

PECB.ISO-IEC-27001-Lead-Auditor-CN.v2026-08-07.q294

試験コード:	ISO-IEC-27001-Lead-Auditor-CN
試験名称:	PECB Certified ISO/IEC 27001 Lead Auditor exam (ISO-IEC-27001-Lead-Auditor中文版)
認定資格:	PECB
無料問題数:	294
バージョン:	v2026-08-07
アクセス数:	108
ページビュー数:	2940
https://www.jpnpdf.com/PECB.ISO-IEC-27001-Lead-Auditor-CN.v2026-08-07.q294-mondaishu.html	

最新問題: 1

質問

当社の経営陣は、情報セキュリティマネジメントシステム（ISMS）の導入状況を報告する担当者を社内から指名しました。これらの担当者は、関連するISMSデータの収集、報告書の作成、および必要な情報を経営陣に確実に伝達する責任を負っています。

この方法はISO/IEC 27001の要件を満たしていますか？

- A. はい、上級幹部は責任と権限を割り当てることができ、ISMSのパフォーマンスを報告する責任があるからです。
- B. いいえ、ISMSのパフォーマンスに関するデータを収集する責任はトップマネジメントのみにあるからです。
- C. いいえ、情報セキュリティ管理システムのパフォーマンスについて報告できるのは最高情報セキュリティ責任者だけだからです。

Answer: (解答を表示する)

このアプローチはISO/IEC 27001:2022に準拠しています。なぜなら、同規格では、ISMSの効果的な運用（パフォーマンス報告を含む）に関して、経営陣が責任と権限を割り当ててることを明示的に認めているからです。ISO/IEC 27001の5.3項では、経営陣は情報セキュリティに関連する役割、責任、権限が組織内で割り当てられ、周知されていることを確認する必要があると規定されています。

ISMSに対する最終的な責任は経営陣にあります。規格では経営陣が自らデータを収集したり、報告書を作成したり、運用監視活動を実施したりすることを義務付けていません。実際には、これらの作業はISMSマネージャー、セキュリティチーム、またはパフォーマンスデータの収集と分析に適したその他の担当者に委任されることがよくあります。重要なのは、経営陣がガバナンス責任を果たすことができるよう、情報がタイムリーかつ正確に経営陣に届くことです。

選択肢Bは、説明責任と責任を誤解しているため誤りです。経営陣はISMSのパフォーマンスに対して責任を負いますが、関連するすべてのタスクを自ら実行する必要はありません。選択肢Cは、ISO/IEC 27001では最高情報セキュリティ責任者（CISO）が報告権限者でなければならないとは規定されていないため誤りです。組織は、その構造、規模、状況に基づいて役割を自由に定義できます。

したがって、ISMSのパフォーマンスについて報告する担当者を個別に割り当ててことは、ISO/IECの基準に完全に合致している。

27001の要件。

最新問題: 2

場景 1 :Fintive 是一家傑出的線上支付和保護解決方案安全提供者。Fintive 於 1999 年由 Thomas Fin 在加州聖荷西創立，為線上營運 希望提高資訊安全、防止詐欺並保護 PII 等用戶資訊的公司提供服務。Fintive的決策和營運流程以以往的案例為中心。他們收集客戶數據，根據情況進行分類並進行分析。該公司需要大量員工才能進行如此複雜的分析。然而，幾年後，協助進行此類分析的技術也取得了進展現在，Fintive 正計劃使用現代工具聊天機器人來實現模式分析，以即時防止詐騙。該工具也將用於幫助改善客戶服務。

這個最初的想法已傳達給軟體開發團隊，他們支持該想法並被分配從事該專案。他們開始將聊天機器人整合到現有系統中。此外，團隊也為聊天機器人設定了一個目標，即回答5% 的聊天查詢。

聊天機器人成功整合後，該公司立即將其發布給客戶使用。

然而，聊天機器人似乎存在一些問題。

由於測試不足，並且在訓練階段缺乏向聊天機器人提供的樣本（在訓練階段，聊天機器人本應學習「口詢模式」），因此聊天機器人無法解決用口口詢並提供正確的答案此外，當聊天機器人收到無效輸入（例如奇怪的點圖案和特殊字元）時，它會向使用者發送隨機檔案。因此，聊天機器人無法正確回答客口的口詢，而傳統的客口支援因聊天口詢而不堪重負，因此無法幫助客口解決他們的請求。因此，Fintive 制定了軟體開發政策。該政策規定，無論軟體是口部開發還是外包，在作業系統上實施之前都將經過黑盒測試。根據該場景，回答以下問題：

在訓練階段測試不充分且缺乏向 Fintive 聊天機器人提供的樣本被視為 1。

參考場景

A. 威脅

B. 漏洞

C. 風險

Answer: B ([メッセージを残す](#))

最新問題: 3

監査人の能力は、知識とスキルの組み合わせです。以下の活動のうち、主に「知識」に関連するものはどれですか？（2つ選択）

A. 発見結果を特定する方法を理解する

B. デザインリスト

C. 準備チェックリストからの逸脱について監査証跡を追跡する

D. 被監査者とのコミュニケーション

E. 被監査者から証拠を収集する方法を決定する。

F. どの証拠を収集するかを決定する

Answer: B,F ([メッセージを残す](#))

知識とは、特定の主題または分野に関連する事実、概念、原則、理論、および実践に関する理解のことです。スキルとは、知識を応用し、ノウハウを使用してタスクを完了し、問題を解決する能力のことです。ISO 19011:2018によると、監査員の知識とスキルには次のものが含まれます。

* Knowledge of audit principles, procedures and methods

* Knowledge of management system standards and reference documents

* Knowledge of the organization's context, scope, processes and objectives

* Knowledge of relevant legal, regulatory and contractual requirements

* Knowledge of applicable industry, sector or technical disciplines

* Knowledge of risk management and risk-based thinking

* Skill in collecting and verifying information

* Skill in evaluating conformity and effectiveness of management systems

* Skill in reporting and communicating audit results

* Skill in managing audit activities and teams

Based on this, the activities that are predominately related to knowledge are designing a checklist and determining what evidence to gather, as they require the auditor to understand the audit criteria, scope, objectives and methods, as well as the organization's context, processes and risks. The other activities are more related to skills, as they involve applying knowledge and using know-how to perform tasks and solve problems during the audit.

References:

ISO 19011:2018, Guidelines for auditing management systems, clauses 7.2.1, 7.2.2 and 7.2.3
PECB Candidate Handbook - ISO 27001 Lead Auditor, pages 9-10 and 16-17
ISO 9001 Auditing Practices Group Guidance on: Auditing Competence, pages 2-3 and 8

最新問題: 4

ISO/IEC 27001によると、情報セキュリティマネジメントシステムは、次のうちどれとどれを保護するために設計されているか？

- A. 情報のアクセス可能性
- B. メッセージの信憑性
- C. 情報の機密保持
- D. 情報の一貫性
- E. 情報統合
- F. 情報の完全性

Answer: C,F (メッセージを残す)

ISO/IEC 27001は、CIAトライアドの中核となる原則に焦点を当てています。

*機密保持：情報のアクセスは、権限のある個人のみに限定する。

*完全性：情報の正確性と完全性を維持し、不正な改ざんから保護すること。

*可用性：情報は、必要なときに権限のあるユーザーがアクセスできる必要があります (これも重要ですが、この特定の質問の選択肢には含まれていません)。

参考文献：

*ISO/IEC 27001:2022、セクション4.2（利害関係者のニーズと期待の理解）このセクションでは、機密性、完全性、可用性への対応を含む、情報セキュリティに関連する利害関係者とその要求を特定することの重要性を強調しています。

*PECB候補者ハンドブック、ISO/IEC 27001主任監査員 :このハンドブックでは、効果的な情報セキュリティマネジメントシステム (ISMS)におけるCIAトライアドの基礎的な役割がしばしば強調されています。

最新問題: 5

質問

ISO/IEC 27001認証を取得したソフトウェア開発会社であるXYZ社は、認証取得から1年後、予定されていたサーベイランス監査を受け入れる準備ができていないことを認証機関に通知し、監査を受けることを拒否しました。この状況はどのような直接的な影響を及ぼすでしょうか？

- A. 認証が一時停止されました。
- B. 現在の認証は、次回の監視監査まで有効です。
- C. 会社は、認証を別の認証機関に移管するために、正式な認証移管プロセスを開始する必要があります。

Answer: A (メッセージを残す)

直接的な結果として認証が停止されるため、選択肢Aが正解となります。ISO/IEC 17021-1では、認証を受けた組織は、規格への継続的な適合性を検証するために、定期的なサーベイランス監査を受け入れなければならないと明確に規定されています。サーベイランス監査は必須であり、3年間の認証サイクルの一部を構成します。

監視監査の実施を拒否または怠ると、認証機関はISMSが有効かつ法令遵守していることを確認できなくなります。これにより、認証の有効性に対する信頼が失われます。そのため、認証機関は監査が実施され、適合性が再確立されるまで認証を一時停止する必要があります。

Option B is incorrect because certification validity is conditional upon ongoing surveillance. Certification does not remain valid if mandatory audits are refused. Option C is incorrect because transferring certification does not remove the obligation to undergo surveillance audits; a transfer would still require evidence of conformity and audit continuity.

Suspension is a protective mechanism to ensure that ISO/IEC 27001 certificates remain credible and trustworthy. If the organization later agrees to the audit and resolves issues, the certification may be reinstated. Therefore, refusal to undergo a surveillance audit leads to immediate suspension.

最新問題: 6

文を最も適切に完成させる単語を選びなさい。

「マネジメントシステムにおけるコンプライアンス維持の目的は、最適な単語で文章を完成させることです。完成させたい空欄をクリックして赤色でハイライト表示し、該当するテキストをクリックしてください。または、オプションを該当する空欄にドラッグ&ドロップすることもできます。」

“The purpose of maintaining regulatory compliance in a management system is to .”

To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

keep good relations
with authorities

pass the audit

avoid financial penalties

fulfil management
system policy

Answer:

“The purpose of maintaining regulatory compliance in a management system is to

fulfil management
system policy

.”

To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

keep good relations
with authorities

pass the audit

avoid financial penalties

fulfil management
system policy

“The purpose of maintaining regulatory compliance in a management system is to

fulfil management system policy

.”

最新問題: 7

シーン8 : テス

1. マリクとマイケルは、セキュリティ、コンプライアンス、事業計画および戦略の分野における独立した資格を有する専門家で構成された監査チームです。彼らは、大手ウェブデザイン会社であるクラスタス社に対し、認証監査を実施しました。監査中、彼らは公平性と客観性を含み卓越した職業倫理を示しました。今回、クラスタス社は、ISO/IEC 27001認証を取得できれば、一歩リードできると確信しています。

監査チームリーダーのテッサは、監査に関する専門知識を有し、IT関連の問題、コンプライアンス、ガバナンスにおいて非常に優れた実績を持っています。マリクは、組織計画とリスク管理のバックグラウンドを持ち、組織のセキュリティ管理とリスク許容度に対する包括的かつ分析的なアプローチに基づき、組織内のリスクレベルを正確に把握することに長けています。一方、マイケルは、厳格な標準化された手順に従って実施される管理評価を通じて、実践的なセキュリティに関する専門知識を有しています。

必要な監査活動を実施した後、テッサは監査チーム会議を開始し、そこでマイケルの発見事項の1つを分析して、その問題について客観的かつ正確な決定を下しました。マイケルが遭遇した問題は、組織の日常業務における些細な問題であり、彼はそれがIT技術者によって引き起こされたと考えていました。そこで、テッサは上級管理職と面談し、責任者の名前を尋ねた後、誰が責任を負うべきかを伝えました。明確化と理解を促進するため、テッサは監査最終日に最終会議を招集しました。この会議で、彼女は発見された不適合をクラスタスの経営陣に報告しました。しかし、テッサはクラスタスの認証監査報告書に不必要な証拠を記載しないように助言され、報告書が簡潔で主要な発見事項に焦点を当てたものになるようにしました。

監査チームは、検討した証拠に基づき監査結論案を作成し、認定を与える前に組織の2つの分野を監査する必要があると判断した。これらの決定は後に被監査組織に提出されたが、被監査組織は調査結果を受け入れず、追加情報を要求した。被監査組織の意見にもかかわらず、監査人は既に認定勧告を受け入れることを決定していたため、追加情報は受け入れなかった。被監査組織の上級管理職は、監査結論は事実を反映していないと主張したが、監査チームは決定を維持した。

上記のシナリオに基づいて、以下の質問に教えてください。

TessaはClastus認証監査報告書に不必要な証拠を提出することを避けるべきだと推奨されています。これは推奨されるのでしょうか？

A. はい、監査の機密性を損なう可能性のある情報を含めないようにするためです。

B. はい、報告書を簡略化して理解しやすくするためです。

C. いいえ、関連するすべての証拠が考慮され、処理されるようにするためです。

Answer: [\(解答を表示する\)](#)

包括的かつ詳細な徹底分析

C. 正解：

ISO 19011:2018では、監査報告書には監査結果を裏付けるすべての関連証拠を含めることが求められています。

簡潔さを優先して証拠を省略することは、透明性と信頼性を損なう。

A. 不正解：

監査の機密性は、証拠を隠蔽することによってではなく、アクセスを制限することによって保護される。

B. 不正解：

明瞭さは重要だが、完全性を犠牲にしてはならない。

関連規格参照：

ISO 19011:2018 6.7項（監査報告のベストプラクティス）

最新問題: 8

文を最も適切に完成させる単語を選びなさい。

Select the words that best complete the sentence:

“The purpose of a third-party audit is to _____ an organisation’s _____ to inform _____ decision.”

To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

approve

inspect

a compliance

an accreditation

products

evaluate

management system

a certification

processes

Answer:

Select the words that best complete the sentence:

"The purpose of a ~~third-party audit~~ is to, evaluate an organisaticmanagement system inform a certification decision."

To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

approve inspect a compliance an accreditation products evaluate management system a certification processes

Explanation:

第三者監査とは、組織やその顧客と関係のない外部監査人が、組織のマネジメントシステムを独立して評価することです。監査人は、マネジメントシステムがISO 27001などの特定の規格の要求事項を満たしていることを確認し、その有効性とパフォーマンスを評価します。また、監査人はマネジメントシステムの強み、弱み、機会、リスクを特定し、改善のための勧告を行います。第三者監査の目的は、組織のマネジメントシステムを客観的かつ公平に評価し、認証機関による認証決定に役立てることです。認証機関とは、監査報告書と証拠を審査し、マネジメントシステムが認証基準を満たしていることを確認した後、組織に適合証明書を発行する組織です。認証決定は認証プロセスの結果であり、肯定的（認証の付与、維持、更新、または範囲の拡大）または否定的（認証の停止、取り消し、または範囲の縮小）のいずれかです。参考文献：

* PECB候補者ハンドブック ISO 27001主任審査員、19～25ページ

* ISO 19011:2018 - マネジメントシステムの監査に関する指針

* ISO 27001監査プロセス | ISMS.online

"The purpose of a third-party audit is to evaluate an organisation's management system to inform a certification decision."

To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

最新問題: 9

以下の事項を定義する際には、法令遵守違反および法的 契約上の要件の不遵守に伴うコストを評価してください。

- A. 重要性
- B. 監査リスク
- C. 合理的な保証

Answer: A ([メッセージを残す](#))

監査における重要性とは、法令遵守や契約遵守に関するものを含め、どの程度の不適合や不備が監査結果に影響を与えるほど重大なものとなるかを評価することです。重要性を判断する際には、これらの問題に関連する費用も考慮されます。

最新問題: 10

監査人の能力は、知識とスキルの組み合わせです。以下の活動のうち、主に 知識」に関連するものはどれですか？ 2つ選択)

- A. 発見結果を特定する方法を理解する
- B. デザインリスト
- C. 準備チェックリストからの逸脱について監査証跡を追跡する
- D. 被監査者とのコミュニケーション
- E. 被監査者から証拠を収集する方法を決定する。

F. どの証拠を収集するかを決定する

Answer: B,F (メッセージを残す)

知識とは、特定の主題または分野に関連する事実、概念、原則、理論、および実践に関する理解のことです。スキルとは、知識を応用し、ノウハウを使用してタスクを完了し、問題を解決する能力のことです。ISO 19011:2018によると、監査員の知識とスキルには次のものが含まれます。

監査の原則、手順、方法に関する知識

* マネジメントシステム規格および参照文書に関する知識

組織の状況、範囲、プロセス、目標に関する知識

* 関連する法律、規制、契約上の要件に関する知識

* 該当する業界、分野、または技術分野に関する知識

リスク管理とリスクベース思考に関する知識

情報の収集と検証に関するスキル

* マネジメントシステムの適合性および有効性を評価する能力

監査結果の報告および伝達に関するスキル

監査活動およびチームの管理スキル

これに基づくと、知識に大きく関連する活動は、チェックリストの作成と収集すべき証拠の決定であり、これらは監査人が監査基準、範囲、目的、方法、そして組織の状況、プロセス、リスクを理解する必要があるためである。その他の活動は、監査中に知識を応用し、ノウハウを用いて業務を遂行し、問題を解決するためであり、スキルにより関連している。

参考文献：

* ISO 19011:2018、マネジメントシステムの監査に関する指針、7.2.1項、7.2.2項および7.2.3項

* PECB候補者ハンドブック - ISO 27001主任審査員、9～10ページおよび16～17ページ

* ISO 9001監査実務グループガイダンス：監査能力2～3ページおよび8ページ

最新問題: 11

您正在對位於歐洲的住宅進行 ISMS 審核

名為 ABC 的療養院提供醫療保健服務。您會發現所有療養院居民都戴著電子腕帶，用於監控他們的位置 心跳和血壓。您了解到，電子腕帶會自動將所有資料上傳到人工智慧 AI）雲端伺服器，供醫護人員進行健康監測和分析
審核計畫的下一步是驗證高階管理人員是否已製定資訊安全策略和目標。

在審計過程中，你們發現以下審計證據

將審核證據與 ISO/IEC 27001:2022 中的相應要求進行配對。

Audit Evidence	ISO/IEC 27001:2022 Requirements
The top management has signed and approved the ISMS policy (Document reference ID: ISMS_L1_01, version 1.3), mobile device policy (Document reference ID: ISMS_L2_07, version 1, release 4), and information security objectives are linked to Annex A's information security control objectives.	
Testing on 5 medical staff's mobile phones, all mobile phones are pin code protected screen lock and the 15 digits IMEI (International Mobile Equipment Identity) are registered in the asset register (Document reference ID: ISMS_L4_01, version 2.1).	
Interview with IT staff (employee ID: NH-1268); he is well informed and understood the mobile device policy. You checked his mobile phone and found it is 6 digits pin code protected and NO resident's data is stored.	
Interview with human resource manager; sampling on medical staff's information security roles and responsibilities are assigned in the job description (Document reference ID: ISMS_L4_04, version 1.0).	

To complete the table click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop each of the following ISO/IEC 27001 clauses to the correct statement.

Clause 5.1 a

Clause 7.3

A.8.1

Clause 5.3

Answer:

Audit Evidence	ISO/IEC 27001:2022 Requirements
The top management has signed and approved the ISMS policy (Document reference ID: ISMS_L1_01, version 1.3), mobile device policy (Document reference ID: ISMS_L2_07, version 1, release 4), and information security objectives are linked to Annex A's information security control objectives.	Clause 5.1 a ☐
Testing on 5 medical staff's mobile phones, all mobile phones are pin code protected screen lock and the 15 digits IME (International Mobile Equipment Identity) are registered in the asset register (Document reference ID: ISMS_L4_01, version 2.1).	A.8.1 ☐
Interview with IT staff (employee ID: NH-1268); he is well informed and understood the mobile device policy. You checked his mobile phone and found it is 6 digits pin code protected and NO resident's data is stored.	Clause 7.3 ☐
Interview with human resource manager; sampling on medical staff's information security roles and responsibilities are assigned in the job description (Document reference ID: ISMS_L4_04, version 1.0).	Clause 5.3 ☐

To complete the table click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop each of the following ISO/IEC 27001 clauses to the correct statement.

Clause 5.1 a

Clause 7.3

A.8.1

Clause 5.3

最新問題: 12

以下の規格のうち、ISMSの第三者認証における監査基準として使用されるのはどれか（2）？

- A. ISO/IEC 27002
- B. ISO/IEC 20000-1
- C. ISO 19011
- D. ISO/IEC 27001

- E. 関連する法律、規制、および規制要件
- F. ISO/IEC 17021-1

Answer: D,E (メッセージを残す)

ISMSの第三者認証監査基準として使用される2つの規格は、ISO/IEC 27001と関連する法的、法令、規制要件です。ISO/IEC 27001は、情報セキュリティマネジメントシステム (ISMS)の確立、実装、維持、および継続的改善のための要件を規定しています1。関連する法的、法令、規制要件とは、組織の情報セキュリティの側面と目標に適用される要件です2。その他の選択肢は、規格ではない (E)か、ISMS認証監査基準に直接関係しない (A、B、C、F)ものです。参照 :1 :ISO/IEC 27001:2022、情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項、第1項 2 :ISO/IEC 27001:2022、情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項、第4.2項

最新問題: 13

以下は、情報セキュリティの基本要素の一つである「完全性」の目的です。

- A. 情報は、権限のない個人に提供または開示されることはありません。
- B. 資産の正確性と完全性を保証する属性。
- C. 情報は、権限のない個人に提供または開示されることはありません。
- D. 権限のあるエンティティの要件に応じてアクセスおよび使用できる属性。

Answer: B (メッセージを残す)

完全性は、機密性および可用性と並んで、情報セキュリティの基本要素の一つです。完全性とは、情報の正確性や完全性に影響を与える可能性のある、不正または偶発的な変更から情報が保護されていることを意味します。完全性によって、情報は信頼性が高く、信用できるものとなります。3. 参照 :ISO/IEC 27001:2022 主任監査員研修コース - BSI

最新問題: 14

あなたは経験豊富な監査チームリーダーであり、監査員の研修を指導する立場にあります。

貴チームは現在、外部顧客のためにデータを保管する組織に対し、第三者監視監査を実施しています。訓練を受けた監査担当者は、適合性報告書 (SoA)に記載され、現場で実施されている人事管理体制を検証する任務を負っています。

研修を希望する監査担当者にレビューしてもらいたい管理項目を、以下のリストから4つ選択してください。

- A. 機密保持および機密保持契約
- B. マルウェア対策の実装方法
- C. 情報セキュリティに関する意識向上、教育、トレーニング
- D. リモートワーク体制
- E. 人員の確認とチェック。
- F. 現場監視カメラおよび入退室管理システムの運用
- G. 組織の情報削除に関する取り決め
- H. 組織の事業継続計画

Answer: A,C,D,E (メッセージを残す)

PEOPLEコントロールは、役割と責任、意識向上とトレーニング、スクリーニングと契約、リモートワークなど、情報セキュリティの人的側面に関連するものです。研修中の監査担当者は、以下のコントロールを確認する必要があります。

機密保持契約および秘密保持契約 A) これらは、組織の従業員および契約業者に対し、取り扱う情報、特に外部顧客のデータの機密性を保護することを義務付ける契約上の義務です。監査人は、これらの契約が組織によって署名、更新、および履行されているかどうかを確認する必要があります。この管理は、ISO/IEC 27001:2022のA.7.2.1項に関連しています。

情報セキュリティに関する意識向上、教育、および研修 :これらは、従業員および契約社員の情報セキュリティに関する知識、スキル、および行動を向上させることを目的とした活動です。監査担当者は、これらの活動が組織によって計画、実施、評価、および改善されているかどうかを確認する必要があります。この管理策は、ISO/IEC 27001:2022 の条項 A.7.2.2 に関連しています。

リモートワークに関する取り決め D) これは、自宅や公共の場所など、組織の施設以外の場所から業務を行う場合の情報セキュリティ面を規定する方針と手順です。監査担当者は、これらの取り決めが組織によって定義、承認、監視されているかどうかを確認する必要があります。この管理策は、ISO/IEC 27001:2022のA.6.2.1項に関連しています。

従業員の身元確認チェックの実施 E) これは、機密情報またはシステムにアクセスする従業員および契約者の身元、資格、および適性を確認するための身元調査です。監査員は、これらのチェックが組織によって実施、文書化、およびレビューされているかどうかを確認する必要があります。この管理策は、ISO/IEC 27001:2022 の A.7.1.1 項に関連しています。

参照：
ISO/IEC 27001:2022、情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステム - 要求事項 PECB 候補者ハンドブック ISO/IEC 27001 主任監査員、1 ISO 27001:2022 主任監査員 - IECB、2 ISO 27001:2022 認定 ISMS 主任監査員 - Jisc、3 ISO/IEC 27001:2022 主任監査員移行トレーニングコース、4 ISO 27001 - 情報セキュリティ主任監査員コース - PwC トレーニングアカデミー、5

最新問題: 15
以下の選択肢の中から、文を最も適切に完成させる単語を選びなさい。
単語一つで文を完成させるには、完成させたい空白部分をクリックして赤くハイライト表示し、表示されるオプションから 「アプリテキスト」をクリックします。または、オプションを適切な空白部分にドラッグすることもできます。

"The purpose of a management system audit is to [] the performance of an organisation's management system."

improve manage evaluate research

Answer:

"The purpose of a management system audit is to evaluate the performance of an organisation's management system."

improve manage evaluate research

最新問題: 16
第三者認証監査においては、効果的なコミュニケーションが非常に重要です。監査におけるコミュニケーションに関する正しい回答を含む選択肢を選んでください。
A. 監査中、各監査人は定期的に懸念事項を被監査者および監査依頼者に伝える必要があります。
B. 監査中は、監査チームリーダーがコミュニケーションを担当します。
C. 監査チームと被監査者との間の正式なコミュニケーションチャネルは、最初の会議中に確立することができます。
D. 正式な連絡手段は必要ありません。被監査者は監査期間中いつでも監査人と連絡を取ることができます。

Answer: C ([メッセージを残す](#))

第三者認証監査においては、監査チームと被監査機関との間で効果的なコミュニケーションを図ることが非常に重要です。監査チームメンバー、被監査機関の代表者、監査依頼者、その他関係者の氏名や連絡先といった正式なコミュニケーションチャネルは、初回会議で確立することができます。これにより、監査の目的、範囲、基準、方法、スケジュール、その他の取り決めが関係者全員に明確に理解され、合意されることが保証されます。また、監査プロセスにおける情報、フィードバック、要望、懸念事項、苦情の交換も円滑に行われます。

参照: = ISO 19011:2022、6.4.2項; PECB候補者ハンドブック ISO 27001主任審査員、25ページ。

有効な **ISO-IEC-27001-Lead-Auditor-CN** 問題集は GoShiken.com が提供された合格しやすい ISO-IEC-27001-Lead-Auditor-CN 試験問題集！ GoShiken.com が最新の **ISO-IEC-27001-Lead-Auditor-CN** 試験問題集を提供しています。GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 問題集をゲットする人はこちら：
<https://www.goshiken.com/PECB/ISO-IEC-27001-Lead-Auditor-CN-mondaishu.html> (**41830%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 17

ビジネスプロセスの計画・実行・評価・改善サイクルにおける「行動」の側面を表すのに適切なフレーズは次のうちどれですか？（2選択可）

A. 審査プロセス
B. 計画変更
C. 測定対象
D. ターゲットをリセット
E. 改善策を実施する
F. 検証トレーニング

Answer: D,E (メッセージを残す)

PDCAサイクルの「実行」フェーズでは、組織は「確認」フェーズの結果に基づいてプロセスとパフォーマンスを改善するための行動を起こします。これには、目標をより現実的、達成可能、または挑戦的なものにするために目標を再設定したり、問題の根本原因に対処して望ましい結果を達成するための変更を実施したりすることが含まれます。「実行」フェーズでは、組織は実行した行動の効果を監視し、その有効性と効率性を評価します。「実行」フェーズは、組織が経験から学び、ISMSを継続的に改善できるため重要です。参考文献：計画、実行、確認、改善」とは？継続的改善のためのフレームワーク、ISO27001におけるPDCA - 無料学習ガイド | Dr. Erdal Ozkaya、PECB候補者ハンドブック ISO 27001主任監査員（12ページ）

最新問題: 18

完成第一階段並準備第二階段初步認証審核後，受審核方通知審核小組負責人，他們希望擴大審核範圍，以包括該組織最近收購的另外兩個場所

考慮到這些訊息，您希望審計小組負責人採取什麼行動？

A. 增加第 2 階段審核的長度以包含額外的站點
B. 取得附加網站的資訊以通知認證機構
C. 安排使用視訊會議平台完成兩個站點的遠端第一階段審核
D. 通知審核方可以接受請求，但必須重複完整的第一階段審核

Answer: B (メッセージを残す)

マネジメントシステムの監査および認証を提供する機関の要求事項を規定するISO/IEC 17021-1によれば、認証機関は、認証の範囲、組織の規模と複雑さ、活動に伴うリスクなどの要素に基づいて、監査時間と監査チームの構成を決定するための基準を確立する必要がある2。したがって、被監査者が最初の認証監査のステージ1を完了した後、監査範囲を2つの追加サイトを含むように拡張することを要求した場合、監査チームリーダーは追加サイトに関する情報を入手して認証機関に通知し、認証機関が範囲の変更をレビューして承認し、監査時間と監査チームをそれに応じて調整できるようにする必要がある2。他の選択肢は、この状況で監査チームリーダーが取るべき適切な行動ではない。たとえば、認証機関に通知せずにステージ2監査の長さを延長して追加サイトを含めることは、認証機関の手順とポリシーに違反する可能性がある。ビデオ会議プラットフォームを使用して2つのサイトのリモートステージ1監査を完了するように手配することは、サイトの性質と場所によっては実現不可能または効果的ではない可能性がある。また、被監査対象者に対し、要求は受け入れられるものの、ステージ1の監査を全面的にやり直す必要があると通知することは、ステージ1以降、被監査対象者のISMSに大きな変更がない場合には、必ずしも必要または合理的ではない可能性がある。参照 :ISO/IEC 17021-1:2015 - 適合性評価 - マネジメントシステムの監査及び認証を提供する機関に対する要求事項 - 第1部：要求事項

最新問題: 19

シナリオ3 :Rebuildyはバンコクを拠点とする建設会社で、住宅の設計、建設、保守を専門としています。機密性の高いプロジェクトデータと顧客情報のセキュリティを確保するため、RebuildyはISO/IEC 27001に基づく情報セキュリティマネジメントシステム (ISMS)を導入することを決定しました。これには、情報セキュリティリスクの包括的な理解、継続的改善のための明確な方法論、そして堅牢なビジネスソリューションが含まれます。

情報セキュリティマネジメントシステム (ISMS)の導入結果を以下に示します。

情報セキュリティは、一連のセキュリティ対策を適用し、ポリシー、プロセス、手順を確立することによって実現されます。

安全管理措置はリスク評価に基づいて実施され、リスクを排除するか、許容可能なレベルまで低減するように設計されています。

すべてのプロセスは、情報セキュリティ管理システムの継続的な改善を確実にするために、計画・実行・評価・改善 (PDCA)モデルに基づいています。

情報セキュリティポリシーは、最良のセキュリティ慣行に基づいて作成されたセキュリティマニュアルの一部であるため、独立した文書ではありません。

各従業員の職務記述書には、情報セキュリティに関する役割と責任が明確に定義されています。

情報セキュリティマネジメントシステムの経営陣によるレビューは、計画された間隔で実施されます。

2回の中間経営レビューと年次内部監査を経て、Rebuildyは認証を申請しました。認証監査の前に、Rebuildyの元従業員が監査チームに連絡を取り、Rebuildyが隠蔽しようとしている複数のセキュリティ問題について報告しました。元従業員は監査チームに書面による証拠を提出しました。Rebuildyの主要顧客であるElectraも同じ問題について証拠を提出しましたが、監査チームは元従業員の証拠ではなくElectraの証拠を採用することにしました。監査完了前に、監査チームは監査中に発見されたコンプライアンス違反について話し合うため、Electraと連絡を取り続けました。Electraはこれらの調査結果を裏付ける補足証拠を提出しました。

監査は、監査チームが上級管理職へのインタビューを行うことから始まった。インタビューでは、情報セキュリティマネジメントシステム (ISMS)の導入に対する上級管理職の取り組みについて議論した。インタビューから得られた証拠は文書化され、RebuildyがISO/IEC 27001規格の特定の規定に準拠しているかどうかを判断した。Electraから入手した文書証拠と不適合報告書は、監査報告書に添付された。特定された不適合項目は以下のとおりである。

同社の財務報告システムが、不適切なユーザーアクセス制御設定を検出しました。

同社はまだ独立した情報セキュリティ戦略を策定していない。その代わりに、セキュリティに関するベストプラクティスに基づいたセキュリティマニュアルを使用している。

監査チームから文書を受け取った後、チームリーダーはRebuildyの経営陣と面談し、監査結果を報告した。監査チームは、財務報告システムに関する問題と、独立した情報セキュリティポリシーの欠如を報告した。経営陣は監査結果に不満を表明し、監査チームリーダーの行動はプロ意識に欠けると示唆し、リーダーの交代を要求する可能性を示唆した。プレッシャーを受けた監査チームリーダーは、経営陣と協力して、特定された違反の深刻度を軽視することにした。そのため、監査チームリーダーは報告書を改訂し、より好ましい内容にすることで、Rebuildyのコンプライアンス問題の真の深刻さを歪曲した。

上記のシナリオに基づいて、以下の質問に教えてください。

質問：

監査チームは、財務報告システムに関連する問題に対処する際に、最良の監査慣行に従ったか？

A. はい、それは監査の範囲外だからです。

B. いいえ、監査チームは認証機関に連絡して状況を報告する必要があります。

C. いいえ、その行為は違法であるため、監査チームは監査から撤退すべきです。

Answer: B (メッセージを残す)

包括的かつ詳細な解説：

* B. 正解:

* 財務報告システムの問題は重大なセキュリティ上の懸念事項であり、監査チームはさらなる措置を講じるため、この状況を認証機関に報告すべきだった。

* ISO 19011:2018では、監査員はコンプライアンスに影響を与える問題をエスカレーションすることが義務付けられています。

* A. 不正解:

* 金融システムは、機密データを含んでいる場合、ISMSの適用範囲に含まれます。適用範囲外ではありません。

* C. 不正解:

法的違反により効果的な監査が妨げられる場合を除き、撤回は不要です。

関連規格参照：

* ISO/IEC 27001:2022 条項 9.2 (内部監査) および ISO 19011:2018 条項 6.7 (監査後のフォローアップおよび重大な問題の報告)

最新問題: 20

下列哪兩個選項是使用抽樣計畫進行審核的優點？

- A. 否定審核員的直覺
- B. 減少審核時間
- C. 防止審核團隊口部發生衝突
- D. 增強對審核結果的信心
- E. 高效率實施審核計劃
- F. 使用計劃進行連續審核

Answer: B,D ([メッセージを残す](#))

A sampling plan for the audit is a method of selecting a representative subset of the audit evidence to evaluate the conformity of the ISMS1. The advantages of using a sampling plan are:

It reduces the audit duration by focusing on the most relevant and significant aspects of the ISMS2.

It gives confidence in the audit results by ensuring that the sample is sufficient, reliable, and unbiased3.

最新問題: 21

フィッシングとは、どのような種類の情報セキュリティインシデントですか？

- A. 個人的な問題
- B. ハッカー/突破攻撃
- C. 技術的な脆弱性
- D. 訴訟事件

Answer: B ([メッセージを残す](#))

Phishing is a type of information security incident that falls under the category of cracker/hacker attacks. Phishing is a form of fraud that uses deceptive emails or other messages to trick recipients into revealing sensitive information, such as passwords, credit card numbers, bank account details, etc. Phishing emails often impersonate legitimate organizations or individuals and create a sense of urgency or curiosity to lure the victims into clicking on malicious links, opening malicious attachments or providing personal information. Phishing is a common and serious threat to information security, as it can lead to identity theft, financial loss, data breach, malware infection or other damages. ISO/IEC 27001:2022 requires the organization to implement awareness and training programs to make users aware of the risks of social engineering attacks, such as phishing, and how to avoid them (see clause A.7.2.2). Reference: CQI & IRCA Certified ISO/IEC 27001:2022 Lead Auditor Training Course, ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements, What is Phishing?

最新問題: 22

パスワードを保護するためのガイドラインは以下のとおりですが、以下の場合には例外となります。

- A. 異なる社内システムへの安全なアクセスに同じパスワードを使用しないでください。
- B. パスワードは誰にも教えないでください。
- C. 覚えやすくするために、会社アカウントと個人アカウントでは同じパスワードを使用します。
- D. 初回ログイン時に一時パスワードを変更してください

Answer: ([解答を表示する](#))

以下はパスワードを保護するためのガイドラインです。覚えやすいという理由以外では、会社アカウントと個人アカウントで同じパスワードを使用してはいけません。パスワードを誰とも共有してはいけません。会社アカウントと個人アカウントで同じパスワードを使用することは、アカウントのいずれかがハッキングまたは侵害された場合にパスワードが漏洩するリスクが高まるため、パスワードを保護するためのガイドラインではありません。各アカウントには異なる固有のパスワードを使用し、定期的に変更する必要があります。パスワードを誰とも共有することは、パスワードのセキュリティと責任が低下するため、パスワードを保護するためのガイドラインではありません。パスワードは機密情報として扱い、たとえ権限がある、または信頼できると主張しても、誰にも開示してはいけません。さまざまな会社のシステムセキュリティアクセスに同じパスワードを使用しないことは、システムのいずれかが侵害または侵害された場合に、パスワードの不正アクセスや悪用を防ぐため、パスワードを保護するためのガイドラインです。

各システムには異なる複雑なパスワードを使用し、組織のパスワードポリシーと標準に従う必要があります。一時パスワードを最初のログオン時に変更することは、一時パスワードが傍受または漏洩した場合に不正アクセスやパスワードの悪用を防ぐため、パスワードを保護するためのガイドラインです。一時パスワードはできるだけ早く個人的で安全なパスワードに変更し、デフォルトまたは予測可能なパスワードの使用は避けてください。参考文献 :CQI & IRCA ISO 27001:2022 主任監査員コースハンドブック、43 ページ。[ISO/IEC 27001 主任監査員 - PECB]、15 ページ。

最新問題: 23

監査リソースを説明するために、次の文を最も適切に完成させる語句を選択してください。

"Audit resources include the _____ resources to complete the audit programme as well as _____ personnel to achieve the audit objectives."

To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

certification

technological

competent

management

backup

essential

Answer:

"Audit resources include the _____ resources to complete the audit programme as well as _____ personnel to achieve the audit objectives."

To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

certification

technological

competent

management

backup

essential

Explanation:

ISO 19011:2018の5.3項によれば、監査プログラムの管理責任者は、監査チームのメンバー、予算、時間、ツールなど、監査プログラムに必要なリソースを決定する必要があります。監査リソースは、監査プログラムと監査結果の質と有効性を確保するために十分かつ適切である必要があります。監査リソースには、次の要素が含まれます12:

* 必須リソース：監査プログラムおよび個々の監査を実施するために必要なリソースであり、監査文書、監査方法、監査ツール、監査スケジュール、監査予算などが含まれます。必須リソースは、監査の目的、範囲、基準、および被監査者の可用性と協力に基づいて特定および割り当てられる必要があります。また、必須リソースは、監査プログラムまたは個々の監査における変更や逸脱を反映するために、必要に応じて見直し、更新する必要があります。

* 有能な担当者：監査を効果的かつ効率的に実施し、信頼できる監査結果と勧告を提供するために必要な知識、スキル、経験を有する監査チームメンバーを指します。有能な担当者には、監査チームリーダー、監査担当者、および監査チームを支援する技術専門家やオブザーバーが含まれます。有能な担当者は、監査の目的、範囲、基準、および監査プログラムと個々の監査に求められる具体的な能力要件に基づいて選定・任命されるべきです。また、有能な担当者は独立性と公平性を保ち、監査結果や監査判断に影響を与える可能性のある利益相反や自己利益を避ける必要があります。

参考文献：

ISO 19011:2018 - マネジメントシステムの監査に関する指針、5.3項 PECB候補者ハンドブック ISO 27001主任監査員、19ページ

最新問題: 24

シナリオ7 :Webvueは、コンピュータソフトウェアの開発、サポート、保守を専門とする日本を拠点とするテクノロジー企業です。Webvueは、さまざまなテクノロジー分野や企業向けにソリューションを提供しています。同社の主力サービスはCloudWebvueで、ストレージ、ネットワーク、仮想コンピューティングサービスを提供する包括的なクラウドコンピューティングプラットフォームであり、企業ユーザーと個人ユーザー向けに設計されています。CloudWebvueは、その柔軟性、拡張性、信頼性で高い評価を得ています。

Webvueは、ISO/IEC 27001認証の範囲にCloudWebvueのみを含めることを決定しました。そのため、フェーズ1とフェーズ2の監査は同時に実施されました。Webvueは、資産の機密性に対する厳格な管理を誇りとしています。CloudWebvueに保存されている情報を保護するために、適切な暗号化制御を使用しています。内部使用、制限付き、機密など、あらゆるレベルの情報は、クラウドに保存される前に固有のハッシュ値で暗号化されます。監査チームは、Keith、Sean、Layla、Sam、Tinaの5名で構成されました。ITおよび情報セキュリティ監査チームで最も経験豊富な監査員であるKeithが監査チームリーダーを務めました。彼の責任には、監査の計画と監査チームの管理が含まれていました。SeanとLaylaは、プロジェクト計画、ビジネス分析、ITシステム（ハードウェアとアプリケーション）に関する豊富な経験を持っています。彼らのタスクには、Webvueの内部システムとプロセスに基づいた監査計画の策定が含まれていました。一方、SamとTinaは最近学業を修了し、日々のタスクを処理しながら監査スキルを向上させる責任を負っていました。ISO/IEC 27001の附属書Aにおける暗号化の使用に関する管理項目8.24への準拠を関係者へのインタビューを通じて検証した結果、監査チームは、暗号化キーが当初、乱数ビット生成器（RNG）およびその他の鍵生成に関するベストプラクティスに基づいて生成されていたことを発見した。Webvueの暗号化ポリシーを確認した結果、インタビューで得られた情報は正確であると結論付けた。しかし、ポリシーに暗号化キーの使用方法和ライフサイクルが明記されていなかったため、これらのキーは引き続き使用されていた。Webvueと認証機関の間で後に合意された内容に基づき、監査チームは仮想監査を選択し、認証範囲と監査目標を満たすために、WebvueがISO/IEC 27001規格の管理要件8.11（データ匿名化）に準拠しているかどうかを検証することに重点を置きました。監査チームはCloudWebvueの内部データ保護プロセスをレビューし、同社がポリシーと規制基準をどのように遵守しているかに焦点を当てました。監査プロセスの一環として、監査チームリーダーのKeithは、Webvueの慣行の有効性を文書化および分析するために、関連文書と暗号化キー管理プログラムのスクリーンショットをキャプチャしました。

Webvueはテストに生成されたテストデータを使用しています。しかし、品質保証マネージャーへのインタビューと部門のプロセスに基づく、リアルタイムのシステムデータが使用される場合もあります。これにより大量のデータが生成されますが、より正確な結果が得られます。テストデータの保護と管理は、監査中に暗号化プロセスをシミュレートしたWebvueの担当者によって検証されました。品質保証マネージャーへのインタビューで、キースは、セキュリティトレーニング部門の従業員が適切な手順に従っていないことを発見しました。この部門は監査範囲外でしたが、セキュリティトレーニング部門の不遵守は、監査範囲内のプロセス、特にCloudWebvueのデータセキュリティと暗号化の実践に影響を与える可能性があります。そのため、キースはこの発見を監査レポートに含め、被監査者に通知しました。

上記のシナリオに基づいて、以下の質問に答えてください。

質問：

シナリオ7に基づく、キースが監査報告書に安全研修部門を含めるという選択は適切でしょうか？

- A.** はい、彼は監査報告書に安全研修部門を含めるべきです。
- B.** いいえ、彼は監査対象者に観察内容を知らせることなく、それを含めるべきです。
- C.** いいえ、彼はそれを含めるべきではありませんでした。彼は監査対象者に、彼らが観察した内容だけを伝えるべきでした。

Answer: A ([メッセージを残す](#))

包括的かつ詳細な解説：

- * A. 正解:
 - * ISO 19011:2018では、監査員は、事前に定義された範囲外で発生した場合でも、監査範囲に影響を与える重要な問題を報告することが認められています。
 - * セキュリティトレーニング部門の不適合事項は、CloudWebvueのISMSに直接影響を与えたため、監査報告書に含めることが正当化される。

* B. 不正解:

監査において透明性は非常に重要であり、キースは報告前に被監査者に適切に情報を提供した。

* C. 不正解:

- * ISMSの導入に影響を与える問題は、認証範囲にリスクをもたらすため、報告しなければなりません。

関連規格参照：

- * ISO 19011:2018 条項 6.6.1（適用範囲外²が影響のある不適合に関する監査報告）

最新問題: 25

第1段階監査の初回会議において、マネジメントシステム代表者（MSR）は、認証申請提出後に拡大された新たな海外拠点を監査対象に含めるよう、監査範囲の拡大を要請した。

監査担当者の対応方法について、2つの選択肢から選んでください。

- A.** MSRを範囲拡大に含めることが提案されていますが、確立された手順に従う必要があります。

- B. MSRIに対し、審査の範囲は最初の申請に基づいて決定されたため、審査は予定通り進めなければならないことを通知する。
- C. MSRIは審査契約を解除し、新たな状況で再申請することをお勧めします。
- D. 管理システムが新規サイトのプロセスを網羅しているかどうかを確認する。網羅している場合は、レビューを続行する。
- E. 新しいワークスペースは既存のスコープ内に問題なく含めることができることをMSRIに通知します。
- F. 監査人が、監査範囲が変更され、新たな業務領域が含まれることを被監査者に通知することを確認します。

Answer: A,D (メッセージを残す)

監査人が対応すべき正しい選択肢は以下のとおりです。

- A. 範囲の拡張が組み込まれる可能性があるが、確立された手順を経る必要があることを MSRI に通知する。D. マネジメント システムが新しいサイトのプロセスをカバーしているかどうかを判断し、カバーしている場合は監査を進める。これらのオプションは、認証範囲の変更はクライアントが認証機関に通知する必要がある、認証機関は手順 1 に従ってこれらの変更を評価し決定する必要があると規定している ISO/IEC 27006:2015 規格と一致しています。監査員はまた、ISMS が認証範囲に含まれるすべてのサイトで実装され、維持されていることを確認する必要があります 1。
- 他の選択肢は、監査人が対応すべき方法として適切ではありません。理由は以下のとおりです。
- B. 監査範囲は当初の申請に基づいて決定されているため、監査は計画通りに進めなければならないことをMSRIに通知する :この選択肢はあまりにも厳格で、クライアントの状況に合わせて柔軟に対応したり、適応したりする余地がありません。監査員は、認証機関によって適切に通知され評価される限り、当初の申請以降に発生した認証範囲の変更を検討する姿勢を持つべきです。
- C. MSRIに監査契約を解除して新たな状況で再申請するよう提案する :この選択肢は極端すぎ、不必要である。クライアントと認証機関の両方に遅延とコストが発生するからである。監査人はクライアントに監査契約の解除を提案するのではなく、認証範囲の拡大を申請・承認するための確立された手続きに従うよう提案すべきである。
- E. MSRIに対し、既存の範囲内で新しい作業領域を問題なく含めると助言する :この選択肢は寛大すぎ、新しい作業領域がISO/IEC 27001およびISMSの要求事項を満たしていることを保証しません。監査員は、新しい作業領域が既存の範囲内で問題なく含めると想定するのではなく、新しいサイトでISMSが実装および維持されていること、および認証範囲の変更が認証機関によって承認されていることを確認する必要があります。
- F. 監査人が被監査者に対し、監査範囲が改訂され、新たな作業領域が含まれることを通知することを確認する :この選択肢はあまりにも独断的であり、認証機関の権限を尊重していません。監査人は、監査範囲を改訂して新たな作業領域を含めることを確認するのではなく、クライアントからの認証範囲の拡大要求を認証機関に通知し、認証機関の決定を待つべきです。

最新問題: 26

あなたは、医療サービスを提供する高齢者向け介護施設でISMS監査を実施しており、ソフトウェアコード管理 (SCM) システムをレビューしています。SCM上で合計10個のユーザーアカウントを特定しました。

