ISO-IEC-27035-Lead-Incident-Manager無料問題、ISO-IEC-27035-Lead-Incident-Manager受験対策解説集

BONUS！！！ TopexamISO-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=1O85_W18OfKUE299YFjWVpcUzJMGLkWyj

あなたは君の初めてのPECBのISO-IEC-27035-Lead-Incident-Manager認定試験を受ける時に認定試験に合格したいか。Topexamでは、私たちは君のすべての夢を叶えさせて、君の最も早い時間でPECBのISO-IEC-27035-Lead-Incident-Manager認定試験に合格するということを保証します。TopexamのPECBのISO-IEC-27035-Lead-Incident-Manager試験トレーニング資料は豊富な経験を持っているIT専門家が研究したもので、問題と解答が緊密に結んでいるものです。Topexamを選ぶなら、絶対に後悔させません。

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	• 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 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。

試験の準備方法-信頼的なISO-IEC-27035-Lead-Incident-Manager無料問題試験-素晴らしいISO-IEC-27035-Lead-Incident-Manager受験対策解説集

試験の概要は毎年新しいポリシーに基づいて変更され、ISO-IEC-27035-Lead-Incident-Manager質問トレントおよびその他の教育用ソフトウェアは、新しい試験の概要の後、シラバスおよび理論と実践の最新の開発および改訂に従って変更されます対応する変更は、アウトラインに非常に同意します。 ISO-IEC-27035-Lead-Incident-Manager試験問題は、教材の完全なセットの完璧な形です。教育概要は、カバーされているすべての知識ポイントの概要を網羅し、ISO-IEC-27035-Lead-Incident-Manager候補者のデッドアングルは、毎年の提案範囲と傾向を示します。

PECB Certified ISO/IEC 27035 Lead Incident Manager 認定 ISO-IEC-27035-Lead-Incident-Manager 試験問題 (Q43-Q48):

質問 # 43
What is the primary function of a single type of IRT?

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

正解：B

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 # 44
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 how often the information security incident policies are updated and revised
- 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 the incident reporting procedures and specify the appropriate contact for further information

正解：C

解説：
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.
-

質問 # 45
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.
According to scenario 3, Leona decided to initially include only the elements provided in Clause 4.3 of ISO /IEC 27035-2, Information security incident management policy content, in the incident management policy.
Is this acceptable?

- A. Yes, because Leona has conducted a thorough risk assessment to identify potential gaps in the incident management policy beyond the scope of clause 4.3 of ISO/IEC 27035-2
- B. No, clause 4.3 of ISO/IEC 27035-2 does not cover elements for an effective incident management policy
- C. Yes, because as a minimum, the policy must cover the elements provided in clause 4.3 of ISO/IEC 27035-2

正解：C

解説：
Comprehensive and Detailed Explanation From Exact Extract:
Clause 4.3 of ISO/IEC 27035-2:2016 outlines the minimum content requirements for an effective incident management policy. These include:
Purpose and objectives of the policy
Scope and applicability
Roles and responsibilities
Key terminology and definitions
High-level processes for incident detection, reporting, response, and learning Obligations of internal stakeholders Leona's decision to base the initial policy draft on Clause 4.3 is fully compliant and appropriate, as it ensures foundational consistency. ISO/IEC 27035-2 explicitly states that these elements form the minimum baseline for effective policy creation, and the document can be expanded later as needed.
Reference:
ISO/IEC 27035-2:2016, Clause 4.3: "The information security incident management policy should, at a minimum, contain the following elements..." Therefore, the correct answer is B: Yes, because as a minimum, the policy must cover the elements provided in clause 4.3 of ISO/IEC 27035-2.
-

