料的中率 □ { ISO-IEC-27035-Lead-Incident-Manager }の試験問題は“ www.goshiken.com ”で無料配信中ISO-IEC-27035-Lead-Incident-Manager的中合格問題集
- ISO-IEC-27035-Lead-Incident-Manager資料的中率 □ ISO-IEC-27035-Lead-Incident-Manager関連合格問題 □ ISO-IEC-27035-Lead-Incident-Managerテスト資料 □ □ www.passtest.jp □から▹ ISO-IEC-27035-Lead-Incident-Manager ◃を検索して、試験資料を無料でダウンロードしてくださいISO-IEC-27035-Lead-Incident-Manager的中合格問題集
- 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.stes.tyc.edu.tw, bbs.gmncg.com, www.stes.tyc.edu.tw, pct.edu.pk, myportal.utt.edu.tt, pct.edu.pk, 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

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