あなたは、ユーザーの一人であるスコットが9ヶ月前に退職したことを確認しました。

以前、SCMシステム管理者は、スコットが最後にソースコードをチェックアウトしたのは1か月前であることを確認した。彼は、安全なエリアにあるローカルネットワーク上の承認済みデスクトップの1台を使用していた。ユーザー登録解除手順を確認すると、管理者は、退職が承認された時点で、関連するICTシステムおよび／またはデバイスからユーザーアカウントと承認が直ちに登録解除されるようにしなければならない」と記載されています。ユーザーScottには登録解除の記録がありません。

ITセキュリティマネージャーの説明によると、スコットは退職後も毎月オフィスに戻り、ソースコードの保守サポートを提供し続けていたとのことだ。そのため、SCM上の彼のアカウントが今も残っているのだという。

監査証拠をさらに収集するために、他の領域についても調査を進めたいと考えています。有効な監査証拠ではないものを3つ選択してください。

- A. セキュリティを維持するためにアクセス制御を定期的に見直す方法について、より多くの証拠を集める (制御措置A.5.35に関連)。
- B. スコットのフルタイム勤務からパートタイム勤務への移行をどのように管理するかについて、より多くの証拠を収集する (管理措置A.6.5に関連)。
- C. 人事部が新たな雇用関係に基づいて実施したスコットの身元調査から、さらなる証拠を収集する。(管理策A.6.1に関連)
- D. スコットの辞任理由と、彼の復職が利益相反に該当するかどうかを判断するために、さらなる証拠を収集する。(管理A.5.3に関連)
- E. スコットが従業員のデスクトップやローカルネットワークにどのようにアクセスしたかについて、さらに証拠を収集する。(管理策A.5.15に関連)
- F. スコットがどのようにして安全区域にアクセスしたかについて、さらに証拠を集める。(管理A.8.4に関連)
- G. 組織がスコットのソースコード保守サポートサービス費用をどのように支払っているかについて、さらに証拠を収集する。(管理策A.6.2に関連)
- H. スコットが見ていた元のコードをどこに保管し、どのように保護していたのかを理解するために、より多くの証拠を集める。(管理項目A.8.4に関連)

Answer: B,D,G (メッセージを残す)

オプションB、D、Gは、ISMS要件または監査基準に直接関連していないため、有効な監査証跡ではありません。これらは、組織の人事管理または契約上の取り決めにより関連しており、ISMS監査の範囲外です。その他のオプションは、アクセス制御、セキュリティエリア、および事業継続管理の情報セキュリティ面に関連するISMSコントロールを組織がどのように実装および維持しているかの証拠を提供できるため、有効な監査証跡です。参考文献：

- * PECB候補者ハンドブック ISO/IEC 27001 主任審査員、16ページ、セクション4.2.1
- * ISO/IEC 27001:2013、条項A.5.3、A.5.15、A.5.35、A.6.1、A.6.2、A.6.5、A.8.4、A.17.1
- * ISO 19011:2018、6.2.2項

最新問題: 27

以下の選択肢のうち、利害関係者の定義はどれですか？

第三者が、ある決定や活動によって影響を受けたと考える場合、その組織に対して苦情を申し立てることができる。

A. 決定や活動に影響を与えることができる、影響を受ける、または影響を受けると考えている個人または組織。

B. 経営上の意思決定に介入できる、または経営上の意思決定に介入される可能性があると考えられるグループや組織を指します。

C. 決定や活動を制御できる、制御される、または制御されていると信じている個人または組織。

Answer: B ([メッセージを残す](#))

これは、ISO 27001:2013の3.16項に基づく利害関係者の定義です。利害関係者とは、基本的にステークホルダー、すなわち情報セキュリティマネジメントシステム (ISMS) またはその活動に影響を与えたり、影響を受けたりする個人または組織のことです。利害関係者はISMSに関して様々なニーズや期待を持っている可能性があり、組織はそれらを特定し、対処する必要があります。

参考文献：

- * ISO/IEC 27001:2013、情報技術—セキュリティ技術—情報セキュリティマネジメントシステム—要求事項、3.16項
- * PECB候補者ハンドブック ISO 27001主任審査員、10ページ
- * ISO 27001 ISMSに関する利害関係者とその期待を特定する
- * ISO 27001の利害関係者の例

最新問題: 28

CEOは、会社の現状と将来戦略、そしてCEOのビジョンと従業員の役割について意見を述べるメールを送信します。このメールは、以下のように分類されるべきです。

A. 社内メール

B. 公開メール

C. 機密メール

D. 制限付きメール

Answer: A ([メッセージを残す](#))

CEOが会社の現状と将来の戦略、CEOのビジョン、従業員の役割について意見を述べたメールは、社内メールとして分類されるべきです。社内メールとは、情報が社内でのみ使用されることを意図しており、許可なく外部に開示してはならないことを示す分類です。CEOが送信するメールには、会社の従業員にとって関連性があり重要な情報が含まれていますが、会社の業績、目標、計画に関する機密情報や秘密情報が含まれている可能性があるため、公開には適さない場合があります。参考文献: : CQI & IRCA ISO 27001:2022 主任監査員コースハンドブック、34 ページ。: CQI & IRCA ISO 27001:2022 主任監査員コースハンドブック、37 ページ。: [ISO/IEC 27001 主任監査員 - PECB]、14 ページ。

最新問題: 29

質問：

X社に対する認証監査を実施するため、3名の監査員が任命されました。監査開始前に、認証機関はX社に監査員の氏名と経歴情報を提供しました。X社は、監査員のうち1名が元従業員であったため、その交代を要請しました。これは妥当な要請でしょうか？

A. 利益相反は、監査人の変更を求める正当な理由となります。

B. いいえ、被監査者は、正当な理由（監査人の非専門的な行為や利益相反など）がある場合にのみ、監査人の変更を要求できます。

C. いいえ、被監査者は監査人の変更を要求することはできません。

Answer: B ([メッセージを残す](#))

包括的かつ詳細な解説：

- * B. 正解:
* ISO/IEC 17021-1（適合性評価—マネジメントシステムの監査及び認証を提供する機関に対する要求事項）では、被監査者は正当な理由がある場合にのみ監査員の交代を要求できると規定されています。
* 監査役を務める元従業員は、潜在的な利益相反（~~実際~~のものか、そう見なされるものかを問わず）を生じさせる。

したがって、X社の要求は正当である。

- * A. 不正解:
利益相反は正当な理由ではあるが、後任人事は個人的な好みではなく、客観的かつ正当な根拠に基づいて行われるべきである。
* C. 不正解:

被監査者は、正当な理由がある場合に限り、監査人の交代を要求することができる。

関連規格参照：

- * ISO/IEC 17021-1:2015 9.1.3項（監査員の公平性および客観性）

最新問題: 30

AppFolkはISO/IEC 27001認証取得を目指すソフトウェア開発会社です。これは認められるでしょうか？

- A. はい、監査の範囲とISMSの範囲は必ずしも同じである必要はありません。
- B. いいえ、被監査企業が事業を展開する産業分野にとって重要でない分野は、監査範囲から除外することができます。
- C. いいえ、監査範囲はISMSの対象となる組織のすべての部門を反映する必要があります。

Answer: C ([メッセージを残す](#))

いいえ、監査範囲はISMSの対象となる組織のすべての部門を反映すべきです。ISMSの範囲に会社全体が含まれると明記されている場合、監査範囲は、特に正当化され、すべての利害関係者によって合意された場合を除き、これと整合させる必要があります。

最新問題: 31

ビジネスプロセスの計画・実行・評価・改善サイクルにおいて、「計画」という言葉に適切な表現は次のうちどれですか？（2選択）

- * 文書を保管してください
- A. 書類を保管してください
- B. 組織変革
- C. 目標を設定する
- D. トレーナー
- E. 情報通信技術資産を提供する

Answer: D,E ([メッセージを残す](#))

PDCAサイクル（計画・実行・評価・改善）は、プロセス、製品、またはサービスを導入および改善するための4段階の手法です。計画」段階では、望ましい結果を達成するために必要な目標とプロセスを確立します。これには、SMART目標の設定、リソースの特定、役割と責任の定義、リスク評価の実施、トレーニング、コミュニケーション、およびモニタリングのための計画の策定などが含まれます。

参考文献：

ISO/IEC 27001:2022 主任審査員（情報セキュリティマネジメントシステム）の目的と内容は Quality.org および PECB から引用。ISO 19011:2018 マネジメントシステムの監査に関するガイドライン [セクション 5.3.1]

有効な **ISO-IEC-27001-Lead-Auditor-CN** 問題集は GoShiken.com が提供された合格しやすい ISO-IEC-27001-Lead-Auditor-CN 試験問題集！ GoShiken.com が最新の **ISO-IEC-27001-Lead-Auditor-CN** 試験問題集を提供しています。GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 問題集をゲットする人はこちら:
<https://www.goshiken.com/PECB/ISO-IEC-27001-Lead-Auditor-CN-mondaishu.html> (418**30%OFF**問題集溶と正解付きで **30%**w特別割引コード: **Freepdfdumps**)

最新問題: **32**

質問：

EquiBankは、財務管理システムの外部監査を受けています。監査人は、EquiBankの財務ソフトウェアによって処理される取引ロジックを評価しています。正確性を確保するため、ソフトウェアアプリケーションに組み込まれた操作、計算、および制御を検証するためにシミュレーションを使用しています。ここで使用されているコンピュータ支援監査（CAAT）の手法はどのようなものですか？

A. 製図 作図ソフトウェアアプリケーション

B. ユーティリティソフトウェア

C. データテスト

Answer: C ([メッセージを残す](#))

包括的かつ詳細な解説：

- * C. 正解:
 - * データテスト技術は、金融ソフトウェア内の取引をシミュレートして、ロジック、計算、およびプログラムされた制御を検証します。
 - * ISO 19011:2018は、CAATをデータ処理の完全性を検証する監査ツールとして認識しています。
- * A. 不正解:
 - * プロットおよび地図作成ソフトウェアは、地理空間分析に使用されるものであり、金融取引のテストに使用されるものではありません。
- * B. 不正解:
 - * ユーティリティソフトウェアは一般的なIT機能をサポートしますが、監査シミュレーションは実行しません。

関連規格参照：

- * ISO 19011:2018 条項 6.4.10（監査におけるCAATの使用）

最新問題: **33**

シナリオ6 :Sinvestmentは、住宅保険、商業保険、生命保険を提供する保険会社です。同社はノースカロライナ州で設立されましたが、近年、ヨーロッパやアフリカを含む他の地域にも事業を拡大しています。Sinvestmentは、業界における適用法令を遵守し、情報セキュリティインシデントの発生を防止することに尽力しています。同社はISO/IEC 27001に基づく情報セキュリティマネジメントシステム（ISMS）を導入し、ISO/IEC 27001認証の申請を行っています。

認証機関は、監査を実施するために2名の監査員を任命した。監査員はSinvestment社と機密保持契約を締結した後、監査を開始した。まず、ISMS適用範囲記述書、情報セキュリティポリシー、内部監査報告書など、必要な標準文書を精査した。Sinvestment社は文書作成手順を確立していると述べていたものの、すべての文書が同じ形式ではなかったため、精査は容易ではなかった。その後、監査チームはSinvestmentの経営幹部に対し、ISMS導入におけるそれぞれの役割を理解するため、複数回のインタビューを実施した。監査の第1段階におけるすべての活動は、Sinvestmentからの要請による現地での文書および情報レビューを除き、リモートで実施された。

この段階で、監査担当者は情報セキュリティ研修および啓発プログラムに関する文書を一切発見できなかった。質問に対し、Sinvestmentの担当者は、全従業員に情報セキュリティ研修コースを提供していると述べた。監査の第1段階により、監査チームはSinvestmentの業務内容とISMS（情報セキュリティマネジメントシステム）について包括的な理解を得ることができた。

第2段階監査は、第1段階監査の3週間後に実施されました。監査チームは、マーケティング部門（監査範囲外において、従業員のアクセス権限を管理するための適切な手順が欠如していることを確認しました。従業員のアクセス権限の管理はISO/IEC 27001の要件であり、既に会社の情報セキュリティポリシーにも含まれているため、この問題は監査報告書に記載されました。さらに、第2段階監査において、監査チームはSinvestmentがユーザーアクティビティをログに記録していないことを確認しました。

同社の手順書には「ユーザー活動を記録したログは保存し、定期的に確認する必要がある」と記載されているが、同社はそのような手順を実施している証拠を一切提示していない。

監査活動全体を通して、監査員は観察、インタビュー、文書化された情報のレビュー、分析、および技術的検証を通じて情報と証拠を収集しました。監査チームはフェーズ1とフェーズ2の両方から得られたすべての監査結果を分析し、肯定的な認証勧告を発行することを決定しました。

監査の第一段階で、監査チームはSinvestment社に情報セキュリティに関する研修や意識向上活動の記録が一切ないことを発見しました。Sinvestment社はこの状況でどのような対応を取るでしょうか？シナリオ6を参照してください。

A. フェーズ2レビューの前に、特定された問題を修正してください。

B. 特定された問題点を記録し、認証監査完了後に修正する。

C. 問題の修正が必要かどうかを判断するために、新しいリスク評価プロセスを導入する。

Answer: A ([メッセージを残す](#))

Sinvestment社は、ステージ2監査の前に、情報セキュリティ研修および意識向上に関する文書の不足という問題点を是正すべきである。このギャップに迅速に対処することで、次の監査段階でISMSが完全に準拠し、有効であることが保証される。

参照規格 :ISO/IEC 27001:2013、7.2項（能力）

最新問題: **34**

あなたは監査チームリーダーとして、初めて第三者機関によるISMS監視監査を実施しています。現在、監査チームの別のメンバーと共に、被監査企業のデータセンターにいます。

同僚は情報セキュリティインシデントと情報セキュリティイベントの違いについてよく理解していないようです。あなたは例を挙げてその違いを説明しようとしています。

以下のシナリオのうち、情報セキュリティインシデントと定義できるものはどれですか？（3）

A. 組織のマルウェア対策ソフトウェアはウイルスを防ぐことができます。

B. 推奨交換日を過ぎたハードドライブを使用してください。

C. 組織はフィッシングメールを受信しました。

D. 従業員が勤務終了時に机を片付けなかった。

E. 支払いを受け取っていない請負業者が、上級管理職のICTアカウントを削除しました。

F. 不満を持った従業員が許可なく給与記録を改ざんした。

G. 組織は第三者による侵入テストに不合格でした。

H. 組織のマーケティング資料がハッカーによってコピーされ、競合他社に売却された。

Answer: ([解答を表示する](#)**)**

情報セキュリティマネジメントシステムの概要と用語を提供するISO/IEC 27000:2018によると、情報セキュリティイベントとは、情報セキュリティポリシーの違反または保護措置の失敗の可能性、あるいはセキュリティに関連する可能性のあるこれまで知られていなかった状況を示す、システム、サービス、またはネットワークの状態の特定された発生を指します1。情報セキュリティインシデントとは、事業運営を損ない、情報セキュリティを脅かす可能性が非常に高い、望ましくない、または予期せぬ情報セキュリティイベントの単一または一連の発生を指します1。したがって、この定義に基づくと、情報セキュリティインシデントの3つの例は次のとおりです。

* 未払いの請負業者が経営陣のICTアカウントを削除する :これは、経営陣のアクセス、データ、または機能の喪失につながる可能性があり、業務運営を損ない、情報セキュリティを脅かす可能性が非常に高い、望ましくないまたは予期しない情報セキュリティ事象の一例です。

* 不満を持った従業員が許可なく給与記録を変更する :これは、望ましくない、または予期せぬ情報セキュリティ事象の一例であり、組織の金銭的詐欺、法的責任、または評判の低下につながる可能性があるため、事業運営を損ない、情報セキュリティを脅かす可能性が非常に高い。

* 組織のマーケティングデータがハッカーによってコピーされ、競合他社に販売される :これは、組織の機密性、競争上の優位性、または顧客からの信頼の喪失につながる可能性があり、事業運営を損ない、情報セキュリティを脅かす可能性が非常に高い、望ましくないまたは予期しない情報セキュリティ事象の一例です。

その他の選択肢は情報セキュリティインシデントの例ではなく、影響と深刻度によってはインシデントにつながる場合もそうでない場合もある情報セキュリティイベントです。例えば：

* 組織のマルウェア対策ソフトウェアがウイルスを阻止する :これは、情報セキュリティポリシーの違反または保護措置の失敗の可能性を示すシステム状態が特定された例ですが、マルウェア対策ソフトウェアによって阻止されるため、業務運営を危険にさらしたり、情報セキュリティを脅かしたりする可能性は高くありません。

* ハードドライブが推奨交換日を過ぎて使用されている場合 :これは、情報セキュリティポリシーの違反または保護措置の失敗の可能性を示すシステム状態の発生例ですが、ハードドライブが故障したり他の問題を引き起こしたりしない限り、業務運営を損なったり情報セキュリティを脅かしたりする可能性は高くありません。

* 組織がフィッシングメールを受信した場合 :これは、情報セキュリティポリシーの違反または保護措置の失敗の可能性を示すネットワーク状態が特定された事例ですが、受信者がメールを開いたり返信したりしない限り、業務運営を危険にさらしたり情報セキュリティを脅かしたりする可能性は高くありません。

* 従業員が勤務終了時に机を片付けない: これは、情報セキュリティ ポリシーの違反または保護措置の失敗の可能性を示すサービス ステートの特定された発生例ですが、机に権限のない人物がアクセスする機密情報や秘密情報が含まれていない限り、業務運営を損なったり、情報セキュリティを脅かしたりする可能性は高くありません。

* 組織が第三者による侵入テストに不合格となる: これは、情報セキュリティ ポリシーの違反または保護措置の不備の可能性を示すシステム状態が特定された例ですが、侵入テストで悪意のある攻撃者によって悪用される深刻な脆弱性が明らかにならない限り、業務運営を危険にさらしたり、情報セキュリティを脅かしたりする可能性は高くありません。

参照規格 :ISO/IEC 27000:2018 - 情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステム - 概要と用語

最新問題: **35**

仮説：

Northstormは、ユニークなヴィンテージおよびモダンなアクセサリーを取り扱うオンライン小売業者です。小規模な市場からスタートしましたが、eコマース市場の拡大とともに成長を遂げてきました。Northstormは完全にオンラインで運営されており、効率的な決済処理、在庫管理、マーケティングツール、配送プロセスを実現しています。また、人気商品を優先的に入荷、補充、発送するシステムを採用しています。

Northstormは従来、ウェブサイトのホスティングと、ハードウェア、ソフトウェア、データ管理を含むインフラストラクチャの完全な制御によってIT運用を管理してきました。しかし、このアプローチではインフラストラクチャの応答性が不十分であったため、成長が阻害されていました。eコマースと決済システムを改善するため、Northstormは社内データセンターの拡張を選択し、3か月かけて2段階で拡張を完了しました。第1段階では、コアサーバー、POSシステム、注文システム、請求システム、データベース、バックアップシステムをアップグレードしました。第2段階では、メール、決済、ウェブ機能の改善に重点を置きました。さらに、この段階でNorthstormは、データ処理方法が安全で信頼性が高く、グローバルな規制に準拠していることを保証するために、個人識別情報 (PII) 処理に関する国際標準を採用しました。

拡張にもかかわらず、ノースストームのデータセンターはアップグレード後も進化するビジネスニーズに対応できませんでした。この不備により、注文の優先順位付けの問題など、一連の新たな課題が発生しました。顧客からは優先的に処理された注文が届かないという報告があり、同社は迅速な対応に苦慮しました。これは主に、注文の優先順位付けや顧客対応のシミュレーションに使用されるアプリケーション「YouDecide」からの注文をメインサーバーが処理できなかったことが原因でした。このアプリケーションは、アップグレード時にインストールされた新しいオペレーティングシステムと互換性のない高度なアルゴリズムに依存していました。

緊急の互換性問題に直面したNorthstormは、十分な検証を行わずにアプリケーションを急いでパッチ適用した結果、改ざんされたバージョンがインストールされてしまいました。このセキュリティ脆弱性によりメインサーバーが影響を受け、同社のウェブサイトが1週間ダウンしました。より信頼性の高いソリューションの必要性を認識した同社は、ウェブサイトのホスティングをeコマースサービスプロバイダーにアウトソーシングすることを決定しました。移行を完了する前に、同社は製品所有権に関する機密保持契約を締結し、セキュリティ強化のためにユーザーアクセス権限の包括的な見直しを実施しました。

質問：

シナリオ1に基づくと、ノースストーム社は拡張の第2段階でどの国際規格を採用しましたか？

- A. ISO/IEC 27701
- B. ISO/IEC 27009
- C. ISO/IEC 27003

Answer: **A** ([メッセージを残す](#))

包括的かつ詳細な解説：

Northstormは、個人情報 (PII) の管理者および処理者に関する国際標準を採用し、データ処理方法が安全かつグローバルな規制に準拠していることを保証しました。これは、ISO/IEC 27001およびISO/IEC 27002を拡張し、特に個人情報の保護を対象とするプライバシー情報管理システム (PIMS) を網羅するISO/IEC 27701と直接整合しています。

* A. ISO/IEC 27701 - 正解。この規格は、個人情報管理者および処理者として活動する組織向けに設計されており、プライバシー管理、規制遵守、およびデータ保護に関するガイドラインを提供します。

* B. ISO/IEC 27009 - この規格はISMSのセクター固有の要件に関するガイダンスを提供するものであり、プライバシーや個人情報保護に関するものではないため、誤りです。

* C. ISO/IEC 27003 - ISMSの一般的な実装ガイダンスを提供するものであり、PII処理のための具体的な管理策を提供するものではないため、誤りです。

これは、プライバシー規制の遵守とプライバシー強化のためのセキュリティ対策の実施に重点を置くISO/IEC 27001:2022附属書A管理A.5.34 プライバシーと個人情報の保護)に準拠しています。

最新問題: **36**

以下の記述を検討し、誤っているものを2つ選びなさい。

A. 仮想監査の前に技術的なチェックを行うことで、監査の有効性と効率性を向上させることができます。

B. バーチャル監査中は、被監査者がインタビュー中にウェブカメラをオンにしておくことを強くお勧めします。

C. 第三者監査に割り当てられる日数は、被監査者の利用可能な時間によって異なります。

D. 機密保持とセキュリティ上の理由から、仮想監査中の画面共有は、監査チームが被監査者の文書を確認するために使用する method です。

E. オンサイト監査、バーチャル監査、または複合監査の選択は、過去の実績と過去の監査結果を考慮に入れる必要があります。

F. オンサイト監査を実施する権限を持つ監査員は、必要なスキルに大きな違いがないため、バーチャル監査のための追加トレーニングは必要ありません。

Answer: C,F (メッセージを残す)

第三者監査に割り当てられる日数は、被監査者の都合ではなく、監査範囲、目的、基準、リスク、リソースを考慮した監査プログラムによって決定されます12。被監査者の都合は、監査計画とスケジュールに影響を与える要因の1つにすぎませんが、監査期間には影響しません3。

オンサイト監査の実施が承認されている監査員は、必要なスキルセットに大きな違いがあるため、仮想監査のための追加トレーニングを受ける必要があります。仮想監査は、コミュニケーション、テクノロジー、セキュリティ、証拠収集など、オンサイト監査とは異なる課題と機会をもたらします4。監査員は、リモート監査を実施するためのツールとテクニック、および仮想環境で期待される倫理的かつ専門的な行動について熟知している必要があります。参考文献:

* PECB候補者ハンドブック - ISO 27001主任審査員、18ページ

* ISO 19011:2018、マネジメントシステムの監査に関する指針、5.3.2項

* ISO 19011:2018、マネジメントシステムの監査に関する指針、6.3.1項

* デロイト - 仮想内部監査の実施、1ページ

* [効果的かつ効率的なリモート監査を実施するためのガイド]、1ページ

* [ISO 19011:2018、マネジメントシステムの監査に関する指針]、7.2.3項

* [リモート監査のベストプラクティスと規制遵守のためのチェックリスト]、1ページ

最新問題: 37
あなたは経験豊富なISMS監査員で、ICTリサイクルサービスを提供する組織の第三者監査を担当しています。この組織は、会社が不要になったICT機器を処理し、修理・再利用するか、安全に廃棄処分します。部屋の隅にあるベンチの上に2台のサーバーが置いてあるのに気づきました。どちらのサーバーにも、サーバー名、IPアドレス、管理者パスワードが書かれたステッカーが貼られています。ICTマネージャーにこれらのサーバーについて尋ねると、それらは昨日、長年の顧客から届いた荷物の一部だと教えてくれました。

あなたはどのような行動を取るべきでしょうか？

A. 情報セキュリティインシデントをICTマネージャーに記録させ、情報セキュリティインシデント管理プロセスを開始させてください。

B. 監査結果に注意し、顧客のITセキュリティに関連する入荷貨物の処理プロセスを確認してください。

C. レビュー結果に表示された内容を記録し、それ以上の行動は取らない。

D. 管理要件の不遵守 5.31 法的、規制、監督、および契約上の要件。

E. 管理措置8.20 「ネットワークセキュリティ」ネットワークおよびネットワーク機器は、システムおよびアプリケーション内の情報を保護するために保護、管理、制御されなければならない)への不遵守が確認されました。

F. 審査対象者にタグの削除を依頼し、審査プロセスを続行します。

Answer: B (メッセージを残す)

ISO 27001:2022 の 8.1.4 項によれば、組織は、情報セキュリティ管理システムに関連する外部提供のプロセス、製品、またはサービスが管理されていることを保証しなければなりません。これには、ICT 機器を回収のために送付する顧客などの外部プロバイダーとの情報セキュリティに関する適切な契約要件の実装が含まれます。12 この場合、組織は ICT 回収サービスを提供しており、機密情報または秘密情報が含まれている可能性のある顧客の ICT 機器の処理が含まれます。組織は、顧客の ICT 機器が安全に、かつ顧客の情報セキュリティ要件に従って取り扱われることを保証するプロセスを整備する必要があります。プロセスには、顧客の身元と承認の確認、機器の在庫と状態の確認、機器または顧客に関する情報を含むラベルやステッカーの除去または破棄、機器に保存されているデータの消去、実行したアクションと達成された結果の文書化などの手順が含まれる必要があります12 監査人が、サーバー名、IP アドレス、管理者パスワードがわかるステッカーが付いたベンチ上の 2 台のサーバーに気づいたという事実は、顧客の IT セキュリティに関連する入荷貨物の処理プロセスが効果的でないか、従われていないことを示しています。これは、顧客の情報またはシステムへの不正アクセス、開示、または変更のリスクをもたらす可能性があります。したがって、監査人は監査結果を記録し、顧客の IT セキュリティに関連する入荷貨物の処理プロセスを確認し、ISO 27001:2022 の条項 8.1.4 に適合していないかどうかを判断する必要があります12 その他のアクションは、次の理由により適切ではありません。

A. ICT マネージャーに情報セキュリティ インシデントを記録し、情報セキュリティ インシデント管理プロセスを開始するよう依頼することは適切ではありません。なぜなら、これは組織自身の情報やシステムに影響を与える情報セキュリティ インシデントではないからです。情報セキュリティ インシデントとは、事業運営を損ない、情報セキュリティを脅かす可能性が非常に高い、望ましくない、または予期せぬ情報セキュリティ イベントの 1 つまた

は一連のものと定義されます。12 この場合、情報セキュリティ イベントは組織の情報やシステムではなく、顧客の情報やシステムに影響を与えます。したがって、組織は情報セキュリティ インシデント管理プロセスではなく、顧客の IT セキュリティに関連する入荷貨物の処理プロセスに従う必要があります。

C. 監査結果で監査人が確認した内容を記録するだけで、それ以上の措置を講じないことは適切ではありません。なぜなら、これでは問題の根本原因や影響に対処できないからです。監査人は、組織の情報セキュリティ 管理システムの有効性とコンプライアンスを検証し、不適合や改善の機会を報告する責任があります12。したがって、監査人は、顧客のITセキュリティに関連する入荷品の処理プロセスを確認し、ISO 27001:2022の8.1.4項に不適合があるかどうかを判断する必要があります。

D. 管理5.31 法律、法令、規制、契約上の要求事項」に対する不適合を指摘することは適切ではありません。なぜなら、この管理は問題に関係がないからです。管理5.31では、組織が情報セキュリティ管理システム12に適用される法律、法令、規制、契約上の要求事項を特定し、遵守することを要求しています。この場合、問題は組織が法律、法令、規制、契約上の要求事項を遵守しているかどうかではなく、情報セキュリティ管理システムに関連する外部提供のプロセス、製品、またはサービスに対する組織の管理に関するものです。したがって、監査人は顧客のITセキュリティに関連する入荷品の処理プロセスを確認し、ISO 27001:2022の条項8.1.4に不適合があるかどうかを判断する必要があります。

E. 管理 8.20 ネットワーク セキュリティ」 ネットワークおよびネットワーク デバイスは、システムおよびアプリケーションの情報を保護するために、保護、管理、制御されなければならない)に対する不適合を指摘することは適切ではありません。なぜなら、この管理は問題とは関係がないからです。管理 8.20 では、組織がシステムおよびアプリケーションの情報を保護するために、組織自身のネットワークおよびネットワーク デバイスを保護、管理、制御することを要求しています 12 この場合、問題は組織のネットワーク セキュリティではなく、情報セキュリティ マネジメント システムに関連する外部提供のプロセス、製品、またはサービスに対する組織の制御です。したがって、監査員は、顧客の IT セキュリティに関連する入荷品の処理プロセスを確認し、ISO 27001:2022 の 8.1.4 項 に不適合があるかどうかを判断する必要があります。

F. 被監査者にラベルを取り外して監査を続けることは、問題の根本原因や影響に対処できないため適切ではありません。監査人は、監査中に被監査者の業務に干渉したり、是正措置を提案したりしてはなりません。これは、監査人の客観性と公平性を損なうことになるからです。12 監査人は、顧客のITセキュリティに関連する入荷貨物の処理プロセスを確認し、ISO 27001:2022の8.1.4項に適合しない点があるかどうかを判断する必要があります。

参照：

1: ISO/IEC 27001:2022 リードオーディター（情報セキュリティマネジメントシステム）コース（CQIおよびIRCA認定トレーニング1） 2: ISO/IEC 27001 リードオーディタートレーニングコース（PECB 2）

最新問題: 38

您的組織目前正在尋求 ISO/IEC27001:2022 認證。您剛剛獲得口部 ISMS 審核員資格，ICT 經理希望利用您新獲得的知識來協助他設計資訊安全事件管理流程。他確定了計劃流程中的以下階段，並要求您確認它們應按哪個順序出現

Step 1	Incident logging
Step 2	
Step 3	
Step 4	
Step 5	
Step 6	
Step 7	
Step 8	Incident closure

To complete the sequence, click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the options to the appropriate blank section.

Incident prioritisation – classify the incident as critical, high, medium, low

Task creation and management – identification and coordination of work needed to resolve the incident

SLA management and escalation – ensure any service level agreements are adhered to whilst resolution is being implemented. If a breach looks likely, escalate to secure more resources

Incident resolution – a temporary workaround or permanent resolution has been identified

Incident assignment – incident is passed to the individual best suited to resolve it

Incident categorisation – determine whether the incident is a hardware issue, network issue or software issue

Answer:

Step 1	Incident logging
Step 2	Incident categorisation – determine whether
Step 3	Incident prioritisation – classify the incident
Step 4	Incident assignment – incident is
Step 5	Task creation and management –
Step 6	SLA management and escalation – ensure
Step 7	Incident resolution – a temporary
Step 8	workaround or permanent resolution has been identified

To complete the sequence, click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the options to the appropriate blank section.

Incident prioritisation – classify the incident as critical, high, medium, low

Task creation and management – identification and coordination of work needed to resolve the incident

SLA management and escalation – ensure any service level agreements are adhered to whilst resolution is being implemented. If a breach looks likely, escalate to secure more resources

Incident resolution – a temporary workaround or permanent resolution has been identified

Incident assignment – incident is passed to the individual best suited to resolve it

Incident categorisation – determine whether the incident is a hardware issue, network issue or software issue

Reference:
ISO/IEC 27001:2022, Information technology - Security techniques - Information security management systems - Requirements1 PECB Candidate Handbook ISO/IEC 27001 Lead Auditor2 ISO 27001:2022 Lead Auditor - PECB3 ISO 27001:2022 certified ISMS lead auditor - Jisc4 ISO/IEC 27001:2022 Lead Auditor Transition Training Course5 ISO 27001 - Information Security Lead Auditor Course - PwC Training Academy6 ISO/IEC 27035:2022, Information technology - Security techniques - Information security incident management

最新問題: 39
監査担当者の責任には、監査活動の促進、ロジスティクスの維持、健康と安全に関する方針の遵守の確保、監査プロセスへの立ち会いにおける被監査者の代理などが含まれます。
A. 内部監査員
B. オブザーバー
C. ガイドライン
Answer: C (メッセージを残す)
ここで述べた責任は、ガイド」の役割に合致する。監査におけるガイドとは、通常、被監査組織のメンバーであり、監査活動を円滑に進め、ロジスティクスを管理し、安全衛生方針の遵守を確保するとともに、監査プロセスに立ち会い、監査チームを支援する人物を指す。
参考文献 :ISO 19011:2018、マネジメントシステムの監査に関する指針

最新問題: 40
あなたは経験豊富なISMS監査チームリーダーで、研修中の監査員を指導しています。研修生は監査報告書における不適合の分類についてあなたに質問します。あなたは彼女の知識を試すため、以下の記述のうちどれが正しいかを4つ尋ねることにしました。
A. 重大な不適合については、現場でのフォローアップが必要となる場合があります。
B. 不適合は 重大」または 軽微」 という用語のみを使用して等級付けする必要があります。

C. 重大な不適合に対処するために講じられる措置は、通常、軽微な不適合に対処するために講じられる措置よりも実質的なものです。

D. 軽微な不適合は、改善の機会として再評価されるべきである。

E. 複数の軽微な不適合をまとめて、1つの重大な不適合とすることができます。

F. 不適合製品の分類は、最初の会議で被監査者に説明されなければならない。

G. 被監査者は、不適合製品の等級基準を決定する責任を常に負います。

H. 不適合は、その重要性を示すために分類することができます。

Answer: A,C,E,H (メッセージを残す)

正しい記述は以下の4つです。

* 重大な不適合については、現場でのフォローアップが行われる場合があります。

* 重大な不適合に対処するために講じられる措置は、通常、軽微な不適合に対処するために講じられる措置よりも大規模である。

* 複数の軽微な不適合は、重大な不適合としてまとめられることがある。

不適合は、その重要度を示すために等級付けされる場合があります。

ISO 19011:2018によると、不適合とは要求事項を満たしていない状態を指します1。不適合は、監査プログラムまたは監査依頼者によって定められた基準に基づいて、その重要度を示すために等級付けされる場合があります2。不適合の等級付けには、監査の性質と状況に応じて、重大、軽微、重大など、さまざまな用語やレベルが使用される場合があります3。ただし、重大および軽微な不適合の一般的な定義は次のとおりです。

* 重大な不適合とは、マネジメントシステムが意図した結果を達成する能力に影響を与える不適合、またはマネジメントシステムの重大な破綻を示す不適合のことです4。重大な不適合には、即時の是正措置と、監査員による現場でのフォローアップによる是正状況の確認が必要となる場合があります5。

* 軽微な不適合とは、マネジメントシステムが意図した結果を達成する能力に影響を与えない不適合、またはマネジメントシステムの単発的な不備を表す不適合のことです4。軽微な不適合には、指定された期間内に是正措置を講じ、監査員によるオフサイトでの検証によって是正が完了したことを確認する必要がある場合があります5。

不適合に対処するために講じる措置は、不適合の重大度と影響、および再発または悪化のリスクによって異なります。一般的に、重大な不適合に対処するための措置は、軽微な不適合に対処するための措置よりも大規模であり、問題の根本原因の特定と排除、予防措置の実施、および解決策の有効性の監視が含まれる場合があります。

複数の軽微な不適合は、同一の要求事項、プロセス、または領域に関連しており、かつ、システム全体の不具合またはマネジメントシステムに対する重大なリスクを示している場合、重大な不適合としてグループ化することができます。監査担当者は、専門的な判断と証拠に基づいたアプローチを用いて、不適合をグループ化するか個別に報告するかを決定する必要があります。

ISO 19011:2018のガイダンスに基づくと、その他の記述は誤りです。例えば、以下のとおりです。

* Option B is false, because nonconformities can be graded using different terms or levels, depending on the criteria established by the audit programme or the audit client2. The terms 'major' and 'minor' are not mandatory or universal, but rather examples of possible grading levels3.

* Option D is false, because very minor nonconformities should not be re-graded as opportunities for improvement, but rather reported as nonconformities, as they still represent a non-fulfilment of a requirement1. An opportunity for improvement is a suggestion for enhancing the performance or effectiveness of the management system, but it is not a nonconformity or a requirement.

* Option F is false, because the grading of nonconformities does not have to be explained to the auditee at the opening meeting, but rather at the closing meeting, where the audit findings and conclusions are presented and discussed. The opening meeting is intended to provide an overview of the audit objectives, scope, criteria, and methods, and to confirm the audit arrangements and logistics.

* Option G is false, because the auditee is not always responsible for determining the criteria for grading nonconformities, but rather the audit programme or the audit client, in consultation with the auditee and other relevant parties2. The auditee is responsible for taking corrective action to address the nonconformities, and for providing evidence of their completion and effectiveness.

最新問題: 41

次のうち、第2段階の第三者監査の主な目的を最もよく表しているのはどれですか？

A. 認証準備状況の確認

B. 組織が法律を遵守しているかどうかを確認する

C. 基準を満たさない状況を特定する

D. 組織の管理システムを理解する

Answer: C (メッセージを残す)

ステージ2の第三者監査の主な目的は、組織のマネジメントシステムの実施状況と有効性を評価し、規格12の要求事項に対する不適合を特定することです。その他の選択肢は、ステージ1監査の目的 A、D) または監査範囲の特定側面 B) のいずれかです。参照 :1 :ISO/IEC 27006:2022、情報技術ーセキュリティ技術ー情報セキュリティマネジメントシステムの監査および認証を提供する機関に対する要求事項、条項9.2 \n2 :PECB認定ISO/IEC 27001主任監査員試験準備ガイド、ドメイン4 :ISO/IEC 27001監査の準備

最新問題: 42
シナリオ6

Sinvestmentは、住宅保険、商業保険、生命保険など、さまざまな保険プランを提供する保険会社です。もともと北カリフォルニアで設立された同社は、ヨーロッパやアフリカを含む他の地域にも事業を拡大しています。Sinvestmentは事業の成長に加え、業界の関連法規制を遵守し、情報セキュリティインシデントを防止することにも尽力しています。同社はISO規格に基づいた情報セキュリティマネジメントシステム (ISMS) を導入しています。

本製品はIEC 27001規格に準拠しており、認証申請中です。

認証機関は監査チームを任命し、監査を実施させた。監査チームはSinvestment社と機密保持契約を締結した後、業務を開始した。監査の第一段階におけるすべての活動は現地で実施されたが、Sinvestment社の要請により、アーカイブ情報のレビューはリモートで実施された。

監査チームはまず、情報セキュリティマネジメントシステム (ISMS) の適用範囲記述書、情報セキュリティポリシー、内部監査報告書などの必要文書をレビューする第1段階監査を実施しました。記録された情報の評価は、主にその内容と管理プロセスに基づいて行われました。

さらに、監査担当者は、情報セキュリティ研修および啓発プログラムに関する文書が不完全で、重要な詳細情報が欠落していることを発見した。これについて質問された際、Sinvestmentの経営陣は、同社は全従業員に情報セキュリティ研修コースを提供したと述べた。

監査の第2段階は、第1段階から3週間後に実施された。監査チームは、マーケティング部門（監査範囲外において、従業員のアクセス権限を管理する手順が欠如していることを発見した。

従業員のアクセス権限の管理はISO/IEC 27001の要件の一つであり、会社の情報セキュリティポリシーにも組み込まれているため、この問題は監査報告書に含められました。

質問

シナリオ6に基づき、監査チームはSinvestment社の情報セキュリティマネジメントシステム (ISMS) の監査において、どのような証拠収集および分析方法を用いましたか？

A. 証拠を収集するために、監査チームは書面による情報レビュー、観察、分析および評価を用いました。

B. 証拠収集のため、監査チームはサンプリングと技術的検証を実施しました。分析目的のため、検証のみを実施しました。

C. 監査チームは、証拠収集にインタビューのみを使用し、傾向分析を実施しました。

Answer: A ([メッセージを残す](#))

監査チームは、証拠収集のために文書情報のレビューと観察を行い、分析のために評価を行ったため、選択肢Aが正解です。これは、文書レビュー、観察、評価を主要な監査手法として定めているISO 19011規格と完全に一致しています。

このシナリオでは、監査員は遠隔でISMS文書をレビューし、ステージ2で部門の業務慣行を観察し、アクセス権限管理やトレーニング文書などの管理策がISO/IEC 27001の要求事項を満たしているかどうかを評価しました。これらの活動は、典型的な証拠に基づく監査手法を構成します。

選択肢Bは、技術的な検証やシステムの大規模なサンプリングが行われたことを示す証拠がないため、誤りです。選択肢Cは、監査がインタビューのみに依存したわけではなく、また傾向分析が主要な分析手法として用いられたわけでもないため、誤りです。インタビューは補足的なものであり、唯一のものではありませんでした。

ISO監査では、監査員は複数の方法を用いて証拠を三角測量的に検証する必要があります。文書レビュー、観察、評価分析を組み合わせることは、適切かつ推奨される監査手法を反映しています。

最新問題: 43
以下のオプションは、ファーストパーティ監査における主要な操作です。操作が行われた順序でステージを並べ替えてください。

Appoint an audit team leader

Issue the report

To complete the sequence click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the options to the appropriate blank section.

Prepare the audit checklist

Gather objective evidence

Review audit evidence

Document findings

Answer:

Prepare the audit checklist

Gather objective evidence

Review audit evidence

Document findings

Issue the report

To complete the sequence click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the options to the appropriate blank section.

Prepare the audit checklist

Gather objective evidence

Review audit evidence

Document findings

Explanation:

Appoint an audit team leader

Prepare the audit checklist

Gather objective evidence

Review audit evidence

Document findings

Issue the report

PECB

To complete the sequence click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the options to the appropriate blank section.