質問 # 46
Scenario 7: Located in central London, Konzolo has become a standout innovator in the cryptocurrency field.
By introducing its unique cryptocurrency, Konzolo has contributed to the variety of digital currencies and prioritized enhancing the security and reliability of its offerings.
Konzolo aimed to enhance its systems but faced challenges in monitoring the security of its own and third- party systems. These

issues became especially evident during an incident that caused several hours of server downtime This downtime was primarily caused by a third-party service provider that failed to uphold strong security measures, allowing unauthorized access.
In response to this critical situation, Konzolo strengthened its information security infrastructure. The company initiated a comprehensive vulnerability scan of its cryptographic wallet software, a cornerstone of its digital currency offerings The scan revealed a critical vulnerability due to the software using outdated encryption algorithms that are susceptible to decryption by modern methods that posed a significant risk of asset exposure Noah, the IT manager, played a central role in this discovery With careful attention to detail, he documented the vulnerability and communicated the findings to the incident response team and management. Acknowledging the need for expertise in navigating the complexities of information security incident management. Konzolo welcomed Paulina to the team. After addressing the vulnerability and updating the cryptographic algorithms, they recognized the importance of conducting a thorough investigation to prevent future vulnerabilities. This marked the stage for Paulina s crucial involvement. She performed a detailed forensic analysis of the incident, employing automated and manual methods during the collection phase. Her analysis provided crucial insights into the security breach, enabling Konzolo to understand the depth of the vulnerability and the actions required to mitigate it.
Paulina also played a crucial role in the reporting phase, as her comprehensive approach extended beyond analysis. By defining clear and actionable steps for future prevention and response, she contributed significantly to developing a resilient information security incident management system based on ISO/IEC
27035-1 and 27035-2 guidelines. This strategic initiative marked a significant milestone in Konzolo's quest to strengthen its defenses against cyber threats Based on scenario 7, a vulnerability scan at Konzolo revealed a critical vulnerability in the cryptographic wallet software that could lead to asset exposure. Noah, the IT manager, documented the event and communicated it to the incident response team and management. Is this acceptable?

- A. No, he should have waited for confirmation of an actual asset exposure before documenting and communicating the vulnerability
- B. Yes, he should document the event and communicate it to the incident response team and management
- C. No, he should have postponed the documentation process until a full investigation is completed

正解：B

解説：
Comprehensive and Detailed Explanation From Exact Extract:
According to ISO/IEC 27035-1:2016, an information security event should be documented and communicated as soon as it is identified-particularly if it has the potential to escalate into an incident. Timely documentation and escalation enable the organization to take immediate and coordinated actions, which are essential to managing risk effectively.
Clause 6.2.1 of ISO/IEC 27035-1 states that events, even before confirmation as incidents, must be logged and assessed to determine appropriate response measures. Waiting until after a breach occurs or delaying documentation may violate both internal policies and regulatory requirements, especially in high-risk domains like cryptocurrency.
Therefore, Noah's actions align fully with the recommended practices outlined in ISO/IEC 27035.
Reference:
* ISO/IEC 27035-1:2016, Clause 6.2.1: "All identified information security events should be recorded and communicated to ensure appropriate assessment and response."
* Clause 6.2.2: "Early communication and documentation are crucial to managing potential incidents effectively." Correct answer: C
-

質問 # 47
Which method is used to examine a group of hosts or a network known for vulnerable services?

- A. Security testing and evaluation
- B. Penetration testing
- C. Automated vulnerability scanning tool

正解：C

解説：
Comprehensive and Detailed Explanation:
An automated vulnerability scanning tool is designed specifically to scan systems, hosts, or networks for known vulnerabilities based on a maintained vulnerability database. These tools are efficient for covering large environments quickly and are commonly used in routine security assessments.
Security testing and evaluation (A) is broader and includes manual assessments. Penetration testing (C) simulates real-world attacks but is usually more targeted and time-intensive.
Reference:

ISO/IEC 27002:2022, Control A.5.27: "Automated vulnerability scanning should be used to identify technical vulnerabilities."
Correct answer: B
-

質問 # 48
.....