Prepare the audit checklist

Gather objective evidence

Review audit evidence

Document findings

正しい手順は以下のとおりです。

監査チェックリストを作成する

客観的な証拠を集める

* 監査証拠を確認する

* 調査結果を文書化する

* 監査準備 :この段階では、監査の目的、範囲、基準、計画を定義します。監査人はまた、監査中に取り上げる質問やトピックのリストである監査チェックリストを作成します。監査チェックリストは、監査人がISMSのすべての関連側面が対処され、監査証拠が体系的かつ一貫した方法で収集されることを保証するのに役立ちます12。

* 監査の実施 :この段階では、開始会議、インタビュー、観察、文書レビュー、終了会議などの監査活動を実施します。監査人は、監査結果と結論を裏付けるあらゆる情報である客観的証拠を収集します。客観的証拠は定性的または定量的であり、記録、声明、物的対象、観察など、さまざまな情報源から入手できます123。

* 監査報告: この段階では、監査証拠のレビュー、監査結果の評価、および監査結果の文書化を行います。監査人は、監査証拠が監査結果を裏付けるのに十分かつ信頼性があり、関連性があるかどうかを判断するために、監査証拠をレビューします。監査人は、監査結果を評価し、ISMSが監査基準に適合しているか不適合であるかを判断します。監査人は、監査結果を監査報告書に文書化します。監査報告書は、監査プロセスと結果を正式に記録したものです。監査報告書には通常、次の要素が含まれます123:

* 実施された作業の範囲、目的、時期、および規模を明確にする序文

* 主要な調査結果、簡単な分析、および結論を示す要約

* 報告書の送付先、および必要に応じて分類と配布に関するガイドライン

* 詳細な調査結果と分析

* 改善のための推奨事項（該当する場合）

* 監査基準への適合または不適合に関する声明

監査範囲または証拠に関する制限または除外事項

* 監査計画または手順からの逸脱

監査人と被監査者の間で未解決の問題や意見の相違がある場合

* レポートで使用されている参考文献、略語、定義の一覧

* 監査計画、監査チェックリスト、監査証拠、監査チームメンバーなどの付録一覧

* 監査フォローアップ :この段階では、監査結果に対処するために被監査組織が講じた是正措置の実施状況と有効性を検証します。監査員は是正措置の進捗状況と完了状況を監視し、ISMSのパフォーマンスと適合性への影響を評価します。監査員は、是正措置を現場で検証するためにフォローアップ監査を実施する場合もあれば、文書レビュー、リモートインタビュー、被監査組織による自己評価などの他の方法を用いる場合もあります。

監査人はフォローアップの結果を文書化し、それに応じて監査報告書を更新します123。

参考文献：

* PECB候補者ハンドブック ISO 27001主任審査員、19～25ページ

* ISO 19011:2018 - マネジメントシステムの監査に関する指針

* ISO 27001監査プロセス | ISMS.online

最新問題: 44

シナリオ9 :UpNetはISO/IEC 27001認証を取得したインターネット企業です。

ISO/IEC 27001認証取得以来、当社の認知度は著しく向上しました。この認証は、UpNefsの事業運営の成熟度と、広く認知され受け入れられている規格への準拠を証明するものです。

しかし、認証はそこで終わりではありません。UpNetは、内部監査を通じて、セキュリティ管理とISMS全体の有効性および効率性を継続的に見直し、強化しています。経営陣は専任の内部監査チームを雇用することに消極的だったため、内部監査機能を外部委託することにしました。この形式の内部監査は、独立性と客観性を確保し、ISMSの継続的な改善のための助言サポートを提供します。

最初の認証監査後まもなく、同社はデータおよびストレージ製品を専門とする新部門を設立した。この部門では、データセンター向けに最適化されたルーターやスイッチ、ネットワーク仮想化やネットワークセキュリティ機器などのソフトウェアベースのネットワーク機器を提供している。これにより、既にISMS認証の対象となっていた他の部門の業務にも変更が生じた。

そのため、UpNetはリスク評価プロセスと内部監査を開始しました。内部監査の結果に基づき、同社は既存および新規のプロセスと管理体制の有効性と効率性を確認しました。

新設された部署がISO/IEC 27001の要件を満たしていたため、経営陣は認証範囲に含めることを決定しました。UpNetは、会社全体を対象とするISO/IEC 27001認証を取得したことを発表しました。

最初の認証監査から1年後、認証機関はUpNefsのISMS（情報セキュリティマネジメントシステム）に対する別の監査を実施した。

この監査は、UpNefsのISMSが規定のISO/IEC 27001の要求事項に準拠しているかどうかを判断し、ISMSの継続的な改善を確保することを目的としていました。監査チームは、認証済みのISMSが引き続き規格の要求事項を満たしていることを確認しました。しかしながら、新設された部署はマネジメントシステムのガバナンスに大きな影響を与えており、さらに認証機関にはこれらの変更について一切通知されていませんでした。そのため、UpNefsの認証は一時停止されました。

上記のシナリオに基づいて、以下の質問に答えてください。

UpNetは、シナリオ9に示すように、内部監査機能を外部委託している。

A. いいえ、内部監査は必ずしも独立性と客観性を備えている必要はありません。なぜなら、内部監査には諮問的な機能があるからです。

B. いいえ、内部監査プロセスには監査計画以外にも多くのものが含まれるからです。

C. はい、監査人がISMSに関連する業務上の役割を担わないため、内部監査の独立性と公平性が高まります。

Answer: C ([メッセージを残す](#))

はい、内部監査機能を外部委託することで、独立性と公平性が向上し、内部監査プロセスに良い影響を与えることができます。これにより、内部監査が企業の内部経営陣からの偏見や影響を受けることなく実施されることが保証されます。

最新問題: 45

あなたは、医療サービスを提供するABCという高齢者向け介護施設でISMS監査を実施しています。すべての入居者が、位置情報、心拍数、血圧をモニタリングするための電子リストバンドを装着していることに気づきました。リストバンドは、医療スタッフが入居者の健康状態を監視 分析するために、すべてのデータを自動的に人工知能 (AI) クラウドサーバーにアップロードしていることが分かりました。

ISMSの適用範囲を確認するため、マネジメントシステム担当者 (MSR) にインタビューを行ったところ、ISMSの適用範囲にはアウトソーシングされたデータセンターも含まれると説明された。

ISMSコンテンツの範囲を定義する正しい記述を1つ選択してください。

A. ISMSの適用範囲は外部サービスプロバイダーを含めるべきではありません。外部サービスプロバイダーは、情報セキュリティポリシーや要件を遵守する上で困難に直面する可能性があるためです。

B. ISMSの範囲は、発生した情報セキュリティ問題と利害関係者の要求事項を考慮に入れる必要があります。

C. ISMSの適用範囲として最も可能性が高いのは、IT部門とアウトソーシングされたデータセンターを対象とするものです。

D. 組織は、ISMS の範囲を定義するために、政府の勧告、すなわち法律および法令のみに従うべきである。

Answer: ([解答を表示する](#))

ISMS の適用範囲の内容を定義する正しい記述は、ISMS の適用範囲は発生した情報セキュリティ問題と利害関係者の要求事項を考慮に入れるべきであるというものです。ISO/IEC 27001:2022 によれば、ISMS の適用範囲は、内部および外部の問題、利害関係者の要求事項と期待、組織と他の関係者間のインターフェースと依存関係、および情報セキュリティリスクを考慮して決定する必要があります。ISMS の適用範囲は、組織の戦略的方向性と整合し、その目的と状況に適切である必要があります。ISMS の適用範囲は、政府の勧告によって制限されるべきではなく、外部サービスプロバイダーを排除すべきでもなく、単一の部門または機能に基づくべきでもありません。ただし、リスク評価と利害関係者のニーズと期待によって正当化される場合はこの限りではありません。参照: = ISO/IEC 27001:2022、条項 4.3; PECB 候補者ハンドブック ISO 27001 主任監査員、15 ページ; ISO 27001 適用範囲記述書 | ISMSの適用範囲を設定する方法 - Advisera

最新問題: 46

あなたは監査チームリーダーとして、初めて第三者機関によるISMS監視監査を実施しています。現在、監査チームの別のメンバーと共に、被監査企業のデータセンターにいます。

あなたが今いる広い部屋は、いくつかの小さな部屋に分割されており、それぞれの部屋のドアにはデジタルキーパッドロックとカードリーダーが設置されています。あなたは、中央受付から提供されたカードと暗証番号を使って、2人の外部業者が顧客の部屋に入り、許可された電気修理を行っていることに気づきます。

受付に行って、クライアントスイートの入退室記録を見せてほしいと頼みます。記録には、カードが1枚しかスワイプされていないと書かれています。受付係に尋ねると、 見え、よくある問題です。全員にカードのスワイプをお願いしていますが、特に請負業者の方は、1人だけがスワイプして、他の人は後からこっそり入ってくることがよくあります」と答えます。しかし、受付でサインインすれば、誰が入室したかは分かります。

上記の状況を踏まえ、あなたは今、次のうちのどの行動を取りますか？

- A. 何も措置は講じられません。いかなる提案があろうとも、請負業者は常にこの方針で行動します。
- B. サプライヤーとの間で情報セキュリティ要件に関する合意がまだ成立していないため、管理措置A.5.20 サプライヤーとの関係における情報セキュリティ問題の解決」に関して不適合が確認されました。
- C. 管理A.7.6 安全な場所での作業」に関して、安全な場所での作業のための安全対策がまだ定義されていないため、不適合が指摘されています。
- D. 個人のセキュリティエリアへのアクセス権を確認するための有効な追加措置（例CCTV）があるかどうかを判断する。
- E. 改善の機会を提供する。請負業者は、セキュリティ施設を訪問する際には必ず同行者を伴わなければならない。
- F. 受付に大きな看板を設置し、入館するすべての人に必ずカードスワイプを使用する必要があることを周知することで、改善の機会を提供する。
- G. セキュリティエリアの保護が不十分なため、管理A.7.2 物理的入場」に関して不適合が確認されました。
- H. 組織に対し、請負業者にアクセスカードの適切な使用の必要性を改めて伝える書面を送付する必要があることを通知する。

Answer: G ([メッセージを残す](#))

情報セキュリティマネジメントシステム (ISMS) の確立、実施、維持、継続的改善に関する要求事項を規定するISO/IEC 27001:2022によると、管理策A.7.2では、組織はセキュリティエリアへの不正アクセスを防止するために適切な物理的入退室管理を実施する必要があるとされています1。組織は、セキュリティエリアへのアクセス権の付与および取り消しの基準を定義し文書化し、そのようなアクセス権の使用状況を監視および記録する必要があります1。したがって、ISMS監査員は、組織による管理策A.7.2の適用状況を監査する際に、これらの側面が監査基準に従って満たされていることを確認する必要があります。

上記のシナリオに基づき、監査員は管理策A.7.2に関して不適合を指摘すべきである。なぜなら、セキュリティエリアは不正アクセスから適切に保護されていないからである。監査員は、不適合の根拠として以下の証拠と理由を提示する必要がある。

* 証拠：監査人は、外部の請負業者2名がセンターの受付から提供されたスワイプカードと暗証番号を使用して顧客のスイートに入り、承認された電気修理を行っているのを目撃した。監査人は顧客のスイートのドアアクセス記録を確認したところ、カードが1枚しかスワイプされていないことがわかった。監査人が受付係に尋ねたところ、請負業者がカードを1枚だけスワイプして不正に入室するのはよくある問題だが、彼らは受付のサインインで顔見知りであると告げられた。

* 根拠 :この証拠は、組織が管理策A.7.2で要求されているように、セキュリティエリアへの不正アクセスを防止するための適切な物理的入退室管理を実施していないことを示しています。組織は、セキュリティエリアへのアクセス権の付与および取り消しの基準を定義し、文書化していません。これは、外部委託業者にスワイプカードと暗証番号を提供するための検証または承認プロセスがないためです。組織は、セキュリティエリアへのアクセス権の使用状況を監視および記録していません。これは、各個人がセキュリティエリアに入る前にカードをスワイプして暗証番号を入力することを保証する仕組みがないためです。組織は、身元確認手段として受付でのサインインに依存していますが、これは情報セキュリティを確保するには不十分で信頼性に欠けます。

その他の選択肢は、管理策A.7.2の監査において有効な措置ではありません。なぜなら、それらは管理策またはその要求事項に関連していないか、不適合に対処するのに適切または効果的ではないからです。例えば、次のとおりです。

* 何もしない: この選択肢は、監査人が不適合を無視または容認することを意味するため、有効ではありません。これは、マネジメントシステムの監査に関するガイドラインを提供する ISO 19011:20182 の監査原則と目的に反します。

- * サプライヤーと情報セキュリティ要件について合意していないため、管理 A.5.20「サプライヤー関係における情報セキュリティへの対応」に対して不適合を提起する: この選択肢は、サプライヤー関係ではなく物理的なアクセス制御に関連する不適合の根本原因に対処していないため、有効ではありません。管理 A.5.20 では、組織は、情報資産 1 の情報インフラストラクチャ コンポーネントにアクセス、処理、保存、通信、または提供する可能性のあるサプライヤーと情報セキュリティ要件について合意する必要があります。この管理は、サプライヤー関係における情報セキュリティの確保に関連する可能性があります、外部の請負業者によるセキュリティ領域への不正アクセスの問題には対処していません。
- * 管理A.7.6「セキュリティエリアでの作業」に対して不適合を提起する。セキュリティエリアでの作業に関するセキュリティ対策が定義されていないため: このオプションは、セキュリティエリアでの作業ではなく、物理的な入退室管理に関連する不適合の根本原因に対処していないため、無効です。管理A.7.6では、組織がセキュリティエリアでの作業に関するセキュリティ対策を定義し、適用することを要求しています1。この管理策は、セキュリティが確保された区域で作業する際の情報セキュリティを確保する上で有効かもしれないが、外部委託業者によるセキュリティ区域への不正アクセスという問題には対処していない。
- * 安全区域への個人のアクセスを確認するための追加の有効な措置（例CCTV）が実施されているかどうかを判断します。このオプションは、不適合に対処または解決するものではなく、その影響または発生確率を軽減する可能性のある代替または補償的な管理策を見つけようとするものであるため、有効ではありません。CCTVなどの追加の措置は、安全区域への個人のアクセスを確認するのに役立つ場合がありますが、管理策A.7.2で規定されている適切な物理的な入退室管理の要件に取って代わるものではありません。
- * 請負業者がセキュリティ施設に立ち入る際は常に同行者が必要であるという改善の機会を提起する :このオプションは、不適合に対処または解決するものではなく、不適合の再発または深刻度を防止または軽減する可能性のある改善策を提案するものであるため、有効ではありません。請負業者がセキュリティ施設に立ち入る際に常に同行することは、情報セキュリティを確保するための良い慣行かもしれませんが、管理策A.7.2で規定されている適切な物理的な入退室管理の要件に取って代わるものではありません。
- * 受付に、アクセスが必要な人は全員常にスワイプカードを使用する必要があることを知らせる大きな看板を設置するという改善の機会を提起する: この選択肢は、不適合に対処または解決するものではなく、既存の管理に対する認識または遵守を高める可能性のある改善策を提案するものであるため、有効ではありません。受付に、アクセスが必要な人は全員常にスワイプカードを使用する必要があることを知らせる大きな看板を設置することは、情報セキュリティを確保するための役立つリマインダーとなるかもしれませんが、管理策 A.7.2 で規定されている適切な物理的な入退室管理の要件に取って代わるものではありません。
- * 組織に対し、請負業者にアクセスカードを適切に使用する必要性を改めて伝えるよう指示する :この選択肢は、不適合に対処または解決するものではなく、情報セキュリティの確保に効果的または十分ではない可能性のある是正措置を組織に指示するものであるため、有効ではありません。請負業者にアクセスカードを適切に使用する必要性を改めて伝えることは、情報セキュリティを確保するためのコミュニケーション手段となり得ますが、管理策Aで規定されている適切な物理的な入退室管理の要件に取って代わるものではありません。

7.2.

参照規格 :ISO/IEC 27001:2022 - 情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステム - 要求事項、ISO 19011:2018 - マネジメントシステムの監査に関する指針

有効な **ISO-IEC-27001-Lead-Auditor-CN** 問題集は GoShiken.com が提供された合格しやすい ISO-IEC-27001-Lead-Auditor-CN 試験問題集！ GoShiken.com が最新の **ISO-IEC-27001-Lead-Auditor-CN** 試験問題集を提供しています。GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 問題集をゲットする人はこちら：
<https://www.goshiken.com/PECB/ISO-IEC-27001-Lead-Auditor-CN-mondaishu.html> (418**30%OFF**問題集溶と正解付きで 30%w特別割引コード: **Freepdfdumps**)

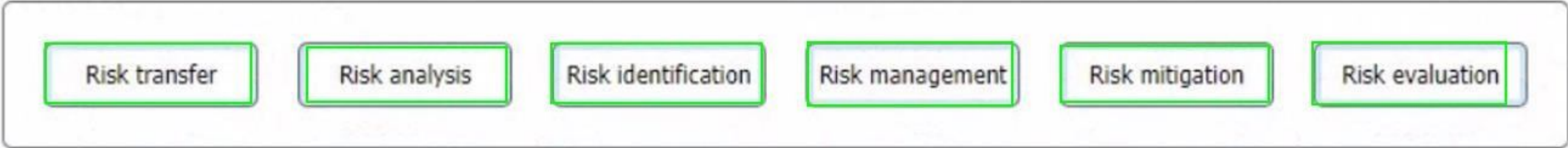
最新問題: 47

您是一位經驗豐富的 ISMS 審核團隊領導，為審核員提供培訓指導，他們對風險流程的理解不清楚，並要求您向他們提供下面詳細介紹的每個流程的範例。將提供的每項描述與下列風險管理流程之一相符。
要填寫表格，請按一下要填寫的空白部分，使其以紅色突出顯示，然後從下面的選項中按一下適用的文字或者，您可以將每個選項拖曳到適當的空白部分。

A process by which the nature of the risk is determined along with its probability and impact	
A process by which a risk is controlled at all stages of its life cycle by means of the application of organisational policies, procedures and practices	
A process by which a risk is recognised and described	
A process by which the impact and /or probability of a risk is compared against risk criteria to determine if it is tolerable	
A process by which the impact and/or probability of a risk is reduced by means of the application of controls	
A process by which a risk is passed to a third party, for example through obtaining appropriate insurance	

Answer:

A process by which the nature of the risk is determined along with its probability and impact	Risk analysis
A process by which a risk is controlled at all stages of its life cycle by means of the application of organisational policies, procedures and practices	Risk management
A process by which a risk is recognised and described	Risk identification
A process by which the impact and /or probability of a risk is compared against risk criteria to determine if it is tolerable	Risk evaluation
A process by which the impact and/or probability of a risk is reduced by means of the application of controls	Risk mitigation
A process by which a risk is passed to a third party, for example through obtaining appropriate insurance	Risk transfer



Reference:
ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements ISO/IEC 27005:2022 Information technology - Security techniques - Information security risk management

最新問題: 48
情報フェーズ
A. 創造、進化、維持、使用、廃棄
B. 設立、使用、廃棄、維持、進化
C. 設立、流通、使用、維持、廃棄
D. 設立、配布、維持、処分、および使用
Answer: C (メッセージを残す)

情報の段階は、作成、配布、使用、保守、廃棄です。これらは、情報が生成された瞬間から破棄またはアーカイブされる瞬間までのライフサイクル中に情報が経るフェーズです。情報の各段階には、異なるセキュリティ要件とリスクがあり、それに応じて管理する必要があります。作成、進化、保守、使用、廃棄は、情報の正しい段階ではありません。進化は明確な段階ではなく、どの段階でも発生する可能性のあるプロセスだからです。作成、使用、廃棄、保守、進化は、正しい順序ではないため、情報の正しい段階ではありません。作成、配布、保守、廃棄、使用は、正しい順序ではないため、情報の正しい段階ではありません。参照: : CQI & IRCA ISO 27001:2022 主任監査員コース ハンドブック、32 ページ。: [ISO/IEC 27001 主任監査員 - PECB]、12 ページ。

最新問題: **49**

監査担当者の責任には、監査活動の促進、ロジスティクスの維持、健康と安全に関する方針の遵守の確保、監査プロセスへの立ち会いにおける被監査者の代理などが含まれます。

A. 内部監査員

B. オブザーバー

C. ガイドライン

Answer: C (メッセージを残す)

ここで述べた責任は、ガイド」の役割に合致する。監査におけるガイドとは、通常、被監査組織のメンバーであり、監査活動を円滑に進め、ロジスティクスを管理し、安全衛生方針の遵守を確保するとともに、監査プロセスに立ち会い、監査チームを支援する人物を指す。

最新問題: **50**

次の記述のうち、正しいものはどれですか？（2選択可）

A. ISMSを導入する主なメリットは、情報セキュリティリスクの低減にあります。

B. ISMS認証のメリットは、政府機関から契約を獲得できることです。

C. ISMSの目的は、リスク管理プロセスを適用して情報セキュリティを維持することです。

D. ISMSの目的は、規制要件への準拠を証明することです。

Answer: A,C (メッセージを残す)

ISMS（情報セキュリティマネジメントシステム）を導入するメリットは、情報セキュリティリスクの低減にとどまらず、ビジネスパフォーマンスの向上、顧客満足度の向上、法令遵守の促進、ステークホルダーの信頼向上などにも及ぶ。

ISMS認証を取得するメリットは、政府機関からの契約獲得だけでなく、組織の情報セキュリティへの取り組みを他の潜在顧客、パートナー、規制当局に示すことにもあります。ISMSの目的は、情報セキュリティを維持するためのリスク管理プロセスを適用することであり、これは組織が直面する情報セキュリティリスクの特定、分析、評価、対処、監視、および見直しを意味します。ISMSの目的は、規制要件への準拠を示すことではなく、組織が自らの情報セキュリティ目標と義務を確実に達成することです。

参考文献:

* ISO/IEC 27001:2022 リードオーディター（情報セキュリティマネジメントシステム）の目的と内容は、Quality.orgおよびPECBによるものです。

* ISO/IEC 27001:2013 情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステム - 要求事項 [セクション 0.1] および [セクション 1]

最新問題: **51**

場景 6 :Cyber ACrypt 是一家網路安全公司，透過提供反惡意軟體和設備安全 資口生命週期管理和設備加密來提供端點保護。為了根據 ISO/IEC 27001 驗證其 ISMS 並證明其對網路安全卓越的承諾，該公司經歷了由指定審計團隊負責人 John 領導的細緻的審計過程。

在接受審計任務後，John 立即組織了一次會議，概述了審計計劃和團隊角色。他們審口了 Cyber ACrypt 的文檔信息，包括資訊安全政策和操作程序，確保每一份文件都符合標準並具有標準化的格式，包括作者標識註口日期、版本號和批准日期。這次徹底的檢口旨在確定持續改進和遵守 ISMS 要求。該文件對於審計團隊和 Cyber ACrypt 了解初步審計結果和需要關注的領域至關重要。

審計組也決定對主要相關方進行訪談。這項決定的目的是收集可靠的審計證據來驗證管理系統是否符合 ISO/IEC 27001 的要求。與 Cyber ACrypt 各個層級的相關方進行接觸為審計團隊提供了寶貴的觀點以及對 ISMS 的實施和有效性的理解。

第一階段審計報告揭露了口得關注的關鍵領域。適用性聲明 (SoA) 和 ISMS 政策在多個方面存在缺陷，包括風險評估不足 存取控制不充分以及缺乏定期政策審口。這促使 Cyber ACrypt 立即採取行動來解決這些缺陷。他們對戰略文件的快速回應和修改體現出了對實現合規的堅定承諾。

為了彌補審計團隊的網路安全知識差距而引入的技術專長在識別風險評估方法中的缺陷和審口網路架構方面發揮了關鍵作用。這包括評估防火牆、入侵偵測和預防系統以及其他網路安全措施，以及評估Cyber ACrypt 如何偵測、回應和恢復外部和口部威脅。在約翰的監督下，技術專家將審計結果傳達給了Cyber ACrypt 的代表。然而，審計小組發現，由於收取了被審計單位的諮詢費，該專家的客觀性可能受到影響考慮到技術專家在審核過程中的行為，審核組長決定與認證機構討論這個問題。

根據上述情景，回答以下問題：

根據情境 6，第一階段審計的訪談目標是否由審計小組相應設定？

- A. 是的，訪談的目的是收集審核證據，以驗證管理系統是否符合SO/IEC 27001 要求
- B. 否，訪談的目的與管理系統的關鍵績效指標(KPI) 不一致，從而降低了審核的有效性
- C. 不，面試的目的是確保充分了解受審核方面臨的挑戰

Answer: A ([メッセージを残す](#))

Comprehensive and Detailed In-Depth

A . Correct Answer:

The primary goal of audit interviews is to validate compliance with ISO/IEC 27001.

ISO 19011:2018 states that interviews are a method to gather audit evidence.

B . Incorrect:

KPIs are relevant for performance measurement, but interviews focus on compliance validation.

C . Incorrect:

Understanding business challenges is secondary; the primary objective is ISO/IEC 27001 compliance verification.

Relevant Standard Reference:

最新問題: **52**
あなたは、医療サービスを提供する高齢者向け介護施設で、ISMS（情報セキュリティマネジメントシステム）の初回認証監査を実施しています。監査計画の次のステップは、最終会議を開催することです。最終監査チーム会議において、監査チームリーダーとして、あなたは以下のとおり、2件の軽微な不適合と1件の改善機会を報告することに同意しました。

Cosmic Certifications Limited				
Summary of audit findings:				
Opportunities for Improvement (OI)				
Item	Findings	Requirements		Follow-up
1.	The organisation should improve the overall awareness of information security incident management responsibility and process.	Clause 7.4 and Control A.5.24		N/A
Nonconformities (NCs)				
Item	Findings	Grade	Requirements	Follow-up
1.	During the audit on the outsourced process, sampling one of the outsourced service contracts with WeCare the medical device manufacturer found that ABC does not include personal data protection and legal compliance as part of the information security requirements in the contract.	Minor	Clause 4.2 and Control A.5.20	Corrective actions are required.
2.	During the audit on information security during the business continuity process, sampling one of the service continuity and recovery plans for the resident's healthy status monitoring service. The auditor found the recovery plan has not yet been tested.	Minor	Clause 8.1 and Control A.5.29	Corrective actions are required.
signed by Audit				
Team Leader				

最終会議で被監査者に提示する、監査プロジェクトマネージャーの提案オプションを選択してください。

- A. すぐに推奨して検証します
- B. 6ヶ月以内に包括的な見直しを行うことをお勧めします。
- C. 将来的に抜き打ち監査を実施することをお勧めします。
- D. 提案された是正措置計画を承認した後、認証を実施することを推奨します。調査結果は、監視監査を通じて1年以内にまとめることをお勧めします。
- E. 3ヶ月以内に部分的な見直しを行うことをお勧めします。

Answer: D (メッセージを残す)

マネジメントシステムの監査および認証を行う機関に対する要求事項を規定するISO/IEC 17021-1:2015によると、9.4.9項では、認証機関は監査中に得られた情報およびその他の関連情報に基づいて認証の決定を行う必要があると規定されています1。認証機関はまた、監査中に特定された不適合に対処するために被監査機関が講じた是正措置の有効性も考慮する必要があります1。したがって、ISMS監査員は、監査プログラムマネージャーに勧告を行う際に、不適合の性質と重大性、および提案された是正措置を考慮する必要があります。

上記のシナリオに基づき、監査人は提案された是正措置計画を承認した後、認証を推奨し、指摘事項は1年後のサーベイランス監査で完了できると推奨すべきである。監査人は、その推奨の根拠として以下の説明を提供するべきである。

正当性 :この勧告は、被監査組織に軽微な不適合が2件と改善の機会が1件のみあり、ISMSの重大なまたは体系的な不備を示すものではないという事実を反映しているため、適切です。軽微な不適合とは、ISO/IEC 27001:2022の1つ以上の要求事項を満たしていないこと、またはISMSプロセスが意図した成果物を達成できるかどうかについて重大な疑義を生じさせる状況を指しますが、その全体的な有効性や適合性には影響しません2。改善の機会とは、ISO/IEC 27001:2022で要求されている以上の改善提案を指します2。したがって、これらの指摘事項は、適切な是正措置が妥当な期間内に実施される限り、認証を妨げたり、無効にしたりすることはありません。監査員は、是

正措置計画が現実的で、達成可能で、効果的であることを確認するために、認証を勧告する前に、提案された是正措置計画を承認する必要があります。監査人はまた、是正措置が実施され、意図どおりに機能していることを確認するため、1年後のサーベイランス監査で指摘事項を解決済みとするよう勧告すべきである。

他の選択肢は、与えられたシナリオに対して寛容すぎるか厳しすぎるかのどちらかであるため、監査プログラマナーにとって有効な推奨事項とは言えません。例えば、次のようになります。

即時認証を推奨する :このオプションは、監査員が不適合を無視または容認することを意味するため、無効です。これは、マネジメントシステムの監査に関するガイドラインを提供するISO 19011:20182の監査原則および目的に反します。また、認証機関が認証決定を行う前に、被認証者が講じた是正措置の有効性を考慮することを要求するISO/IEC 17021-1:20151の要件にも矛盾します。

6か月以内に全面的な再監査が必要であると推奨する :このオプションは、監査員が不適合に過剰反応したり誇張したりすることを示唆するため、ISO 19011:20182の監査原則と目的に反するため、有効ではありません。また、不適合の性質と範囲、およびその他の関連要因に基づいて再監査が必要かどうかを認証機関が判断することを要求するISO/IEC 17021-1:20151の要求事項にも矛盾します。全面的な再監査は通常、重大な不適合、またはISMSの深刻または広範囲にわたる不適合を示す複数の軽微な不適合に対してのみ行われます。

後日、抜き打ち監査を実施することを推奨する :この選択肢は、監査人が被監査者の是正措置を実施する意思や能力を疑っていることを示唆するため、ISO 19011:20182 の監査原則および目的に反するため、有効ではありません。また、ISO/IEC 17021-1:20151 の要求事項にも矛盾します。ISO/IEC 17021-1:20151 では、認証機関は、ISMS に重大な問題がある兆候がある場合や、セクター固有の制度で要求されている場合など、特定の条件下でのみ抜き打ち監査を実施する必要があると規定されています。

3か月以内に部分監査が必要であると推奨する :このオプションは、監査員が是正措置の検証に特定の期間や範囲を課したり規定したりすることを意味するため、ISO 19011:20182の監査原則と目的に反するため、有効ではありません。また、不適合の性質と程度、およびその他の関連要因に基づいて、認証機関が部分監査が必要かどうかを判断することを要求するISO/IEC 17021-1:20151の要求事項にも矛盾します。軽微な不適合には部分監査が適切である可能性があります、期間と範囲は被監査者と合意し、提案された是正措置計画に基づいて決定する必要があります。

最新問題: 53

メールアカウントを引き続き使用するには、名前、メールアドレス、パスワードを送信するように求めるメールが届きます。これらの情報を送信しないと、メールアカウントは無効になります。このシナリオは何を示しているでしょうか？

A. 人員に関連する脆弱性

B. 無許可の脅迫行為の種類

C. 脅威メッセージの種類に関する妥協

Answer: (解答を表示する)

ここで説明したシナリオは、フィッシング攻撃の典型的な例です。フィッシング攻撃とは、攻撃者が電子通信において信頼できる組織になりすますソーシャルエンジニアリングの一種です。その目的は、個人を騙して機密情報を提供させることです。これは、攻撃者が個人情報への不正アクセスを試みるという点で、不正行為型の脅威に該当します。参考資料：⇒フィッシングを脅威として捉えるこの理解は、情報セキュリティ管理システムの原則と一致しており、フィッシング攻撃とその防止策を説明する資料によって裏付けられています。

最新問題: 54

質問：

情報セキュリティにおける脅威と脆弱性に関して、次の記述のうち誤っているものはどれですか？

A. 脆弱性は、内在的脆弱性と外在的脆弱性に分けられます。前者は資産自体の特性に関係し、後者は外部要因に関係します。

B. 脅威は、情報の機密性、完全性、および/または可用性に悪影響を与える脆弱性を悪用する必要があります。

C. すべての脆弱性は、根本的な脅威に関係なく、直ちに制御措置を講じる必要があります。

Answer: C (メッセージを残す)

包括的かつ詳細な解説：

* C. 誤った記述 - すべての脆弱性に対して即時の修復が必要なわけではありません。リスク評価によって、対策が必要かどうか判断されます。リスクの低い脆弱性は、緊急の修正を必要としない場合があります。

* A. 正しい記述 - 脆弱性は、内在的（固有の欠陥）または外在的（外部の設定ミスによって引き起こされる）である可能性があります。

* B. 正しい記述 - 脅威は、損害を引き起こすために脆弱性を悪用しなければならない。

これは、ISO/IEC 27001:2022 附属書A 管理策A.8.8（技術的脆弱性の管理）に準拠しています。

質問

監査の結果、ITスタッフ15名のうち2名が十分な情報セキュリティ研修を受けていなかったことが判明しました。これは何を意味するのでしょうか？

- A. 監査結果
- B. 監査証拠
- C. 情報源

Answer: A (メッセージを残す)

This situation represents an audit finding, making option A the correct answer. An audit finding is the result of evaluating audit evidence against audit criteria and identifying conformity, nonconformity, or opportunities for improvement. In this case, the auditor evaluated training records and discovered that two employees did not receive adequate information security training, which is a deviation from ISO/IEC 27001 training and awareness requirements.

Audit evidence consists of the records, interviews, or observations used to support findings. The training records themselves are evidence, not the finding. Information sources are where evidence originates, such as documents, personnel, or systems, but they are not the conclusion drawn by the auditor.

Option B is incorrect because the lack of training is not evidence; it is the conclusion derived from evaluating evidence. Option C is incorrect because employees or records may be information sources, but the situation described is the auditor's evaluative conclusion.

ISO 19011 emphasizes that audit findings must be based on objective evidence and clearly documented.

Therefore, identifying that some employees lacked adequate training constitutes an audit finding.

最新問題: 56

情境 6 :Sinvestment 是一家提供家庭保険、商業保険和人壽保険の保険公司。該公司成立於北卡羅來納州，但最近在其他地區進行了擴張，包括歐洲和非洲

Sinvestment 致力於遵守適用於其行業的法律法規，並防止任何資訊安全事件。他們實施了基於 ISO/IEC 27001 的 ISMS 並申請了 ISO/IEC 27001 認證。

認證機構指派兩名審核員進行審核。與Sinvestment簽訂保密協議後。他們開始了審計活動。首先，他們審計了標準要求的文件，包括SMS 範圍聲明、資訊安全政策和口部稽核報告。審計過程並不容易，因為儘管Sinvestment 表示他們已製定文件程序，但並非所有文件都具有相同的格式

隨後，審計小組對Sinvestment的高階主管進行了多次訪談，以了解他們在SMS實施中的作用。第一階段審計的所有活動都是遠端進行的，除了根據Sinvestment 的要求在現場進行的文件資訊審計之外。

在此階段，審計人員發現沒有與資訊安全培訓和意識計劃相關的文件。被問及時，Sinvestment代表表示，公司已為所有員工提供資訊安全培訓課程。第一階段審計讓審計團隊對 Sinvestment 的營運和 ISMS 有了整體了解。

第二階段審核在第一階段審核三週後進行。審計小組觀察到，行銷部門（未包含在審計範圍口）沒有適當的程序來控制員工的存取權限。由於控制員工的存取權限是ISO/IEC 27001的要求之一，並且已包含在公司的資訊安全政策中，因此該問題包含在審計報告中。此外，在第二階段審計中，審計小組觀察到investment沒有記錄使用者活動日誌。

該公司的程序規定“記錄用口活動的日誌應保留並定期審計”，但該公司沒有提供任何執行該程序的證據

在所有審核活動中，審核員透過觀察 訪談、文件化資訊審計、分析和技術驗證來收集資訊和證據。對第一階段和第二階段的所有審核結果進行了分析，審核小組決定發布積極的認證建議

シナリオ6によると、監査の第一段階で、監査員はISMS関連文書の一部に異なるフォーマットが使用されていることを発見しました。このような状況で、監査員はどのような対応を取るべきでしょうか？

- A. 記録された情報が適切な形式であり、会社の記録手順に準拠していることを確認してください。これは標準的な要件です。
- B. これは標準の要件ではないため、形式に関係なく、標準で要求されている情報が記録されているかどうかのみを確認してください。
- C. この観察結果を、フェーズ2の監査期間中に検証すべき問題として記録してください。

Answer: B (メッセージを残す)

監査員は、規格で要求される情報が文書化されているかどうかを確認する必要がある、必ずしも形式にこだわる必要はありません。内容が規格の要件を満たしていれば問題ありません。ISO/IEC 27001は、文書化の特定の形式を義務付けているわけではなく、必要な情報が適切に文書化、維持、管理されていることのみを要求しています。

最新問題: 57

ISMS監査チームリーダーとして、あなたはオンライン小売業者の代理として、国際物流会社のセカンドパーティ監査を実施しています。監査中に、チームメンバーの1人が、ISO/IEC 27001:2022の附属書Aの管理措置5.18 (アクセス権)に関連する不適合を報告しました。彼女は、過去3か月以内に退職した20人のサーバーアクセス契約の削除に最大1週間かかっている証拠を発見しました。一方、社内規定では、退職後24時間以内にアクセス権を削除することが求められています。

文章に適切な単語をできるだけ入れて記入してください。空欄を埋めたい箇所にチェックを入れて赤色でハイライト表示し、下の選択肢から適切なテキストをクリックしてください。または、選択肢を適切な空欄にドラッグすることもできます。

"The purpose of including access rights in an information management system to ISO/IEC 27001:2022 is to provide, review, modify and remove these in accordance with the organisation's and for access .

guidance

rules

process

options

policy

rights

permissions

control

Answer:

"The purpose of including access rights in an information management system to ISO/IEC 27001:2022 is to provide, review, modify and remove these in accordance with the organisation's and for access .

guidance

rules

process

options

policy

rights

permissions

control

最新問題: 58

制限文書と機密文書の違いは何ですか？

- A. 制限付き - 承認されたグループ間で共有
機密情報 - 指定された個人間で共有
- B. 制限付き - 指定された個人間で共有
機密情報 - 承認されたグループ間で共有
- C. 制限付き - 指定された個人間で共有
機密情報 - 組織内でのみ共有
- D. 制限付き - 指定された個人間で共有
機密情報 - 友人や家族と共有する

Answer: B (メッセージを残す)

制限付き文書と機密文書の違いは、制限付き文書は指定された個人間で共有されるのに対し、機密文書は権限を与えられたグループ間で共有されるという点です。

制限付きと機密は、情報の機密性と価値、およびそれに必要な保護の度合いを示す情報分類レベルの例です。制限付き文書には、権限のない人に開示された場合、組織またはその利害関係者に重大な損害または危害を与える可能性のある情報が含まれています。したがって、正当な知る必要性があり、情報所有者によって承認された特定の個人のみがアクセスする必要があります。機密文書には、権限のない人に開示された場合、組織またはその利害関係者に損害または危害を与える可能性のある情報が含まれています。したがって、正当な知る必要性があり、情報所有者によって承認された定義されたグループのみがアクセスする必要があります。ISO/IEC 27001:2022 では、組織は、法的要件、価値、重要度、および不正な開示または変更に対する機密性の観点から情報を分類する必要があります (条項 A を参照)。

8.2.1) 参考文献: CQI & IRCA 認定 ISO/IEC 27001:2022 主任審査員トレーニングコース、ISO/IEC

最新問題: **59**

あなたはABCヘルスケアサービス社の介護施設でISO 27001 ISMS監視監査を実施しています。ABC社は、入居者の健康状態を監視するために、ベンダーであるWeCare社が設計・保守するヘルスケアモバイルアプリケーションを使用しています。監査中に、入居者の家族の90%が毎週、WeCare社の医療機器広告をメールやテキストメッセージで定期的に受け取っていることが判明しました。ABC社とWeCare社とのサービス契約では、ベンダーが入居者の個人データを使用することを禁じています。ABC社は、入居者とその家族から多数の苦情を受けています。サービスマネージャーは、これらの苦情は情報セキュリティインシデントとして調査され、正当なものであると判断されたと述べた。不適合および是正措置管理手順に従って、是正措置が計画され、実施されました。あなたは、ABCは、入居者とその家族の個人データに関する情報セキュリティ管理A.5.34 プライバシーおよび個人情報保護)に準拠していません。ベンダーであるWeCareは、入居者の個人情報を使用して家族と連絡を取っています。」という不適合報告書を提出しました。記載されている是正措置および改善措置の中から、この不適合に対してABCが取るべき措置を3つ選択してください。

- A. ABCはサイバー犯罪を防止するため、ISMSコンサルタントにABCヘルスケアのモバイルアプリのテストを依頼しました。
- B. ABCはWeCareとのサービス契約を解除します。
- C. ABCは、情報セキュリティ管理策A.5.34が適用範囲宣言書 \$oA)に含まれていることを確認します。
- D. ABCはABCヘルスケアのモバイルアプリケーションの使用を中止しました。
- E. ABCは、すべてのサプライヤーの情報セキュリティパフォーマンスに関する背景調査を導入しました。
- F. ABCは、第三者に関わるすべての適用可能な法的および契約上の要件の遵守状況を定期的に監視しています。
- G. ABCは契約違反でWeCareに対して法的措置を取っています。
- H. ABCは、情報セキュリティプロトコルを維持することの重要性について、全従業員に研修を実施しています。

Answer: **B,E,F (メッセージを残す)**

ABC社が不適合に対して行うと予想される修正および是正措置の選択肢は以下の3つです。

- * B. ABCはWeCareとのサービス契約を解除する。
- * E. ABC社は、すべてのサプライヤーに対し、情報セキュリティのパフォーマンスに関する身元調査を導入する。
- * F. ABCは、第三者に関わるすべての適用法令および契約上の要件の遵守状況を定期的に監視します。
- * B. この選択肢は、ABCが不適合に対処するために講じることができる是正措置です。是正とは、検出された不適合を解消するために講じる措置であり、是正措置とは、不適合の原因を解消し、その再発を防止するために講じる措置です'。WeCareとのサービス契約を解除することで、ABCは居住者の個人データの不正使用を阻止し、居住者のプライバシーと権利を保護することができます。これにより、居住者とその家族からのさらなる苦情や法的問題も防止できます。ただし、この選択肢には、サービス提供者の喪失、代替ソリューションを見つける必要性、居住者の幸福への潜在的な影響など、いくつかの欠点もあります。
- * E. このオプションは、ABCが不適合に対処するために講じることができる是正措置の一つです。すべてのサプライヤーの情報セキュリティパフォーマンスに関するバックグラウンドチェックを導入することで、ABCは、取り扱う情報の機密性、完全性、可用性を尊重する信頼できるパートナーを選定し、協力関係を築くことができます。これはまた、組織がサプライヤーによる組織資産へのアクセスに伴うリスクを軽減するための情報セキュリティ要件を合意し文書化することを要求する情報セキュリティ管理A.15.1.1 サプライヤー関係の情報セキュリティポリシー)への準拠にも役立ちます。
- * F. このオプションは、ABC が不適合に対処するために講じることができる是正措置の 1 つです。ABC は、第三者が関与するすべての適用法令および契約上の要件への準拠を定期的に監視することにより、サプライヤーが情報セキュリティに関する義務と責任を果たしていることを確認できます。これはまた、組織が従うべき関連する法令、規制、契約、およびその他の要件を特定、文書化し、最新の状態に保つことを要求する情報セキュリティ管理 A.18.1.1 (適用法令および契約上の要件の特定) を ABC が遵守するのにも役立ちます 3。

参考文献：

- 1: ISO 27000:2018 - 情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステム - 概要と用語、3.9項および3.10項 2: ISO/IEC 27001:2022 - 情報技術 - セキュリティ技術 - 情報セキュリティ管理システム - 要求事項、附属書A、管理A。15.1.1 3: ISO/IEC 27001:2022 - 情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステム - 要求事項、附属書A、管理策A.18.1.1

最新問題: **60**

あなたはISMS監査チームのリーダーとして、第三者機関による監視監査後の最終会議の議長を務める準備をしています。最終会議の議題を作成し、被監査者と話し合いたいトピックを概説しています。

以下のうち、含めるのが適切なものはどれですか？

- A. 認証機関の異議申し立て手続きに関する詳細な説明
- B. 監査計画とその目的の説明
- C. 証拠サンプリングに基づく監査結果に関する免責事項
- D. 不適合に関係する監査担当者の氏名

Answer: (解答を表示する)

このオプションは、ISMS12を含むマネジメントシステムの監査に関するガイドラインを提供するISO 19011規格の要件であるため、最終会議の議題に含めるのに適切です。この規格では、監査チームリーダーは、監査範囲、アクセス、またはサンプリングの制限など、監査結論に対する信頼性を低下させる可能性のある監査中に遭遇した状況を被監査者に通知する必要があると規定しています3。また、この規格では、監査報告書には、監査は監査時に利用可能な情報のサンプルに基づいており、監査は監査対象のマネジメントシステムの適合性または有効性について絶対的な保証を提供するものではないという記述を含める必要があると規定しています4。したがって、監査チームリーダーは、監査の性質と制限を被監査者に知らせ、誤解や誤った期待を避けるために、最終会議の議題に免責事項を含める必要があります。その他のオプションは、無関係、不正確、または不完全であるため、最終会議の議題に含めるのに適切ではありません。例：

認証機関の苦情処理プロセスの詳細な説明は、監査結果や結論とは関係がないため、最終会議の議題には適していません。認証機関の苦情処理プロセスは、監査合意書または契約書の一部として、監査前に被監査者に伝えられるべきです。

監査計画とその目的の説明は、最終会議の議題にはふさわしくありません。これは、開始会議または監査前に行うべきことです。監査計画とは、監査の範囲、目的、基準、方法論、監査スケジュール、監査チーム、監査場所、および監査成果物を記述した文書です。監査計画は、事前に被監査者と協議し合意を得る必要があります、変更や逸脱が生じた場合は、監査中に通知する必要があります。

不適合に関連する被監査者の名前は、不適合の詳細や証拠を提供しないため、最終会議の議題としては不完全です。監査チームリーダーは、各不適合の説明、監査基準、監査証拠、監査結論、監査勧告を含む監査結果を提示する必要があります。また、監査チームリーダーは個人を名指ししたり非難したりすることは避け、プロセスとシステムに焦点を当てる必要があります。

参考文献: = 1: PECB 候補者ハンドブック - ISO/IEC 27001 主任監査員、222 ページ: ISO 19011:2018 マネジメントシステムの監査に関するガイドライン、第 13 項: ISO 19011:2018 マネジメントシステムの監査に関するガイドライン、第 6.4.94 項: ISO 19011:2018 マネジメントシステムの監査に関するガイドライン、第 19011:2018 マネジメントシステムの監査に関するガイドライン、第 10 項

7.5.25: ISO/IEC 17021-1:2015 適合性評価 - マネジメントシステムの監査及び認証を行う機関に対する要求事項 - 第 1 部: 要求事項、9.8 項。: ISO 19011:2018 マネジメントシステムの監査に関する指針、6.4.1 項。: ISO/IEC 27007:2011 情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステムの監査に関する指針、6.2.1 項。: ISO 19011:

2018 マネジメントシステムの監査に関するガイドライン、条項 6.4.2。: ISO 19011:2018 マネジメントシステムの監査に関するガイドライン、条項 6.4.10。: ISO/IEC 27007:2011 情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステムの監査に関するガイドライン、条項 6.3.3。

最新問題: 61

シナリオ6

Sinvestmentは、住宅保険、商業保険、生命保険など、さまざまな保険プランを提供する保険会社です。もともと北カリフォルニアで設立された同社は、ヨーロッパやアフリカを含む他の地域にも事業を拡大しています。Sinvestmentは事業の成長に加え、業界の関連法規制を遵守し、情報セキュリティインシデントを防止することにも尽力しています。同社はISO規格に基づいた情報セキュリティマネジメントシステム（ISMS）を導入しています。

本製品はIEC 27001規格に準拠しており、認証申請中です。

認証機関は監査チームを任命し、監査を実施させた。監査チームはSinvestment社と機密保持契約を締結した後、業務を開始した。監査の第一段階におけるすべての活動は現地で実施されたが、Sinvestment社の要請により、アーカイブ情報のレビューはリモートで実施された。

監査チームはまず、情報セキュリティマネジメントシステム（ISMS）の適用範囲記述書、情報セキュリティポリシー、内部監査報告書などの必要文書をレビューする第1段階監査を実施しました。記録された情報の評価は、主にその内容と管理プロセスに基づいて行われました。

さらに、監査担当者は、情報セキュリティ研修および啓発プログラムに関する文書が不完全で、重要な詳細情報が欠落していることを発見した。これについて質問された際、Sinvestmentの経営陣は、同社は全従業員に情報セキュリティ研修コースを提供したと述べた。

監査の第2段階は、第1段階から3週間後に実施された。監査チームは、マーケティング部門（監査範囲外）において、従業員のアクセス権限を管理する手順が欠如していることを発見した。

従業員のアクセス権限の管理はISO/IEC 27001の要件の一つであり、会社の情報セキュリティポリシーにも組み込まれているため、この問題は監査報告書に含められました。

質問

Sinvestmentは、第1段階監査で指摘された情報セキュリティに関する研修および意識向上手順の不足に対処するために、どのような措置を講じるべきでしょうか？シナリオ6を参照してください。

- A. 第二段階の審査を実施する前に、文書に必要な修正を加え、修正済みの文書を審査チームに提出してください。
- B. 発見された問題点を記録し、認証監査完了後に修正する。
- C. 問題に修正が必要かどうかを判断するために、新しいリスク評価プロセスを導入する。

Answer: (解答を表示する)

Sinvestment社は、ステージ2監査に進む前に文書の不備を修正する必要があるため、選択肢Aが正解です。ステージ1監査の目的は、必要な文書情報の適切性と完全性を含め、認証取得に向けた組織の準備状況を評価することです。ステージ1で特定された不備は、重大な不適合を回避するために、ステージ2の前に解決されることが意図されています。

ISO/IEC 27001では、組織は情報セキュリティに関する意識向上、教育、およびトレーニングのための文書化された情報を維持することが求められています。Sinvestmentの経営陣はトレーニングを実施したと述べていますが、完全な文書化がないため、適合性を証明できていません。監査は口頭での保証ではなく、客観的な証拠に基づいて行われます。

選択肢Bは、認証後まで是正措置を延期することは、2段階監査プロセスの趣旨に反するため誤りです。第2段階は、準備状況のギャップが解消されてからのみ進めるべきです。選択肢Cも、問題はリスク特定ではなく、文書化と証拠に関する問題であるため誤りです。訓練の実施自体は問題ではなく、適切な文書化が不足していることが問題なのです。

したがって、Sinvestmentは速やかに文書を更新し、ステージ2の前に監査チームに提出する必要がある。

有効な **ISO-IEC-27001-Lead-Auditor-CN** 問題集は GoShiken.com が提供された合格しやすい ISO-IEC-27001-Lead-Auditor-CN 試験問題集！ GoShiken.com が最新の **ISO-IEC-27001-Lead-Auditor-CN** 試験問題集を提供しています。GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 問題集をゲットする人はこちら：
<https://www.goshiken.com/PECB/ISO-IEC-27001-Lead-Auditor-CN-mondaishu.html> (**41830%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 62

あなたは経験豊富な監査チームリーダーであり、監査員の研修を指導する立場にあります。

貴チームは現在、外部顧客のためにデータを保管する組織に対し、第三者監視監査を実施しています。訓練を受けた監査担当者は、適合性報告書 \$oA)に記載され、現場で実施されている人事管理体制を検証する任務を負っています。

研修を希望する監査担当者にレビューしてもらいたい管理項目を、以下のリストから4つ選択してください。

- A. 機密保持および機密保持契約
- B. マルウェア対策の実装方法
- C. 情報セキュリティに関する意識向上、教育、トレーニング
- D. リモートワーク体制
- E. 人員の確認とチェック。
- F. 現場監視カメラおよび入退室管理システムの運用
- G. 組織の情報削除に関する取り決め
- H. 組織の事業継続計画

Answer: (解答を表示する)

研修中の監査員が確認すべき、リストにある4つの統制事項は以下のとおりです。

*A. 機密保持契約および秘密保持契約 :この管理策では、機密情報にアクセスするすべての従業員、契約業者、および第三者が、当該情報の機密性と完全性を保護する義務を負う適切な契約に署名することを組織が保証する必要があります。これは、外部顧客に代わってデータを保存する組織にとって特に重要であり、顧客の情報資産を保護し、契約上の義務を遵守するという組織の姿勢を示すものです。

*C. 情報セキュリティに関する意識向上、教育、および研修 :この管理策では、組織の情報システムおよび情報資産にアクセスするすべての従業員、契約業者、および第三者に対し、定期的かつ適切な情報セキュリティに関する意識向上、教育、および研修を提供することが求められます。これは、彼らが自身の役割と責任、情報セキュリティに関する方針と手順、潜在的な脅威とリスク、および情報セキュリティインシデントの防止と対応に関するベストプラクティスを確実に理解するために不可欠です。

*D. リモートワーク体制 :この管理策では、組織はテレワーク、モバイルワーク、在宅勤務などのリモートワーク体制に伴う情報セキュリティリスクを管理するためのポリシーと手順を確立し、実施する必要があります。これには、承認されたデバイス、アプリケーション、ネットワーク、暗号化および認証方法、バックアップおよび復旧手順、報告および監視メカニズムなど、リモートワークの条件と要件を定義することが含まれます。これは、外部クライアントのためにデータを保存する組織にとって重要です。なぜなら、従業員の場所や使用するデバイスに関係なく、情報セキュリティレベルが維持されることが保証されるからです。

*E. 人材の身元確認 :この管理策では、組織の情報システムおよび情報資産にアクセスするすべての従業員、契約社員、および第三者の経歴、資格、および推薦状について、適切な身元確認を行うことが求められます。これは、彼らの身元、適性、および信頼性を確認するため、また、組織および顧客の情報セキュリティを損なう可能性のある、権限のない者や悪意のある者の雇用を防止するために必要です。

参照: = ISO/IEC 27001:2022、附属書A、条項A.5.7、A.7.2、A.7.3、およびA.7.4; ISO 27001 人的管理: 人員が情報セキュリティを確保する方法; ISO 27001の11の新しいセキュリティ管理策とは何か: 2022年? - Advisera。

最新問題: 63

情報セキュリティの各側面間の関係を最も正確に説明しているのは、次のうちどれですか?

A. 脆弱性を悪用して資産に損害を与えたり破壊したりする脅威。

B. 脅威を軽減することで資産を保護する

C. リスクとは、資産に損害を与える可能性のある脆弱性の関数です。

Answer: (解答を表示する)

この記述は、情報セキュリティの文脈における脅威、脆弱性、および資産の関係を要約したものです。脅威とは、システムや組織に損害を与える可能性のある、望ましくないインシデントの潜在的な原因です。脆弱性とは、脅威によって悪用され、損害を引き起こす可能性のある弱点です。資産とは、保護が必要な組織にとって貴重なリソースです。したがって、脅威が脆弱性を悪用すると、資産に損害を与えたり、破壊したりする可能性があります。参考文献: ≡この説明は、情報セキュリティマネジメントシステム (ISMS)の一部として、脅威、脆弱性、および資産の相互作用を理解することを含む、ISO/IEC 27001で概説されている情報セキュリティの基本概念に基づいています。

最新問題: 64

あなたは、医療サービスを提供する高齢者向け介護施設でISMS監査を実施しています。監査計画の次のステップは、事業継続管理プロセスの情報セキュリティを検証することです。

監査中に、組織が最近のパンデミックの間、医療サービスの継続を確保するために事業継続計画 (BCP)の一つを発動していたことが判明しました。そこで、サービスマネージャーに対し、組織が事業継続管理プロセスの中で情報セキュリティをどのように管理しているかを説明するよう求めました。

サービスマネージャーは、パンデミックに対応して継続的ケア計画を提案し、そのプロセスを以下のように要約した。

新規入居者の受け入れを中止してください。

事務職員の70%、医療従事者の30%が在宅勤務となる。

従業員による定期的な自己検査。これには、出社前日に陰性検査結果報告書を提出することも含まれます。

ABCのヘルスケアモバイルアプリをインストールして、従業員の行動を追跡し、現場での健康チェックのために緑色の健康状態QRコードを表示しましょう。

あなたはサービスマネージャーに、従業員が在宅勤務をしている際に、無関係の家族や関係者が居住者の個人データにアクセスできないようにするにはどうすればよいか尋ねました。サービスマネージャーは回答できず、セキュリティマネージャーに相談するよう提案しました。

監査証拠をさらに収集するために他の領域をさらに調査したい場合は、監査証拠に含まれる3つのオプションのうち1つを選択してください。

A. 組織がモバイルデバイスおよびリモートワーク中の情報セキュリティをどのように管理しているかについて、より多くの証拠を収集する (管理措置A.6.7に関連)。

B. 在宅勤務に対する従業員の気持ちを理解するために、より多くの従業員にインタビューすることで、より多くの証拠を集めることができます。

(第2項に関連)

C. 在宅勤務中の従業員を支援するために組織がどのようなリソースを提供しているかを理解するために、より多くの証拠を収集する。(第1項に関連)

D. 介護施設の既存入居者の退去率を評価するために、組織がどのように事業リスク評価を実施しているかについて、より多くの証拠を収集する。(第項に関連)

E. 事業継続性WANのテスト方法とテスト時期に関する証拠をさらに収集する。(対策A.5.29に関連)

F. 組織が検査結果が陰性の従業員のみが組織に入場できるようにしていることを示すさらなる証拠を収集する (管理措置A.7.2に関連)。

Answer: A,E,F (メッセージを残す)

情報セキュリティマネジメントシステム（ISMS）の確立、実装、維持、継続的改善に関する要件を規定するISO/IEC 27001:2022によると、管理策A.5.29では、組織は、障害発生後も必要なレベルで情報および情報システムが継続的に利用可能であることを保証するため、事業継続管理プロセスを確立し維持することが求められています¹。組織は、重要な情報資産およびプロセスを特定して優先順位を付け、障害発生リスクと影響を評価し、事業継続計画（BCP）を策定して実装し、BCPをテストおよびレビューし、関係者がそれぞれの役割と責任を認識していることを確認する必要があります¹。したがって、ISMS監査人は、事業継続管理プロセスの情報セキュリティを検証する際に、これらの側面が監査基準に従って満たされていることを確認する必要があります。

コントロールA.5.29を検証するための監査証拠には、以下の3つのオプションが含まれます。

* 組織がモバイル デバイスおよびテレワーク中の情報セキュリティをどのように管理しているかについて、より多くの証拠を収集する（管理策A.6.7に関連）このオプションは、従業員がラップトップ、タブレット、スマートフォンなどのモバイル デバイスを使用して自宅で作業する際に、情報および情報システムの機密性、完全性、可用性を保護するために組織が適切な管理策をどのように実施しているかについての証拠を提供できるため、関連しています。これは、組織がテレワークおよびモバイル デバイスの使用に関するポリシーと手順を確立することを要求する管理策 A.6.7に関連しています¹。

* 事業継続計画がどのように、いつテストされたかに関する証拠をさらに収集する（管理策A.5.29に関連）このオプションは、組織が事業継続計画をどのようにテストおよびレビューして、パンデミックなどのさまざまなシナリオに対する有効性と適合性を確保したかの証拠を提供できるため、関連があります。これは、組織が計画された間隔で、または重大な変更が発生した場合に事業継続計画をテストおよびレビューすることを要求する管理策 A.5.29に関連しています¹。

* 組織が検査で陰性となったスタッフのみが組織に入場できるようにするための方法について、より多くの証拠を収集する（管理策A.7.2に関連）このオプションは、定期的なスタッフの自己検査や健康状態アプリの使用など、スタッフや居住者の間での感染症や疾病の伝播リスクを予防または軽減するために組織が適切な管理策を実施していることを示す証拠を提供できるため、関連があります。これは、すべての従業員と契約者が情報セキュリティの脅威と懸念、責任と義務を認識し、この点に関して組織の方針と手順を支援できるように組織が準備していることを保証することを要求する管理策 A.7.2に関連しています¹。

その他の選択肢は、コントロールA.5.29またはその要件とは関係がないため、コントロールA.5.29の検証には関係ありません。例えば、次のようになります。

* 在宅勤務に対する従業員の気持ちについてインタビューして、より多くの証拠を集める（条項7.2に関連）このオプションは、組織が事業継続管理プロセスを確立および維持した方法、または混乱事象発生後に情報および情報システムの継続的な可用性を確保した方法の証拠を提供しないため、関連性はありません。これは、組織が利害関係者のニーズと期待を理解することを要求する条項4.2に関連している可能性があります、A.5.29を具体的に制御するものではありません。

* 在宅勤務中のスタッフをサポートするために組織が提供するリソースに関する証拠をさらに収集する（条項7.1に関連）このオプションは、組織が事業継続管理プロセスを確立および維持する方法、または障害発生後に情報および情報システムの継続的な可用性を確保する方法の証拠を提供しないため、関連性はありません。これは、組織が ISMS に必要なリソースを決定して提供することを要求する条項 7.1に関連している可能性があります、A.5.29 を具体的に管理するためのものではありません。

* 組織が事業リスク評価を実施して、既存の入居者を介護施設から退所させるスピードを評価する方法に関する証拠をさらに収集する（条項6に関連）このオプションは、組織が事業継続管理プロセスを確立および維持した方法、または混乱事象発生後に情報および情報システムの継続的な可用性を確保した方法に関する証拠を提供しないため、関連性はありません。これは、組織が ISMS のリスクと機会に対処するための行動を計画することを要求する条項 6に関連している可能性があります、A.5.29 を具体的に管理するものではありません。

参照規格 :ISO/IEC 27001:2022 - 情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステム - 要求事項

最新問題: 65
シナリオ2 :ナイト社は、米国カリフォルニア州北部を拠点とする電子機器メーカーで、ビデオゲーム機を開発しています。ナイト社は世界中に300人以上の従業員を抱えています。創業5周年を機に、同社は次世代ビデオゲーム機「G-Console」をグローバル市場向けに発売することを決定しました。G-Consoleは2021年の究極のメディアコンソールと位置づけられ、プレイヤーに最高のゲーム体験を約束します。

メインユニットパッケージには、VRヘッドセット、2つのゲームやその他のギフト。

長年にわたり、同社は誠実さ、正直さ、そして顧客への敬意を通して確固たる評判を築いてきました。この評判こそが、多くの熱心なゲーマーがKnightのGコンソールを発売と同時に手に入れたいと願った理由の一つです。ナイト社は顧客志向の企業であることに加えて、彼らの開発品質はゲーム業界で広く認められている。しかし、価格は妥当な範囲を超えて高額である。

しかし、ナイト社の製品の品質は最高レベルであるため、ほとんどの忠実な顧客にとってこれは問題ではない。世界有数のビデオゲーム機開発企業であるナイト社は、悪意のある攻撃の標的となることも少なくありません。同社の情報管理システム（ISMS）は1年以上前から運用されており、財務部門と人事部門を除くナイト社の全部門を網羅しています。

最近、ナイト社の機密情報を含むファイルの一部がハッカーによって流出しました。ナイト社のインシデント対応チーム（IRT）は、直ちにシステム全体と事件の詳細の分析を開始しました。

IRTは当初、ナイト社の従業員が脆弱なパスワードを使用していたため、不正なハッカーがアカウントに容易にアクセスできたのではないかと疑っていた。しかし、徹底的な調査の結果、ハッカーはファイル転送プロトコル（FTP）の通信を傍受することでアカウントにアクセスしていたことが判明した。

FTPは、アカウント間でファイルを転送するために使用されるネットワークプロトコルです。認証には平文のパスワードを使用します。

この情報セキュリティインシデントの結果、ナイト社はIRTの助言に基づき、FTPをセキュアシェル（SSH）に置き換えることを決定した。これにより、通信を傍受した者は暗号化されたデータしか見ることはできないようになる。

これらの変更を受けて、ナイト社はリスク評価を実施し、管理策の導入によって同様の事象のリスクが最小限に抑えられたかどうかを検証した。この評価結果はISMSプロジェクトマネージャーによって承認され、新しい管理策の導入後のリスクレベルは同社のリスク許容度と一致していると判断された。

このシナリオに基づいて、以下の質問に答えてください。

FTPは認証に平文パスワードを使用します。以下はFTPサーバーの例です。

A. リスク

B. 脅威

C. 脆弱性

Answer: C ([メッセージを残す](#))

最新問題: 66

あなたは経験豊富なISMS監査チームリーダーです。訓練を受けた監査員から、実施する必要のある監査の種類について確認するため、あなたに連絡がありました。

以下の監査の種類と説明を照合してください。

フォームに入力するには、入力したい空白部分をクリックして「In fed」をハイライト表示し、下のオプションから適切なテキストをクリックしてください。または、各オプションを対応する空白部分にドラッグすることもできます。

PECB

1. Also known as a first party audit, this type of audit involves an organisation auditing itself
2. A third party audit which assesses an organisation's conformity with every clause of a Standard
3. An audit whose scope requires the assessment of two or more Standards
4. An audit carried out at a single auditee by two or more auditing organisations
5. An audit carried out to verify the effectiveness of corrections, corrective action, and agreed opportunities for improvement
6. An audit forming part of a programme of certification body audits in which elements of the auditees' information system management system will be examined

A joint audit

A surveillance audit

An internal audit

A combined audit

A follow-up audit

A certification audit

Answer:

1. Also known as a first party audit, this type of audit involves an organisation auditing itself

2. A third party audit which assesses an organisation's conformity with every clause of a Standard

3. An audit whose scope requires the assessment of two or more Standards

4. An audit carried out at a single auditee by two or more auditing organisations

5. An audit carried out to verify the effectiveness of corrections, corrective action, and agreed opportunities for improvement

6. An audit forming part of a programme of certification body audits in which elements of the auditees' information system management system will be examined

An internal audit

A certification audit

A combined audit

A joint audit

A follow-up audit

A surveillance audit

A joint audit

A surveillance audit

An internal audit

A combined audit

A follow-up audit

A certification audit

1. Also known as a first party audit, this type of audit involves an organisation auditing itself

2. A third party audit which assesses an organisation's conformity with every clause of a Standard

3. An audit whose scope requires the assessment of two or more Standards

4. An audit carried out at a single auditee by two or more auditing organisations

5. An audit carried out to verify the effectiveness of corrections, corrective action, and agreed opportunities for improvement

6. An audit forming part of a programme of certification body audits in which elements of the auditees' information system management system will be examined

An internal audit

A certification audit

A combined audit

A joint audit

A follow-up audit

A surveillance audit

最新問題: 67

文を最も適切に完成させる単語を選びなさい。

マネジメントシステムにおけるコンプライアンス維持の目的は、最適な単語で文章を完成させることです。完成させたい空欄をクリックして赤色でハイライト表示し、該当するテキストをクリックしてください。または、オプションを該当する空欄にドラッグ&ドロップすることもできます。」

"The purpose of maintaining regulatory compliance in a management system is to _____."

To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

keep good relations
with authorities

pass the audit

avoid financial penalties

fulfil management
system policy

Answer:

"The purpose of maintaining regulatory compliance in a management system

fulfil management
system policy

To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

keep good relations
with authorities

pass the audit

avoid financial penalties

fulfil management
system policy

Explanation:

"The purpose of maintaining regulatory compliance in a management system is to fulfil management system policy."

ISO 27001:2013の5.2項によれば、組織の最高経営陣は、組織の目的に適した情報セキュリティ方針を策定、実施、維持し、情報セキュリティ目標を設定するための枠組みを提供しなければなりません。情報セキュリティ方針には、適用される法令、規制、契約上の要件、および組織が遵守するその他の要件を遵守するというコミットメントも含まれていなければなりません。したがって、規制遵守を維持することは、マネジメントシステム方針を履行し、その有効性と適切性を確保することの一部です。参考文献：

* ISO/IEC 27001:2013、情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項、5.2項

* PECB候補者ハンドブック ISO 27001主任審査員、10ページ

* ISO 27001ポリシー :ISO 27001に準拠したポリシーの書き方

最新問題: 68

以下の事項を定義する際には、法令遵守違反および法的 契約上の要件の不遵守に伴うコストを評価してください。

A. 重要性

B. 監査リスク

C. 合理的な保証

Answer: A ([メッセージを残す](#))

監査における重要性とは、法令遵守や契約遵守に関するものを含め、どの程度の不適合や不備が監査結果に影響を与えるほど重大なものとなるかを評価することを指します。

これらの問題に関連する費用は、重要性を判断する際に考慮される。

参考文献 :ISO 19011:2018、マネジメントシステムの監査に関する指針

最新問題: 69

監査報告書に関する以下の4つの記述のうち、正しいものはどれですか？

- A. 監査報告書は、監査チームのコメントに基づいて監査チームリーダーが作成する必要があります。
- B. 監査報告書には、監査計画を含めるか、監査計画を参照する必要があります。
- C. 監査報告書は、その内容が不都合な場合もあるため、まず組織の最高経営陣に送付すべきです。
- D. 監査報告書は、特に機密扱いと明記されていない限り、広く配布するのに適しているとみなすべきである。
- E. 監査報告書には不適合事項のみを記載すべきである。
- F. 監査報告書は合意された期間内に作成されるべきです。
- G. 不要になった監査報告書は、組織の一般廃棄物の一部として処分することができます。
- H. 監査報告書は必ずクライアントによって確認され、日付が記入され、承認」の署名がなされるべきです。

Answer: (解答を表示する)

ISO/IEC 27001 主任審査員向け PECB 候補者ハンドブックによると、監査報告書は、監査証拠の収集と分析を担当する監査チームリーダーが監査チームからの意見を取り入れて作成する必要があります1。監査報告書には、監査の目的、範囲、基準、および方法論の基礎となる監査計画を含めるか、または参照する必要があります2。さらに、監査報告書は、監査プログラム管理の一部であり、監査結果のタイムリーな伝達を保証するため、合意された期間内に作成する必要があります3。加えて、監査報告書は常にクライアントによってレビューされ、日付が記入され、承認済み」として署名される必要があります。これは、監査の完了と監査結果および結論に関する正式な合意を確認するためです4。

他の記述が誤りである理由は以下のとおりです。

監査報告書は、その内容が組織の経営陣にとって都合の悪いものになる可能性があるため、最初に経営陣に送付すべきではありません。これは監査の公平性と機密性を損なうこととなります。監査報告書は、監査プログラムの手順と監査計画に従って配布されるべきです。

監査報告書は、機密扱いと明記されていない限り、一般に公開すべきではありません。これは、監査の機密保持義務および個人情報保護の原則に違反するからです。監査報告書は機密文書として扱い、権限のある関係者のみに開示する必要があります。

監査報告書は、不適合事項のみを記載するべきではない。なぜなら、それでは監査の範囲と価値が限定されてしまうからである。監査報告書は、適合性、改善の機会、優良事例、および監査上の所見も記載すべきである。

不要になった監査報告書は、組織の一般廃棄物として廃棄してはなりません。これは、監査の機密性および情報セキュリティにリスクをもたらすためです。監査報告書は、監査プログラムの手順および適用される法的要件に従って、保管、廃棄、または破棄する必要があります。

最新問題: 70

監査目的」を表すのに適切なフレーズは次のうちどれですか？（2選択可）

- A. レビュー期間
- B. 一貫性を判断する
- C. 法令遵守を確認する
- D. 監査人の能力
- E. 管理方針の変更
- F. 必要に応じて、改善の機会を特定する。

Answer: (解答を表示する)

監査目的とは、監査依頼者と監査人によって定義された監査の目的と範囲のことです。ISO/IEC 27001 規格によれば、ISMS 監査の監査目的には、ISMS が監査基準にどの程度適合しているかを判断すること、組織が情報セキュリティ目標を達成していることを保証する ISMS の能力を評価すること、ISMS の改善の可能性のある領域を特定することなどが含まれます。12. 参照: = 1: PECB 候補者ハンドブック - ISO/IEC 27001 主任監査人、19 ページ 2: ISO/IEC 27007:2011 情報技術 - セキュリティ技術 - 情報セキュリティ管理システム監査のガイドライン、条項 4.2.1。

最新問題: 71

あなたは、機密文書およびリムーバブルメディアの安全な廃棄を専門とする組織の第三者認証監査を実施する、経験豊富なISMS監査チームリーダーです。文書とメディアは軍事レベルの機器を使用してシュレッダー処理されており、元のファイルを復元することは不可能です。

監査は順調に進み、最終会議まであと30分となったところで、監査報告書の作成に取りかかろうとしていました。その時、組織の従業員があなたのドアをノックし、話がしたいと申し出てきました。その従業員は、業務が忙しくなると、上司から低グレードの産業用シュレッダーを使うように言われる、なぜなら組織にはそういう機械がたくさんあって、稼働も速いからだと説明しました。被監査組織は、これらの機械の存在や使用についてあなたに一切知らせていませんでした。

このメッセージへの返信方法を決定するために、3つの選択肢から1つを選んでください。

- A. 認証前に実施する追加監査に関して、監査プログラムを管理する担当者への提案はありますか。
- B. 監査報告書を作成する代わりに、組織と顧客との契約を精査し、低グレードの機械の使用が許可されているかどうかを確認してください。
- C. 発見されたその他の情報に基づいて、4週間以内にフォローアップレビューが必要かどうかを検討してください。
- D. 何もする必要はありません。すべての監査はサンプルに基づいて行われます。収集したサンプルには、下位レベルのマシンに対する計画された監査は含まれていません。
- E. 認証監査期間を延長し、下位レベルのマシンの使用状況を監査する時間を増やす。
- F. 組織がまだそのプロセスを開示していないため、これは8.1 運用計画と管理の要件を満たしていません。
- G. 特定の状況下で下位レベルの機械が使用されたかどうかを被監査者に確認する。

Answer: ([解答を表示する](#))

ISO/IEC 27001:2022の8.1項によれば、組織は情報セキュリティ要件を満たすために必要なプロセスを計画、実施、管理し、6.1項で定められた措置を実施しなければならない。また、組織はアウトソーシングされたプロセスが管理または影響を受けることを保証しなければならない。

管理策A.5.24によれば、組織は情報セキュリティインシデント管理プロセスを確立し、維持する必要がある、これには情報セキュリティ事象および脆弱性の報告が含まれます。したがって、機密文書およびメディアの安全な廃棄に低グレードの機器を使用することは、重大な情報セキュリティリスクおよび顧客との契約違反につながる可能性があります。監査人はこの情報に対し、以下の対応を取るべきです。

* A. 認証前に追加監査を実施すべきという勧告を監査プログラムを管理する担当者に通知すること。これは、監査チームリーダーが監査結果または認証決定に重大な影響を与える可能性のある状況を認証機関に報告し、監査計画に必要な変更を提案しなければならないと規定するISO/IEC 27006:2022の7.4.3項に準拠しています。

* C. 新たに明らかになった情報に基づき、4週間以内に再監査の必要性を検討する。これは、監査チームリーダーが監査結果および監査中に収集されたその他の適切な情報を確認し、監査の結論を決定し、再監査の必要性を特定することを規定するISO/IEC 27006:2022の7.5.2項に準拠している。

* G. 特定の状況下で低グレードの機械が使用されていることを被監査者に確認する。これは、監査チームリーダーが監査が監査計画に従って実施され、計画への変更が合意され文書化されることを保証する必要があると規定するISO/IEC 27006:2022の7.4.2項に準拠している。

その他の選択肢は、情報を無視したり、監査の範囲を超えたり、十分な証拠がないまま時期尚早に不適合を指摘したりするため、適切な対応とは言えません。例えば、次のようになります。

* B. 監査報告書の作成を中止し、代わりに組織と顧客との契約を精査して、低グレードのマシンの使用を許可しているかどうかを確認する。これは適切な対応ではありません。監査プロセスと認証決定が遅れるだけでなく、ISMS監査の範囲外の文書を精査する必要が生じるためです。監査担当者は、低グレードのマシンの使用に関連する情報セキュリティリスク評価および対策プロセス、ならびに情報セキュリティインシデント管理プロセスの検証に重点を置くべきです。

* D. 何もしない。すべての監査はサンプルに基づいて行われますが、あなたが採取したサンプルには、低グレードの機械の計画的なレビューが含まれていませんでした。これは適切な対応ではありません。重大な情報セキュリティリスクと、監査結果や認証決定に影響を与える可能性のある不適合を無視することになるからです。監査担当者は、従業員から提供された情報に基づいてフォローアップを行い、その妥当性と影響を検証する必要があります。

* E. 認証監査期間を延長して、低グレード機器の使用状況を監査するための追加時間を確保する。これは、監査スケジュールや監査チームおよび被監査者の対応に支障をきたすため、適切な対応策ではありません。監査員は、状況を認証機関に報告し、監査計画に必要な変更（例えば、後続監査の実施など）を提案する必要があります。

* F. 組織がプロセスを公開していないことを理由に、8.1 運用計画および管理に対する不適合を指摘する。これは、検証または裏付けされていない単一の情報源に基づくものであるため、適切な対応とは言えません。監査人は、不適合を裏付ける十分かつ適切な監査証拠を収集し、不適合の根本原因と重大度も考慮する必要があります。

参考文献：

ISO/IEC 27001:2022、条項8.1および附属書A管理A.5.24

ISO/IEC 27006:2022、7.4.2項、7.4.3項、および7.5.2項

[PECB候補者ハンドブック ISO/IEC 27001主任監査員]、18-19ページ、23-24ページ ISO 27001内部監査を実施するためのステップバイステップガイド ISO 27001 - 附属書A.16：情報セキュリティインシデント管理

最新問題: 72

シナリオ6

Sinvestmentは、住宅保険、商業保険、生命保険など、さまざまな保険プランを提供する保険会社です。もともと北カリフォルニアで設立された同社は、ヨーロッパやアフリカを含む他の地域にも事業を拡大しています。Sinvestmentは事業の成長に加え、業界の関連法規制を遵守し、情報セキュリティインシデントを防止することにも尽力しています。同社はISO規格に基づいた情報セキュリティマネジメントシステム（ISMS）を導入しています。

本製品はIEC 27001規格に準拠しており、認証申請中です。

認証機関は監査チームを任命し、監査を実施させた。監査チームはSinvestment社と機密保持契約を締結した後、業務を開始した。監査の第一段階におけるすべての活動は現地で実施されたが、Sinvestment社の要請により、アーカイブ情報のレビューはリモートで実施された。

監査チームはまず、情報セキュリティマネジメントシステム（ISMS）の適用範囲記述書、情報セキュリティポリシー、内部監査報告書などの必要文書をレビューする第1段階監査を実施しました。記録された情報の評価は、主にその内容と管理プロセスに基づいて行われました。

さらに、監査担当者は、情報セキュリティ研修および啓発プログラムに関する文書が不完全で、重要な詳細情報が欠落していることを発見した。これについて質問された際、Sinvestmentの経営陣は、同社は全従業員に情報セキュリティ研修コースを提供したと述べた。

監査の第2段階は、第1段階から3週間後に実施された。監査チームは、マーケティング部門（監査範囲外において、従業員のアクセス権限を管理する手順が欠如していることを発見した。

従業員のアクセス権限の管理はISO/IEC 27001の要件の一つであり、会社の情報セキュリティポリシーにも組み込まれているため、この問題は監査報告書に含められました。

質問

Sinewstmentが記録された情報の遠隔レビューを要求することは許容されますか？

A. はい、録画された情報は遠隔で閲覧できます。

B. いいえ、それは守秘義務違反につながる可能性があるからです。

C. いいえ、異なる場所の組み合わせは監査効率に悪影響を与える可能性があるためです。

Answer: A ([メッセージを残す](#))

Sinvestment社によるステージ1監査中の文書情報の遠隔レビューの要求は許容範囲内であり、確立された監査慣行に合致しているため、オプションAが正解です。ISO/IEC 17021-1およびISO

19011:2018は、監査の機密性、完全性、有効性が維持されることを条件として、リモート技術の使用を含め、監査活動の実施方法に柔軟性を認めている。

ステージ1監査は、主に文書化された情報のレビュー、組織の状況の理解、ISMSの適用範囲の確認、およびステージ2への準備状況の評価に重点を置いています。特に適切な機密保持契約が締結されている場合、文書を遠隔でレビューすることは広く受け入れられている手法であり、今回のケースもその通りでした。監査担当者は既に機密保持契約に署名していたため、情報漏洩のリスクは軽減されていました。

選択肢Bは誤りです。なぜなら、遠隔での文書レビューは必ずしも機密保持義務違反につながるわけではないからです。

リスクは管理すべきものであり、想定すべきものではありません。安全な文書共有プラットフォームと機密保持契約は、適切に実施されれば十分な安全策となります。選択肢Cは誤りです。異なる場所や遠隔方式を使用しても、監査効率が自動的に低下するわけではありません。多くの場合、移動時間の短縮や準備の効率化により、効率が向上します。

したがって、ステージ1において文書化された情報の遠隔レビューを許可することは、ISO監査基準および認められた認証機関の慣行と完全に整合している。

最新問題: 73

あなたは、医療サービスを提供する高齢者向け介護施設でISMS監査を実施しています。監査計画の次のステップは、情報セキュリティインシデント管理プロセスを検証することです。ITセキュリティマネージャーは、情報セキュリティインシデント管理手順を提示し、そのプロセスがISO/IEC 27035-1:2016に基づいていることを説明しました。

文書を確認すると、「情報セキュリティ上の脆弱性、インシデント、または事象は、発見後1時間以内に連絡担当者（PoC）に報告しなければならない」という記述が見つかります。従業員に聞き取り調査を行ったところ、「脆弱性、インシデント、および事象」の意味について、従業員間で認識のずれがあることが判明しました。

イベント追跡システムから過去6か月間のイベント報告記録のサンプルを抽出しました。結果は以下の表にまとめられています。

Type of report	Description	Resolution/Recovery Actions	Resolution/Recovery Time
Information security weakness, report ID: 056	The human resources manager's mobile phone was hacked by ransomware, asking for \$1000 to unlock (decrypt) the data	IT department suggests the person shall pay the ransom to unlock the phone. No further action is needed.	24 hours
Information security weakness, report ID: 078	The medical staff's company mobile phone (with patient data) was hacked by ransomware, asking for \$5000 to unlock (decrypt) the data	IT department suggests the company shall pay the ransom to unlock the company phone. No further action is needed.	24 hours
Information security event, report ID: 090	The cloud server does not respond and healthcare monitoring stops for 8 hours.	IT department reboots the cloud server remotely. No further action is needed.	24 hours
Information security incident, report ID: 012	The cloud server does not respond and healthcare monitoring stops for 48 hours.	IT department reboots the cloud server remotely. No further action is needed.	24 hours

監査証拠をさらに収集するために、他の領域についても調査を進めたいと考えています。監査証拠に表示されないオプションを2つ選択してください。

- A. より多くの従業員にインタビューを行い、報告プロセスに対する彼らの理解度を把握することで、より多くの証拠を集める。
(管理措置A.6.8に関連)
- B. 会社が携帯電話とデータのロックを解除するために、どのように、そしていつ身代金を支払ったか クレジットカードや銀行振込など)に関する証拠をさらに収集する。(管理措置A.5.26に関連)
- C. 人事部長が個人活動データ クレジットカードや銀行振込など)のロックを解除するために、どのように、そしていつ身代金を支払ったのかに関するさらなる証拠を収集する。(管理策A.5.26に関連)
- D. 組織がインシデント復旧時間をどのように決定しているかについて、より多くの証拠を収集する。(管理措置A.5.27に関連)
- E. 組織が事件後、それ以上の措置は不要と判断した理由を説明するため、さらなる証拠を収集する。(管理措置A.5.26に関連)
- F. インシデント復旧手順に関するさらなる証拠を収集する。(管理措置A.5.26に関連)

Answer: (解答を表示する)

*C. 人事部長が個人用モバイルデータのロック解除のために身代金をどのように、いつ支払ったか クレジットカード、銀行振込など)について、より多くの証拠を収集する。(管理策A.5.26に関連)これは、組織のインシデント管理プロセスの監査には関連しません。人事部長の個人用電話と、その電話に対するランサムウェア攻撃への対処方法は、ISMS監査の範囲外です。組織は個人用デバイスについて責任を負いません。

*B. 会社の携帯電話とデータのロックを解除するために、会社が身代金をどのように、いつ支払ったか クレジットカード、銀行振込など)について、より多くの証拠を収集する。(管理策A.5.26に関連) 一見関連性があるように見えるが、これは身代金の支払い方法に焦点を当てている。根本的な問題は、組織が身代金を支払ったこと自体であり、これは一般的にインシデント対応におけるベストプラクティスではない。監査では、なぜこのような決定がなされたのか、また代替ソリューション データのバックアップ、デバイスの消去と復元など)が検討されたかどうかに関心がある。監査では、なぜこのような決定がなされたのか、また代替ソリューション データのバックアップ、デバイスの消去と復元など)が検討されたかどうかに関心がある。

他の選択肢が重要な理由：

*A. 報告プロセスに関する理解度について、より多くの職員にインタビューを行い、証拠をさらに収集する。
(管理策A.6.8に関連)これは、「弱点、事象、およびインシデント」の理解における認識のずれに直接対処するものであり、適切なインシデント報告にとって極めて重要です。

- *D. 組織がインシデント復旧時間をどのように決定したかについて、より多くの証拠を収集する。（管理策A.5.27に関連）これは、恣意的で全てのインシデントに適切ではない可能性のある24時間復旧時間の根拠を調査するものです。
- *E. 組織が事件後、それ以上の措置は不要と判断した経緯について、より多くの証拠を収集する。（管理策A.5.26に関連）これは、事件対応の適切性、特に身代金支払い後の予防措置の欠如を検証するものである。
- *F. インシデント復旧手順に関する証拠をさらに収集する。（管理策A.5.26に関連）これは、実際の手順を検証し、その有効性とベストプラクティスとの整合性を評価するものです。

最新問題: 74

あなたは、ABCヘルスケアサービス（介護施設めISO 27001情報セキュリティマネジメントシステム ISMS）監視監査を実施しています。ABCは、入居者の健康状態を監視するために、ベンダーであるWeCareが設計・保守するヘルスケアモバイルアプリケーションを使用しています。監査中に、入居者の家族の90%が、WeCareから毎週、電子メールとSMSで医療機器の広告を受け取っていることが判明しました。ABCとWeCare間のサービス契約では、ベンダーが入居者の個人データを使用することを禁じています。ABCは、入居者とその家族から多数の苦情を受けています。

サービスマネージャーは、これらの苦情は情報セキュリティインシデントとして調査され、調査結果から苦情の内容が事実であることが判明したと述べた。

不適合および是正措置管理手順に従って、是正措置が策定され、実施されました。

貴社は、ABC社は、居住者およびその扶養家族の個人データに関する情報セキュリティ管理基準A.5.34 プライバシーおよび個人識別情報の保護）を遵守していません。当社のプロバイダーであるWeCare社は、居住者の個人情報を使用して、その扶養家族に広告を送信しています。」という内容の不遵守報告書を提出されました。この不遵守に対し、ABC社が取るべき是正措置および改善措置を、以下のリストから3つ選択してください。

ABCは、サイバー犯罪を防止するため、ISMSコンサルタントにABCヘルスケアのモバイルアプリのテストを依頼した。

A. ABCはWeCareとのサービス契約を解除します。

B. ABCは、情報セキュリティ管理策A.5.34が適用範囲宣言書 SoA)に含まれていることを確認します。

C. ABCはABCヘルスケアのモバイルアプリケーションの使用を中止しました。

D. ABCは、すべてのサプライヤーの情報セキュリティパフォーマンスに関する背景調査を導入します。

E. ABCは、第三者に関わるすべての適用法および契約上の要件の遵守状況を定期的に監視しています。

F. ABCはWeCareを契約違反で訴えた。

G. ABCは、情報セキュリティプロトコルを維持することの重要性を従業員全員に理解してもらうための研修を実施しています。

Answer: (解答を表示する)

ABC社が不適合に対して行うと予想される修正および是正措置の選択肢は以下の3つです。

- * B. ABCはWeCareとのサービス契約を解除する。
- * E. ABC社は、すべてのサプライヤーに対し、情報セキュリティのパフォーマンスに関する身元調査を導入する。
- * F. ABCは、第三者に関わるすべての適用法令および契約上の要件の遵守状況を定期的に監視します。
- * B. この選択肢は、ABCが不適合に対処するために講じることができる是正措置です。是正とは、検出された不適合を解消するために講じる措置であり、是正措置とは、不適合の原因を解消し、その再発を防止するために講じる措置です¹。WeCareとのサービス契約を解除することで、ABCは居住者の個人データの不正使用を阻止し、居住者のプライバシーと権利を保護することができます。これにより、居住者とその家族からのさらなる苦情や法的問題も防止できます。ただし、この選択肢には、サービス提供者の喪失、代替ソリューションを見つける必要性、居住者の幸福への潜在的な影響など、いくつかの欠点もあります。
- * E. このオプションは、ABCが不適合に対処するために講じることができる是正措置の一つです。すべてのサプライヤーの情報セキュリティパフォーマンスに関するバックグラウンドチェックを導入することで、ABCは、取り扱い情報の機密性、完全性、可用性を尊重する信頼できるパートナーを選定し、協力関係を築くことができます。これはまた、組織がサプライヤーによる組織資産へのアクセスに伴うリスクを軽減するための情報セキュリティ要件を合意し文書化することを要求する情報セキュリティ管理A.15.1.1 (サプライヤー関係の情報セキュリティポリシー)への準拠にも役立ちます。
- * F. このオプションは、ABC が不適合に対処するために講じることができる是正措置の 1 つです。ABC は、第三者が関与するすべての適用法令および契約上の要件への準拠を定期的に監視することにより、サプライヤーが情報セキュリティに関する義務と責任を果たしていることを確認できます。これはまた、組織が従うべき関連する法令、規制、契約、およびその他の要件を特定、文書化し、最新の状態に保つことを要求する情報セキュリティ管理 A.18.1.1 (適用法令および契約上の要件の特定) を ABC が遵守するのにも役立ちます 3。

参考文献：

- 1: ISO 27000:2018 - 情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステム - 概要と用語、3.9項および3.10項 2: ISO/IEC 27001:2022 - 情報技術 - セキュリティ技術 - 情報セキュリティ管理システム - 要求事項、附属書A、管理A。 15.1.1 3: ISO/IEC 27001:2022 - 情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステム - 要求事項、附属書A、管理策A.18.1.1

最新問題: 75

あなたは、地元の病院や官公庁などの大規模組織に輸送サービスを提供する国際物流組織の出荷部門でISMS監査を実施しています。荷物には通常、医薬品、生物学的サンプル、パスポートや運転免許証などの書類が含まれています。会社の記録を見ると、ラベルの住所が間違っていることや、15%のケースで1つの荷物に2つ以上の異なる住所のラベルが貼られていることなどが原因で、返品が大量に発生していることがわかります。あなたは輸送マネージャー \$M)の面接を行っています。

出荷前に商品の検査は行いましたか？

SM：明らかに破損している商品は、出荷前に担当スタッフが取り除きますが、利益率が非常に低いため、正式な検査プロセスを実施するのは経済的ではありません。

商品を返品した後、どのような措置を講じますか？

SM：これらの契約のほとんどは比較的少額なので、調査を行うよりも、ラベルを再印刷して個々の荷物を再送する方が簡単で便利だと考えています。

貴社が提起されたクレームは、ラベル表示プロセスに対する管理体制の不備により、ISO 27001:2022に準拠していません。

最終会議で、配送担当マネージャーは、自分の発言が誤解された可能性があるとして謝罪しました。彼は、正しいラベルが正しい荷物に貼られているかを自動的にチェックするバックエンドのITプロセスについて知らなかったため、ラベル貼付中に荷物が剥がれてしまうことを説明しました。そして、不適切な行為を撤回するようあなたに求めました。

監査チームリーダーとして、輸送マネージャーの依頼に対してあなたが取るべき正しい対応を表す3つの選択肢から選んでください。

- A. 輸送マネージャーに、彼の要望が監査報告書に含まれることを伝えてください。
- B. 監査人がより多くの時間を確保できるときに、経営陣が提供された新しい情報について話し合うことをお勧めします。
- C. 輸送管理者に、違反は軽微であり、直ちに是正する必要があることを通知してください。
- D. 審査チームのメンバーに、何が起こるべきだと考えているのか説明してもらってください。
- E. 彼にあなたの理解を伝え、不服従を撤回してください。
- F. 輸送マネージャーの正直なご意見に感謝しますが、不適合品を撤去するという提案は正しいアプローチではありません。
- G. 証拠の取得には非常に費用がかかるため、輸送管理者がこの違反を立証することを推奨します。
- H. 不適合項目が表示されるということは、修正が必要なより深刻なシステム障害の証拠です。

Answer: (解答を表示する)

- A. 出荷マネージャーに、彼の要求が監査報告書に含まれることを伝えてください。これは、監査報告書には、被監査者から提起された要求や異議を含め、監査に関連するすべての関連情報と証拠を文書化する必要があるためです。監査報告書には、監査の結論と勧告の根拠も記載する必要があります12。
- B. 経営陣に対し、提供された新しい情報は監査人がより多くの時間を確保できるようになった時点で議論されることを伝える。これは、監査人が不完全または未検証の情報に基づいて性急な決定を下すべきではないためである。監査人は新しい情報を体系的かつ客観的に検討および評価し、それが監査結果、不適合、または結論に影響を与えるかどうかを判断する必要がある12。
- F. 出荷マネージャーの誠実さに感謝しつつも、不適合の撤回は適切な対応ではないと助言する。これは、監査員は被監査者の協力と透明性を認め、感謝すべきであると同時に、専門家としての誠実さと独立性を維持すべきだからである。監査員は、不適合が誤って提起されたか、または効果的に修正され検証されたと確信しない限り、不適合を撤回すべきではない12。

参照：

ISO 19011:2022 マネジメントシステムの監査に関する指針

ISO/IEC 17021-1:2022 適合性評価－マネジメントシステムの監査及び認証を行う機関に対する要求事項－第1部：要求事項

最新問題: 76

在後續審核期間，您注意到在後續審核之前確定要完成的不合格項仍懸而未決。

您應該採取下列哪四項行動？

A. 向組織的最高管理階層

報告未能針對突出的不符合項採取糾正措施的情況

B. 由於已超過完成日期，因此立即提出不合格項

C. 如果延遲合理，請與受審核方審核客口同意清除不合格項的修改日期

D. 聯絡管理審核計畫的個人，尋求他們關於如何進行的建議

- E. 決定延遲解決不合格項是否合理
- F. 當收到不合格項已清除的保證時，取消後續審核並回傳
- G. 注意不合格項仍然突出，並遵循審核追蹤以確定原因
- H. 如果延遲不合理，請告知受審核方審核客口並同意採取補救措施

Answer: A,C,E,G (メッセージを残す)

According to the ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) course, the following actions should be taken when a nonconformity identified for completion before the follow-up audit is still outstanding:

A . Report the failure to address the corrective action for the outstanding nonconformity to the organisation's top management. This is part of the auditor's responsibility to communicate the audit results and ensure that the audit objectives are met12.

C . If the delay is justified agree on a revised date for clearing the nonconformity with the auditee/audit client. This is part of the auditor's responsibility to verify the effectiveness of the corrective actions taken by the auditee and to close the nonconformity when the evidence is satisfactory12.

不適合への対応の遅延が正当化されるかどうかを判断する。これは、被監査者から提示された証拠を評価し、専門的な判断と客観性を用いて遅延の理由の妥当性を判断するという監査人の責任の一部である12。

G. 不適合がまだ未解決であることに注意し、監査証拠をたどってその理由を特定します。これは、監査証拠を収集および検証し、不適合の根本原因を特定するという監査人の責任の一部です12。

参照：

1 :ISO/IEC 27001:2022 リードオーディター（情報セキュリティマネジメントシステム）コース、CQIおよびIRCA認定トレーニング、1

2 :ISO/IEC 27001主任審査員研修コース、PECB、2

有効な **ISO-IEC-27001-Lead-Auditor-CN** 問題集は GoShiken.com が提供された合格しやすい ISO-IEC-27001-Lead-Auditor-CN 試験問題集！ GoShiken.com が最新の **ISO-IEC-27001-Lead-Auditor-CN** 試験問題集を提供しています。GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 問題集をゲットする人はこちら：

<https://www.goshiken.com/PECB/ISO-IEC-27001-Lead-Auditor-CN-mondaishu.html> (418**30%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

- 最新問題: 77
- あなたは経験豊富なISMS監査チームリーダーで、研修中の監査員を指導しています。あなたのチームは、モバイル通信事業者に対する第三者監視監査を完了したばかりです。研修中、監査員は最終会議に向けてどのように準備する予定か尋ねます。次のうち、適切な回答はどれですか？ 4つ選択)
- A. 最終会議の目的は、監査チームが調査結果を伝えることであり、被監査者が調査結果に異議を申し立てる機会ではないことを、被監査者に伝えます。
 - B. 最終会議が終わったらすぐに退出できるよう、監査チームには被監査会社のオフィスの外で待機するよう指示します。そうすることで、私たちとクライアント双方の時間を節約できます。
 - C. 最終会議の準備は必要ありません。私と同じくらい検討を重ねれば、話し合うべき内容は既に分かっているはずです。
 - D. 我將安排與受審核方代表舉行閉幕會議，會中將提出審核結論
 - E. 我將聯繫總部以確保我們的發票已支付，如果沒有，我將取消末次會議並暫時扣留審計報告
 - F. 我將與我的審核團隊討論所需的任何後續行動
 - G. 我將審口並酌情批准我的團隊的審計結論
 - H. 我將與團隊其他成員一起檢視審核證據和審核結果

Answer: A,D,F,H (メッセージを残す)

According to ISO 19011:2018, which provides guidelines for auditing management systems, clause 6.6 requires the audit team leader to conduct a closing meeting with the auditee's representatives at the end of the audit to present the audit conclusions and any findings1. The closing meeting should also provide an opportunity for the auditee to ask questions, clarify issues, acknowledge the findings, and comment on the audit process1. Therefore, when preparing for the closing meeting, an ISMS auditor should consider the following actions:

I will advise the auditee that the purpose of the closing meeting is for the audit team to communicate our findings. It is not an opportunity for the auditee to challenge these: This action is appropriate because it reflects the fact that the auditor has followed a systematic and consistent approach to collecting and evaluating audit evidence and reaching audit conclusions. The auditor should advise the auditee that the purpose of the closing meeting is for

the audit team to communicate their findings, which are based on objective evidence and professional judgement. The auditor should also explain that it is not an opportunity for the auditee to challenge these findings, as they have already been discussed and confirmed during the audit. However, the auditor should also invite the auditee to ask questions, clarify issues, acknowledge the findings, and comment on the audit process1.

I will schedule a closing meeting with the auditee's representatives at which the audit conclusions will be presented: This action is appropriate because it reflects the fact that the auditor has followed a planned and agreed audit programme and schedule. The auditor should schedule a closing meeting with the auditee's representatives at which the audit conclusions will be presented, in accordance with clause 6.6 of ISO 19011:20181. The auditor should also ensure that the closing meeting is attended by those responsible for managing or implementing the ISMS, as well as any other relevant parties1.

I will discuss any follow-up required with my audit team: This action is appropriate because it reflects the fact that the auditor has followed a risk-based approach to determining and reporting any follow-up actions required by the auditee or the certification body. The auditor should discuss any follow-up required with their audit team, such as verifying corrective actions for nonconformities or conducting a subsequent audit1. The auditor should also document any follow-up actions in the audit report1.

I will review and, as appropriate, approve my teams audit conclusions: This action is appropriate because it reflects the fact that the auditor has followed a rigorous and professional process to reaching and reporting audit conclusions. The auditor should review and, as appropriate, approve their teams audit conclusions, which are based on objective evidence and professional judgement. The auditor should also ensure that their teams audit conclusions are consistent with the audit objectives and scope, and reflect the overall performance and conformity of the ISMS1.

最新問題: 78

當審計員使用基於機率的抽樣進行事件日誌審口時， 使用了哪種類型的抽樣？

- A. 統計抽樣
- B. 基於判斷的抽樣
- C. 多地點抽樣

Answer: (解答を表示する)

Comprehensive and Detailed In-Depth

A . Correct Answer:

Statistical sampling follows probability theory and ensures objective selection.

ISO 19011:2018 supports statistical sampling for unbiased audit conclusions.

B . Incorrect:

Judgment-based sampling is subjective, not probability-based.

C . Incorrect:

Multi-site sampling applies to organizations with multiple locations.