ISO-IEC-27035-Lead-Incident-Manager試験問題を購入する前に、無料でダウンロードして試してみることができます。また、WebサイトのISO-IEC-27035-Lead-Incident-Manager学習ガイドのページにアクセスして、ISO-IEC-27035-Lead-Incident-Manager試験問題を理解することができます。 TopexamのISO-IEC-27035-Lead-Incident-Managerガイドトレントのページはデモを提供し、タイトルの一部とソフトウェアの形式を理解できます。そのため、購入する前にISO-IEC-27035-Lead-Incident-Manager試験問題を理解し、ISO-IEC-27035-Lead-Incident-Manager試験問題を購入するかどうかを決定できます。

ISO-IEC-27035-Lead-Incident-Manager受験対策解説集: https://www.topexam.jp/ISO-IEC-27035-Lead-Incident-Manager_shiken.html

- ISO-IEC-27035-Lead-Incident-Manager過去問無料 □ ISO-IEC-27035-Lead-Incident-Manager試験関連赤本 □ ISO-IEC-27035-Lead-Incident-Manager参考書勉強 □ □ www.japancert.com □は、[ISO-IEC-27035-Lead-Incident-Manager]を無料でダウンロードするのに最適なサイトですISO-IEC-27035-Lead-Incident-Manager認証資格
- PECBのISO-IEC-27035-Lead-Incident-Manager認証試験の最新の訓練の手引き □ { www.goshiken.com }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模擬試験最新版
- ISO-IEC-27035-Lead-Incident-Manager試験の準備方法 | 実用的なISO-IEC-27035-Lead-Incident-Manager無料問題試験 | 真実的なPECB Certified ISO/IEC 27035 Lead Incident Manager受験対策解説集 □ ➥ www.jpexam.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模擬問題集
- ISO-IEC-27035-Lead-Incident-Manager赤本合格率 □ ISO-IEC-27035-Lead-Incident-Manager受験料 □ ISO-IEC-27035-Lead-Incident-Manager認証資格 □ 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日本語版参考資料
- ISO-IEC-27035-Lead-Incident-Manager日本語版参考資料 □ ISO-IEC-27035-Lead-Incident-Manager勉強の資料 □ ISO-IEC-27035-Lead-Incident-Manager資格練習 □ □ www.jpexam.com □に移動し、➥ ISO-IEC-27035-Lead-Incident-Manager □を検索して、無料でダウンロード可能な試験資料を探しますISO-IEC-27035-Lead-Incident-Manager模擬試験最新版
- 高品質なISO-IEC-27035-Lead-Incident-Manager無料問題一回合格-実用的なISO-IEC-27035-Lead-Incident-Manager受験対策解説集 □ 検索するだけで➤ www.goshiken.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模擬試験最新版
- 実用的なISO-IEC-27035-Lead-Incident-Manager無料問題試験-試験の準備方法-素晴らしいISO-IEC-27035-Lead-Incident-Manager受験対策解説集 □▹ 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最新対策問題
- 素晴らしいISO-IEC-27035-Lead-Incident-Manager無料問題 - 合格スムーズISO-IEC-27035-Lead-Incident-Manager受験対策解説集 | 正確的なISO-IEC-27035-Lead-Incident-Manager日本語 □ □ 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日本語解説集
- 素敵なISO-IEC-27035-Lead-Incident-Manager無料問題試験-試験の準備方法-最新のISO-IEC-27035-Lead-Incident-Manager受験対策解説集 □ 最新【 ISO-IEC-27035-Lead-Incident-Manager 】問題集ファイルは《 www.pass4test.jp 》にて検索ISO-IEC-27035-Lead-Incident-Manager模擬問題集
- 高品質なISO-IEC-27035-Lead-Incident-Manager無料問題一回合格-実用的なISO-IEC-27035-Lead-Incident-Manager受験対策解説集 □ □ www.goshiken.com □を入力して➡ ISO-IEC-27035-Lead-Incident-Manager □□□を検索し、無料でダウンロードしてくださいISO-IEC-27035-Lead-Incident-Manager受験料
- ISO-IEC-27035-Lead-Incident-Manager参考書勉強 □ ISO-IEC-27035-Lead-Incident-Manager勉強ガイド □ ISO-IEC-27035-Lead-Incident-Manager模擬試験最新版 □ □ www.pass4test.jp □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模擬問題
- 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, 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, shortcourses.russellcollege.edu.au, learn.cnycreativeconcepts.com, billfor6581.suomiblog.com,

BONUS！！！ Topexam 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=1O85_W18OfKUE299YFjWVpcUzJMGLkWyj