Relevant Standard Reference:

ISO 19011:2018 Clause 6.4.9 (Using Statistical Sampling for Audits)

最新問題: 79

EquiBankは、財務管理システムの外部監査を受けています。監査人は、EquiBankの財務ソフトウェアによって処理される取引ロジックを評価しています。正確性を確保するため、ソフトウェアアプリケーションに組み込まれた操作、計算、および制御を検証するためにシミュレーションを使用しています。使用されているコンピュータ支援監査 (CAAT)の手法はどのようなものですか？

- A. 製図 製図ソフトウェアアプリケーション
- B. ユーティリティソフトウェア
- C. データテスト

Answer: C (メッセージを残す)

包括的かつ詳細な徹底分析

C. 正解：

データテスト技術は、金融ソフトウェア内の取引をシミュレートすることで、ロジック、計算、およびプログラムされた制御を検証します。

ISO 19011:2018は、CAATをデータ処理の完全性を検証する監査ツールとして認識している。

A. 不正解：

作図・地図作成ソフトウェアは、地理空間分析に使用されるものであり、金融取引のテストに使用されるものではありません。

B. 不正解：

ユーティリティソフトウェアは一般的なIT機能をサポートするが、監査シミュレーションは実行しない。

関連規格参照：

ISO 19011:2018 条項 6.4.10（監査におけるCAATの使用）

最新問題: 80

シナリオ6 :Cyber ACryptは、マルウェア対策やデバイスセキュリティ、資産ライフサイクル管理、デバイス暗号化などのエンドポイント保護サービスを提供するサイバーセキュリティ企業です。同社は、情報セキュリティマネジメントシステム（ISMS）がISO/IEC 27001規格に準拠していることを検証し、優れたサイバーセキュリティへの取り組みを示すため、指定された監査チームリーダーであるジョンが主導する厳格な監査プロセスを受けました。監査業務を引き受けたジョンは、監査計画とチームの役割を概説するための会議をすぐに開催しました。この段階は、チームを監査の目的と範囲に合わせる上で非常に重要でした。しかし、Cyber ACryptのスタッフとの最初のブリーフィングでは、監査の範囲と目的についての理解に大きなギャップがあることが明らかになり、社内での準備上の潜在的な課題が示されました。監査の第1段階の開始に伴い、チームは現場活動の準備を行いました。彼らは、Cyber ACryptの情報セキュリティポリシーと運用手順を含む文書をレビューし、各文書が標準形式に準拠し、作成者識別情報、作成日、バージョン番号、承認日が含まれていることを確認しました。さらに、監査チームは、各文書に、関連する標準条項で要求される情報が含まれていることを確認しました。この段階で、タスクの実行を記述した文書の詳細な監査は不要であることが明らかになり、プロセスが合理化され、チームは重要な領域に集中することができました。現場活動の段階では、チームはCyber ACryptのポリシーの管理責任を評価しました。この徹底的なレビューは、継続的な改善と情報セキュリティマネジメントシステム（ISMS）要件への準拠を確保することを目的としていました。その後、監査成果の第1段階に関する文書において、監査チームは調査結果を詳細に記述し、第1段階の目標達成に関する結論を強調しました。この文書は、監査チームとCyberACryptが予備的な監査結果と注意が必要な領域を理解する上で非常に重要でした。

監査チームは、主要な関係者への聞き取り調査も実施することにしました。この措置は、経営システムがISO規格に準拠しているかどうかを検証するための信頼できる監査証拠を収集することを目的としていた。

IEC 27001 の要求事項。サイバー ACrypt のあらゆるレベルのステークホルダーとのコミュニケーションにより、監査チームは貴重な視点を得ることができ、情報セキュリティ マネジメント システム (ISMS) の実装と有効性についての理解を深めることができました。

第1段階の監査報告書では、いくつかの重要な問題点が明らかになりました。適用範囲宣言書（SoA）および情報セキュリティマネジメントシステム（ISMS）ポリシーには、リスク評価の不備、アクセス制御の不備、定期的なポリシー見直しの欠如など、複数の点で不備がありました。これを受け、CyberACryptはこれらの不備に対処するため、直ちに行動を起こしました。迅速な対応と戦略文書の改訂は、同社のコンプライアンスに対する強いコミットメントを示すものでした。

監査チームのネットワークセキュリティに関する知識不足を補うために招集された技術専門家は、リスク評価手法の欠陥を特定し、ネットワークアーキテクチャをレビューする上で重要な役割を果たしました。これには、ファイアウォール、侵入検知・防御システム、その他のネットワークセキュリティ対策の評価、およびCyber ACryptが外部および内部の脅威をどのように検知、対応、復旧しているかの評価が含まれていました。ジョンの指導の下、技術専門家は監査結果をCyber ACryptの担当者に伝えました。しかし、監査チームは、専門家が被監査企業からコンサルティング料を受け取っていたため、専門家の客観性が損なわれた可能性があるとして指摘しました。監査プロセス中の技術専門家の行動を考慮し、監査チームリーダーは認証機関とこの件について話し合うことにしました。

上記のシナリオに基づいて、以下の質問に答えてください。

質問：

シナリオ6によると、CyberACryptは第1段階の監査報告書を受けて、SoAおよびISMSポリシーを修正した。

この状況をどのように定義しますか？

A. 受け入れられません。外部監査が第一段階を通過した後は、セキュリティ契約（SoA）および情報セキュリティマネジメントシステム（ISMS）ポリシーを変更することはできません。

B. 許容される状況下では、第2段階監査中に重大な不適合につながる状況は是正されるべきである。

C. 最終監査報告書を提出する前に、セキュリティプロトコルおよび情報セキュリティ管理システムポリシーに対して、許容範囲内の軽微な修正を行うことができます。

Answer: B ([メッセージを残す](#))

包括的かつ詳細な解説：

* B. 正解:

* ステージ1監査では、ギャップを特定し、ステージ2認証の前に組織が主要な不適合を修正できるようにします。

* ISO/IEC 27006では、組織はステージ2に進む前に、重大な不適合に対処する必要があると規定されています。

- * A. 不正解:
 - * 組織は、ステージ1で特定された不適合を修正することが認められています。
 - * C. 不正解:
- 軽微な修正だけでなく、重大な変更にも対応する必要がある。
- 関連規格参照：
- * ISO/IEC 27006:2020 9.2.3項 8ステージ1およびステージ2監査プロセス）

最新問題: **81**

シナリオ9 :Techmanicは1995年に設立されたベルギーの企業で、現在はブリュッセルに拠点を置いています。ITコンサルティング、ソフトウェア設計、ハードウェア/ソフトウェアサービス（導入保守を含む）を提供しています。公共サービス、金融、通信、エネルギー、医療、教育などの業界にサービスを提供しています。顧客中心主義の企業として、顧客との強固な関係構築と最先端のセキュリティ対策を最優先事項としています。Techmanicは、ISO/IEC 27001認証を1年間保持していることを誇りに思っています。認証監査において、監査員はISMSの実装にいくつかの不整合を発見しました。しかし、発見された問題はISMSの意図された成果達成能力に影響を与えなかったため、監査員がリモートで根本原因分析と是正措置を実施した後、Techmanicは認証を取得しました。継続的な改善と過去の評価からの学習の価値を認識し、Techmanicは過去の監視監査レポートをレビューする慣行を導入しました。この積極的なアプローチは、潜在的な不適合を特定して対処するのに役立つだけでなく、ITコンサルティング分野における再認証プロセスを効率化することも目的としています。監視監査中に、複数の不適合が特定されました。内部監査員の報告書によると、ISMSは引き続きISO/IEC 27001*の要求事項を満たしていましたが、Techmanicはマネージドサービスに関連する不適合に対処していませんでした。さらに、内部監査報告書にはいくつかの矛盾があり、マネージドサービス監査における内部監査員の独立性について疑問が生じました。このため、認証の延長は承認されませんでした。そこで、Techmanicは別の認証機関への移管を申請しました。同時に、同社は顧客に対し、ISO/IEC 27001認証はITサービスとマネージドサービスの両方を対象としている旨の声明を発表しました。

上記のシナリオに基づいて、以下の質問に答えてください。

内部監査報告書に矛盾点が見られることを踏まえると、内部監査人の独立性を問うことは重要だろうか？

- A. いいえ、内部監査人は、自分たちの調査結果に依拠する監査を監督する場合に限り、独立性を維持すべきです。
- B. いいえ、内部監査人はコンサルタントとしての役割を担っているため、独立性を保つことはできません。
- C. はい、内部監査人は監査対象となる活動から独立していなければなりません。

Answer: [\(解答を表示する\)](#)

包括的かつ詳細な徹底分析

- C. 正解：
- ISO/IEC 27001:2022の9.2.2項では、内部監査員は監査対象となる活動から独立していなければならないと規定している。
- 内部監査報告書における矛盾点は、独立性に関して正当な懸念を引き起こす。
- A. 不正解：
- 内部監査人は、監視監査に限らず、常に独立していなければならない。
- B. 不正解：
- 内部監査員は、単なる助言者ではなく、コンプライアンス遵守を担う役割も担っている。
- 関連規格参照：

最新問題: **82**

シナリオ6 :Sinvestmentは、住宅保険、商業保険、生命保険を提供する保険会社です。同社はノースカロライナ州で設立されましたが、近年、ヨーロッパやアフリカを含む他の地域にも事業を拡大しています。Sinvestmentは、業界における適用法令を遵守し、情報セキュリティインシデントの発生を防止することに尽力しています。同社はISO/IEC 27001に基づく情報セキュリティマネジメントシステム (ISMS)を導入し、ISO/IEC 27001認証の申請を行っています。

認証機関は、監査を実施するために2名の監査員を任命した。監査員はSinvestment社と機密保持契約を締結した後、監査を開始した。まず、ISMS適用範囲記述書、情報セキュリティポリシー、内部監査報告書など、必要な標準文書を精査した。Sinvestment社は文書作成手順を確立していると述べていたものの、すべての文書が同じ形式ではなかったため、精査は容易ではなかった。

その後、監査チームはSinvestmentの経営幹部に対し、ISMS導入におけるそれぞれの役割を理解するため、複数回のインタビューを実施した。監査の第1段階におけるすべての活動は、Sinvestmentからの要請による現地での文書および情報レビューを除き、リモートで実施された。

この段階で、監査担当者は情報セキュリティ研修および啓発プログラムに関する文書を一切発見できなかった。質問に対し、Sinvestmentの担当者は、全従業員に情報セキュリティ研修コースを提供していると述べた。監査の第1段階により、監査チームはSinvestmentの業務内容とISMS（情報セキュリティマネジメントシステム）について包括的な理解を得ることができた。

第2段階監査は、第1段階監査の3週間後に実施されました。監査チームは、マーケティング部門（監査範囲外において、従業員のアクセス権限を管理するための適切な手順が欠如していることを確認しました。従業員のアクセス権限の管理はISO/IEC 27001の要件であり、既に会社の情報セキュリティポリシーにも含まれているため、この問題は監査報告書に記載されました。さらに、第2段階監査において、監査チームはSinvestmentがユーザーアクティビティをログに記録していないことを確認しました。

同社の手順書には「ユーザー活動を記録したログは保存し、定期的に確認する必要がある」と記載されているが、同社はそのような手順を実施している証拠を一切提示していない。

監査活動全体を通して、監査員は観察、インタビュー、文書化された情報のレビュー、分析、および技術的検証を通じて情報と証拠を収集しました。監査チームはフェーズ1とフェーズ2の両方から得られたすべての監査結果を分析し、肯定的な認証勧告を発行することを決定しました。

シナリオ6によると、マーケティング部門の従業員はアクセス制御ポリシーを遵守していなかった。

この状況では、どの選択肢が正しいですか？

A. マーケティング部門は監査の対象外であるため、この問題は投資担当者にのみ伝えるべきです。

B. 従業員のアクセス制御はSinvestmentの情報セキュリティポリシーに含まれているため、この問題はSinvestmentの担当者に伝え、監査レポートに含める必要があります。

C. Sinvestment が従業員のアクセス権限を管理していないことは、潜在的な情報セキュリティリスクをもたらすため、重大な不適合として報告されるべきです。

Answer: B ([メッセージを残す](#))

マーケティング部門は監査対象に含まれていませんでしたが、従業員のアクセス権限管理の問題は、Sinvestmentの情報セキュリティポリシーの一部であるため、Sinvestmentの担当者に伝え、監査報告書に含める必要があります。これは、ISMS要件への全体的な遵守状況を反映するものです。

最新問題: 83
シナリオ2 :ナイト社は、米国カリフォルニア州北部を拠点とする電子機器メーカーで、ビデオゲーム機を開発しています。ナイト社は世界中に300人以上の従業員を抱えています。創業5周年を機に、同社は次世代ビデオゲーム機「G-Console」をグローバル市場向けに発売することを決定しました。G-Consoleは2021年の究極のメディアコンソールと位置づけられ、プレイヤーに最高のゲーム体験を約束します。

メインユニットパッケージには、VRヘッドセット、2つの

ゲームやその他のギフト。

長年にわたり、同社は誠実さ、正直さ、そして顧客への敬意を通して確固たる評判を築いてきました。この評判こそが、多くの熱心なゲーマーがKnightのGコンソールを発売と同時に手に入れたいと願った理由の一つです。

ナイト社は顧客志向の企業であることに加えて、

彼らの開発品質はゲーム業界で広く認められている。しかし、価格は妥当な範囲を超えて高額である。

しかし、ナイト社の製品の品質は最高レベルであるため、ほとんどの忠実な顧客にとってこれは問題ではない。

世界有数のビデオゲーム機開発企業であるナイト社は、悪意のある攻撃の標的となることも少なくありません。同社の情報管理システム（ISMS）は1年以上前から運用されており、財務部門と人事部門を除くナイト社の全部門を網羅しています。

最近、ナイト社の機密情報を含むファイルの一部がハッカーによって流出しました。ナイト社のインシデント対応チーム（IRT）は、直ちにシステム全体と事件の詳細の分析を開始しました。

IRTは当初、ナイト社の従業員が脆弱なパスワードを使用していたため、不正なハッカーがアカウントに容易にアクセスできたのではないかと疑っていた。しかし、徹底的な調査の結果、ハッカーはファイル転送プロトコル（FTP）の通信を傍受することでアカウントにアクセスしていたことが判明した。

FTPIは、アカウント間でファイルを転送するために使用されるネットワークプロトコルです。認証には平文のパスワードを使用します。

この情報セキュリティインシデントの結果、ナイト社はIRTの助言に基づき、FTPをセキュアシェル（SSH）に置き換えることを決定した。これにより、通信を傍受した者は暗号化されたデータしか見ることはできないようになる。

これらの変更を受けて、ナイト社はリスク評価を実施し、管理策の導入によって同様の事象のリスクが最小限に抑えられたかどうかを検証した。この評価結果はISMSプロジェクトマネージャーによって承認され、新しい管理策の導入後のリスクレベルは同社のリスク許容度と一致していると判断された。

このシナリオに基づいて、以下の質問に答えてください。

シナリオ2に基づき、ISMSプロジェクトマネージャーはリスク評価の結果を承認しました。これは許容範囲内でしょうか？

- A. いいえ、リスク軽減後に残るリスクは、どの段階においても経営陣の承認を得る必要があります。
- B. いいえ、新しいISMS管理策を実施した後に残るリスクは、ISMSチームによって承認される必要があります。
- C. はい、リスク軽減後に残るリスクはすべてISMSプロジェクトマネージャーの承認を得る必要があります。

Answer: A (メッセージを残す)

ISO/IEC 27001の文脈では、リスクアセスメントの承認と、処理後の残存リスクレベルの受容は、通常、最高経営陣の責任となります。これは、最高経営陣が情報セキュリティマネジメントシステムとその結果に対して責任を負い、組織を代表してリスクを受け入れる権限を持っているためです12。参考文献：＝提供された情報は、ISO/IEC 27001のリスクアセスメントおよび処理プロセスの標準的な実践に基づいています。このプロセスでは、リスクの承認と受容における最高経営陣の役割が強調されています。

最新問題: 84

あなたは経験豊富なISMS監査チームリーダーであり、現在、ISO/IEC 27001:2022を規格として、新規顧客向けに最初の第三者認証監査を実施しています。

2日間の監査の2日目の午後、あなたは監査報告書の作成に取りかかろうとしています。

これまでのところ、法令違反は発見されておらず、あなたとあなたのチームはウェブサイトと組織のISMS（情報セキュリティマネジメントシステム）に大変感銘を受けています。

この時点で、チームのメンバーの一人があなたに近づき、変更計画の検討に時間をかけすぎたため、リーダーシップとコミットメントの評価を完了できないと告げます。

このメッセージに対して、あなたは次のうちのどの行動をとりますか？

- A. 顧客に謝罪し、後日改めてリーダーシップとコミットメントについてレビューするために訪問することを伝えてください。
- B. お客様に、復路のフライトをファーストクラスにアップグレードする予定がある場合は、明日の空き時間にリーダーシップとコミットメントについてレビューすることを伝えてください。
- C. 被監査者と監査クライアントに対し、現時点では肯定的な提案はできないことを通知する。
- D. 被監査者に対し、認証監査を中止し、日程を変更する必要があることを通知する。
- E. 監査プログラムを管理している担当者に連絡を取り、監査報告書に肯定的な推奨事項を記載する許可を得てください。
- F. 本部へ連絡し、今後の対応に関する指示をお待ちください。
- G. 不適合事項は発見されず、組織の全体的な印象は良好であるため、監査報告書に肯定的な認証勧告を記録してください。
- H. 監査計画とクライアントの都合を確認し、最終会議の前に他のチームメンバーがこのタスクを引き継ぐ機会があるかどうかを判断します。

Answer: C (メッセージを残す)

ISO/IEC 27001:2022では、リーダーシップとコミットメントが重要な要件となっています。これは、ISMSの確立、実施、維持、継続的改善におけるトップマネジメントの役割と責任を明確にするためです。この側面を評価しなければ、監査チームはISMSが効果的であり、規格に適合していると結論付けることはできません。したがって、監査チームリーダーは、被監査者と監査クライアントに対し、現時点では肯定的な勧告を行うことができない旨を伝え、その理由と影響を説明する必要があります。また、監査チームリーダーは、認証機関の方針と監査クライアントの合意に基づき、監査期間の延長、フォローアップ監査の実施、条件付き認証の発行など、次のステップについて認証機関および監査プログラムマネージャーと協議する必要があります。

* ISO/IEC 27001:2022、第5項、リーダーシップ

* PECB候補者ハンドブック ISO 27001主任審査員、19ページ、監査プロセス

* PECB候補者ハンドブック ISO 27001主任審査員、22ページ、監査報告書

* PECB候補者ハンドブック ISO 27001主任審査員、23ページ、監査結果と勧告

最新問題: 85

次のうち、人間の介入を伴わない監査方法の例を2つ挙げてください。

* リモート会議プラットフォームを使用してインタビューを実施する

- A. 監査の準備として、被監査者の手続きが見直されます。
- B. 監査結果に対する被監査者の対応をレビューする。
- C. 監査対象者のサーバーにリモートアクセスしてデータを分析する。

D. 遠隔監視によって実施された作業を観察する。

E. 監査の日時を確認してください

Answer: B,D (メッセージを残す)

監査手法とは、監査人が監査証拠を収集・評価するために用いる技術と手順のことである。

監査方法は、人的交流を伴うものと伴わないものの2つのカテゴリーに分類できます。人的交流を伴う方法は、インタビュー、アンケート、調査、観察、ウォークスルーなど、被監査者またはその他の関係者との直接的または間接的なコミュニケーションを必要とするものです。人的交流を伴わない方法は、文書レビュー、データ分析、遠隔監視など、被監査者またはその他の関係者とのコミュニケーションを一切必要としないものです。

人間とのやり取りを伴わない監査方法の例としては、以下のようなものがあります。

* 監査準備のための被監査組織の手順レビューの実施 :この方法は、被監査組織の方針、プロセス、記録、報告書などの文書化された情報を精査し、監査基準を満たす上での適切性と有効性を検証するものです。この方法を実施するにあたり、監査人は被監査組織やその他の関係者と直接やり取りする必要はありません。

* 被監査企業のサーバーにリモートアクセスしてデータを分析する :この方法では、被監査企業のパフォーマンス指標、ログ、メトリクス、統計などのデータにアクセスして処理し、監査基準を満たしているかどうかの正確性と信頼性を検証します。この方法を実行するにあたり、監査担当者は被監査企業やその他の関係者と直接やり取りする必要はありません。

参考文献：

ISO/IEC 27001:2022 主任審査員（情報セキュリティマネジメントシステム）の目的と内容は Quality.org および PECB から引用。ISO 19011:2018 マネジメントシステムの監査に関するガイドライン [セクション 6.2.2]

最新問題: 86

第三者認証監査の文脈において、監査および監査チームの管理における監査チームリーダーの責任を定義する2つの選択肢はどれですか？

A. ISMSマネージャーへのインタビュー

B. 計画と監査にリスクベースのアプローチを採用する。

C. 上級管理職の見直し

D. 被監査者と連絡を取る

E. マネジメントシステム認証書の発行

F. 不遵守に関する報告書を作成する。

Answer: B,D (メッセージを残す)

第三者認証監査の文脈において、監査および監査チームの管理における監査チームリーダーの管理責任には、監査計画にリスクベースのアプローチを採用し、被監査者と連絡を取ることが含まれます。監査計画にリスクベースのアプローチを採用するとは、チームリーダーが、監査目標、範囲と基準、監査方法と技術、リソースの配分、監査チームメンバーへのタスクの割り当ての達成に影響を与える可能性のあるリスクと機会を考慮する必要があることを意味します。被監査者と連絡を取るとは、チームリーダーが監査の手配を確認し、関連情報を入手し、問題や懸念事項に対処し、フィードバックを提供し、監査結果と結論を報告するために、監査の前、監査中、監査後に被監査者と連絡を取る必要があることを意味します。参照: = ISO 19011:2022、6.4.1 項および 6.4.2 項、PECB 候補者ハンドブック ISO 27001 主任監査員、24 ページおよび 25 ページ。

最新問題: 87

あなたは、医療サービスを提供する高齢者向け介護施設で、ISMS（情報セキュリティマネジメントシステム）の初回認証監査を実施しています。監査計画の次のステップは、最終会議を開催することです。最終監査チーム会議において、監査チームリーダーとして、あなたは以下のとおり、2件の軽微な不適合と1件の改善機会を報告することに同意しました。

Cosmic Certifications Limited				
Summary of audit findings:				
Opportunities for Improvement (OI)				
Item	Findings		Requirements	Follow-up
1.	The organisation should improve the overall awareness of information security incident management responsibility and process.		Clause 7.4 and Control A.5.24	N/A
Nonconformities (NCs)				
Item	Findings	Grade	Requirements	Follow-up
1.	During the audit on the outsourced process, sampling one of the outsourced service contracts with WeCare the medical device manufacturer found that ABC does not include personal data protection and legal compliance as part of the information security requirements in the contract.	Minor	Clause 4.2 and Control A.5.20	Corrective actions are required.
2.	During the audit on information security during the business continuity process, sampling one of the service continuity and recovery plans for the resident's healthy status monitoring service. The auditor found the recovery plan has not yet been tested.	Minor	Clause 8.1 and Control A.5.29	Corrective actions are required.
signed by Audit				
Team Leader				

最終会議において、マネジメントシステム担当者（MSR）は、ABC社が今後3ヶ月以内に医療機器メーカーのWeCare社と合併することをあなたに伝えました。合併後の組織名はABC社となります。担当者は、WeCare社の医療機器製造拠点を今後の認証監査に含めることができるかどうかを尋ねました。また、WeCare社は既にISO/IEC 27001:2022認証を取得していると述べました。

MSRからの要求に適切に対応するためのオプションを選択してください。

- A. WeCareは初回審査を受けることが推奨されますが、これはABCによるその後の審査と組み合わせることも可能です。
- B. 初回監査では、認証範囲に影響を与える変更については、事前に確認しておくことをお勧めします。組織は、WeCareとの合併に関する決定を円滑に進めるため、合意された期間内に認証機関に最新情報を提供する責任があります。
- C. その提案は正しいです。WeCareが認証機関から承認を得ることができれば、新規事業者もすぐに認証対象に含めることができます。
- D. 認証プロセスを延期し、事業買収者が完了するまで待つことをお勧めします。

Answer: B (メッセージを残す)

ISO/IEC 27001のガイドラインによれば、合併など、ISMSの適用範囲に重大な変更が生じた場合は、認証機関に通知する必要があります。これにより、認証の有効性が維持され、すべての拠点とプロセスが適用範囲に含まれることが保証されます。認証機関は、新しい組織を既存の認証に組み込むための適切な措置を決定します。

参考文献：

*ISO/IEC 27001主任審査員向け参考資料

*PECB ISO 27001主任審査員候補者ハンドブック

最新問題: 88

シナリオ 1: Fintive は、オンライン決済およびセキュリティ保護ソリューションの大手プロバイダーです。1999 年にカリフォルニア州サンノゼでトーマス・フィンによって設立された Fintive は、情報セキュリティの向上、不正行為の防止、および PII (個人情報注入) などのユーザー情報の保護を希望するオンライン企業にサービスを提供しています。Fintive の意思決定および運用プロセスは、過去の事例に基づいています。顧客データを収集し、分類し、分析します。このような複雑な分析を実行するには、大規模な人員が必要でした。しかし、長年にわたり、このような分析を容易にする技術も進歩してきました。現在、Fintive はチャットボットなどの最新ツールを使用してパターン分析を実行し、不正行為を即座に防止することを計画しています。このツールは、顧客サービスの向上にも役立ちます。

この最初のアイデアはソフトウェア開発チームに伝えられ、彼らはそれを支持してプロジェクトを担当することになった。彼らはチャットボットを既存のシステムに統合する作業を開始した。さらに、チームはチャットボットがチャットの問い合わせの85%に回答するという目標を設定した。

チャットボットの統合が成功すると、同社は直ちに顧客向けにリリースした。

しかし、チャットボットにはいくつか問題があるようだ。

トレーニング段階 チャットボットがクエリパターンを 学習」する段階)において、テストが不十分であったり、サンプルデータが不足していたりするため、チャットボットはユーザーのクエリを解決して正しい回答を提供することができません。さらに、チャットボットが無効な入力（奇妙なドットパターンや通常とは異なる文字など）を受け取ると、ランダムなファイルをユーザーに送信してしまいます。そのため、チャットボットは顧客のクエリに適切に対応できず、従来のカスタマーサポートはチャットによる問い合わせで手一杯になり、顧客の要望を解決することができなくなっています。

そのため、Fintiveはソフトウェア開発ポリシーを策定しました。このポリシーでは、ソフトウェアが社内で開発されたか外部委託されたかにかかわらず、オペレーティングシステムに実装する前にブラックボックステストを実施することを規定しています。

このシナリオに基づいて、以下の質問に答えてください。

シナリオ1に基づく、チャットボットは顧客からの問い合わせに正しく回答できませんでした。この事例は、情報セキュリティのどの原則に影響を与えたでしょうか？

- A. 入手可能性
- B. 誠実さ
- C. 機密保持

Answer: (解答を表示する)

この事例では、情報セキュリティの完全性原則が侵害されました。チャットボットが正確な回答を提供できなかったこと、およびテスト不足と適切なトレーニングサンプルの欠如により意図しない動作 ランダムなファイルの送信)が発生したことが、システムの完全性を損ないました。

最新問題: 89

場景 9 :Techmanic 是一家比利時公司，成立於1995 年，目前在布魯塞爾運作。該公司提供 IT 諮詢、軟體設計以及軟體硬體服務，包括部署和維護。其服務業涵蓋公共服務、金融、電信、能源、醫療保健和教育等領域。作為一家以客戶為中心的公司，Techmanic 重視與客戶建立牢固的關係，並致力於採用領先的安全實踐。

Techmanic 已獲得 ISO/IEC 27001 認證一年，並對此認證引以為傲。在認證審核期間，審核員發現其資訊安全管理系統(ISMS) 的實施存在一些不一致之處。由於發現的問題並未影響其 ISMS 實現預期結果的能力，因此在審核員遠端跟進根本原因分析和糾正措施後，Techmanic 獲得了認證。同年，該公司在其服務清單中新增了主機託管服務，並申請擴大認證範圍以涵蓋該領域負責審核的審核員批准了該申請，並通知Techmanic 將在監督審核期間進行擴展審核。Techmanic 接受了監督審核，以驗證其ISMS 的持續有效性以及是否符合 ISO/IEC 27001 標準。此次監督審核旨在確保 Techmanic 的安全實踐(包括最近新增的主機託管服務)與認證的嚴格要求無縫銜接。審核員在重新認證過程中巧妙地利用了先前監督審核報告中的發現，旨在避免進行額外的重新認證審核，尤其是在T 諮詢領域。認識到持續改進的價值，並從過去的評估中吸取經驗教訓。

Techmanic實施了一項審核以往監督審計報告的慣例。這種積極主動的做法不僅有助於識別和解決潛在的不符合項，而且旨在簡化T諮詢行業的重新認證流程。

在監督審核過程中，發現了一些不符合項。資訊安全管理系統(ISMS)持續符合ISO/IEC標準。

Techmanic公司雖然符合ISO/IEC 27001*標準的要求，但其內部稽核員報告稱，該公司未能解決與託管服務相關的不符合項此外，內部稽核報告存在多處不一致之處，令人質疑內部稽核員在託管服務稽核過程中的獨立性基於此，Techmanic公司未獲得擴展認證。因此，該公司申請轉至其他認證機構。同時，該公司向客戶發布聲明稱,ISO/IEC 27001認證涵蓋其IT服務以及託管服務。

根據以上情景，回答以下問題：

問題：

下列哪些選項是內部稽核程序不允許的？

- A. 驗證糾正措施的有效性
- B. 減少人工審計任務

C. 不合格品の預防

Answer: C ([メッセージを残す](#))

Comprehensive and Detailed In-Depth Explanation:

* C. Correct Answer:

* Internal audits detect nonconformities but do not actively prevent them.

* A. Incorrect:

* Internal audits verify corrective actions.

* B. Incorrect:

* Technology can reduce manual tasks in internal audits.

Relevant Standard Reference:

* ISO 19011:2018 Clause 6.4.7 (Audit Program Limitations)

最新問題: 90

シナリオ6 :Sinvestmentは、住宅保険、商業保険、生命保険を提供する保険会社です。同社はノースカロライナ州で設立されましたが、近年、ヨーロッパやアフリカを含む他の地域にも事業を拡大しています。

Sinvestmentは、業界における適用法令を遵守し、情報セキュリティインシデントの発生を防止することに尽力しています。同社はISO/IEC 27001に基づく情報セキュリティマネジメントシステム (ISMS)を導入し、ISO/IEC 27001認証の申請を行っています。

認証機関は、監査を実施するために2名の監査員を任命した。監査員はSinvestment社と機密保持契約を締結した後、監査を開始した。まず、ISMS適用範囲記述書、情報セキュリティポリシー、内部監査報告書など、必要な標準文書を精査した。Sinvestment社は文書作成手順を確立していると述べていたものの、すべての文書が同じ形式ではなかったため、精査は容易ではなかった。

その後、監査チームはSinvestmentの経営幹部に対し、ISMS導入におけるそれぞれの役割を理解するため、複数回のインタビューを実施した。監査の第1段階におけるすべての活動は、Sinvestmentからの要請による現地での文書および情報レビューを除き、リモートで実施された。

この段階で、監査担当者は情報セキュリティ研修および啓発プログラムに関する文書を一切発見できなかった。質問に対し、Sinvestmentの担当者は、全従業員に情報セキュリティ研修コースを提供していると述べた。監査の第1段階により、監査チームはSinvestmentの業務内容とISMS (情報セキュリティマネジメントシステム)について包括的な理解を得ることができた。

第2段階監査は、第1段階監査の3週間後に実施されました。監査チームは、マーケティング部門 (監査範囲外において、従業員のアクセス権限を管理するための適切な手順が欠如していることを確認しました。従業員のアクセス権限の管理はISO/IEC 27001の要件であり、既に会社の情報セキュリティポリシーにも含まれているため、この問題は監査報告書に記載されました。さらに、第2段階監査において、監査チームはSinvestmentがユーザーアクティビティをログに記録していないことを確認しました。

同社の手順書には「ユーザー活動を記録したログは保存し、定期的に確認する必要がある」と記載されているが、同社はそのような手順を実施している証拠を一切提示していない。

監査活動全体を通して、監査員は観察、インタビュー、文書化された情報のレビュー、分析、および技術的検証を通じて情報と証拠を収集しました。監査チームはフェーズ1とフェーズ2の両方から得られたすべての監査結果を分析し、肯定的な認証勧告を発行することを決定しました。

上記のシナリオに基づいて、以下の質問に教えてください。

監査チームは、Sinvestment社の要請に基づき、Sinvestment社の現地で文書を精査しました。これは許容範囲内でしょうか？

A. はい、Sinvestmentは、文書審査プロセス中にサイトから文書が削除されないよう要求する権利を有します。

B. いいえ、Sinvestmentは文書レビューをどこで実施するかを決定することはできません。なぜなら、最初のレビュー段階の前に機密保持契約が締結されているからです。

C. いいえ、オンサイトとオフサイトの活動を組み合わせると、審査プロセスに悪影響を与える可能性があります。

Answer: A ([メッセージを残す](#))

はい、Sinvestmentが文書情報のレビューをオンサイトで実施するよう要求することは許容されます。同社は、特に機密情報の管理を維持し、機密性を確保するために、文書を社外に持ち出さないことを規定する権利を有しており、これはISO/IECで求められるセキュリティ管理に合致しています。

27001。

参照規格 :ISO/IEC 27001:2013、7.5項 (文書化された情報)

最新問題: 91

あなたは経験豊富なISMS監査チームリーダーで、監査員の研修を指導しています。あなたは彼女に一連の質問をすることで、今後の監査に関する彼女の理解度をテストします。質問の答えは「正解」か「不正解」です。

不正解」。以下の質問のうち、正解となるべき4つの質問はどれですか？

- A. 違反が重大な場合は、追加の監査が必要になる場合があります。
- B. 違反が軽微な場合は、フォローアップレビューが実施されることがあります。
- C. その後の監査の結果は、経営陣と、最初に不適合をレビューした監査チームリーダーに報告する必要があります。
- D. その後の監査により、重大な不遵守が軽微な不遵守に軽減される可能性があります。
- E. その後の審査の結果、顧客認証の一時停止が勧告される可能性があります。
- F. フォローアップ監査の結果は、監査プログラムを管理する担当者と監査依頼者に報告する必要があります。
- G. 法令違反が確認されたすべてのケースにおいて、フォローアップ監査が必要です。
- H. 重大な不適合が発見された場合にのみ、フォローアップ監査が必要です。

Answer: A,B,C,F (メッセージを残す)

重大な不適合が発見された場合、フォローアップ監査が実施されることがあります。これは、重大な不適合とは、組織のマネジメントシステムが意図した結果を達成できるかどうかについて重大な疑義を生じさせる状況であり、したがって即時の是正措置が必要となるためです。フォローアップ監査は、是正措置の有効性とマネジメントシステムの適合性を検証するために必要です12。

軽微な不適合の場合、フォローアップ監査を実施することがあります。これは、軽微な不適合とは、マネジメントシステムが意図した結果を達成する能力に影響を与えないものの、規定された要求事項からの逸脱を示す状況であるためです。フォローアップ監査は、是正措置の実施状況とマネジメントシステムの改善状況を確認するために実施されます12。

フォローアップ監査の結果は、経営陣および最初に不適合が特定された監査を実施した監査チームリーダーに報告されるべきである。これは、経営陣がマネジメントシステムの有効性と継続的な改善を確保する責任を負い、監査チームリーダーが監査プロセスと監査結果に責任を負うためである。フォローアップ監査報告書は、被監査企業が講じた不適合の状況と是正措置に関する客観的な証拠を彼らに提供する必要がある¹³。

フォローアップ監査の結果は、監査プログラムを管理する担当者と監査依頼者に報告する必要があります。これは、監査プログラムを管理する担当者が監査活動の計画、実施、監視、およびレビューに責任を負い、監査依頼者が監査を依頼する組織または個人であるためです。フォローアップ監査報告書には、フォローアップ監査の結果と被監査者の認証ステータスの変更点を通知する必要があります13。

参照：

ISO 19011:2022 マネジメントシステムの監査に関する指針

ISO/IEC 27001:2022 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項 ISO/IEC 17021-1:2022 適合性評価－マネジメントシステムの監査及び認証を行う機関に対する要求事項－第1部：要求事項

有効な **ISO-IEC-27001-Lead-Auditor-CN** 問題集は GoShiken.com が提供された合格しやすい ISO-IEC-27001-Lead-Auditor-CN 試験問題集！ GoShiken.com が最新の **ISO-IEC-27001-Lead-Auditor-CN** 試験問題集を提供しています。GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 問題集をゲットする人はこちら：

<https://www.goshiken.com/PECB/ISO-IEC-27001-Lead-Auditor-CN-mondaishu.html> (418**30%OFF**問題集溶と正解付きで 30%w 特別割引コード: **Freepdfdumps**)

最新問題: 92

大數據等新科技的使用對審計有何影響？

- A. 它提出了新的挑戰，例如，結合結構化和非結構化數據
- B. 透過使審核員能收集更高品質的審核證據來提高審核質量
- C. 它會造成嚴重中斷，例如，引入對於傳統資料庫管理工具處理來口太大或太複雜的數據

Answer: A (メッセージを残す)

The use of new technologies such as big data presents new challenges in auditing, particularly the issue of combining structured and unstructured data. Big data environments often include diverse data sets that auditors need to understand and interpret, which requires new skills and approaches to ensure effective and comprehensive audit coverage.

References: ISO/IEC 27001:2013 Standards and supplementary literature on the impact of technology on auditing practices

最新問題: 93

次の記述のうち、正しいものはどれですか？（2選択可）

- A. ISMS認証の利点は、認定証がウェブサイトに表示されることです。
- B. ISMSの目的は、経営陣が情報セキュリティ問題を理解していることを示すことです。
- C. ISMS認証を取得するメリットは、顧客数の増加です。
- D. ISMSを導入する主なメリットは、情報セキュリティリスクの低減にあります。
- E. ISMSの目的は、リスク管理プロセスを使用して情報セキュリティを保護することです。
- F. ISMSの目的は、規制要件への準拠を証明することです。

Answer: D,E (メッセージを残す)

ISMS（情報セキュリティマネジメントシステム）を導入することによるメリットは、主に情報セキュリティリスクの低減からもたらされる。

E) ISMSの目的は、情報セキュリティを維持するためのリスク管理プロセスを適用することです。包括的かつ詳細な説明 :ISO 27001規格によると、ISMSを導入するメリットには次のものがあります1：

顧客やその他の利害関係者に対し、情報の機密性、完全性、可用性を保証する。情報セキュリティインシデントへの対応能力を強化し、その影響を最小限に抑える。情報セキュリティのガバナンスと管理を改善する。情報セキュリティ侵害に関連するコストと損失を削減する。組織の競争力と評判を高める。法的、規制的、契約上の義務を遵守する。

ISMSの目的は、PDCAサイクル1に基づき、情報セキュリティリスクを管理するための体系的なアプローチを提供することです。

ISMSは、組織が事業目標および利害関係者のニーズと期待に沿って、情報セキュリティのパフォーマンスを確立、実装、維持、継続的に改善することを可能にします1。

ISMSは以下の要素で構成されています1：

情報セキュリティポリシーと目的

ISMSの範囲と境界

情報セキュリティリスク評価および対策のためのプロセスと手順

情報セキュリティのためのリソースと能力

情報セキュリティにおける役割と責任

ISMSのパフォーマンス評価と改善

ISMSの内部および外部コミュニケーションと認識

参照：

ISO/IEC 27001:2013、情報技術ーセキュリティ技術ー情報セキュリティマネジメントシステムー要求事項、条項1、4、5、6、7、8、9、10 PECB候補者ハンドブック ISO 27001主任審査員、9～11ページ ISO/IEC 27001:2013 情報セキュリティマネジメント規格 ISO 27001導入の4つの主なメリット | ISMS.online

ISO/IEC 27001:2022

An Introduction to the ISO 27001 ISMS | Secureframe

最新問題: 94

下列哪一個選項存在輕微不符合項？

- A. 風險評估方法阻礙了資訊安全風險的評估
- B. 公司與其供應商的合約沒有適當的文件版本控制
- C. 資料的備份每月進行一次，而公司的流程則要求每天備份一次

Answer: C (メッセージを残す)

This is a minor nonconformity. The backup frequency not adhering to the company's procedure of daily backups but occurring once a month represents a deviation from established processes, yet it might not immediately impact the effectiveness of the information security management system.

References: ISO/IEC 27001:2013, Clause A.12.3 (Backup)

最新問題: 95

情報セキュリティとは、_____を確立し維持することである。

- A. 機密保持
- B. 信頼
- C. 保護
- D. ファイアウォール

Answer: B (メッセージを残す)

Information security is a matter of building and maintaining trust. Trust is the confidence that information and information processing facilities are protected from unauthorized or malicious actions that could compromise their confidentiality, integrity or availability. Trust is essential for establishing and maintaining relationships with customers, partners, suppliers, employees and other stakeholders who rely on the organization's information and services. Trust is also a key factor for achieving compliance with legal, regulatory and contractual obligations, as well as meeting the organization's own information security objectives and policies. ISO/IEC 27001:2022 defines information security as "preservation of confidentiality, integrity and availability of information" (see clause 3.28) and states that "the purpose of an information security management system is to provide a framework for managing activities that influence the trustworthiness of information" (see Introduction). Reference: CQI & IRCA Certified ISO/IEC 27001:2022 Lead Auditor Training Course, ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements, What is Trust?

最新問題: 96

レビュープロセスにおいて、レビューチームリーダーは論理的な推論と分析を通して、タイムリーに結論に達した。監査チームリーダーはどのような職業倫理に基づいた行動を示したか？

- A. 決定的
- B. オープンマインド
- C. 道徳
- D. 洞察力に富む

Answer: A (メッセージを残す)

ISO/IEC 27001主任監査員のためのPECB候補者ハンドブックによると、監査チームリーダーに求められる専門的な行動の一つは決断力を持つことであり、これは 論理的な推論と分析に基づいてタイムリーな結論に達すること」を意味します 8ページ)。偏見がなく、倫理的で、洞察力があることも監査チームリーダーにとって望ましい資質ですが、質問で示された記述とは一致しません。

参考文献 :ISO/IEC 27001主任審査員向けPECB候補者ハンドブック、8ページ。

最新問題: 97

シナリオ3 :Rebuildyはバンコクを拠点とする建設会社で、住宅の設計、建設、保守を専門としています。機密性の高いプロジェクトデータと顧客情報のセキュリティを確保するため、RebuildyはISO/IEC 27001に基づいた情報セキュリティマネジメントシステム (SMS)を導入することにしました。

ISMS導入の結果は以下のとおりです。

情報セキュリティは、一連のセキュリティ対策の適用と、ポリシー、プロセス、手順の開発によって実現される。

安全対策はリスク評価に基づいて実施され、リスクを排除するか、許容できるレベルまで低減するように設計されています。

すべてのプロセスは、ISMSの継続的な改善を確実にするために、計画・実行・評価・改善 (PDCA)モデルに基づいています。

情報セキュリティポリシーは、最良のセキュリティ慣行に基づいて作成されたセキュリティマニュアルの一部であるため、独立した文書ではありません。

* 情報セキュリティに関する役割と責任は、各従業員の職務記述書に明確に定義されています。

情報セキュリティ管理システムの経営陣によるレビューは、計画された間隔で実施されます。

Rebuildyは、2回の間経営レビューと年次内部監査を経て、認証を申請しました。元従業員は、監査チームの一員であるElectraに書面による証拠を提出しました。Rebuildyの主要顧客であるElectraも同じ問題について証拠を提出しており、監査担当者は元従業員の証拠ではなく、この証拠を採用することにしました。監査チームのメンバーは、監査が完了するまでElectraと連絡を取り続け、監査中に発見された不適合事項について話し合いました。Electraは、これらの調査結果を裏付ける追加の証拠を提供しました。

監査開始時、監査チームは経営陣にインタビューを行い、ISMS導入への取り組みについて話し合いました。これらの話し合いから得られた証拠は、RebuildyがISO/IEC 27001のいくつかの条項に準拠しているかどうかを判断するための書面による確認書に記録されました。以下の不適合が発見されました。

同社の財務報告システムにおいて、不適切なユーザーアクセス制御設定が検出されました。

独立した情報セキュリティポリシーは策定されていません。代わりに、当社はセキュリティに関するベストプラクティスに基づいて作成されたセキュリティマニュアルを使用しています。

監査チームからこれらの文書を受け取った後、チームリーダーはRebuildyの経営陣と面談し、監査結果を報告した。監査チームは、財務報告システムと独立した情報セキュリティポリシーの欠如に関する調査結果を報告した。経営陣は調査結果に不満を表明し、監査チームリーダーの行動を非専門的だと考え、交代を要求する可能性を示唆した。プレッシャーを受けた監査チームリーダーは、経営陣に協力し、発見された不適合の重要性を軽視することにした。そのため、監査チームリーダーは報告書を改ざんしてより好ましい内容にし、Rebuildyのコンプライアンス問題の真の深刻さを歪曲した。

上記のシナリオに基づいて、以下の質問に教えてください。

シナリオ3に基づき、監査チームは上級幹部へのインタビューから得られた情報を用いて、RebuildyがISO/IEC 27001のいくつかの規定に準拠しているかどうかを判断しました。これは許容範囲内でしょうか？

A. いいえ、監査チームは、コンプライアンスが必要かどうかを判断するために、方針や手順などの書面による証拠のみを使用する必要があります。

B. はい、監査チームは経営陣からの書面による確認を通じて口頭証拠を入手しており、これは基準への準拠が達成されているかどうかを判断するために使用できます。

C. はい、上級幹部へのインタビューは最も信頼性の高い監査証拠であり、追加の検証なしに基準が満たされているかどうかを判断するために使用できます。

Answer: B ([メッセージを残す](#))

包括的かつ詳細な徹底分析

B. 正解：

監査の証拠は、インタビュー、観察、および文書から得られる。

経営陣からの口頭による証言は、文書化され、書面で確認されている場合に限り、受け入れられる。

A. 不正解：

ISO 19011では、口頭による証拠は、それが立証されていれば認められる。

C. 不正解：

面接だけでは不十分であり、追加の確認が必要である。

関連規格参照：

最新問題: 98

情報資産の許容される使用はすべて禁止されていますが、以下の例外があります。

A. 電子チェーンメール

B. 重要度の低い読者にはメールでコピーを送付する

C. 上司/チームリーダーが承認した社内メール。

D. 非常に大きな添付ファイルが付いたメール、または多数の受信者に送信されるメール。

Answer: C ([メッセージを残す](#))

情報資産の許容使用において禁止されていない唯一のオプションは、C：上司/チームリーダーの許可を得た全社宛メールです。このオプションは、送信者が上司またはチームリーダーから組織内のすべての従業員にメールを送信するための必要な承認を得ていることを意味します。これは、全員に関連する重要なニュース、イベント、または更新の発表など、正当な業務目的で行うことができます。ただし、このオプションは、悪用または誤用された場合、受信者に不必要な混乱や迷惑を引き起こす可能性があるため、控えめに責任を持って使用する必要があります。その他のオプションは、組織の情報セキュリティポリシーおよび手順に違反する可能性があり、リソースと帯域幅を浪費する可能性があるため、情報資産の許容使用において禁止されています。電子チェーンメール A)は、多くの場合、虚偽または誤解を招く主張や約束を伴い、受信者に複数の他の人に転送するように促すメッセージです。これらはスパムとみなされ、情報セキュリティを危険にさらす可能性のある悪意のあるリンクや添付ファイルが含まれている可能性があります。重要でない受信者への電子メールコピー B)は、受信する必要のない、または関心のない受信者に送信されるメッセージです。これらは不要とみなされ、受信トレイを乱雑にし、受信者がより重要なメッセージから注意をそらす可能性があります。非常に大きな添付ファイルを持つメッセージ、または多数の受信者へのメッセージ D)は、多くのネットワークリソースを消費し、情報システムのパフォーマンスまたは可用性に影響を与える可能性があります。また、受信者のメールボックスのストレージ容量またはクォータ制限を超え、問題を引き起こす可能性もあります。ISO/IEC 27001:2022では、組織が資産の許容使用に関する規則を実装することを要求しています（条項8.1.3を参照）。参照：CQIおよびIRCA認定ISO/IEC 27001:2022主任監査員トレーニングコース、ISO/IEC 27001:2022情報技術 - セキュリティ技術 - 情報セキュリティ管理システム - 要件、許容される使用とは何か？

最新問題: 99

シーン8 :テスト

1. マリクとマイケルは、セキュリティ、コンプライアンス、事業計画および戦略の分野における独立した資格を有する専門家で構成された監査チームです。彼らは、大手ウェブデザイン会社であるクラスタス社に対し、認証監査を実施しました。監査中、彼らは公平性と客観性を含む卓越した職業倫理を示しました。今回、クラスタス社は、ISO/IEC 27001認証を取得できれば、一歩リードできると確信しています。監査チームリーダーのテッサは、監査に関する専門知識を有し、IT関連の問題、コンプライアンス、ガバナンスにおいて非常に優れた実績を持っています。マリクは、組織計画とリスク管理のバックグラウンドを持ち、組織のセキュリティ管理とリスク許容度に対する包括的かつ分析的なアプローチに基づき、組織内のリスクレベルを正確に把握することに長けています。一方、マイケルは、厳格な標準化された手順に従って実施される管理評価を通じて、実践的なセキュリティに関する専門知識を有しています。

必要な監査活動を実施した後、テッサは監査チーム会議を開始し、そこでマイケルの発見事項の1つを分析して、その問題について客観的かつ正確な決定を下しました。マイケルが遭遇した問題は、組織の日常業務における些細な問題であり、彼はそれがIT技術者によって引き起こされたと考えていました。そこで、テッサは上級管理職と面談し、責任者の名前を尋ねた後、誰が責任を負うべきかを伝えました。明確化と理解を促進するため、テッサは監査最終日に最終会議を招集しました。この会議で、彼女は発見された不適合をクラスタスの経営陣に報告しました。しかし、テッサはクラスタスの認証監査報告書に不必要な証拠を記載しないように助言され、報告書が簡潔で主要な発見事項に焦点を当てたものになるようにしました。

監査チームは、検討した証拠に基づき監査結論案を作成し、認定を与える前に組織の2つの分野を監査する必要があると判断した。これらの決定は後に被監査組織に提出されたが、被監査組織は調査結果を受け入れず、追加情報を要求した。被監査組織の意見にもかかわらず、監査人は既に認定勧告を受け入れることを決定していたため、追加情報は受け入れなかった。被監査組織の上級管理職は、監査結論は事実を反映していないと主張したが、監査チームは決定を維持した。

上記のシナリオに基づいて、以下の質問に答えてください。

監査報告書の作成および内容について、主に誰が責任を負うのか？

- A. 監査チームリーダー
- B. 監査チームメンバー
- C. 認証機関

Answer: A ([メッセージを残す](#))

包括的かつ詳細な徹底分析

A. 正解：

ISO 19011:2018では、監査チームリーダーは監査報告書の作成と最終化に責任を負うと規定されている。

B. 不正解：

チームメンバーは調査結果を提供するが、最終的な決定はリーダーが行う。

C. 不正解：

認証機関は報告書を審査するが、作成は行わない。

関連規格参照：

最新問題: 100

あなたは経験豊富な監査チームリーダーであり、監査員の研修を指導する立場にあります。

貴チームは現在、外部顧客のためにデータを保管する組織に対し、第三者監視監査を実施しています。訓練を受けた監査担当者は、適合性報告書 \$oA)に記載され、現場で実施されている技術的管理策を検証する任務を負っています。

研修を希望する監査担当者にレビューしてもらいたい管理項目を、以下のリストから4つ選択してください。

- A. 機密保持および機密保持契約
- B. ソースコードと開発ツールへのアクセスを管理する方法
- C. 電力ケーブルとデータケーブルはどのようにして建物内に引き込まれるのですか？
- D. マルウェア対策の実装方法
- E. 組織が自社の技術的な脆弱性がどの程度露呈しているかをどのように評価するか。
- F. 情報セキュリティ意識向上、教育、研修
- G. 組織の情報削除に関する取り決め

H. 組織の事業継続計画

Answer: B,D,E,G ([メッセージを残す](#))

研修中の監査員が確認すべき、リストにある4つの統制事項は以下のとおりです。

*B. ソースコードおよび開発ツールへのアクセス管理方法 :この管理では、外部クライアントのデータを処理または保存するソフトウェアアプリケーションおよびシステムの作成、変更、または保守に使用されるソースコードおよび開発ツールへのアクセスを組織が制限および監視することを要求します。これは、ソフトウェアおよびデータの完全性、機密性、可用性を確保するとともに、不正な変更、エラー、または悪意のあるコードの挿入を防止するために重要です。

*D. マルウェア対策の実施方法 :この管理策では、組織は外部クライアントのデータを処理または保存するITシステムおよびデバイスからマルウェアを検出、防止、削除するための適切な対策を実施する必要があります。これには、ウイルス対策ソフトウェア、ファイアウォール、メールフィルタリング、Webフィルタリング、その他のツールを使用して、ウイルス、ワーム、ランサムウェア、スパイウェア、その他の悪意のあるソフトウェアから保護することが含まれます。これは、マルウェアによるデータおよびシステムの破損、盗難、または損傷を防ぐために不可欠です。

*E. 組織が技術的脆弱性への露出をどのように評価するか :この管理策では、組織が外部顧客のデータを処理または保存するITシステムおよびデバイスに影響を与える可能性のある技術的脆弱性を特定し、評価することが求められます。これには、脆弱性スキャンツール、侵入テストツール、脅威インテリジェンスソース、およびその他の方法を使用して、システムおよびデバイスのセキュリティ上の弱点やギャップを発見および評価することが含まれます。これは、脆弱性によって生じるリスクを軽減するための適切な是正措置および管理策を優先順位付けして実施するために必要です。

*G. 組織の情報削除に関する取り決め :この管理策では、組織は、外部顧客のデータが不要になった場合、または必要なくなった場合に、ITシステムおよびデバイスからデータを削除するためのポリシーと手順を確立し、実施する必要があります。これには、安全な消去、暗号化、物理的破壊など、データ削除の基準と方法を定義することが含まれます。これは、データの保持と廃棄に関する契約上の義務、法的要件、規制要件を遵守するため、またデータの機密性と完全性を保護するために重要です。

参照文献 :ISO/IEC 27001:2022、附属書A、条項A.8.9、A.8.10、A.8.11、およびA.8.28 :Understanding ISO

ISO 27001:2022: 人、プロセス、テクノロジー、6〜7ページ :ISO 27001における11の新しいセキュリティ管理策とは何ですか？

2022年？ - Advisera。

最新問題: 101

シナリオ5

CyberShielding Systems Inc.は、情報技術インフラ全体を網羅するセキュリティサービスを提供しています。同社は、エンドポイントセキュリティ、ファイアウォール、ウイルス対策ソフトウェアなどのネットワークセキュリティソフトウェアを提供しています。CyberShielding Systems Inc.は20年以上にわたり、高度な製品とサービスを通じて数多くの企業のネットワークセキュリティ強化を支援してきました。情報およびネットワークセキュリティにおける卓越した実績を基盤に、CyberShielding Systems Inc.は、自社および顧客の資産をより効果的に保護し、競争優位性を獲得するために、ISO/IEC 27001規格に基づくセキュリティ情報マネジメントシステム (ISMS)を導入し、認証を取得することを決定しました。

認証機関は、まずサイバーシールドシステムズ社からISO監査チームを選定し、このプロセスを開始した。

IEC 27001認証に関して、認証機関は各監査員の氏名と経歴情報を同社に提供しました。しかし、CyberShielding Systems Inc.が調査したところ、監査員の1人が必要な安全資格を保有していないことが判明しました。そのため、同社はその監査員の任命に異議を申し立てました。調査の結果、認証機関はCyberShielding Systems Inc.の異議申し立てを受けて、その監査員を交代させました。

監査プロセスの一環として、CyberShielding Systems Inc.のリスクおよび機会特定アプローチが別途評価されました。これには、同社のリスクおよび機会の特定と管理方法のレビューが含まれます。監査チームの主要な目的は、CyberShielding Systems Inc.のリスクおよび機会特定メカニズムの有効性を確保し、特定されたリスクおよび機会に対処するための同社の戦略をレビューすることでした。その過程で、監査チームはファイアウォール構成レビュープロセスにおける監督不行き届きのリスク、具体的には適切な承認なしに行われた変更の実装によるセキュリティ脆弱性のリスクも特定しました。この発見は、このような問題の発生を防ぐために内部統制を強化する必要性を強調するものです。

監査チームは、主要な業務プロセスと統制を理解するために、プロセス記述書と組織図を精査しました。サードパーティのサービスプロバイダーの制約により、ITインフラストラクチャとアプリケーションへのアクセスが制限されたため、ITリスクと統制の分析が制限されました。しかし、監査チームは、CyberShieldingのプロセスのほとんどが自動化されているため、CyberShieldingの情報セキュリティ管理システム (ISMS)に重大な欠陥が生じるリスクは低いと判断しました。そこで、ITの責任、統制の有効性、マルウェア対策についてCyberShieldingの担当者に質問し、ISMSの標準への全体的な準拠状況を評価しました。CyberShieldingの担当者は、これらの質問すべてに十分かつ適切な証拠を提供しました。

監査に先立ち、監査の範囲、基準、目的を概説した合意書が締結されたものの、監査は主に、確立された基準への準拠を評価し、法的および規制上の要件を遵守していることを確認することに重点が置かれた。

質問

シナリオ5に基づく、CyberShielding Systems Inc.は監査目標を定義する際に、他にどのような要素を含めるべきでしょうか？

- A. 会社の安全対策における改善点を特定する。
- B. 監査範囲は、最近発生した事象や経営上の問題が存在する領域に主に焦点を当てるようにしてください。
- C. 効率性を維持するために、監査範囲を管理文書の検証に限定する。

Answer: A (メッセージを残す)

CyberShielding Systems Inc.は、監査目標を定義する際に改善すべき領域を特定することを含めるべきであったため、選択肢Aが正解となります。ISO/IEC 27001監査は、コンプライアンスの検証に限定されるものではなく、ISMSの継続的な改善も支援します。ISO 19011は、監査が弱点、改善の機会、および有効性を高めることができる領域を特定することで価値を提供することを推奨しています。このシナリオでは、監査の目的は主に基準への適合性および法令 規制要件への準拠に重点が置かれていました。これは不可欠ですが、明確に定義された監査目的には、セキュリティ対策、統制の有効性、リスク管理の成熟度を向上させる機会の評価も含まれるべきです。改善領域を特定することで、組織は基本的なコンプライアンスを超えてISMSを強化することができ、継続的改善に関するISO/IEC 27001の第10項にも合致することになります。選択肢Bは、監査の目的を最近の出来事や経営上の懸念事項のみに狭く限定すると、偏った、あるいは不完全な監査につながる可能性があるため、誤りです。選択肢Cは、監査を文書レビューのみに限定すると、監査の有効性が損なわれ、運用管理の証拠に基づく評価という要件に反するため、誤りです。したがって、監査目標に改善点の特定を含めることで、監査の価値が高まり、ISO/IEC 27001の原則との整合性も強化されたであろう。

最新問題: 102

あなたは認証機関によって任命されたISMS監査チームのリーダーであり、データセンターの顧客に対するフォローアップ監査を実施する責任を負っています。

ISO 19011:2018によると、フォローアップ監査の目的は次のうちどれを検証することでしょうか？

- A. 管理システムの有効性
- B. ISMS目標の実施
- C. リスク管理計画の実施
- D. 是正措置の完了と有効性

Answer: (解答を表示する)

フォローアップ監査の目的は、前回の監査で特定された不適合に対して被監査者が講じた是正措置の完了と有効性を検証することです1。フォローアップ監査は、初回監査の後に実施される監査の一種であり、不適合が発見され、是正措置が合意された特定の領域に焦点を当てます2。フォローアップ監査は、不適合の性質と深刻度、および監査プログラムの目的に応じて、独立した監査として、または定期監査の一部として実施できます3。

その他の選択肢は、フォローアップ監査の目的ではなく、他の種類の監査の目的です。例えば、

*オプションAはパフォーマンス監査の目的であり、これは経営システムが意図した結果を達成する上での有効性を評価する監査の一種です4。

*オプションBはコンプライアンス監査の目的であり、ISMS目標5などの指定された要求事項に対するマネジメントシステムの適合性を検証する監査の一種です。

*オプションCはプロセス監査の目的です。プロセス監査とは、リスク処理プロセスなど、マネジメントシステム内の特定のプロセスのインプット、アクティビティ、アウトプット、および相互作用を調査するタイプの監査です。

参照: 1: ISO 19011:2018、6.7; 2: ISO 19011:2018、3.7; 3: ISO 19011:2018、5.5.2; 4: ISO 19011:2018、3.6; 5: ISO 19011:2018、3.5; : ISO 19011:2018、3.4; : ISO 19011:2018; : ISO 19011:2018; : ISO 19011:2018; : ISO 19011:2018; : [ISO 19011:2018]

最新問題: 103

次の記述のうち、正しいものはどれですか？（2選択可）

情報セキュリティマネジメントシステム (ISMS)を導入する主なメリットは、情報セキュリティリスクの低減にある。

A. 情報セキュリティマネジメントシステムの認証を取得する利点の1つは、政府機関から契約を獲得できることです。

情報セキュリティマネジメントシステム (ISMS)の目的は、リスク管理プロセスを適用することによって情報セキュリティを保護することです。

B. 情報セキュリティマネジメントシステム (ISMS)の目的は、規制要件への準拠を証明することです。

Answer: A,B (メッセージを残す)

ISMS（情報セキュリティマネジメントシステム）を導入するメリットは、情報セキュリティリスクの低減にとどまらず、ビジネスパフォーマンスの向上、顧客満足度の向上、法令遵守の促進、ステークホルダーの信頼向上などにも及ぶ。

ISMS認証を取得するメリットは、政府機関からの契約獲得だけでなく、組織の情報セキュリティへの取り組みを他の潜在顧客、パートナー、規制当局に示すことにもあります。ISMSの目的は、情報セキュリティを維持するためのリスク管理プロセスを適用することであり、これは組織が直面する情報セキュリティリスクの特定、分析、評価、対処、監視、および見直しを意味します。ISMSの目的は、規制要件への準拠を示すことではなく、組織が自らの情報セキュリティ目標と義務を確実に達成することです。

参考文献：

ISO/IEC 27001:2022 主任審査員（情報セキュリティマネジメントシステム）の目的と内容 Quality.org および PECB より）ISO/IEC 27001:2013 情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステム - 要求事項 [セクション 0.1] および [セクション 1]

最新問題: 104

次のうち、情報セキュリティ攻撃の種類ではないものはどれですか？

- A. 法的イベント
- B. 交通事故
- C. 技術的な脆弱性
- D. プライバシー問題

Answer: (解答を表示する)

車両事故は情報セキュリティ攻撃の一種ではありません。車両事故とは、車両またはその運転者が人や財産に損害や傷害を与える事象を指します。車両事故は、車両によって輸送またはアクセスされる情報やシステムの可用性や完全性に影響を与える場合、情報セキュリティに影響を与える可能性があります、情報セキュリティに対する意図的または悪意のある攻撃ではありません。

法的インシデントは、情報またはシステムの機密性または完全性を損なう可能性のある法的措置または紛争を伴う情報セキュリティ攻撃の一種です。技術的脆弱性は、情報またはシステムの機密性、完全性、または可用性を損なう可能性のあるソフトウェアまたはハードウェアの弱点または欠陥を悪用する情報セキュリティ攻撃の一種です。プライバシーインシデントは、個人情報または機密情報への不正アクセスまたは開示を伴う情報セキュリティ攻撃の一種であり、情報またはシステムの機密性または完全性を損なう可能性があります。参照: : CQI & IRCA ISO 27001:

2022年主任審査員コースハンドブック、25ページ。[ISO/IEC 27001 主任審査員 - PECB]、13ページ。

最新問題: 105

質問

認証監査プロセスにおいて、被監査者は、リスク評価を実施し、情報セキュリティを確保するための複数の管理策を選択したことを示す文書を監査人に提出します。このような場合、監査人は何を検証すべきでしょうか？

- A. 監査対象企業は、リスク評価を実施するために外部コンサルタントを起用しました。
- B. 選択されたすべての制御項目は校正制御です。
- C. 被監査者は、選択された統制を適合性に関する声明に含めています。

Answer: C (メッセージを残す)

監査人は、選択された管理策が適用範囲宣言書 \$oA)に含まれていることを確認する必要があり、選択肢Cが正解となります。ISO/IEC 27001:2022では、組織はリスク評価およびリスク処理プロセスの結果に基づいて、附属書Aの管理策のうちどれが適用可能であるかを文書化することが求められています。SoAは、管理策の包含または除外の根拠を含め、これらの決定を記録する正式な文書です。

リスク評価が存在するだけでは十分ではありません。監査人は、特定されたリスク、選択された対策、およびSoA セキュリティ監査基準)におけるそれらの正式な文書との間のトレーサビリティを確認する必要があります。これにより、組織が情報セキュリティリスクをどのように管理しているかについて、透明性、一貫性、および説明責任が確保されます。

Option A is incorrect because ISO/IEC 27001 does not require organizations to use external consultants for risk assessments. Risk assessments may be conducted internally, provided they follow a defined and systematic methodology. Option B is incorrect because controls can be preventive, detective, or corrective; there is no requirement that selected controls be corrective only.

Therefore, verifying that selected controls are properly reflected in the Statement of Applicability is a mandatory audit activity and a core requirement of ISO/IEC 27001 compliance.

最新問題: 106

なぜ最初の接触時に重要性を考慮すべきなのでしょう？

- A. レビュー期間を決定する
- B. 監査チームの役割を定義する

C. 監査目標を設定する

Answer: C (メッセージを残す)

包括的かつ詳細な徹底分析

C. 正解：

重要性は、監査人が監査の重点分野を特定するのに役立ち、監査目標を適切に設定するために用いられる。

重要性とは、効果的なISMS導入を実現するために、どのプロセス、リスク、または統制が重要かを決定するものです。

A. 不正解：

重要性は監査範囲に影響を与えるが、監査期間を直接決定するものではない。

B. 不正解：

チームの役割は、重要性ではなく専門知識に基づいて割り当てられます。

関連規格参照：

ISO 19011:2018 6.2.3項（監査の実施可能性の判断）

有効な **ISO-IEC-27001-Lead-Auditor-CN** 問題集は GoShiken.com が提供された合格しやすい ISO-IEC-27001-Lead-Auditor-CN 試験問題集！ GoShiken.com が最新の **ISO-IEC-27001-Lead-Auditor-CN** 試験問題集を提供しています。GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 問題集をゲットする人はこちら：
<https://www.goshiken.com/PECB/ISO-IEC-27001-Lead-Auditor-CN-mondaishu.html> (418**30%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 107

あなたは、医療サービスを提供するヨーロッパの高齢者向け介護施設ABCでISMS監査を実施しています。監査計画の次のステップは、継続的改善プロセスの有効性を検証することです。

監査の結果、入居者の家族のほとんど（90%）が、中国農業銀行のヘルスケアモバイルアプリを通じて、WeCare医療機器の宣伝広告を週に1回、メールとSMSで受け取っていたことが明らかになった。彼らは全員、収集した個人データを、ABCとのサービス契約に明記されているケアや治療以外の目的でマーケティングやその他の目的で使用することに反対していた。彼らは、ABCが入居者とその家族の個人情報を無関係の第三者に開示していると強く疑う根拠があり、苦情を申し立てた。

サービスマネージャーは、調査の結果、これらの苦情はすべて法令違反に該当する問題であると判断されたと述べた。

不適合および是正管理手順（文書参照ID: ISMS_L2_10.1、バージョン1）に従って、是正措置が計画され、実施されました。

間違っている項目を書き留めてください。後ほどご連絡いたします。文を最も適切に完成させる単語を選択してください。

"When reviewing the _____ of action taken in response to a _____, an auditor seeks evidence of _____ that will _____ recurrence of the issue."

To complete the sentence with the best words, click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

repair

assurance

responsibility

effectiveness

nonconformity

prevent

change

problem

Answer:

"When reviewing the **effectiveness** of action taken in response to a **nonconformity**, an auditor seeks evidence of **change** that will **prevent** recurrence of the issue."

To complete the sentence with the best words, click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

repair

assurance

responsibility

effectiveness

nonconformity

prevent

change

problem

最新問題: 108

質問 :

なぜ最初の接触時に実質的な問題を検討する必要があるのでしょうか？

- A. 監査期間を決定する
- B. 監査チームの役割を定義する
- C. 監査目標の設定

Answer: C ([メッセージを残す](#))

包括的かつ詳細な解説 :

* C. 正解:

重要性は、監査人が監査の重点を置くべき重要な領域を特定するのに役立ち、監査目標を適切に設定するために使用されます。

* 重要性とは、効果的なISMS導入を実現するために、どのプロセス、リスク、または統制が重要かを決定するものです。

* A. 不正解:

重要性は監査範囲に影響を与えますが、監査期間を直接決定するものではありません。

* B. 不正解:

* チームの役割は、重要性の考慮ではなく、専門知識に基づいて割り当てられます。

関連規格参照：

* ISO 19011:2018 6.2.3項（監査の実施可能性の判断）

最新問題: 109

次のうち、有効な監査結論はどれですか？（2選択可）

A. ISMS入門研修では、マルウェア対策に関するガイダンスは提供されていません。

B. リスク登録簿は202X年6月以降更新されていません。

C. 2件の内部監査に基づく是正措置はまだ完了していません。

D. ISMSポリシーは組織全体に効果的に伝達されています。

E. 組織のISMS目標はISO/IEC 27001:2022の要求事項に準拠しています。

F. 適用範囲はISO/IEC 27001 2013バージョンに基づいており、2022バージョンではありません。

Answer: D,E (メッセージを残す)

有効な監査結論となる2つの記述は以下のとおりです。

ISMSポリシーは組織全体に効果的に伝達されている。

*組織のISMS目標はISO/IEC 27001:2022の要求事項を満たしています。ISO 19011:2018によると、監査結論は監査チームが監査目標とすべての監査結果1を考慮した後に提供する監査の結果です。監査結論は、監査基準が満たされているかどうかに応じて、肯定的または否定的になります。監査結論には、改善のための推奨事項や優れた実践の評価が含まれる場合もあります。

記述DとEは、監査基準と監査結果に基づいて監査結果を表現しているため、有効な監査結論です。例えば、次のようになります。

*ステートメントDは肯定的な監査結論です。これは、組織がISO/IEC 27001:2022の条項5.2.2の要求事項を満たしていることを示しているためです。条項5.2.2では、ISMSポリシーは組織内および関連する利害関係者に伝達されなければならないと規定されています2。監査チームは、この結論を裏付けるために、コミュニケーション記録、啓発活動、フィードバックなどの十分かつ適切な監査証拠を入手する必要があります。

*ステートメントEは肯定的な監査結論です。これは、組織がISO/IEC 27001:2022の6.2項の要求事項を満たしていることを示しているためです。6.2項では、組織はISMSポリシーと整合し、情報セキュリティリスク3に関連するISMS目標を設定しなければならないと規定されています。監査チームは、目標設定、リスク評価、ポリシーとの整合性などの記録など、この結論を裏付ける十分かつ適切な監査証拠を入手している必要があります。

その他の記述は、監査基準と監査結果に基づく監査結果を表していないため、有効な監査結論ではありません。これらはむしろ監査結果の例であり、監査基準4に照らして収集した監査証拠を評価した結果です。監査結果は、監査基準への適合または不適合、あるいは改善の機会を示すことができます。例えば、次のようになります。

*声明Aは、条項の要件への不適合を示しているため、否定的な監査結果です。

ISO/IEC 27001:2022の7.2.2項では、組織は管理下にある者に対して情報セキュリティ意識向上教育およびトレーニングを提供しなければならないと規定されています5。監査チームはこの不適合を特定して文書化し、被監査者に報告しなければなりません。

*声明Bは、条項の要件への不適合を示しているため、否定的な監査結果です。

ISO/IEC 27001:2022の6.1.2項では、組織は計画された間隔で、または重大な変更が発生した場合に、情報セキュリティリスク評価を維持および見直す必要があると規定されています。監査チームは、この不適合を特定して文書化し、被監査者に報告する必要があります。

*声明Cは、条項の要件への不適合を示しているため、否定的な監査結果です。

ISO/IEC 27001:2022の10.1項では、組織は不適合の原因を排除し、再発を防止するための措置を講じなければならないと規定されています7。監査チームは、この不適合を特定して文書化し、被監査者に報告しなければなりません。

*声明Fは、条項の要件への不適合を示しているため、否定的な監査結果です。

ISO/IEC 27001:2022の6.1.3項では、組織はリスク処理計画を実施するために必要な管理策を決定し、適用範囲の声明書に文書化しなければならないと規定されています8。監査チームはこの不適合を特定して文書化し、被監査者に報告しなければなりません。

参照: 1: ISO 19011:2018、3.15; 2: ISO/IEC 27001:2022、5.2.2; 3: ISO/IEC 27001:2022、6.2; 4: ISO 19011:2018、3.14; 5: ISO/IEC 27001:2022、7.2.2; 6: ISO/IEC 27001:2022、6.1.2; 7: ISO/IEC 27001:2022、10.1; 8: ISO/IEC 27001:2022、6.1.3; : ISO 19011:2018; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022; : ISO 19011:2018; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022; : ISO/IEC 27001:2022

最新問題: 110

情報フェーズ

- A. 創造、進化、維持、使用、廃棄
- B. 設立、使用、廃棄、維持、進化
- C. 設立、流通、使用、維持、廃棄
- D. 設立、配布、維持、処分、および使用

Answer: C ([メッセージを残す](#))

情報の段階は、作成、配布、使用、保守、廃棄です。これらは、情報が生成された瞬間から破棄またはアーカイブされる瞬間までのライフサイクル中に情報が経るフェーズです。情報の各段階には、異なるセキュリティ要件とリスクがあり、それに応じて管理する必要があります。作成、進化、保守、使用、廃棄は、情報の正しい段階ではありません。進化は明確な段階ではなく、どの段階でも発生する可能性のあるプロセスだからです。作成、使用、廃棄、保守、進化は、正しい順序ではないため、情報の正しい段階ではありません。作成、配布、保守、廃棄、使用は、正しい順序ではないため、情報の正しい段階ではありません。参照: : CQI & IRCA ISO 27001:2022 主任監査員コース ハンドブック、32 ページ。: [ISO/IEC 27001 主任監査員 - PECB]、12 ページ。

最新問題: 111

CEOは、会社の現状と将来戦略、そしてCEOのビジョンと従業員の役割について意見を述べるメールを送信します。このメールは、以下のように分類されるべきです。

- A. 社内メール
- B. 公開メール
- C. 機密メール
- D. 制限付きメール

Answer: ([解答を表示する](#))

CEOが会社の現状と将来の戦略、CEOのビジョン、そして従業員の役割について意見を述べたメールは、社内メールとして分類されるべきです。社内メールとは、情報が社内でのみ使用されることを意図しており、許可なく外部に開示してはならないことを示す分類です。CEOが送信するメールには、会社の従業員にとって関連性があり重要な情報が含まれていますが、会社の業績、目標、計画に関する機密情報や秘密情報が含まれている可能性があるため、公開には適さない場合があります。参照: : CQI & IRCA ISO 27001:2022 主任監査員コースハンドブック、34 ページ。: CQI & IRCA ISO 27001:2022 主任監査員コースハンドブック、37 ページ。: [ISO/IEC 27001 主任監査員 - PECB]、14 ページ。

最新問題: 112

あなたは経験豊富な監査チームリーダーであり、監査員の研修を指導しています。研修を受けた監査員の任務は、適合性報告書 (SoA)に記載され、現場で実施されている技術的統制をレビューすることです。研修を希望する監査担当者にレビューしてもらいたい管理項目を、以下のリストから4つ選択してください。

- A. 情報資産目録の作成と維持
- B. 組織内および他組織へのメッセージ伝達に関する規則
- C. 機密保持および機密保持契約
- D. マルウェア対策の実装方法
- E. 荷積みエリアへの出入り口通路
- F. 人員の確認とチェック。

- G. リモートワーク体制
- H. サプライヤー契約における情報セキュリティ問題への対処方法とは？
- I. 組織は、自社の技術的な脆弱性がどの程度露呈しているかをどのように評価するか。
- J. 組織における事業継続計画
- K. 組織の情報削除に関する取り決め
- L. 情報セキュリティに関する意識向上、教育、トレーニング
- M. ソースコードと開発ツールへのアクセスを管理する方法
- N. 現場監視カメラおよび入退室管理システムの運用
- O. 機器保守のための組織的取り決め
- P. 電源ケーブルとデータケーブルはどのように建物内に引き込まれるのですか？

Answer: [\(解答を表示する\)](#)

情報セキュリティマネジメントシステム (ISMS) の確立、実装、維持、継続的改善に関する要求事項を規定するISO/IEC 27001:2022によれば、組織は情報セキュリティの目的を達成するために適切な管理策を選択して実装する必要がある1。管理策はリスク評価とリスク処理の結果から導き出され、ISMSに適用可能かつ必要な管理策を特定する文書である適用性宣言書 (SoA) と整合していなければならない1。管理策は、情報セキュリティ管理策の実施規範を提供するISO/IEC 27002:2013など、さまざまな情報源から選択できる2。したがって、研修中の監査員が、外部顧客のためにデータを保存する組織のサイトで実装され、SoAに記載されている技術的管理策をレビューするよう指示された場合、レビューが想定される4つの管理策は次のとおりである。

- * マルウェア対策の実施方法 :これは、情報または情報システムの機密性、完全性、可用性を損なう可能性のある悪意のあるソフトウェア (ウイルス、ワーム、ランサムウェアなど) を防止、検出、削除することを目的とした技術的制御です。この制御は、ISO/IEC 27002:2013の制御A.12.2.1に関連しています。
- * 組織が技術的な脆弱性への露出をどのように評価するか: これは、悪意のある行為者によって悪用される可能性のある、または偶発的な障害を引き起こす可能性のある情報システムまたはネットワークの潜在的な弱点または欠陥を特定および評価することを目的とした技術的コントロールです。このコントロールは、ISO/IEC 27002:20132 のコントロール A.12.6.1 に関連しています。
- * ソースコードと開発ツールへのアクセス管理方法 :これは、組織またはその外部プロバイダーによって開発または保守されるソフトウェアアプリケーションまたはシステムの知的財産権と完全性を保護することを目的とした技術的管理です。この管理は、ISO/IEC 27002:20132の管理A:14.2.5に関連しています。
- * 敷地内のCCTVおよびドア制御システムの運用 :これは、情報または情報システムが保存または処理される施設または設備への物理的なアクセスを監視および制限することを目的とした技術的制御です2。この制御は、ISO/IEC 27002:20132の制御A.11.1.4に関連しています。

その他の選択肢は、技術的統制の例ではなく、ISMS 監査に関連する可能性のある組織的、法的、または手続き的統制の例ですが、研修中の監査員のタスクの範囲外です。たとえば、情報資産インベントリの開発と維持 (統制 A に関連) などです。

8.1.1)、組織内および他の組織への情報転送に関する規則 (管理策 A.13.2.1 に関連)、機密保持および非開示契約 (管理策 A.13.2.4 に関連)、従業員の検証チェック (管理策 A.7.1.2 に関連)、リモートワークの取り決め (管理策 A.6.2.1 に関連)、サプライヤー契約内の情報セキュリティ (管理策 A.15.1.1 に関連)、事業継続の取り決め (管理策 A.17 に関連)、情報の削除 (管理策 A.8.3 に関連)、情報セキュリティの意識向上、教育およびトレーニング (管理策 A.7.2 に関連)、機器の保守 (管理策 A.11.2 に関連)、および電力およびデータケーブルが建物に入る方法 (管理策 A.11 に関連) は、技術的な管理策ではなく、組織的、法的または手続き的な管理策であり、ISMS 監査にも関連する可能性があります。研修中の監査員の業務範囲には含まれません。参照規格 :ISO/IEC 27001:2022 - 情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステム - 要求事項、ISO/IEC 27002:2013 - 情報技術 - セキュリティ技術 - 情報セキュリティ管理の実施規範

最新問題: 113

身為資訊安全管理系統審核小組組長，您正在代表一家線上零售商對一家國際物流公司進行第二方審核。在審核期間，您的一名團隊成員報告了與ISO/IEC 27001 附錄 A 的控制 5.18（存取權限）相關的不合格項：2022 年。她發現證據表明，刪除過去3 個月已離開的 20 名人員的伺服器存取協定需要長達 1 週的時間，而政策要求在他們離開後24 小時已刪除存取權限。當被審核方被問及為何延遲刪除訪問權限時，他們回答已，“由於 COVID-19 的影響，IT 部門在此期間沒有人可用。”一旦 IT 官員出現，這些權利就被取消。您注意到她打算針對存取權限控制 (5.18) 提出輕微不符合項。對此你該如何回應？

- A. 在確定不合格項是否適當之前，需要先取得額外的審核證據
- B. 不同意提出輕微不符合項，因為已儘早採取適當行動。相反，提出改進的機會
- C. 不同意提出輕微不符合項，有足夠的證據證明昇級為重大不符合項是合理的

- D. 不同意提出輕微合規性，因為已儘早採取適當行動，不再採取進一步行動
- E. 同意提出輕微不合格項，但反對控制措施5.15，而不是5.18。
- F. 同意針對 5.18 提出輕微不符合項。

Answer: (解答を表示する)

最新問題: 114

三名審核員被指派到 X 公司進行認證審核。這可以接受嗎？

- A. 利益衝突的情況是要求更換審計師的正當理由
- B. 不可以，受審計方只有在提出正當理由的情況下才可以要求更換審計員，例如不專業的行為或存在實際利益衝突的情況
- C. 不可以，受審計方不能要求更換審計員

Answer: B (メッセージを残す)

Comprehensive and Detailed In-Depth

B . Correct Answer:

ISO/IEC 17021-1 (Conformity assessment - Requirements for bodies providing audit and certification of management systems) states that the auditee may request a replacement of an auditor only for valid reasons.

A former employee of the company serving as an auditor presents a potential conflict of interest (real or perceived).

Therefore, Company X's request is valid.

A . Incorrect:

While a conflict of interest is a valid reason, the replacement must be based on an objective, justified claim, and not just personal preference.

C . Incorrect:

Auditees can request an auditor's replacement, but only under justified circumstances.

Relevant Standard Reference:

ISO/IEC 17021-1:2015 Clause 9.1.3 (Impartiality and Objectivity of Auditors)

最新問題: 115

次のうち、情報セキュリティ攻撃の種類ではないものはどれですか？

- A. 法的イベント
- B. 交通事故
- C. 技術的な脆弱性
- D. プライバシー問題

Answer: B (メッセージを残す)

車両事故は情報セキュリティ攻撃の一種ではありません。車両事故とは、車両またはその運転者が人や財産に損害や傷害を与える事象です。車両事故は、車両によって輸送またはアクセスされる情報やシステムの可用性や完全性に影響を与える場合、情報セキュリティに影響を与える可能性があります。情報セキュリティに対する意図的または悪意のある攻撃ではありません。法的インシデントは、情報やシステムの機密性や完全性を損なう可能性のある法的措置や紛争を伴う情報セキュリティ攻撃の一種です。技術的脆弱性は、情報やシステムの機密性、完全性、または可用性を損なう可能性のあるソフトウェアまたはハードウェアの弱点や欠陥を悪用する情報セキュリティ攻撃の一種です。プライバシーインシデントは、個人情報または機密情報への不正アクセスまたは開示を伴う情報セキュリティ攻撃の一種で、情報やシステムの機密性または完全性を損なう可能性があります。参照: : CQI & IRCA ISO 27001:2022 主任審査員コースハンドブック、25 ページ。: [ISO/IEC 27001 主任審査員 - PECB]、13 ページ。

最新問題: 116

監査の結果、15名のITスタッフのうち2名が十分な情報セキュリティ研修を受けていなかったことが判明しました。これはどういう意味でしょうか？

- A. 監査結果
- B. 監査証拠

C. 情報源

Answer: A (メッセージを残す)

このシナリオは「監査結果」に該当します。監査結果とは、期待されるパフォーマンスや基準からの逸脱を示す結果のことです。従業員2名が必要な研修を受けていないことが判明した場合、それは組織の研修要件への不遵守を示す監査結果となります。

参考文献 :ISO 19011:2018、マネジメントシステムの監査に関する指針

最新問題: 117

您是一位經驗豐富的 ISMS 口部稽核師。

當 IT 經理找到您並要求您協助修改公司的適用性聲明時， 您剛剛完成了組織的預定資訊安全審核。

IT 經理正在嘗試將基於 ISO/IEC 27001:2013 的適用性聲明更新為與 ISO/IEC 27001:2022 中的 4 個控制主題（組織控制、人員控制、實體控制、技術控制）一致的聲明。

IT 經理對控制權的重新分配感到滿意， 但以下情況除外。他詢問您以下每個控制類別應出現在哪四個控制類別下。

How would you respond? Match the control description to the category.

8.1 Information stored on, processed by, or accessible via user endpoint devices shall be protected	
7.8 Equipment shall be sited securely and protected	
5.2 Information security roles and responsibilities shall be defined and allocated according to the organisation's needs	
6.7 Security measures shall be implemented when personnel are working remotely to protect information processed, processed, or stored outside the organisation's premises	

To complete the table click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop each option to the appropriate blank section.

Technological control

People control

Organizational control

Physical control

Answer:

How would you respond? Match the control description to the category.

8.1 Information stored on, processed by, or accessible via user endpoint devices shall be protected	Technological control
7.8 Equipment shall be sited securely and protected	Physical control
5.2 Information security roles and responsibilities shall be defined and allocated according to the organisation's needs	Organizational control
6.7 Security measures shall be implemented when personnel are working remotely to protect information processed, processed, or stored outside the organisation's premises	People control

To complete the table click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop each option to the appropriate blank section.

Technological control

People control

Organizational control

Physical control

最新問題: 118

リストを使用する利点を説明する選択肢を2つ選んでください。

* 全ての監査で同じチェックリストが使用され、見直しは一切行われなかった。

- A. インタビューを特定の場所に限定する。
- B. 関連する監査証拠が確実に守られていることを確認する。
- C. 監査計画が確実に実施されるようにする
- D. 監査期間を短縮する
- E. 必要に応じてチェックリストから逸脱しないでください。

Answer: C,D (メッセージを残す)

チェックリストは、監査人が監査の目的と範囲に関連する情報を収集し、検証するのに役立つツールです。チェックリストには、次のような利点があります。

* 関連する監査証拠が確実に追跡されるようにする :チェックリストは、監査対象基準の適合性または不適合性を裏付ける証拠の出所を特定し、追跡するのに役立ちます。また、監査の重要な側面を見落としたり、漏らしたりすることを防ぐのにも役立ちます。

監査計画の確実な実施 :チェックリストは、監査担当者が監査計画に従って作業を進めるのに役立ちます。監査計画には、監査の目的、範囲、基準、スケジュール、役割、責任など、監査の手順と詳細が記載されています。また、監査担当者が時間とリソースを効果的かつ効率的に管理するのにも役立ちます。

その他の選択肢はチェックリストを使用する利点ではなく、むしろ次の点である。

* 見直しを行わずにすべての監査で同じチェックリストを使用すること :これはチェックリストを使用する際の欠点であり、硬直的で非効率的な監査アプローチにつながる可能性があります。チェックリストは、監査対象者および監査基準の状況、リスク、変更点を考慮して、個々の監査に合わせてカスタマイズおよび調整する必要があります。また、チェックリストの妥当性と関連性を確保するために、定期的に見直しと更新を行う必要があります。

* インタビュー対象者を指名された関係者に限定すること :これはチェックリストを使用する際の欠点であり、監査の範囲と深さを制限してしまう可能性があります。チェックリストは、監査担当者が監査にとって貴重な証拠や洞察を提供する可能性のある、その他の関連関係者や情報源にインタビューすることを妨げるものであってはなりません。

チェックリストは、制約としてではなく、あくまでも指針として使用すべきです。

監査期間の短縮 :これは必ずしもチェックリストの使用による利点とは限りません。被監査企業のISMSの複雑さ、規模、成熟度、証拠の入手可能性と質、監査員の能力と経験、監査員と被監査企業間の協力とコミュニケーションのレベルなど、さまざまな要因に左右されるからです。チェックリストは効率性と組織性を向上させることで監査期間の短縮に役立つ場合もありますが、より多くの証拠や検証が必要となることで監査期間が長くなる可能性もあります。

必要に応じてチェックリストから逸脱しないこと :これはチェックリストを使用する際の欠点であり、表面的な、あるいは不完全な監査につながる可能性があります。チェックリストは、監査中に発生した問題や懸念事項（チェックリストに含まれていない場合でも）を監査担当者が調査・検討することを妨げるものであってはなりません。チェックリストはあくまで補助的なものであり、代替となるものではありません。

参考文献：
ISO/IEC 27001:2022 主任審査員（情報セキュリティマネジメントシステム）の目的と内容は Quality.org および PECB から引用。ISO 19011:2018 マネジメントシステムの監査に関するガイドライン [セクション 6.2.2]

最新問題: 119
シナリオ5 :Data Grid Inc.は、ITインフラ全体に対するセキュリティサービスを提供する著名な企業です。エンドポイントセキュリティ、ファイアウォール、ウイルス対策ソフトウェアなど、ネットワークセキュリティソフトウェアを提供しています。Data Grid Inc.は20年以上にわたり、高度な製品とサービスを通じて数多くの企業のネットワークセキュリティ保護を支援してきました。情報およびネットワークセキュリティ分野で高い評価を得ているData Grid Inc.は、自社および顧客の資産をより適切に保護し、競争優位性を獲得するために、ISO/IEC 27001認証の取得を決定しました。Data Grid Inc.は監査チームを任命し、監査チームは監査業務の条件に同意した。さらに、Data Grid Inc.は監査範囲と基準を定義し、5日以内に監査を完了することを推奨した。Data Grid Inc.は従業員数が多く、業務プロセスが複雑であるため、監査チームは5日以内に監査を実施するというData Grid Inc.の提案を拒否した。Data Grid Inc.は5日以内に監査を完了する予定であると主張したため、両当事者は規定の期間内に監査を実施することに合意した。監査チームはリスクベースの監査アプローチを採用した。主要な業務プロセスと統制の概要を把握するため、監査チームはプロセス記述書と組織図を参照しました。ITインフラストラクチャとアプリケーションへのアクセスが制限されていたため、ITリスクと統制に関するより詳細な分析は実施できませんでした。しかし、監査チームは、Data Grid Inc.のISMSにおける重大な欠陥のリスクは、同社のプロセスのほとんどが自動化されているため低いと判断しました。そこで、Data Grid Inc.の担当者に以下の質問をすることで、ISMSの標準への全体的な準拠状況を評価しました。

ITおよびIT管理に関する責任は、どのように定義され、割り当てられるべきでしょうか？
*データグリッド社 管理措置が望ましい結果を達成したかどうかをどのように評価しますか？
Data Grid Inc.は、マルウェアから自社の運用環境とデータを保護するために、どのような対策を講じていますか？
ファイアウォール関連の制御は実装されていますか？
データグリッド社の担当者は、これらの問題すべてに対処するための十分かつ適切な証拠を提出した。
監査チームリーダーは監査結果をまとめ、データグリッド社の経営陣に報告した。
監査人はデータグリッド社を認証対象として推奨したが、監査目的に関してデータグリッド社と認証機関の間で誤解が生じた。データグリッド社は、監査目的には改善の可能性のある領域の特定が含まれていたにもかかわらず、監査チームはそのような情報を提供しなかったと主張した。
このシナリオに基づいて、以下の質問に教えてください。

シナリオ5に基づき、監査チームはデータグリッド社が提案したISMS監査の監査期間に同意していません。この状況をどのように説明しますか？
A. 問題ありません。監査人が監査期間が不十分だと感じた場合、異議を申し立てたり、監査の承認を拒否したりする権利があります。
B. 不適切。監査期間は被監査者によって定められており、監査人が変更することはできません。
C. 不可。審査依頼が承認されると、審査期間は変更できません。

Answer: ([解答を表示する](#))
監査人は、被監査企業が提案する監査期間がISMSを徹底的に評価するのに不十分であると判断した場合、監査依頼に異議を申し立てたり、拒否したりする権限を有します。監査は、システムの有効性とコンプライアンスを確保するために、システムのあらゆる必要な側面を網羅する包括的な内容であることが不可欠です。

最新問題: 120
シナリオ8 :EsBankは9月からエストニアの銀行業界に銀行および金融ソリューションを提供する。
2010年時点で、同社は全国に30の支店と100台以上のATMを保有していた。

規制の厳しい業界で事業を展開するEsBankは、データセキュリティとプライバシーに関する数多くの法律や規制を遵守しなければなりません。そのため、技術的および非技術的な両方の管理策を実施することで、事業運営全体にわたって情報セキュリティを管理する必要があります。EsBankは、ISO/IEC規格に基づいた情報セキュリティマネジメントシステム（ISMS）を導入することを決定しました。

27001は、より優れたセキュリティ、より高度なリスク管理、および主要な法的 規制上の要件への準拠を提供するため、採用する価値がある。

ISMSの導入に成功してから9か月後、EsBankはISO/IEC 27001に準拠した独立した認証機関によるISMSの認証を受けることを決定した。

監査の第1段階と第2段階は同時並行で実施され、いくつかの法令違反が特定された。最初の違反は、EsBankの情報表示に関するものであった。同社は情報分類体系は持っていたものの、情報表示の手順がなかった。その結果、同じレベルの保護が必要な文書でも、異なるラベルが付けられていた（機密文書の場合もあれば、機密性の高い文書の場合もあった）。

すべての文書が電子的に保存されていたため、この法令違反はメディアの取り扱いにも影響を及ぼしました。監査チームはサンプリング調査の結果、200個のリムーバブルメディアのうち50個に、機密情報として誤って分類されていた機密情報が保存されていたことを突き止めました。情報分類体系によれば、リムーバブルメディアへの機密情報の保存は許可されていますが、機密情報の保存は厳しく禁止されています。これは、もう一つの法令違反となります。

彼らは不適合報告書を作成し、監査結果についてEsBankの担当者と協議した。担当者は、特定された不適合事項に対する改善計画を2か月以内に提出することに同意した。

EsBankは監査チームリーダーが提案した解決策を受け入れた。物理フォーマットと電子フォーマットの分類体系に基づいた情報表示プログラムを策定し、法令違反の問題を解決した。また、このプログラムに基づいてポータブルメディアアプリもアップデートされた。

監査完了から2週間後、EsBankは一般的な改善計画を提出した。その計画書には、指摘された不適合事項と講じた是正措置が記載されていたが、影響を受けたシステム、管理体制、または業務に関する詳細な情報は含まれていなかった。監査チームは改善計画を評価し、不適合事項は解消されると結論付けた。しかしながら、EsBankは不利な認証勧告を受けた。

上記のシナリオに基づいて、以下の質問に教えてください。

シナリオ8に示されている行動のうち、外部監査において容認できないものはどれですか？

A. 監査チームのリーダーは、不適合を解決するための具体的な解決策を提案しました。

B. 審査の第1段階と第2段階は同時に実施されます。

C. 情報表示手順の欠如は、軽微な不適合として示されます。

Answer: A (メッセージを残す)

監査チームリーダーが不適合事項の解決方法について具体的な解決策を提案することは、外部監査においては容認できません。これは、監査対象者が是正措置を講じる際に支援しているように見え、監査プロセスの公平性を損なう可能性があります。是正措置は、ISMSの完全性と有効性を確保するために、監査対象者自身が独自に策定すべきものです。

最新問題: 121

あなたは認証機関の監査員であり、ICT施設向けマネージドサービスを提供する顧客が運営するデータセンターに対して、ISO/IEC 27001:2022に基づく監視監査を実施する責任を負っています。

お客様とガイドは現在、クライアントが貸し出しているプライベートスイートのいずれかにご滞在いただいています。各スイートへのアクセスはキーパッドロックで管理されています。また、各スイートには監視カメラが設置されています。

各キットには、顧客がミッションクリティカルなサーバーや、スイッチやルーターなどのネットワーク機器を設置できるキャビネットが3つ含まれています。

スイート内のキャビネットのうち2つは施錠されているのに、3つ目のキャビネットは開いていることに気づきます。ツアーガイドに理由を尋ねると、ガイドは「お客様が現在ハードドライブユニットを交換している最中だからです。技術者の方々が昼休憩を取っているところです」と答えます。

次取るべき3つの行動は何ですか？

A. 何もしなくても、部屋は十分に保護されているように見えるので、セキュリティ上の問題が発生する可能性は低いでしょう。

B. 管理措置5.16「本人確認管理」に違反が見つかりました。ロッカーを施錠していない人を特定することが不可能な場合があるためです。

C. 顧客の機器が設置されているエリアが保護されていないため、管理措置7.2「エンティティの進入」に違反していることが判明しました。

D. 管理措置7.4「物理的セキュリティ監視」に違反が見つかりました。プライベートスイートが不正な物理的アクセスに対して継続的に監視されていなかったためです。

E. 改善の機会を提案します。ゲストがスイートを離れる際は、たとえすぐに戻ってくる予定であっても、キャビネットのドアを施錠することを提案します。

F. 監視カメラの映像を確認し、最後に施錠されていたことが確認されて以降、顧客のみがキャビネットを訪れたことを確認します。

G. 技術者たちが昼食から戻ってくると、キャビネットを開けなかったことで叱責された。

H. ウィザードが許可する場合は、顧客に連絡して、ドライブを交換することを確認します。

Answer: E,F,H (メッセージを残す)

技術者が昼休み中にキャビネットの鍵をかけずに放置すると、顧客の機器やデータが盗難、破損、改ざんなどの物理的なセキュリティリスクにさらされる可能性があります。これは、情報処理設備や資産への不正アクセスを防止することを目的とした、ISO/IEC 27001:2022の物理的入退室（管理策.2）および物理的セキュリティ監視（管理策.4）に関する要求事項に違反します。したがって、監査員が取るべき適切な措置は以下のとおりです。

改善点（OFI）として、顧客がスイートを離れる際は、たとえ短時間で戻る予定であっても、キャビネットの扉を施錠することを提案します。これにより、顧客の機器とデータのセキュリティが強化され、セキュリティインシデントの発生確率が低減されます。

監視カメラの映像を確認し、最後に施錠が確認されて以降、キャビネットにアクセスしたのはクライアントのみであることを確認してください。これにより、クライアントの機器とデータの完全性と可用性が検証され、不正アクセスや妨害行為の可能性が特定されます。

ガイドの許可を得て、顧客に連絡を取り、ドライブの交換作業中であることを確認してください。これにより、キャビネットのロックを解除したままにしておく理由が正当化され、この作業が顧客の情報セキュリティに及ぼす影響とリスクを評価できます。

参照：

ISO/IEC 27001:2022、7.2項、物理的搬入

ISO/IEC 27001:2022、7.4項、物理的セキュリティ監視

PECB候補者ハンドブック ISO 27001主任監査員、19ページ、監査プロセス

PECB候補者ハンドブック ISO 27001主任審査員、21ページ、監査結果

有効な **ISO-IEC-27001-Lead-Auditor-CN** 問題集は GoShiken.com が提供された合格しやすい ISO-IEC-27001-Lead-Auditor-CN 試験問題集！ GoShiken.com が最新の **ISO-IEC-27001-Lead-Auditor-CN** 試験問題集を提供しています。GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 問題集をゲットする人はこちら：

<https://www.goshiken.com/PECB/ISO-IEC-27001-Lead-Auditor-CN-mondaishu.html> (418**30%OFF**問題集溶と正解付きで 30%w特別割引コード: **Freepdfdumps**)

最新問題: 122

貴社は現在、ISO/IEC 27001:2022認証の取得を目指しています。あなたは先日、内部ISMS監査員の資格を取得しました。ICTマネージャーは、あなたの新たな知識を活用して、情報セキュリティインシデント管理プロセスの設計を支援してもらいたいと考えています。

彼は計画策定プロセスにおける以下の段階を特定し、それらがどのような順序で行われるべきかを確認するようあなたに依頼しました。

Step 1	Incident logging
Step 2	
Step 3	
Step 4	
Step 5	
Step 6	
Step 7	
Step 8	Incident closure

To complete the sequence, click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the options to the appropriate blank section.

Incident prioritisation – classify the incident as critical, high, medium, low

Task creation and management – identification and coordination of work needed to resolve the incident

SLA management and escalation – ensure any service level agreements are adhered to whilst resolution is being implemented. If a breach looks likely, escalate to secure more resources

Incident resolution – a temporary workaround or permanent resolution has been identified

Incident assignment – incident is passed to the individual best suited to resolve it

Incident categorisation – determine whether the incident is a hardware issue, network issue or software issue

Answer:

Step 1	Incident log	
Step 2		Incident categorisation – determine whether the incident is a hardware issue, network issue
Step 3		Incident prioritisation – classify the incident as critical, high, medium, low
Step 4		
Step 5		SLA management and escalation – ensure any service level agreements are adhered to whilst resolution is being implemented. If a
Step 6		Incident resolution – a temporary
Step 7		workaround or permanent resolution has been identified
Step 8	Incident closure	

To complete the sequence, click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the options to the appropriate blank section.

Incident prioritisation – classify the incident as critical, high, medium, low

Task creation and management – identification and coordination of work needed to resolve the incident

SLA management and escalation – ensure any service level agreements are adhered to whilst resolution is being implemented. If a breach looks likely, escalate to secure more resources

Incident resolution – a temporary workaround or permanent resolution has been identified

Incident assignment – incident is passed to the individual best suited to resolve it

Incident categorisation – determine whether the incident is a hardware issue, network issue or software issue

Explanation:

ステップ 1 = インシデントのログ記録 ステップ 2 = インシデントの分類 ステップ 3 = インシデントの優先順位付け ステップ 4 = インシデントの割り当て ステップ 5 = タスクの作成と管理 ステップ 6 = SLA の管理とエスカレーション ステップ 7 = インシデントの解決 ステップ 8 = インシデントのクローズ 情報セキュリティインシデント管理プロセスの各段階の順序は、インシデント、イベント、脆弱性に対して迅速、効果的、かつ秩序だった対応を保証する論理的な順序に従う必要があります。また、この順序は、ISO/IEC 27001:2022 および ISO が提供するベストプラクティスとガイダンスにも準拠している必要があります。

/IEC 27035:2022。したがって、以下の順序が推奨されます。

- * ステップ 1 = インシデントの記録: このステップでは、発生日時、発生源、説明、影響、報告者など、潜在的なインシデント、イベント、または脆弱性の詳細を記録します。このステップは、インシデントの追跡可能な記録を提供し、その後の分析と対応を容易にするために重要です。このステップは、情報セキュリティのインシデント、イベント、および脆弱性の管理に関する責任と手順を組織が確立することを要求する ISO/IEC 27001:2022 の管理策 A.16.1.1 に関連しています。このステップは、インシデント、イベント、および脆弱性の記録方法に関するガイダンスを提供する ISO/IEC 27035:2022 の条項 6.2 にも関連しています。
- * ステップ 2 = インシデントの分類: このステップでは、ハードウェアの問題、ネットワークの問題、ソフトウェアの問題など、インシデント、イベント、または脆弱性の種類と性質を判断します。このステップは、インシデントを分類し、適切な解決担当者またはチームに割り当てるために重要です。このステップは、組織が情報セキュリティのイベントと脆弱性を適切な管理チャネルを通じてできるだけ迅速に報告することを要求する ISO/IEC 27001:2022 の管理策 A.16.1.2 に関連しています。このステップは、インシデント、イベント、および脆弱性を分類する方法に関するガイダンスを提供する ISO/IEC 27035:2022 の条項 6.3 にも関連しています。
- * ステップ 3 = インシデントの優先順位付け: このステップでは、インシデント、イベント、または脆弱性の深刻度と緊急度を評価し、それを重大、高、中、または低に分類します。このステップは、インシデントの優先順位付けと、対応に必要なリソースと時間の割り当てに重要です。このステップは、組織が定義された基準に従って情報セキュリティイベントと脆弱性を評価し、優先順位付けすることを要求している ISO/IEC 27001:2022 の管理策 A.16.1.3 に関連しています。このステップは、インシデント、イベント、および脆弱性の優先順位付け方法に関するガイダンスを提供する ISO/IEC 27035:2022 の条項 6.4 にも関連しています。
- * ステップ 4 = インシデントの割り当て: このステップでは、スキル、知識、および可用性に基づいて、インシデント、イベント、または脆弱性を解決するのに最も適した個人またはチームにインシデント、イベント、または脆弱性を引き渡します。

この手順は、インシデントが適切な担当者またはチームによって処理され、遅延や混乱を避けるために重要です。この手順は、組織が合意された手順に従って、情報セキュリティインシデントおよび脆弱性にタイムリーに対応することを要求する ISO/IEC 27001:2022 の管理策 A.16.1.4 に関連しています。また、この手順は、インシデント、イベント、および脆弱性の割り当て方法に関するガイダンスを提供する ISO/IEC 27035:2022 の条項 6.5 にも関連しています。

- * ステップ 5 = タスクの作成と管理: このステップでは、根本原因分析の実施、ソリューションのテスト、変更の実装、アクションの文書化など、インシデント、イベント、または脆弱性を解決するために必要な作業を特定し、調整します。このステップは、インシデントが効果的かつ効率的に解決され、アクションが追跡および管理されることを保証するために重要です。このステップは、情報セキュリティのイベントや脆弱性から得られた教訓を組織に適用して是正措置および予防措置を講じることを要求する ISO/IEC 27001:2022 の管理策 A.16.1.5 に関連しています。このステップは、インシデント、イベント、および脆弱性に対するタスクの作成と管理方法に関するガイダンスを提供する ISO/IEC 27035:2022 の条項 6.6 にも関連しています。
- * ステップ 6 = SLA の管理とエスカレーション: このステップでは、解決策の実施中にサービスレベル契約 (SLA) が遵守されていることを確認し、違反が発生する可能性が高い場合または発生した場合は、インシデントを上位の権限またはサポートレベルにエスカレーションします。このステップは、インシデントが合意された時間枠と品質内で解決され、逸脱や問題が伝達され対処されることを保証するために重要です。このステップは、ISO の管理 A.16.1.6 に関連しています。

ISO/IEC 27001:2022 では、組織が情報セキュリティ上のインシデントや脆弱性を、必要に応じて関連する内部および外部の関係者に伝達することが求められています。この手順は、インシデント、イベント、脆弱性に関する SLA およびエスカレーションの管理方法に関するガイダンスを提供する ISO/IEC 27035:2022 の 6.7 項にも関連しています。

- * ステップ 7 = インシデント解決 : このステップでは、インシデント、イベント、または脆弱性を解決するために、一時的な回避策または恒久的な解決策を適用し、情報および情報処理施設の正常な動作を復旧します。このステップは、インシデントが完全に満足のいく形で解決され、情報セキュリティが望ましいレベルまで回復されることを保証するために重要です。

この手順は、ISO/IEC 27001:2022 の管理策 A.16.1.7 に関連しています。この管理策では、組織が情報セキュリティインシデントおよび脆弱性の原因を特定し、それらの再発または発生を防止するための措置を講じることを求めています。また、この手順は、インシデント、イベント、および脆弱性を解決する方法に関するガイダンスを提供する ISO/IEC 27035:2022 の条項 6.8 にも関連しています。

- * ステップ 8 = インシデントのクローズ: このステップでは、インシデント、イベント、または脆弱性が満足のいく形で解決され、すべてのアクションが完了して文書化されたことを確認した後、それらをクローズします。この手順は、インシデントが正式に解決され、それ以上の対応が不要であることを確認するために重要です。この手順は、情報セキュリティインシデントと脆弱性、および講じた措置に関する証拠を収集し文書化することを組織に求める ISO/IEC 27001:2022 の管理策 A.16.1.8 に関連しています。また、この手順は、インシデント、イベント、および脆弱性を解決する方法に関するガイダンスを提供する ISO/IEC 27035:2022 の条項 6.9 にも関連しています。

参考文献：

ISO/IEC 27001:2022、情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステム - 要求事項1 PECB 候補者ハンドブック ISO/IEC 27001 主任監査員2 ISO 27001:2022 主任監査員 - PECB3 ISO 27001:2022 認定 ISMS 主任監査員 - Jisc4 ISO/IEC 27001:2022 主任監査員移行トレーニングコース5 ISO 27001 - 情報セキュリティ主任監査員コース - PwC トレーニングアカデミー6 ISO/IEC 27035:2022、情報技術 - セキュリティ技術 - 情報セキュリティインシデント管理

最新問題: 123

根據 ISO/IEC 27001 第 5.1 條（領導與承諾），下列何者不是高階管理人員的責任？

- A. 確保 ISMS 資源的可用性並促進持續改進
- B. 定期進行口部審核，以評估ISMS 的有效性
- C. 指導和支援人員為 ISMS 的有效性做出貢獻

Answer: B ([メッセージを残す](#))

Comprehensive and Detailed In-Depth

ISO/IEC 27001 Clause 5.1 (Leadership and Commitment) defines top management's role in ensuring the effectiveness of the Information Security Management System (ISMS). It requires top management to:

Ensure the availability of resources for the ISMS (Correct Responsibility).

Promote continual improvement of the ISMS (Correct Responsibility).

Direct and support employees to contribute to ISMS effectiveness (Correct Responsibility).

B . Conducting regular internal audits - Incorrect Responsibility:

Internal audits are not a direct responsibility of top management. Instead, Clause 9.2 (Internal Audit) requires audits to be conducted independently of management.

Top management is responsible for ensuring audits are conducted but does not need to conduct them personally.

Thus, top management is responsible for oversight and support but not for conducting internal audits themselves.

Relevant Standard Reference:

ISO/IEC 27001:2022 Clause 5.1 (Leadership and Commitment)

ISO/IEC 27001:2022 Clause 9.2 (Internal Audit)

最新問題: 124

您正在國際物流組織的出貨部門進行 ISMS 審核，該組織為當地醫院和政府辦公室等大型組織提供運輸服務。包裹通常包含藥品、生物樣本以及護照和駕駛執照等文件。您注意到，公司記錄顯示大量退貨，原因包括標籤地址錯誤，以及在 15% 的公司案例中，一個包裹的不同地址有兩個或多個標籤。您正在面試運輸經理 (SM)。

您：出貨前檢口過嗎？

SH：任何明顯損壞的物品都會在出貨前由口班人員移除，但利潤微薄，因此實施正式檢口流程並不經濟。

您：退貨後會採取什麼措施？

SM：這些合約大多價口相對較低，因此我們認為，簡單地重新列印標籤並重新發送單一包裹比實施調口更容易方便。

您提出不符合項。參考該場景，您希望受審核方在進行後續審核時實施下列哪六項附錄A 控制措施？

- A. 5.11 資口返還
- B. 8.12 資料外洩保護
- C. 5.3 職責分離
- D. 6.3 資訊安全意識、教育與培訓
- E. 7.10 儲存介質
- F. 8.3 資訊存取限制
- G. 5.6 與特殊利益團體的聯繫
- H. 6.4 紀律程序
- I. 7.4 實體安全監控
- J. 5.13 資訊標籤
- K. 5.32 智慧財口權

Answer: B,D,E,F,I,J ([メッセージを残す](#))

B . 8.12 Data leakage protection. This is true because the auditee should have implemented measures to prevent unauthorized disclosure of sensitive information, such as personal data, medical records, or official documents, that are contained in the parcels. Data leakage protection could include encryption, authentication, access control, logging, and monitoring of data transfers12.

D . 6.3 Information security awareness, education, and training. This is true because the auditee should have ensured that all employees and contractors involved in the shipping process are aware of the information security policies and procedures, and have received appropriate training on how to handle and protect the information assets in their custody. Information security awareness, education, and training could include induction programmes, periodic refreshers, awareness campaigns, e-learning modules, and feedback mechanisms13.

E . 7.10 Storage media. This is true because the auditee should have implemented controls to protect the storage media that contain information assets from unauthorized access, misuse, theft, loss, or damage. Storage media could include paper documents, optical disks, magnetic tapes, flash drives, or hard disks14. Storage media controls could include physical locks, encryption, backup, disposal, or destruction14.

F . 8.3 Information access restriction. This is true because the auditee should have implemented controls to restrict access to information assets based on the principle of least privilege and the need-to-know basis. Information access restriction could include identification, authentication, authorization, accountability, and auditability of users and systems that access information assets15.

I . 7.4 Physical security monitoring. This is true because the auditee should have implemented controls to monitor the physical security of the premises where information assets are stored or processed. Physical security monitoring could include CCTV cameras, alarms, sensors, guards, or patrols16. Physical security monitoring could help detect and deter unauthorized physical access or intrusion attempts16.

J . 5.13 Labelling of information. This is true because the auditee should have implemented controls to label information assets according to their classification level and handling instructions. Labelling of information could include markings, tags, stamps, stickers, or barcodes1 . Labelling of information could help identify and protect information assets from unauthorized disclosure or misuse1 .

Reference:

ISO/IEC 27002:2022 Information technology - Security techniques - Code of practice for information security controls ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements ISO/IEC 27003:2022 Information technology - Security techniques - Information security management systems - Guidance ISO/IEC 27004:2022 Information technology - Security techniques - Information security management systems - Monitoring measurement analysis and evaluation ISO/IEC 27005:2022 Information technology - Security techniques - Information security risk management ISO/IEC 27006:2022 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems [ISO/IEC 27007:2022 Information technology - Security techniques - Guidelines for information security management systems auditing]

最新問題: **125**

シナリオ7 :Webvueは、コンピュータソフトウェアの開発、サポート、保守を専門とする日本を拠点とするテクノロジー企業です。Webvueは、さまざまなテクノロジー分野や企業向けにソリューションを提供しています。同社の主力サービスはCloudWebvueで、ストレージ、ネットワーク、仮想コンピューティングサービスを提供する包括的なクラウドコンピューティングプラットフォームであり、企業ユーザーと個人ユーザー向けに設計されています。CloudWebvueは、その柔軟性、拡張性、信頼性で高い評価を得ています。

Webvueは、ISO/IEC 27001認証の範囲にCloudWebvueのみを含めることを決定しました。そのため、フェーズ1とフェーズ2の監査は同時に実施されました。Webvueは、資産の機密性に対する厳格な管理を誇りとしています。CloudWebvueに保存されている情報を保護するために、適切な暗号化制御を使用しています。内部使用、制限付き、機密など、あらゆるレベルの情報は、クラウドに保存される前に固有のハッシュ値で暗号化されます。監査チームは、Keith、Sean、Layla、Sam、Tinaの5名で構成されました。ITおよび情報セキュリティ監査チームで最も経験豊富な監査員であるKeithが監査チームリーダーを務めました。彼の責任には、監査の計画と監査チームの管理が含まれていました。SeanとLaylaは、プロジェクト計画、ビジネス分析、ITシステム（ハードウェアとアプリケーション）に関する豊富な経験を持っています。彼らのタスクには、Webvueの内部システムとプロセスに基づいた監査計画の策定が含まれていました。一方、SamとTinaは最近学業を修了し、日々のタスクを処理しながら監査スキルを向上させる責任を負っていました。ISO/IEC 27001の附属書Aにおける暗号化の使用に関する管理項目8.24への準拠を関係者へのインタビューを通じて検証した結果、監査チームは、暗号化キーが当初、乱数ビット生成器（RNG）およびその他の鍵生成に関するベストプラクティスに基づいて生成されていたことを発見した。Webvueの暗号化ポリシーを確認した結果、インタビューで得られた情報は正確であると結論付けた。しかし、ポリシーに暗号化キーの使用方法和ライフサイクルが明記されていなかったため、これらのキーは引き続き使用されていた。Webvueと認証機関の間で後に合意された内容に基づき、監査チームは仮想監査を選択し、認証範囲と監査目標を満たすために、WebvueがISO/IEC 27001規格の管理要件8.11（データ匿名化）に準拠しているかどうかを検証することに重点を置きました。監査チームはCloudWebvueの内部データ保護プロセスをレビューし、同社がポリシーと規制基準をどのように遵守しているかに焦点を当てました。監査プロセスの一環として、監査チームリーダーのKeithは、Webvueの慣行の有効性を文書化および分析するために、関連文書と暗号化キー管理プログラムのスクリーンショットをキャプチャしました。

Webvueはテストに生成されたテストデータを使用しています。しかし、品質保証マネージャーへのインタビューと部門のプロセスに基づく、リアルタイムのシステムデータが使用される場合もあります。これにより大量のデータが生成されますが、より正確な結果が得られます。テストデータの保護と管理は、監査中に暗号化プロセスをシミュレートしたWebvueの担当者によって検証されました。品質保証マネージャーへのインタビューで、キースは、セキュリティトレーニング部門の従業員が適切な手順に従っていないことを発見しました。この部門は監査範囲外でしたが、セキュリティトレーニング部門の不遵守は、監査範囲内のプロセス、特にCloudWebvueのデータセキュリティと暗号化の実践に影響を与える可能性があります。そのため、キースはこの発見を監査レポートに含め、被監査者に通知しました。

上記のシナリオに基づいて、以下の質問に教えてください。

質問：

シナリオ7に基づき、監査チームはWebvueの暗号化戦略を検証し、インタビューで得られた情報の信頼性を合理的に確保しました。どのような監査手順が用いられましたか？

- A. 観察
- B. 裏付けとなる証拠
- C. 評価

Answer: B ([メッセージを残す](#))

Comprehensive and Detailed In-Depth Explanation:

- * B. Correct answer:
 - * Corroboration is the process of validating verbal statements with documented evidence.
 - * ISO 19011:2018 emphasizes cross-verification of audit evidence to ensure accuracy.
- * A. Incorrect:
 - * Observation involves witnessing real-time processes, but here, the audit team compared interview data with documentation.
- * C. Incorrect:
 - * Evaluation assesses compliance with criteria, but corroboration focuses on evidence validation.

Relevant Standard Reference:

- * ISO 19011:2018 Clause 6.4.7 (Corroboration of Audit Evidence)

最新問題: 126

シナリオ9 :UpNetはISO/IEC 27001認証を取得したインターネット企業です。

ISO/IEC 27001認証取得以来、当社の認知度は著しく向上しました。この認証は、UpNefsの事業運営の成熟度と、広く認知され受け入れられている規格への準拠を証明するものです。

しかし、認証はそこで終わりではありません。UpNetは、内部監査を通じて、セキュリティ管理とISMS全体の有効性および効率性を継続的に見直し、強化しています。経営陣は専任の内部監査チームを雇用することに消極的だったため、内部監査機能を外部委託することにしました。この形式の内部監査は、独立性と客観性を確保し、ISMSの継続的な改善のための助言サポートを提供します。

最初の認証監査後まもなく、同社はデータおよびストレージ製品を専門とする新部門を設立した。この部門では、データセンター向けに最適化されたルーターやスイッチ、ネットワーク仮想化やネットワークセキュリティ機器などのソフトウェアベースのネットワーク機器を提供している。これにより、既にISMS認証の対象となっていた他の部門の業務にも変更が生じた。

そのため、UpNetはリスク評価プロセスと内部監査を開始しました。内部監査の結果に基づき、同社は既存および新規のプロセスと管理体制の有効性と効率性を確認しました。

新設された部署がISO/IEC 27001の要件を満たしていたため、経営陣は認証範囲に含めることを決定しました。UpNetは、会社全体を対象とするISO/IEC 27001認証を取得したことを発表しました。

最初の認証監査から1年後、認証機関はUpNefsのISMS（情報セキュリティマネジメントシステム）に対する別の監査を実施した。

この監査は、UpNefsのISMSが規定のISO/IEC 27001の要求事項に準拠しているかどうかを判断し、ISMSの継続的な改善を確保することを目的としていました。監査チームは、認証済みのISMSが引き続き規格の要求事項を満たしていることを確認しました。しかしながら、新設された部署はマネジメントシステムのガバナンスに大きな影響を与えており、さらに認証機関にはこれらの変更について一切通知されていませんでした。そのため、UpNefsの認証は一時停止されました。

上記のシナリオに基づいて、以下の質問に答えてください。

シナリオ9に基づく、UpNefsの認証が停止された理由は何だったのでしょうか？

- A. UpNetは、その範囲を超えて認証を使用および適用しているためです。
- B. UpNetは内部監査機能を外部委託したため
- C. UpNefs ISMS は標準要件を満たしていないためです。

Answer: A ([メッセージを残す](#))

UpNetの認証は、認証機関が新設部署による重大な変更、すなわちマネジメントシステムのガバナンスに影響を与える変更について通知を受けていなかったため、一時停止されました。ISO/IEC 27001では、組織はISMSに重大な影響を与える変更について認証機関に通知することが義務付けられています。

最新問題: 127

シナリオ3 :Rebuildyはバンコクを拠点とする建設会社で、住宅の設計、建設、保守を専門としています。機密性の高いプロジェクトデータと顧客情報のセキュリティを確保するため、RebuildyはISO/IEC 27001に基づく情報セキュリティマネジメントシステム (ISMS)を導入することを決定しました。これには、情報セキュリティリスクの包括的な理解、継続的改善のための明確な方法論、そして堅牢なビジネスソリューションが含まれます。情報セキュリティマネジメントシステム (ISMS)の導入結果を以下に示します。

情報セキュリティは、一連のセキュリティ対策を適用し、ポリシー、プロセス、手順を確立することによって実現されます。

安全管理措置はリスク評価に基づいて実施され、リスクを排除するか、許容可能なレベルまで低減するように設計されています。

すべてのプロセスは、情報セキュリティ管理システムの継続的な改善を確実にするために、計画・実行・評価・改善 (PDCA)モデルに基づいています。

情報セキュリティポリシーは、最良のセキュリティ慣行に基づいて作成されたセキュリティマニュアルの一部であるため、独立した文書ではありません。

各従業員の職務記述書には、情報セキュリティに関する役割と責任が明確に定義されています。

情報セキュリティマネジメントシステムの経営陣によるレビューは、計画された間隔で実施されます。

2回の中間経営レビューと年次内部監査を経て、Rebuildyは認証を申請しました。認証監査の前に、Rebuildyの元従業員が監査チームに連絡を取り、Rebuildyが隠蔽しようとしている複数のセキュリティ問題について報告しました。元従業員は監査チームに書面による証拠を提出しました。Rebuildyの主要顧客であるElectraも同じ問題について証拠を提出しましたが、監査チームは元従業員の証拠ではなくElectraの証拠を採用することにしました。監査完了前に、監査チームは監査中に発見されたコンプライアンス違反について話し合うため、Electraと連絡を取り続けました。Electraはこれらの調査結果を裏付ける補足証拠を提出しました。

監査は、監査チームが上級管理職へのインタビューを行うことから始まった。インタビューでは、情報セキュリティマネジメントシステム (ISMS)の導入に対する上級管理職の取り組みについて議論した。インタビューから得られた証拠は文書化され、RebuildyがISO/IEC 27001規格の特定の規定に準拠しているかどうかを判断した。Electraから入手した文書証拠と不適合報告書は、監査報告書に添付された。特定された不適合項目は以下のとおりである。

同社の財務報告システムが、不適切なユーザーアクセス制御設定を検出しました。

同社はまだ独立した情報セキュリティ戦略を策定していない。その代わりに、セキュリティに関するベストプラクティスに基づいたセキュリティマニュアルを使用している。

監査チームから文書を受け取った後、チームリーダーはRebuildyの経営陣と面談し、監査結果を報告した。監査チームは、財務報告システムに関する問題と、独立した情報セキュリティポリシーの欠如を報告した。経営陣は監査結果に不満を表明し、監査チームリーダーの行動はプロ意識に欠けると示唆し、リーダーの交代を要求する可能性を示唆した。プレッシャーを受けた監査チームリーダーは、経営陣と協力して、特定された違反の深刻度を軽視することにした。そのため、監査チームリーダーは報告書を改訂し、より好ましい内容にすることで、Rebuildyのコンプライアンス問題の真の深刻さを歪曲した。

上記のシナリオに基づいて、以下の質問に答えてください。

質問：

監査人が、元従業員から提供された証拠よりも、エレクトラ社から提供された証拠を優先的に保持することは妥当でしょうか？

A. いいえ、元従業員が提供する証拠は、顧客が提供する証拠よりも常に信頼性が高いからです。

B. いいえ、両方の証拠源は等しく保存され、評価されるべきです。

C. はい、クライアントの証拠は独立性があるため、より信頼性が高いとみなされるからです。

Answer: B (メッセージを残す)

包括的かつ詳細な解説：

* B. 正解: ISO 19011:2018 (マネジメントシステムの監査に関するガイドライン) では、すべての証拠は平等に扱われ、関連性、信頼性、客観性に基づいて評価されなければならないと規定されています。

* どちらか一方を優先するのではなく、両方の情報源を保持し、検討し、検証すべきだった。

* A. 不正解:

* A former employee may have insider knowledge, but their credibility must be verified-it is not inherently more reliable.

* C. Incorrect:

* While a client is independent, their evidence is not automatically more credible than a former employee's.

Relevant Standard Reference:

* ISO 19011:2018 Clause 6.4.7 (Collecting and Verifying Information)

最新問題: **128**

以下の記述を検討し、誤っているものを2つ選びなさい。

- A. 仮想監査の前に技術的なチェックを行うことで、監査の有効性と効率性を向上させることができます。
- B. バーチャル監査中は、被監査者がインタビュー中にウェブカメラをオンにしておくことを強くお勧めします。
- C. 第三者監査に割り当てられる日数は、被監査者の利用可能な時間によって異なります。
- D. 機密保持とセキュリティ上の理由から、仮想監査中の画面共有は、監査チームが被監査者の文書を確認するために使用する方法です。
- E. オンサイト監査、バーチャル監査、または複合監査の選択は、過去の実績と過去の監査結果を考慮に入れる必要があります。
- F. オンサイト監査を実施する権限を持つ監査員は、必要なスキルに大きな違いがないため、バーチャル監査のための追加トレーニングは必要ありません。

Answer: C,F (メッセージを残す)

第三者監査に割り当てられる日数は、被監査者の都合ではなく、監査範囲、目的、基準、リスク、およびリソースを考慮した監査プログラムによって決定されます12。被監査者の都合は、監査計画とスケジュールに影響を与える要因の1つにすぎませんが、監査期間には影響しません3。オンサイト監査の実施が承認された監査人は、必要なスキルセットに大きな違いがあるため、仮想監査のための追加トレーニングを受ける必要があります。仮想監査は、コミュニケーション、テクノロジー、セキュリティ、証拠収集など、オンサイト監査とは異なる課題と機会をもたらします4。監査人は、リモート監査を実施するためのツールとテクニック、および仮想環境で期待される倫理的および専門的な行動に精通している必要があります。参照:

PECB候補者ハンドブック - ISO 27001主任審査員、18ページ

ISO 19011:2018、マネジメントシステムの監査に関する指針、5.3.2項 ISO 19011:2018、マネジメントシステムの監査に関する指針、6.3.1項 デロイト - 仮想内部監査の実施、1ページ

【効果的かつ効率的なリモート監査を実施するためのガイド】1ページ

[ISO 19011:2018、マネジメントシステムの監査に関する指針]、7.2.3項

【リモート監査のベストプラクティスと規制遵守のためのチェックリスト】、1ページ目

最新問題: 129

あなたは経験豊富なISMS監査チームリーダーで、現在研修中のチームに配属された監査担当者と話しています。あなたは、彼らが情報セキュリティ管理システムの運用において、PDCAサイクルの監査フェーズの重要性を理解していることを確認したいのです。

これは、文を最も適切に完成させる単語を彼に選ばせることで行うことができます。

文を適切な単語で完成させるには、完成させたい空欄をタップして赤くハイライト表示し、下の選択肢から適切なテキストをタップしてください。または、選択肢を適切な空欄にドラッグすることもできます。

The purpose of is to the information security management system at intervals to ensure it's continuing , adequacy and effectiveness.

planned

assess

Risk Assessment

efficiency

suitability

review

Risk Management

regular

Management Review

random

Answer:

Explanation:

レビューは、ISO規格に準拠した情報セキュリティマネジメントシステム (ISMS)の導入と改善のための4段階モデルであるPDCAサイクル（計画実行 評価 改善）の第3段階です。

1/IEC 27001:202212. レビューでは、確立されたポリシー、目標、基準に照らしてISMSのパフォーマンスを評価および測定します12。

- * 「評価する」とは、ISMS をレビューする行為を表す動詞です。評価するとは、体系的かつ客観的な方法で何かを評価、分析、または測定することを意味します 3。ISMS の評価には、監査証拠の収集と検証、強みと弱みの特定、適合度または不適合度の判定が含まれます 12。
 - * 「定期的」とは、ISMS の見直しの頻度や間隔を表す形容詞です。定期的とは、固定された、または一定の間隔で発生するか、または実行されることを意味します 4。ISMS を定期的に見直すということは、組織のニーズとリスクに応じて、毎年、四半期ごと、または毎月など、定期的に内部監査とマネジメントレビューを実施することを意味します 12。
 - * 適合性とは、ISMS のレビューの質や結果を説明する属性の 1 つです。適合性とは、特定の目的、人、または状況に適切または適合していることを意味します 5。ISMS の適合性をレビューするとは、組織の戦略的方向性、ビジネス目標、および情報セキュリティ要件 12 と整合していることを確認することです。
- 参考文献：
- * ISO/IEC 27001:2022 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項
 - * ISO/IEC 27003:2022 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－ガイダンス
 - * 評価する | Merriam-Websterによる評価の定義
 - * レギュラー | メリアム・ウェブスターによるレギュラーの定義
 - * 適合性 | メリアム・ウェブスター辞典による適合性の定義

最新問題: 130

情境 4

SendPay是一家金融服務公司，專注於透過代理商和機構網路提供全球匯款服務。作為市場新秀，SendPay致力於提供優質服務，其去年推出的免手續費數位平台讓客戶可以隨時隨地透過智慧型手機和筆記型電腦收發款項。當時，SendPay將軟體營運外包給外部團隊，該團隊也負責管理公司的技術基礎設施。

最近，該公司在實施資訊安全管理系統(ISMS) 近一年後，申請了ISO/IEC 27001 認證。

在審計過程中，審計人員重點審計了SendPay 的外包業務，特別是外包公司負責的軟體開發和技術基礎設施維護。

他們採取了一套結構化的方法，其中包括審計和評估SendPay用於監控外包業務品質的流程。這包括核實該公司是否履行了合約義務，確保其在聘用外包實體方面擁有適當的管理程序，以及評估SendPay在預期或意外終止外包協議的情況下所採取的應對措施。

然而，審計人員委婉地指出，SendPay的協議並未充分考慮到外包協議意外取消的情況。此外，SendPay委派的技術專家協助審計人員，提供了與受審計外包業務相關的專業知識和經驗。

審計團隊計算了員工接受資訊安全管理系統 (ISMS) 培訓的小時數，以確保其符合既定目標。他們也基於審計期間抽取的樣本，計算了資訊安全事件的平均解決時間，從而深入了解了SendPay 的事件管理實務。此外，審計人員還評估了審計期間收集的證據的可靠性。他們考慮了影響審計證據可靠性的多個因素。例如，與照片相比，監視錄影提供的證據更為客觀。時間因素也對可靠性有著至關重要的作用，交易記錄等機制可以增強證據的可信度。

SendPay 使用雲端平台來提高營運效率和可擴展性。然而，由於資源限制，審計人員在審計過程中並未要求SendPay 提供其雲端活動清單，而是依賴SendPay 的陳述。

問題

在審計過程中，審計人員使用了哪些類型的證據來驗證SendPay資訊安全管理系統的各個面向？請參考情境4。

- A. 分析證據
- B. 數學證據
- C. 技術證據

Answer: A ([メッセージを残す](#))

The correct answer is Analytical evidence, because the auditors relied heavily on analysis, calculations, and evaluation of performance data to validate the effectiveness of SendPay's ISMS. Analytical evidence involves examining trends, metrics, ratios, averages, and performance indicators to draw conclusions about how well processes are functioning.

In the scenario, the auditors calculated the number of training hours employees received on ISMS topics and computed the average resolution time of information security incidents based on sampled data. These activities are clear examples of analytical techniques, as they involve processing numerical and performance-related information to assess alignment with objectives and effectiveness of controls. Additionally, the auditors assessed the reliability of evidence by comparing different sources and considering timing factors, which further supports the use of analytical judgment rather than purely technical inspection.

Option B is incorrect because mathematical evidence is not a recognized audit evidence category under ISO standards. While calculations were performed, the purpose was analytical evaluation, not mathematical proof.

Option C is incorrect because technical evidence would primarily involve direct inspection of systems, configurations, or infrastructure, such as firewall rule reviews or system settings. While some technical elements existed in the audit, the question focuses on the type of evidence used to validate ISMS performance broadly, which was predominantly analytical.

Therefore, analytical evidence best describes the evidence utilized by the auditors during SendPay's audit.

最新問題: 131

OrgXYはISO/IEC 27001認証を取得したソフトウェア開発会社です。認証取得から1年後、OrgXYの経営陣は認証機関に対し、同社はまだサーベイランス監査を実施する準備ができていないと伝えました。このような場合、どのような事態が発生するでしょうか？

- A. 認証が一時停止されました。
- B. 現在の認証は、次回の監視監査まで引き続き使用されます。
- C. OrgXYは登録を別の認証機関に移管しました。

Answer: A (メッセージを残す)

OrgXYのような組織が、予定通りに監視監査を実施する準備ができていないことを認証機関に通知した場合、認証が一時停止される可能性があります。これは、監視監査が継続的な認証維持の重要な部分であり、規格への継続的な準拠を確保するために必要なものだからです。

参考文献 :PECB ISO/IEC 27001主任審査員コース教材、ISO/IEC 27001:2013、認証および監視要件に関する一般ガイドライン

最新問題: 132

認証監査における監査チームの法務技術専門家の責任として、以下の2つの選択肢のうち1つを選択してください。

- A. 被監査者の法的知識を評価する
- B. 組織の法令遵守問題に対する批判
- C. 被監査者と複雑な法的問題について議論する。
- D. 監査チームに法的チェックポイントに関する推奨事項を提供する。
- E. 組織の法的地位を確認する
- F. 組織の法律代理人との面談

Answer: D,E (メッセージを残す)

A legal technical expert (LTE) is a person who provides specific knowledge or expertise related to the legal aspects of the information security management system (ISMS) during a certification audit. The LTE is not an auditor, but a member of the audit team who supports the auditors in collecting and evaluating the audit evidence. The LTE is not responsible for evaluating the auditee's legal knowledge, criticising the organisation's legal compliance issues, or debating complex legal points with the auditee, as these tasks may be beyond the scope of the audit, or may compromise the objectivity and impartiality of the audit. The LTE is responsible for advising on legal checkpoints for the audit team, such as the applicable legal, regulatory, and contractual requirements, the relevant sources of information, the methods of verification, and the criteria of evaluation. The LTE is also responsible for verifying the legal status of the organisation, such as the registration, licensing, authorisation, or accreditation of the organisation, and the compliance with the relevant laws and regulations. Reference:

What is the role of a technical expert in ISO audit?

Roles, Responsibilities & Authorities for ISO 27001 5.3

Guide to Become an ISO 27001 Lead Auditor

最新問題: 133

次のうち、利害関係者の定義はどれですか？

- A. 第三者が、決定や活動によって影響を受けたと考える場合、組織に苦情を申し立てることができます。
- B. 意思決定や活動に影響を与えることができる個人または組織、意思決定や活動によって影響を受ける個人または組織、あるいは意思決定や活動によって影響を受けていると信じている個人または組織。
- C. 経営上の意思決定に干渉できる、または経営上の意思決定によって干渉されていると考えるグループまたは組織。
- D. 意思決定や活動を制御できる個人または組織、意思決定や活動によって制御される個人または組織、または意思決定や活動によって制御されていると信じている個人または組織。

Answer: (解答を表示する)

これは、ISO 27001:2013、3.16項に基づく利害関係者の定義です。利害関係者とは、基本的にステークホルダー、つまり情報セキュリティマネジメントシステム (ISMS) またはその活動に影響を与えたり、影響を受けたりする個人または組織のことです。利害関係者はISMSに関して異なるニーズや期待を持つ可能性があり、組織はこれらを特定し、対処する必要があります。参照：

ISO/IEC 27001:2013、情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項、3.16項 PECB候補者ハンドブック ISO 27001主任審査員、10ページ ISO 27001 ISMSに対する利害関係者とその期待の特定 ISO 27001の利害関係者の例

最新問題: 134

監査の実施前に、被監査者と監査チームがリモートアクセスプロトコルについて合意する必要がある監査の種類はどれですか？

- A. バーチャル
- B. 内部
- C. 外部

Answer: A (メッセージを残す)

包括的かつ詳細な徹底分析

A. 正解：

仮想監査では、データレビューのための安全で承認された接続を確保するために、事前に定義されたりリモートアクセスプロトコルが必要です。

ISO 19011:2018は、仮想監査におけるセキュリティ対策に関するガイドラインを提供する。

B. 不正解：

内部監査ではリモートアクセスを使用することができますが、同意は必須ではありません。

C. 不正解：

外部監査ではリモートアクセスが伴う場合があるが、必ずしも事前に合意しておく必要はない。

関連規格参照：

最新問題: 135

當應用於 ISO 19011 中所述的口部稽核計畫管理流程時，哪兩項活動與計畫執行檢口行動循環的「檢口」階段一致？

- A. 保留口部審核記錄
- B. 定義每次口部審核的審核標準和範圍
- C. 更新口部審核計劃
- D. 建立基於風險的口部稽核計劃
- E. 進行口部審核
- F. 驗證口部稽核計畫的有效性
- G. 檢討口部稽核結果的趨勢

Answer: F,G (メッセージを残す)

PDCAサイクルのチェック段階では、プロセスのパフォーマンスを監視および測定し、計画された目標および基準と比較します。内部監査プログラムの管理においては、この段階では、内部監査プログラムが目標、範囲、基準を満たしているか、またISO 19011ガイドライン1に従って実施されているかを評価することにより、プログラムの有効性を検証します。また、監査結果、不適合、是正措置、改善の機会、顧客からのフィードバック1など、監査から収集したデータを分析することにより、内部監査結果の傾向をレビューします。参考文献 :ISO 19011:2018 - マネジメントシステムの監査に関するガイドライン

最新問題: 136

シナリオ2：

1990年代に設立されたClinicは、心臓病治療と複雑な外科手術を専門とする医療機器メーカーです。ヨーロッパに本社を置き、患者と医療従事者にサービスを提供しています。Clinicは、患者データを収集して、個別の治療計画の策定、治療効果のモニタリング、機器機能の向上を図っています。データセキュリティを強化し、信頼を築くため、ClinicはISO/IEC 27001に基づく情報セキュリティマネジメントシステム (ISMS)を導入しています。これは、機密性の高い患者情報と独自の技術を安全に管理するというClinicの強い決意を示すものです。

当クリニックは、情報セキュリティマネジメントシステム (ISMS)の適用範囲を、内部の問題、インターフェース、内部活動と外部委託活動間の依存関係、および利害関係者の期待のみを考慮して決定しています。この適用範囲は文書化され、詳細に公開されています。ISMSを定義するにあたり、当クリニックは研究開発、患者データ管理、顧客サポートといった主要部門の主要プロセスに焦点を当てることを選択しました。

当初は困難に直面したものの、クリニックは情報セキュリティマネジメントシステム（ISMS）の導入を継続し、セキュリティ対策を独自のニーズに合わせて調整しました。プロジェクトチームは、ISO/IEC 27001規格の附属書Aから特定の対策を除外する一方で、業界固有の対策を取り入れることでセキュリティを強化しました。チームは、これらの対策の適用可能性を内部要因と外部要因の両方の観点から評価し、最終的に、対策の選択と導入の根拠を詳細に記した包括的な適用性宣言書（SoA）を作成しました。

認定取得に向けた準備が進むにつれ、チームリーダーに任命されたブライアンは、積極的なリスク評価手法を用いて、会社の戦略的な課題とセキュリティ対策を特定して評価した。この積極的なアプローチにより、クリニックのリスク評価が目標と使命に合致することが保証された。

質問：

当該クリニックのSoA（So-A）文書は、ISO/IEC 27001のSoAに関する要件に準拠していますか？

A. はい、ISO附属書Aには適用可能なすべての管理策の詳細なリストが含まれているからです。

ISO/IEC 27001およびその他の情報源

B. いいえ、ISO/IEC 27001の附属書A以外の情報源から選択された安全管理策が含まれているためです。

C. いいえ、ISO/IEC Annex A から特定の管理策を除外する理由が含まれていないためです。

27001

Answer: C (メッセージを残す)

包括的かつ詳細な解説：

適用性に関する声明書（SoA）は、ISO/IEC 27001:2022において必須の文書であり、附属書Aに記載されているすべての管理策、それらの適用範囲、および含めるまたは除外する理由を一覧にしたものです。

* C. 正解：SoAには、附属書Aの管理策を除外する理由を記載する必要があります。シナリオでは、プロジェクトチームが特定の管理策を除外したと述べられていますが、その理由が文書化されているとは述べられていません。これは、除外理由を文書化することを義務付けているISO/IEC 27001の6.1.3項（情報セキュリティリスクの取り扱い）に違反します。

* A. 誤り：SoAには管理策の網羅的なリストを含める必要がありますが、除外が正当化されない限り、附属書Aやその他の資料から適用可能な管理策を単にリストアップするだけでは要件を満たしません。

* B. 誤り：他のソースからのセキュリティ制御を含めることは許可されており、組織はリスク評価に基づいて附属書A以外の追加の制御を定義できるため、SoAを無効にするものではありません。

したがって、クリニックのSoAは、附属書Aの管理策を除外する正当な理由を示していないため不完全であり、ISO/IEC 27001の要求事項に準拠していません。

有効な **ISO-IEC-27001-Lead-Auditor-CN** 問題集は GoShiken.com が提供された合格しやすい ISO-IEC-27001-Lead-Auditor-CN 試験問題集！ GoShiken.com が最新の **ISO-IEC-27001-Lead-Auditor-CN** 試験問題集を提供しています。GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 問題集をゲットする人はこちら：
<https://www.goshiken.com/PECB/ISO-IEC-27001-Lead-Auditor-CN-mondaishu.html> (**41830%OFF**問題集溶と正解付きで **30%**w 特別割引コード: **Freepdfdumps**)

最新問題: 137

あなたは経験豊富なISMS監査チームリーダーで、研修中の監査員を指導しています。彼女は、不適合の分類に関する具体的な基準を策定することがなぜ重要なのかをあなたに尋ねます。

次の回答のうち、正しいものはどれですか？

なぜなら、評価基準は組織全体における不適合を評価するための共通の基準を提供するからである。

A. ISO/IEC 27001:2022にこの要求事項があるからです。

B. 採点基準の開発と実施は、是正措置プロセスに高い重要性が置かれていることを示しているからです。

C. 採点基準により、すべての監査員が不適合をまったく同じ方法で採点することが保証されるためです。

Answer: A (メッセージを残す)

正解はAです。なぜなら、評価基準は組織全体における不適合の評価のための共通基盤を提供するからです。評価基準とは、不適合の重大度や影響を定義する規則や基準であり、適切な是正措置やフォローアップ活動を決定するのに役立ちます。

評価基準は、以下のようないくつかの理由から重要です。

* 不適合の評価および報告において一貫性と客観性を確保し、主観的または恣意的な判断を避ける。

* これらは、監査人、被監査者、および監査クライアント間の不適合に関するコミュニケーションと理解を促進し、異なるプロセス、機能、または場所間での不適合の比較とベンチマークを可能にします。

- * 不適合の解決のためのリソースの優先順位付けと配分、および是正措置の有効性の監視と測定を支援します。
- * これらは、組織がISMSの継続的な改善、およびISMSの要件と期待事項への準拠に尽力し、責任を負っていることを示すものです。

参考文献：

ISO/IEC 27001:2022、情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステム - 要求事項1 PECB 候補者ハンドブック ISO/IEC 27001 主任監査員2 ISO 27001:2022 主任監査員 - PECB3 ISO 27001:2022 認定ISMS 主任監査員 - Jisc4 ISO/IEC 27001:2022 主任監査員移行トレーニングコース5 ISO 27001 - 情報セキュリティ主任監査員コース - PwC トレーニングアカデミー ISO 19011:2022、マネジメントシステムの監査に関するガイドライン

最新問題: 138

質問：

認証機関の複数の部署が関与する場合、どのような点を確保する必要がありますでしょうか？

- A. 各事務所は、顧客と個別の法的拘束力のある契約を結んでいます。
- B. 認証の対象となるすべてのサイトを対象とする法的拘束力のある契約。
- C. 本社と顧客のみが法的拘束力のある契約を締結しています。

Answer: B ([メッセージを残す](#))

包括的かつ詳細な解説：

- * B. 正解:
- * 認証範囲に含まれるすべてのサイトを網羅する、法的拘束力のある単一の契約書を作成し、以下の事項を確実にする必要があります。
- * 監査手法の一貫性
- * 全ての当事者間の法的明確性
- * 多国籍企業にとってグローバルな適用性

* A. 不正解:

各オフィスごとに個別の契約を結ぶと、矛盾が生じ、法的にも複雑化する。

* C. 不正解:

* 認証に関わるすべての拠点が契約の対象となり、本社だけでは不十分です。

関連規格参照：

- * ISO/IEC 17021-1:2015 条項 8.2.1（認証に関する法的拘束力のある合意）

最新問題: 139

あなたは、医療サービスを提供する高齢者向け介護施設でISMS監査を実施しています。監査計画の次のステップは、情報セキュリティインシデント管理プロセスを検証することです。ITセキュリティマネージャーは、情報セキュリティインシデント管理手順書（文書参照D ISMS_L2_16、バージョン4）を作成しました。

あなたは文書を確認し、情報セキュリティ上の脆弱性、インシデント、およびインシデントは、特定後1時間以内に連絡担当者（PoC）に報告する必要があります」という記述に気づきました。従業員への聞き取り調査を行ったところ、脆弱性」、インシデント」、インシデント」という用語の意味について、従業員によって理解が異なることがわかりました。

ITセキュリティマネージャーは、6か月前にオンラインの「情報セキュリティ対応」研修ワークショップが開催されたと説明した。参加者全員が参加し、報告演習とコース評価に合格した。

監査証拠をさらに収集するために、他の領域についても調査を進めたいと考えています。有効な監査証拠ではないものを3つ選択してください。

- A. 情報セキュリティ障害発生時に情報セキュリティを維持するために、情報セキュリティインシデントに対して脆弱な領域をどのように隔離するかを理解するため、より多くの証拠を収集する（制御措置A.5.29に関連）。
- B. 適切な経路を通じて情報セキュリティインシデントを報告する方法に関する証拠をさらに収集する（管理措置A.6.8に関連）
- C. 組織が情報セキュリティインシデント対応訓練をどのように実施しているか、またその有効性をどのように評価しているかについて、より多くの証拠を収集する。（第2項に関連）
- D. 組織が情報セキュリティインシデントから学び、改善していくための方法について、より多くの証拠を収集する。（管理策A.5.27に関連）
- E. 組織が脆弱性監視のための連絡窓口（PoC）をどのように管理しているかについて、より多くの証拠を収集する。セクション8.1に関連）

F. 組織が事業継続計画をどのようにテストしているかについて、より多くの証拠を収集する。（管理策A.5.30に関連）

G. 情報セキュリティポリシーに用語と定義が含まれているかどうかについて、さらに証拠を収集する。（管理策.32に関連）

H. ISO 27035（情報セキュリティインシデント管理）を内部監査基準として使用すべきかどうかを判断するために、さらなる証拠を収集する。 §.13項に関連）

Answer: E,G,H (メッセージを残す)

有効な監査証拠とはみなされない3つの選択肢は以下のとおりです。

組織が脆弱性を監視する連絡窓口（PoC）をどのように管理しているかについて、より多くの証拠を収集する。（条項.1に関連）

情報セキュリティポリシーに用語と定義が含まれているかどうかについて、さらに証拠を収集してください。
（管理項目.32に関連）

*ISO 27035（情報セキュリティインシデント管理）が内部監査基準として使用されているかどうかを判断するために、より多くの証拠を収集してください。 §.13項に関連）これらのオプションは、監査の焦点である情報セキュリティインシデント管理プロセスに直接関連していないため、有効な監査証拠ではありません。監査証拠は、監査の目的、範囲、および基準に関連している必要があります、監査結果と結論を裏付ける十分かつ信頼できる証拠を提供する必要があります1。

オプションEは無効です。PoCは情報セキュリティインシデント管理プロセスの一部ではなく、情報セキュリティインシデントを適切な当局に報告およびエスカレーションする責任を負う役割だからです2。監査証拠は、組織がPoCをどのように管理するかではなく、PoCがこの機能をどのように実行するかに焦点を当てるべきです。

オプションGは無効です。なぜなら、用語と定義は情報セキュリティインシデント管理プロセスの一部ではなく、組織の情報セキュリティの目的、原則、責任を定義する高レベルの文書である情報セキュリティポリシーの一部だからです3。監査証拠は、情報セキュリティポリシーに用語と定義が含まれているかどうかではなく、情報セキュリティポリシーがどのように伝達、実装、レビューされているかに焦点を当てるべきです。

オプションHは無効です。ISO 27035は情報セキュリティインシデント管理プロセスの一部ではなく、情報セキュリティインシデントを管理するためのベストプラクティスを提供するガイダンス文書だからです4。監査証拠は、組織がISO/IEC 27001の要件をどのように遵守しているかに焦点を当てるべきです。

情報セキュリティインシデント管理に関する2022年の基準であり、内部監査基準としてISO 27035を使用しているかどうかではない。

その他の選択肢は、情報セキュリティインシデント管理プロセスに関連しているため、有効な監査証拠であり、プロセスの適合性と有効性を評価するための有用な証拠を提供できます。例えば、次のようになります。

*オプションAは、情報セキュリティインシデントが発生した領域を隔離および検疫するための手順を確立し、さらなる損害を防ぎ、証拠を保全することを組織に求める管理策A.5.29に関連しているため、有効です。監査証拠では、組織がこれらの手順をどのように実装およびテストしているか、また、障害発生時に情報セキュリティの継続性をどのように確保しているかについての証拠を収集する必要があります。

*オプションBは、情報セキュリティイベントや脆弱性を報告するためのメカニズムを確立し、それらが組織内の適切なレベルにタイムリーに伝達されることを保証することを組織に求める管理策A.6.8に関連しているため、有効です。監査証拠には、組織がこれらのメカニズムをどのように定義して使用しているか、また報告プロセスをどのように監視およびレビューしているかについての証拠を収集する必要があります。

*オプションCは、組織が管理下にあるすべての人に情報セキュリティに関する意識向上、教育、トレーニングを提供し、これらの活動の有効性を評価することを義務付ける条項7.2に関連しているため、有効です。監査証拠には、組織が情報セキュリティトレーニングのニーズをどのように特定するか、トレーニングをどのように提供および記録するか、学習成果とフィードバックをどのように測定するかについての証拠を収集する必要があります。

*オプションDは、組織が情報セキュリティインシデントから学び、再発防止または影響軽減のための是正措置を実施することを要求する管理A.5.27に関連しているため、有効です8。

監査証拠には、組織が情報セキュリティインシデントの根本原因と結果をどのように分析し文書化しているか、是正措置をどのように特定し実施しているか、そしてこれらの措置の有効性をどのように検証しているかに関する証拠を収集する必要がある。

*オプションFは、重大な情報セキュリティインシデントが発生した場合に情報および情報処理施設が利用可能であることを保証するため、組織が事業継続計画を策定および維持することを義務付ける管理策A.5.30に関連しているため有効です9。監査証拠には、組織が事業継続計画をどのように策定および更新するか、計画をどのようにテストおよびレビューするか、計画について関係者にどのように伝達およびトレーニングするかについての証拠を収集する必要があります。

参照: 1: ISO 19011:2018、6.2;

2: ISO/IEC 27001:2022、A.6.8.1;

3: ISO/IEC 27001:2022、5.2;

4 :ISO/IEC 27035:2016、序論；

5: ISO/IEC 27001:2022、A.5.29;

6: ISO/IEC 27001:2022、A.6.8;

7: ISO/IEC 27001:2022、7.2;

8: ISO/IEC 27001:2022、A.5.27;

- 9: ISO/IEC 27001:2022、A.5.30;
- 10: ISO 19011:2018;
- 11: ISO/IEC 27001:2022;
- 12: ISO/IEC 27001:2022;
- 13: ISO/IEC 27035:2016;
- 14: ISO/IEC 27001:2022;
- 15: ISO/IEC 27001:2022;
- 16: ISO/IEC 27001:2022;
- 17: ISO/IEC 27001:2022;
- 18: ISO/IEC 27001:2022

最新問題: 140

文を最も適切に完成させる単語を選びなさい。

"In a third-party audit an indica at organisation is not required to take action."

To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

nonconformity

an observation

a recommendation

criteria

conformity

a finding

Answer:

"In a third-party audit an observation an indica conformity at organisation is not required to take action."

To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

nonconformity

an observation

a recommendation

criteria

conformity

a finding

Explanation:

第三者監査では、観察事項は組織の適合性を示すことができますが、是正措置を講じる必要はありません。」PECB候補者ハンドブック1によると、観察事項とは「監査中に述べられ、客観的な証拠によって裏付けられた事実の記述」です。観察事項は適合性または不適合性を示すことができますが、監査対象組織に是正措置を講じる必要はありません。一方、勧告は、「観察に基づいた改善提案」。勧告は、監査対象組織によって受け入れられる場合もあれば、受け入れられない場合もある。

基本原則－第三者監査」2によると、第三者監査とは「組織のプロセスおよび手順を監査する法的権利を有する外部組織によって実施される監査」である。第三者監査の結果、監査結果（監査が収集した監査証拠に基づいて到達した結論）が示されることがある。

監査結果は、監査対象組織が監査基準を満たしているか否かによって、肯定的または否定的となる。不適合とは、「要求事項を満たしていないことを示す所見」である。不適合が認められた場合、監査対象組織は再発防止のために是正措置を講じる必要がある。

最新問題: 141

シナリオ4 :そのブランドプロモーション会社は、米国で最も有名な企業のいくつかと取引のあるマーケティング会社です。

社内コスト削減のため、Branding社は2年以上にわたり、ソフトウェア開発とITヘルプデスク業務をTechvology社にアウトソーシングしています。Techvology社は、Branding社のソフトウェア、ネットワーク、ハードウェアに関する要件を管理するために必要な専門知識を有しています。Branding社は情報セキュリティマネジメントシステム（ISMS）を導入し、ISO/IEC 27001認証を取得しており、高い情報セキュリティ基準を維持するという強い意志を示しています。Branding社は、アウトソーシング先のTechvology社の業務がISO/IEC 27001のセキュリティ要件を満たしていることを確認するため、定期的に監査を実施しています。

前回の監査では、ブランディングの監査チームは監査対象となるプロセスと監査計画を特定しました。テックボロジーが過去1年間に2件の情報セキュリティインシデントを報告したことを踏まえ、証拠に基づくアプローチを採用しました。監査は、これらのインシデントへの対応を評価し、アウトソーシング契約の条件を遵守していることを確認することに重点を置いています。監査は、提供されたサービスがブランディングの期待と確立された基準を満たしているかどうかを評価するために、テックボロジーのアウトソーシング業務の品質を監視する方法を包括的にレビューすることから始まりました。監査人はまた、テックボロジーが両当事者間の契約上の要件を遵守していることを確認しました。これには、情報セキュリティ対策を含むすべての側面を遵守していることを確認するために、アウトソーシング契約の条件を徹底的にレビューすることが含まれます。

さらに、今回の監査では、Techvologyのアウトソーシング業務およびその他の組織を管理するためのガバナンスプロセスについても厳格な評価が行われました。このステップはブランドプロモーションにとって非常に重要であり、アウトソーシング契約に伴う潜在的なリスクを軽減するための適切な管理および監督メカニズムが確立されているかどうかを確認するのに役立ちます。

監査担当者は、Techvology社の全階層の従業員に聞き取り調査を行い、インシデント対応記録を分析した。Techvology社は、従業員に対しインシデント管理に関する意識向上トレーニングを実施していたことを示す記録も提出した。収集した情報に基づき、監査担当者は、2件のサイバーセキュリティインシデントはいずれも従業員の能力不足が原因であると推測した。そのため、監査担当者は、関係する従業員の人事ファイルへのアクセスを要求し、関連する経験、資格、トレーニング記録などの能力を確認した。

ブランディング社の監査担当者は、入手した証拠の妥当性を厳密に評価し、受け取った記録の信頼性を損なったり、矛盾させたりする可能性のある証拠に対して常に警戒を怠りませんでした。テックボロジー社の監査においても、監査担当者はこの原則を遵守し、インシデント対応記録を厳密に評価するとともに、様々なレベルや職務の従業員に対して詳細なインタビューを実施しました。彼らはテックボロジー社の担当者の発言を鵜呑みにするのではなく、インシデント管理プロセスに関する主張を裏付ける具体的な証拠を求めました。

上記のシナリオに基づいて、以下の質問に答えてください。

質問：

シナリオ4に基づく、ブランド部門はどのような種類の監査を実施したか？

A. 自社監査

B. 第三者監査

C. 第三者監査

Answer: B ([メッセージを残す](#))

包括的かつ詳細な解説：

* B. 正解:

* 第三者監査とは、組織が契約上および規制上の要件を遵守していることを確認するために、サプライヤーまたは外部委託先のサービスプロバイダーに対して実施する監査のことです。

* Branding社は、アウトソーシングされたITサービスプロバイダーであるTechvology社を監査したため、これは第三者機関による監査となります。

* A. 不正解:

* ファーストパーティ監査は内部監査ですが、Techvologyは内部組織ではありません。

* C. 不正解:

* 第三者監査は独立した認証機関によって実施されますが、本件ではそうではありません。

関連規格参照：

* ISO 19011:2018 3.8項（監査の種類：第一者監査、第三者監査、第三者監査）

最新問題: 142

シナリオ 5: Cobt。ロンドンを拠点とする保険会社で、商業、産業、生命保険など幅広い保険ソリューションを提供しています。Cobt は近年、顧客数が大幅に増加しています。取り扱うデータ量が膨大であるため、ISO/IEC 27001 認証を取得することで情報セキュリティに多くのメリットがもたらされ、継続的な改善への取り組みを示すことができると考えています。同社は定期的なリスク評価を的確に実施していますが、ISMS を導入すると日々の業務に大きな変化が生じます。リスク評価プロセス中に、組織の内部統制が重大な欠陥を検出または防止できなかったリスクが特定されました。

同社はISMS導入のための方法論に従い、わずか数ヶ月で実用的なISMSを構築した。監査チームのメンバーにはそれぞれ責任が割り当てられた。

サラは、Cobtが多様な商業および保険ソリューションを提供することで著しい事業拡大を遂げた一方で、被監査者の確保や協力、証拠へのアクセスといった点において、依然として一部のプロセスが手作業に依存していることを認めた。今回のケースでは、Cobtの拒否により、監査の信頼性および合理的な保証を提供できる能力について疑問が生じた。これに対し、サラは認証契約に署名する前に監査から撤退することを決定し、Cobtおよび認証機関にその旨を通知した。この決定は、監査原則の遵守と透明性の維持を確実にするためであり、これらの原則を堅持するという彼女の一貫した姿勢を示すものである。

上記のシナリオに基づいて、以下の質問に答えてください。

シナリオ5によると、コブト社は、監査計画が監査範囲の最近の変更を正確に反映していないと述べています。サラはこの状況でどうすべきでしょうか？

A. 監査計画は、監査対象となる活動の状況と重要性を反映させる必要があるため、Cobtの要求に従って修正されました。

B. 当初の範囲で監査を継続してください。Cobt は、使用されているテクノロジーが最近変更された場合にのみ監査範囲の変更を要求できます。

C. 監査計画は、Cobt、Sarah、および認証機関が監査範囲の変更に同意した場合にのみ変更されるものとする。

Answer: C (メッセージを残す)

包括的かつ詳細な徹底分析

C . 正解: 監査範囲の変更は、被監査者、監査人によって承認されなければなりません。A . 不正解: 監査スケジュールは、監査人の要求だけで変更することはできません。承認が必要です。

B. 誤り：監査の範囲は技術的な変更に限らず、組織的および手続き的な変更も含まれます。

関連規格参照：

ISO 19011:2018 5.5.2項（監査範囲およびスケジュールの決定）

最新問題: 143

シナリオ2：

1990年代に設立されたClinicは、心臓病治療と複雑な外科手術を専門とする医療機器メーカーです。ヨーロッパに本社を置き、患者と医療従事者にサービスを提供しています。Clinicは、患者データを収集して、個別の治療計画の策定、治療効果のモニタリング、機器機能の向上を図っています。データセキュリティを強化し、信頼を築くため、ClinicはISO/IEC 27001に基づく情報セキュリティマネジメントシステム（ISMS）を導入しています。これは、機密性の高い患者情報と独自の技術を安全に管理するというClinicの強い決意を示すものです。

当クリニックは、情報セキュリティマネジメントシステム（ISMS）の適用範囲を、内部の問題、インターフェース、内部活動と外部委託活動間の依存関係、および利害関係者の期待のみを考慮して決定しています。この適用範囲は文書化され、詳細に公開されています。ISMSを定義するにあたり、当クリニックは研究開発、患者データ管理、顧客サポートといった主要部門の主要プロセスに焦点を当てることを選択しました。

当初は困難に直面したものの、クリニックは情報セキュリティマネジメントシステム（ISMS）の導入を継続し、セキュリティ対策を独自のニーズに合わせて調整しました。プロジェクトチームは、ISO/IEC 27001規格の附属書Aから特定の対策を除外する一方で、業界固有の対策を取り入れることでセキュリティを強化しました。チームは、これらの対策の適用可能性を内部要因と外部要因の両方の観点から評価し、最終的に、対策の選択と導入の根拠を詳細に記した包括的な適用性宣言書（SoA）を作成しました。

認定取得に向けた準備が進むにつれ、チームリーダーに任命されたブライアンは、積極的なリスク評価手法を用いて、会社の戦略的な課題とセキュリティ対策を特定 評価した。この積極的なアプローチにより、クリニックのリスク評価が目標と使命に合致することが保証された。

質問：

シナリオ2に基づく、クリニックの情報セキュリティ管理システム（ISMS）の適用範囲は正しく定義されているでしょうか？

A. いいえ、クリニックは外部要因も考慮する必要があります。

B. はい、クリニックの情報セキュリティ管理システムの範囲は正しく定義されています。

C. いいえ、クリニックの情報セキュリティ管理システムの範囲には、除外事項とその理由も含まれるべきです。

Answer: A (メッセージを残す)

包括的かつ詳細な解説：

* A. 正解: ISO/IEC 27001 の 4.1 項 (組織とその状況の理解) および 4.2 項 (利害関係者のニーズと期待の理解) では、組織は ISMS の範囲を定義する際に、内部と外部の両方の問題を考慮する必要があると規定されています。

* このシナリオでは、クリニックは内部の問題のみを考慮し、規制要件、業界標準、サイバーセキュリティの脅威などの外部要因を評価しなかったとされています。

* B. 誤り：外部要因が考慮されていないため、範囲が完全に正しくありません。

* C. 誤り：除外事項の正当化は、ISMS スコープ記述書ではなく、SoA が必要です。

外部要因を考慮していないため、当クリニックのISMSはISO/IEC 27001の要求事項を完全に満たしていません。

最新問題: 144

シナリオ3

NightCoreは、米国に拠点を置く多国籍テクノロジー企業で、電子商取引、クラウドコンピューティング、デジタルストリーミングメディア、人工知能（AI）を専門としています。情報セキュリティマネジメントシステム（ISMS）を導入してから1年以上が経過した時点で、NightCoreは認証機関にISO/IEC 27001認証監査の実施を依頼しました。

認証機関は5名の監査員からなるチームを編成し、ジャックがチームリーダーを務めた。ジャックは、リスク管理、情報セキュリティ対策、インシデント管理における豊富な監査経験で知られている。彼のスキルは監査の原則とプロセスに高度に合致しており、監査範囲を効果的に理解し、関連する基準を適用することが可能です。ジャックはまた、ナイトコアの組織構造、ミッション、経営慣行、および事業活動に適用される法的規制上の要件についても深い理解を示しました。

監査チームは、信頼性が高く再現性のある結論を体系的に導き出すために、合理的な監査手法に従います。チームは、ある程度検証可能な情報のみが有効な証拠とみなされることを認識しています。監査プロセスにおいて、まれに特定の情報の検証が困難な場合や検証可能性が低い場合、監査人は専門的な判断に基づいて、そのような証拠の信頼性を評価し、信憑性を判断します。

監査中、監査担当者は、NightCoreの情報セキュリティ管理システム（ISMS）の運用計画と管理に関する所見とレビューメモを記録しました。また、NightCoreの情報インベントリおよび関連資産に関する所見も記録しました。さらに、ネットワークサービス接続を保護するために実装されたファイアウォール構成についてもレビューを行いました。

審査プロセスが最終段階に入るにつれ、NightCoreが最高水準の情報セキュリティを維持するという強い意志がますます明らかになってきています。ISO/IEC 27001認証は容易に取得可能であり、NightCoreはこの認証を取得することで、テクノロジー業界における評判をさらに高めることができますでしょう。

質問

シナリオ3に基づくと、監査人は、ある程度しか検証できない情報を適切に処理したと言えるでしょうか？

- A. はい、なぜなら彼らは専門家の判断に基づいてその信頼性を評価したからです。
- B. いいえ、監査人は完全に検証できない情報はすべて無視すべきだからです。
- C. いいえ、監査人は外部の専門家に連絡して確認する必要があります。

Answer: A (メッセージを残す)

監査員は、部分的にしか検証できない情報を専門的な判断に基づいて適切に処理したため、選択肢Aが正解です。ISO 19011:2018では、監査は単なる機械的なプロセスではなく、監査員が証拠を評価する際に適切な専門的注意を払う必要があることを強調しています。監査証拠は多くの場合サンプルに基づいており、検証可能性の程度は様々です。重要な要件は、監査員が監査結論を裏付けるために証拠を使用する前に、その証拠の信頼性、関連性、および十分性を評価することです。

このシナリオでは、監査チームは一部の情報が限定的な範囲でしか検証できないことを明確に認識し、その情報にどの程度依存できるかを慎重に評価することで対応しました。これは、ISO 19011の原則、特に証拠に基づくアプローチと適切な職業的注意義務に合致しています。

監査人は、完全な検証が現実的でない場合には、証拠の限界を明確に理解し、その信頼性を過大評価しない限り、適切な判断を下すことが求められる。

選択肢Bは誤りです。ISO規格では、監査員が部分的にしか検証できない情報をすべて破棄することを義務付けていません。そうすると、監査結果が不完全になり、監査プロセスが非現実的なものになる可能性があります。選択肢Cも誤りです。特定の専門的なケースでは外部の専門家を起用することは可能ですが、ISO 19011では、証拠の検証が困難な場合に必ず外部の専門家の関与を義務付けているわけではありません。このシナリオにおける監査員の対応は、ISO監査ガイダンスに沿った適切な能力と専門的判断を示しています。

最新問題: 145

クライアントのデザインファイルのハードコピーを処分したい場合、どうしますか？

- A. どのゴミ箱にも捨ててください
- B. グライNDERを使って焼いてください。
- C. それをオフィスボーイに渡して、他の用途に再利用してもらいましょう。
- D. 環境に優しく、繰り返し使える筆記具

Answer: B (メッセージを残す)

顧客設計文書のハードコピーを処分する最良の方法は、シュレッダーで細断することです。細断することで文書が確実に破壊され、権限のない者が復元したりアクセスしたりすることができなくなるためです。顧客設計文書には、開示されると顧客または組織に損害を与える可能性のある機密情報や秘密情報が含まれている場合があります。そのため、文書が安全に処分されるまで、機密性と完全性を保護することが重要です。ゴミ箱に捨てたり、事務員に渡して他の用途に再利用させたり、書き物に再利用したりすることは、文書を不正アクセス、盗難、紛失、または破損にさらす可能性があるため、安全な処分方法ではありません。ISO/IEC 27001:2022では、組織は情報を含む媒体を安全に処分するための手順を実施することが求められています（A.8.3.2項を参照）。参考資料: CQI および IRCA 認定 ISO/IEC 27001:2022 主任監査員トレーニングコース、ISO/IEC 27001:2022 情報技術 - セキュリティ技術 - 情報セキュリティ管理システム - 要求事項、安全な廃棄とは？

最新問題: 146

ISO/IEC 27001の認証を受けたこの組織は、編集およびウェブサイトホスティングサービスを提供していると明記しています。しかし、組織内の変更により、ウェブサイトホスティングサービスに関する技術サポートは外部委託されることになりました。このような状況で、スコープ変更を開始すべきでしょうか？

- A. はい、外部環境の変化はスコープの変化を引き起こすからです。
- B. いいえ、変更には新たなセキュリティ対策の導入が必要ないからです。
- C. いいえ、組織は既に編集およびウェブサイトホスティングサービスの認証を取得しています。

Answer: A (メッセージを残す)

はい、スコープの変更に着手すべきです。ウェブホスティング関連の技術サポートなど、サービスの重要な部分を外部委託すると、リスク環境やそれらのリスクを管理するために必要な統制に影響を与える可能性があるためです。この変更は外部環境とISMSの運用方法に影響を与えるため、スコープの見直しと調整が必要となります。

参照 :ISO/IEC 27001:2013、第4.3項（情報セキュリティマネジメントシステムの適用範囲の決定）

最新問題: 147

在發生資訊安全事件時，應遵守系統使用者的角色和責任，但以下情況除外：

- A. 透過服務台發現後通報可疑或已知事件
- B. 必要時保留證據
- C. 如有需要，在調口期間與調口人員合作
- D. 讓所有員工了解資訊安全事件詳細信息

Answer: (解答を表示する)

情報セキュリティインシデント発生時にシステムユーザーが果たすべきでない役割と責任は、D：情報セキュリティインシデントの詳細を全従業員に周知することです。これは、インシデント対応プロセスに関与していない従業員の間で不必要なパニック、混乱、憶測を引き起こす可能性があるため、システムユーザーにとって適切な役割や責任ではありません。また、機密情報や秘密情報を含むインシデント情報の機密性と完全性を損なう可能性もあります。情報セキュリティインシデントの詳細を全従業員に周知することは、組織の情報セキュリティポリシーおよび手順に違反する可能性があり、インシデントへの対応には一定の裁量と機密保持が求められる場合があります。その他の役割と責任は、情報セキュリティインシデント発生時にシステムユーザーが行うべきことを説明しているため、適切です。例えば、サービスデスクにインシデントを報告する A)、必要に応じて証拠を保全する B)、必要に応じて調査担当者に協力するなどです。これらの役割と責任は、情報セキュリティインシデントへの迅速、効果的、かつ秩序だった対応を確保するのに役立ちます。ISO/IEC 27001:2022では、組織が情報セキュリティインシデントの報告と管理の手順を実施することを要求しています（条項16.1を参照）。参照 :CQIおよびIRCA認定ISO/IEC 27001:2022主任監査員トレーニングコース、ISO/IEC 27001:2022 情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステム - 要求事項、情報セキュリティインシデント管理とは？

最新問題: 148

您正在國際物流組織的出貨部門進行 ISMS 審核，該組織為當地醫院和政府辦公室等大型組織提供運輸服務，包裹通常包含藥品、生物樣本以及護照和駕駛執照等文件。您注意到公司記錄顯示大量退貨，原因包括標籤地址錯誤，以及在 15% 的情況下，一個包裹的不同地址有兩個或多個標籤。您正在面試運輸經理 (SM)。

您：出貨前檢口過嗎？

SM：任何明顯損壞的物品都會在出貨前由口班人員移除，但利潤微薄，因此實施正式檢口流程並不經濟。

您：退貨後會採取什麼措施？

SM：這些合約大多價口相對較低，因此我們認為，簡單地重新列印標籤並重新發送單一包裹比實施調口更容、更方便。

您提出不符合項。參考該場景，您希望受審核方在進行後續審核時實施下列哪三項附件A 控制措施？

- A. 5.11 資口返還
- B. 5.13 資訊標籤
- C. 5.3 職責分離
- D. 5.32 智慧財口權
- E. 5.34 隱私與個人識別資訊 (PII) 的保護

F. 5.6 與特殊利益團體的聯繫

G. 6.3 資訊安全意識、教育與培訓

H. 6.4 紀律程序

Answer: B,E,G ([メッセージを残す](#))

The three Annex A controls that you would expect the auditee to have implemented when you conduct the follow-up audit are:

* B. 5.13 Labelling of information

* E. 5.34 Privacy and protection of personal identifiable information (PII)

* G. 6.3 Information security awareness, education, and training

* B. This control requires the organisation to label information assets in accordance with the information classification scheme, and to handle them accordingly¹². This control is relevant for the auditee because it could help them to avoid misaddressing labels and sending parcels to wrong destinations, which could compromise the confidentiality, integrity, and availability of the information assets. By labelling the information assets correctly, the auditee could also ensure that they are delivered to the intended recipients and that they are protected from unauthorized access, use, or disclosure.

* E. この管理策では、組織が処理する個人識別情報 (PII)の個人のプライバシーと権利を保護し、適用される法的義務および契約上の義務を遵守することが求められます¹³。この管理策は、入居者の個人データが供給業者によって不正に使用されることを防ぐのに役立つため、被監査者にとって重要です。不正使用は、入居者とその家族のプライバシーと権利を侵害し、被監査者を法的リスクや評判リスクにさらす可能性があります。また、入居者とその家族のPIIを保護することで、被監査者は信頼と満足度を高め、苦情や紛争を回避することもできます。

* G. この管理策では、組織はすべての従業員と契約社員が情報セキュリティポリシー、それぞれの役割と責任、および関連する情報セキュリティ手順と管理策を認識していることを確認する必要があります¹⁴。この管理策は、被監査組織にとって重要です。なぜなら、被監査組織が従業員の情報セキュリティ文化と行動を改善し、情報セキュリティインシデントにつながる可能性のある人的ミスや過失を減らすのに役立つからです。被監査組織は、従業員に情報セキュリティに関する意識向上、教育、トレーニングを提供することで、従業員の能力とパフォーマンスを向上させ、情報セキュリティプロセスと管理策の有効性と効率性を確保することもできます。

参考文献：

1: ISO/IEC 27001:2022 - 情報技術 - セキュリティ技術 - 情報セキュリティ管理システム - 要求事項、附属書 A 2: ISO/IEC 27002:2022 - 情報技術 - セキュリティ技術 - 情報セキュリティ管理の実施規範、条項 8.2.1 3: ISO/IEC 27002:

2022 - 情報技術 - セキュリティ技術 - 情報セキュリティ管理の実施基準、条項 18.1.4 4: ISO/IEC 27002:2022 - 情報技術 - セキュリティ技術 - 情報セキュリティ管理の実施基準、条項 7.2.2

最新問題: 149

組織の情報セキュリティマネジメントシステム (ISMS)に関連する記録を保持する目的を最も適切に説明しているのは、次のうちどれですか？

A. すべての作業員が定められた手順に従っていることを確認してください。

B. 法的要件への準拠を示します。

C. 第三者監査人に対して客観的な証拠を提示する。

D. 必要に応じて、プロセスが計画通りに進んでいることを確認する。

Answer: D ([メッセージを残す](#))

組織のISMSに関連する文書化された情報を保持する目的は、必要な範囲で、プロセスが計画どおりに実行されたことを確信できるようにすることです。つまり、文書化された情報は、ISMSの適合性と有効性、情報セキュリティ目標の達成、およびISMSの継続的な改善の証拠となります。また、文書化された情報は、ISMSのパフォーマンスの分析と評価、および改善の機会の特定にも役立ちます。参照 :ISO/IEC 27001:2022、7.5.1項、PECB候補者ハンドブックISO 27001主任監査員、17ページ。

最新問題: 150

シナリオ 5: Cobt。ロンドンを拠点とする保険会社で、商業、産業、生命保険など幅広い保険ソリューションを提供しています。Cobt は近年、顧客数が大幅に増加しています。取り扱うデータ量が膨大であるため、ISO/IEC 27001 認証を取得することで情報セキュリティに多くのメリットがもたらされ、継続的な改善への取り組みを示すことができると考えています。同社は定期的なリスク評価を的確に実施していますが、ISMS を導入すると日々の業務に大きな変化が生じます。リスク評価プロセス中に、組織の内部統制が重大な欠陥を検出または防止できなかったリスクが特定されました。

同社はISMS導入のための方法論に従い、わずか数ヶ月で実用的なISMSを構築した。監査チームのメンバーにはそれぞれ責任が割り当てられた。

サラは、Cobtが多様な商業および保険ソリューションを提供することで著しい事業拡大を遂げた一方で、被監査者の確保や協力、証拠へのアクセスといった点において、依然として一部のプロセスが手作業に依存していることを認めた。今回のケースでは、Cobtの拒否により、監査の信頼性および合理的な保証を提供できる能力について疑問が生じた。これに対し、サラは認証契約に署名する前に監査から撤退することを決定し、Cobtおよび認証機関にその旨を通知した。この決定は、監査原則の遵守と透明性の維持を確実にするためであり、これらの原則を堅持するという彼女の一貫した姿勢を示すものである。

上記のシナリオに基づいて、以下の質問に教えてください。

シナリオ5に基づき、サラは認証契約書に署名する前に監査から撤退することを決定しました。これは許容されるでしょうか？

A. はい、サラは監査から辞退できますが、認証機関が彼女の辞退を承認した場合に限ります。

B. ええ、サラが監査および認証契約から撤退したことは、それとは全く関係ありません。

C. いいえ、認証契約は監査人の存在に直接関係しています。

Answer: ([解答を表示する](#))

包括的かつ詳細な徹底分析

B. 正解: 認証契約は認証機関と A. 不正解: サラはまだ認証契約に署名していないため、脱退するには認証機関の承認は必要ありません。

C. 誤) : 認証契約は特定の監査員に依存するものではなく、組織と認証機関との間の契約です。

関連規格参照 :

最新問題: 151

シナリオ5 :Data Grid Inc.は、ITインフラ全体に対するセキュリティサービスを提供する著名な企業です。エンドポイントセキュリティ、ファイアウォール、ウイルス対策ソフトウェアなど、ネットワークセキュリティソフトウェアを提供しています。Data Grid Inc.は20年以上にわたり、高度な製品とサービスを通じて数多くの企業のネットワークセキュリティ保護を支援してきました。情報およびネットワークセキュリティ分野で高い評価を得ているData Grid Inc.は、自社および顧客の資産をより適切に保護し、競争優位性を獲得するために、ISO/IEC 27001認証の取得を決定しました。

Data Grid Inc.は監査チームを任命し、監査チームは監査業務の条件に同意した。さらに、Data Grid Inc.は監査範囲と基準を定義し、5日以内に監査を完了することを推奨した。Data Grid Inc.は従業員数が多く、業務プロセスが複雑であるため、監査チームは5日以内に監査を実施するというData Grid Inc.の提案を拒否した。Data Grid Inc.は5日以内に監査を完了する予定であると主張したため、両当事者は規定の期間内に監査を実施することに合意した。監査チームはリスクベースの監査アプローチを採用した。

主要な業務プロセスと統制の概要を把握するため、監査チームはプロセス記述書と組織図を参照しました。ITインフラストラクチャとアプリケーションへのアクセスが制限されていたため、ITリスクと統制に関するより詳細な分析は実施できませんでした。しかし、監査チームは、Data Grid Inc.のISMSにおける重大な欠陥のリスクは、同社のプロセスのほとんどが自動化されているため低いと判断しました。そこで、Data Grid Inc.の担当者に以下の質問をすることで、ISMSの標準への全体的な準拠状況を評価しました。

ITおよびIT管理に関する責任は、どのように定義され、割り当てられるべきでしょうか？

*データグリッド社 管理措置が望ましい結果を達成したかどうかをどのように評価しますか？

Data Grid Inc.は、マルウェアから自社の運用環境とデータを保護するために、どのような対策を講じていますか？

ファイアウォール関連の制御は実装されていますか？

データグリッド社の担当者は、これらの問題すべてに対処するための十分かつ適切な証拠を提出した。

監査チームリーダーは監査結果をまとめ、データグリッド社の経営陣に報告した。

監査人はデータグリッド社を認証対象として推奨したが、監査目的に関してデータグリッド社と認証機関の間で誤解が生じた。データグリッド社は、監査目的には改善の可能性のある領域の特定が含まれていたにもかかわらず、監査チームはそのような情報を提供しなかったと主張した。

このシナリオに基づいて、以下の質問に教えてください。

シナリオ5に基づくと、監査チームが各プロセスの有効性やコンプライアンスを評価するのではなく、ISMS全体の評価を実施することは許容されるでしょうか？

A. はい、監査を完了するための時間枠が限られているため、監査チームはISMSの包括的な評価を通じて絶対的な保証を得る必要があります。

B. いいえ、監査チームは各プロセスを評価することによって、ISMSが標準要件を満たしていることを確認する必要があります。

C. はい、監査チームがISMS準拠を評価するのに役立つ合理的な保証を得ている場合です。

Answer: ([解答を表示する](#))

はい、監査チームがシステムが標準要件に適合しているという合理的な確証を得られるのであれば、ISMS全体を評価することは許容されます。監査チームが採用するアプローチは、ISMSのすべての重要な側面が適切に評価されることを保証するものでなければならず、これが包括的な評価によって達成されれば、十分であるとみなされます。

参考文献 :ISO 19011:2018、マネジメントシステムの監査に関する指針

有効な **ISO-IEC-27001-Lead-Auditor-CN** 問題集は GoShiken.com が提供された合格しやすい ISO-IEC-27001-Lead-Auditor-CN 試験問題集！ GoShiken.com が最新の **ISO-IEC-27001-Lead-Auditor-CN** 試験問題集を提供しています。GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 問題集をゲットする人はこちら：
<https://www.goshiken.com/PECB/ISO-IEC-27001-Lead-Auditor-CN-mondaishu.html> (418**30%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: **152**

シナリオ9 :Techmanicは1995年に設立されたベルギーの企業で、現在はブリュッセルに拠点を置いています。同社はITコンサルティング、ソフトウェア設計、ハードウェアおよびソフトウェアサービス（導入保守を含む）を提供しています。サービス対象分野は、公共サービス、金融、通信、エネルギー、医療、教育など多岐にわたります。顧客中心主義を掲げるTechmanicは、顧客との強固な関係構築を重視し、最先端のセキュリティ対策の導入に尽力しています。

Techmanic は ISO/IEC 27001 認証を取得してから 1 年が経過し、この認証を誇りに思っていました。認証監査中に、監査員は同社の情報セキュリティマネジメントシステム (ISMS) の実装にいくつかの矛盾を発見しました。特定された問題は ISMS が意図した結果を達成する能力に影響を与えなかったため、監査員がリモートで根本原因分析と是正措置を実施した後、Techmanic は認証されました。同年、同社はサービス一覧にホスティングサービスを追加し、この分野をカバーするように認証範囲を拡大するよう申請しました。監査を担当した監査員は申請を承認し、監視監査中に拡張監査を実施することを Techmanic に通知しました。Techmanic は、ISMS の継続的な有効性と ISO/IEC 27001 規格への準拠を確認するために監視監査を受けました。この監視監査は、最近追加されたホスティングサービスを含む Techmanic のセキュリティ対策が、認証の厳格な要件にシームレスに整合していることを確認することを目的としていました。監査担当者は、特にITコンサルティング分野において、再認証プロセス中に前回の監視監査報告書の調査結果を巧みに活用し、追加の再認証監査を回避することを目指しました。これは、継続的な改善と過去の評価からの学習の価値を示すものです。

Techmanicは、過去の監査報告書をレビューする取り組みを実施しています。この積極的なアプローチは、潜在的な不適合事項の特定と解決に役立つだけでなく、ITコンサルティング業界における再認証プロセスの効率化も目指しています。

監視監査において、いくつかの不適合事項が確認されました。情報セキュリティマネジメントシステム (ISMS)は、引き続きISO/IEC規格に準拠しています。

Techmanic公司雖然符合ISO/IEC 27001*標準的要求，但其口部稽核員報告稱，該公司未能解決與託管服務相關的不符合項此外，口部稽核報告存在多處不一致之處，令人質疑口部稽核員在託管服務稽核過程中的獨立性基於此，Techmanic公司未獲得擴展認證。因此，該公司申請轉至其他認證機構。同時，該公司向客口發布聲明稱,ISO/IEC 27001認證涵蓋其IT服務以及託管服務。

根據以上情景，回答以下問題：

問題：

鑑於口部稽核報告中發現的不一致之處，質疑口部稽核師的獨立性是否重要？

- A. 不，口部稽核人員只有在監督稽核依賴其調口結果時才應保持獨立性。
- B. 不，口部稽核人員不可能獨立，因為他們承擔諮詢角色
- C. 是的，口部稽核人員必須獨立於被稽核活動

Answer: C (メッセージを残す)

Comprehensive and Detailed In-Depth Explanation:

- * C. Correct Answer:
- * ISO/IEC 27001:2022 Clause 9.2.2 requires internal auditors to be independent of the activities they audit.
- * Inconsistencies in the internal audit report raise valid concerns about independence.
- * A. Incorrect:
- * Internal auditors must always be independent, not just for surveillance audits.
- * B. Incorrect:
- * Internal auditors have a compliance role, not just an advisory role.

Relevant Standard Reference:
* ISO/IEC 27001:2022 Clause 9.2.2 (Internal Auditor Independence)

最新問題: 153

あなたは経験豊富なISMS監査チームリーダーです。訓練を受けた監査員から、実施する必要のある監査の種類について確認するため、あなたに連絡がありました。以下の監査の種類と説明を照合してください。フォームに入力するには、入力したい空白部分をクリックして「In fed」をハイライト表示し、下のオプションから適切なテキストをクリックしてください。または、各オプションを対応する空白部分にドラッグすることもできます。

1. Also known as a first party audit, this type of audit involves an organisation auditing itself	
2. A third party audit which assesses an organisation's conformity with every clause of a Standard	
3. An audit whose scope requires the assessment of two or more Standards	
4. An audit carried out at a single auditee by two or more auditing organisations	
5. An audit carried out to verify the effectiveness of corrections, corrective action, and agreed opportunities for improvement	
6. An audit forming part of a programme of certification body audits in which elements of the auditees' information system management system will be examined	

A joint audit

A surveillance audit

An internal audit

A combined audit

A follow-up audit

A certification audit

Answer:

PECB

1. Also known as a first party audit, this type of audit involves an organisation auditing itself

An internal audit

2. A third party audit which assesses an organisation's conformity with every clause of a Standard

A certification audit

3. An audit whose scope requires the assessment of two or more Standards

A combined audit

4. An audit carried out at a single auditee by two or more auditing organisations

A joint audit

5. An audit carried out to verify the effectiveness of corrections, corrective action, and agreed opportunities for improvement

A follow-up audit

6. An audit forming part of a programme of certification body audits in which elements of the auditees' information system management system will be examined

A surveillance audit

A joint audit

A surveillance audit

An internal audit

A combined audit

A follow-up audit

A certification audit

最新問題: 154

次のうち、対人交流を伴わないレビュー方法の例を2つ挙げてください。

- A. テレビ会議プラットフォームを使用してインタビューを実施する。
- B. 監査に備えて、被監査者の手順を確認する。
- C. 監査結果に対する被監査者の対応を確認する。
- D. 被監査者のサーバーにリモートアクセスしてデータを分析する
- E. 遠隔監視システムによって実行される作業を観察します。
- F. レビューの日時を確認してください。

Answer: (解答を表示する)

監査手法とは、監査人が監査証拠を収集 評価するために用いる技術と手順のことである。

監査方法は、人的交流を伴うものと伴わないものの2つのカテゴリーに分類できます。人的交流を伴う方法は、インタビュー、アンケート、調査、観察、ウォークスルーなど、被監査者またはその他の関係者との直接的または間接的なコミュニケーションを必要とするものです。人的交流を伴わない方法は、文書レビュー、データ分析、遠隔監視など、被監査者またはその他の関係者とのコミュニケーションを一切必要としないものです。

人間とのやり取りを伴わない監査方法の例としては、以下のようなものがあります。

* 監査準備のための被監査組織の手順レビューの実施 :この方法は、被監査組織の方針、プロセス、記録、報告書などの文書化された情報を精査し、監査基準を満たす上での適切性と有効性を検証するものです。この方法を実施するにあたり、監査人は被監査組織やその他の関係者と直接やり取りする必要はありません。

* 被監査企業のサーバーにリモートアクセスしてデータを分析する :この方法では、被監査企業のパフォーマンス指標、ログ、メトリクス、統計などのデータにアクセスして処理し、監査基準を満たしているかどうかの正確性と信頼性を検証します。この方法を実行するにあたり、監査担当者は被監査企業やその他の関係者と直接やり取りする必要はありません。

参考文献：

* ISO/IEC 27001:2022 リードオーディター（情報セキュリティマネジメントシステム）の目的と内容は、Quality.orgおよびPECBによるものです。

* ISO 19011:2018 マネジメントシステムの監査に関する指針 [6.2.2項]

最新問題: 155

情境 5 :Data Grid Inc. 是一家知名公司，為整個資訊科技基礎設施提供安全服務。它提供網路安全軟體，包括端點安全、防火牆和防毒軟體。二十年來，Data Grid Inc. 透過先進的口品和服務幫助多家公司保護其網路安全。Data Grid Inc. 在資訊和網路安全領域享有盛譽，決定獲得ISO/IEC 27001 認證，以更好地保護其口部和客口資口並獲得競爭優勢。

Data Grid Inc. 任命了審計團隊，該團隊同意審計任務的條款。此外，Data Grid Inc.明確了審核範圍，明確了審核標準，並建議在五天内結束審核。由於Data Grid Inc.員工人數眾多，流程複雜，審計小組拒口Data Grid Inc.在五天内進行審計的提議。Data Grid Inc.堅稱他們計劃在五天内完成審核，因此雙方同意在規定的時間口進行審核。審計小組遵循基於風險的審計方法。

為了獲得主要業務流程和控制的概述，審計團隊存取了流程描述和組織圖表。他們無法對 IT 風險和控制進行更深入的分析，因為他們對IT 基礎架構和應用程式的存取受到限制。然而，審計小組表示，Data Grid Inc. 的 ISMS 出現重大缺陷的風險很低，因為該公司的大部分流程都是自動化的。因此，他們透過詢問Data Grid Inc. 的代表以下問題來評估 ISMS 整體上符合標準要求：

*如何定義和指派 IT 和 IT 控制的職責？

*Data Grid Inc. 如何評估控制措施是否達到了預期效果？

*Data Grid Inc. 採取了哪些控制措施來保護操作環境和資料免受惡意軟體的侵害？

*是否實施了與防火牆相關的控制？

Data Grid Inc. 的代表提供了充分且適當的證據來解決所有這些問題。

審計組長起草審計結論並向Data Grid Inc. 的最高管理階層報告。

監査人はデータグリッド社を認証対象として推奨したが、監査目的に関してデータグリッド社と認証機関の間で誤解が生じた。データグリッド社は、監査目的には改善の可能性のある領域の特定が含まれていたにもかかわらず、監査チームはそのような情報を提供しなかったと主張した。

このシナリオに基づいて、以下の質問に答えてください。

Data Grid Inc.は、以下の行為を除く、以下のすべての行為について責任を負います。

A. 監査基準を指定する

B. 審査チームを任命する

C. レビューの範囲を定義する

Answer: B ([メッセージを残す](#))

ISO/IEC 27001監査においては、監査チームは認証機関によって任命され、被監査組織によって任命されるわけではありません。Data Grid Inc.は監査基準の策定と監査範囲の定義を担当しますが、監査チームの任命は担当しません。

最新問題: **156**

以下に情報の定義を示すが、以下の場合は例外とする。

A. 正確かつタイムリーなデータ

B. 特定の目的に使用される、具体的かつ体系化されたデータ

C. 成熟した測定可能なデータ

D. 理解を促進し、不確実性を軽減することができる

Answer: C ([メッセージを残す](#))

正しくない情報の定義は、C：成熟した測定可能なデータです。これは情報の有効な定義ではありません。情報は成熟している必要も測定可能である必要もありません。情報は、特定の状況において誰かまたは何かに意味や価値があるデータであれば何でも構いません。情報は、解釈や使用方法によって、主観的、定性的、不完全、不確実になる可能性があります。成熟した測定可能なデータは、一部の種類の情報に当てはまる特性ですが、すべてに当てはまるわけではありません。その他の情報の定義は、正確性と適時性 A)、具体性と組織性 B)、理解と不確実性の低減 D)など、情報のさまざまな側面を説明しているため、正しいです。ISO/IEC 27001:2022では、情報を「意味のあるデータ」と定義しています (§.25項を参照)。参考資料: CQI & IRCA 認定 ISO/IEC 27001:2022 主任監査員トレーニングコース、ISO/IEC 27001:2022 情報技術 - セキュリティ技術 - 情報セキュリティ管理システム - 要求事項、情報とは何か？

最新問題: **157**

あなたは経験豊富なISMS監査チームリーダーで、現在研修中のチームに配属された監査員たちと話しています。あなたは、情報セキュリティ管理システムの運用において、計画、実行、確認、改善サイクルの検査フェーズがいかに重要であるかを彼らに理解してもらいたいと考えています。

検査活動の目的を最もよく表している選択肢を彼に選ばせることで、これを行うことができます。

経営陣によるレビュー。

経営陣によるレビューの目的は次のうちどれですか？ 1つ選択してください

- A. 情報セキュリティ管理システムの継続的な効率性、適切性、有効性を確保するために、定期的に評価を実施する。
- B. 情報セキュリティ管理システムを定期的に見直し、その継続的な準拠性、適切性、有効性を確保する。
- C. 情報セキュリティ管理システムを計画された間隔で見直し、その継続的な適用性、適切性、有効性を確保する。
- D. 情報セキュリティ管理システムを定期的に更新し、その継続的な準拠性、適切性、有効性を確保する。

Answer: C (メッセージを残す)

マネジメントレビューは、PDCAサイクル（計画・実行・評価・改善）の「チェック」段階における重要な要素です。その主な目的は、ISMS全体を評価し、改善のための戦略的な意思決定を行うことです。他の選択肢が正確でない理由は以下のとおりです。

- * A. ランダムな間隔：一貫性を保ち、進捗状況を追跡するために、計画された間隔でレビューを実施する必要があります。
- * B. コンプライアンス: コンプライアンスも考慮事項ですが、主な焦点は、システムが組織のニーズに適しているか、リスク管理が適切か、情報セキュリティの目的を達成する上で全体的に有効であるかにあります。
- * D. 更新: 経営陣によるレビューは更新につながる可能性があります、その主な目的は評価であり、即時の変更ではありません。

参照：

- * ISO/IEC 27001:2022、第9.3項（マネジメントレビュー） マネジメントレビューを実施する目的と要件を概説する。

最新問題: 158

あなたは経験豊富なISMS監査員で、ICTリサイクルサービスを提供する組織の第三者監査を担当しています。この組織は、会社が不要になったICT機器を処理し、修理・再利用するか、安全に廃棄処分します。

部屋の隅にあるベンチの上に2台のサーバーが置いてあるのに気づきました。どちらのサーバーにも、サーバー名、IPアドレス、管理者パスワードが書かれたステッカーが貼られています。ICTマネージャーにこれらのサーバーについて尋ねると、それらは昨日、長年の顧客から届いた荷物の一部だと教えてくれました。

あなたはどのような行動を取るべきでしょうか？

- A. 情報セキュリティインシデントをICTマネージャーに記録させ、情報セキュリティインシデント管理プロセスを開始させてください。
- B. 監査結果に注意し、顧客のITセキュリティに関連する入荷貨物の処理プロセスを確認してください。
- C. レビュー結果に表示された内容を記録し、それ以上の行動は取らない。
- D. 管理要件の不遵守 5.31 法的、規制的、監督的、および契約上の要件。
- E. 管理措置8.20 「ネットワークセキュリティ」 ネットワークおよびネットワーク機器は、システムおよびアプリケーション内の情報を保護するために保護、管理、制御されなければならない)への不遵守が確認されました。
- F. 審査対象者にタグの削除を依頼し、審査プロセスを続行します。

Answer: B (メッセージを残す)

ISO 27001:2022 の 8.1.4 項によれば、組織は、情報セキュリティ管理システムに関連する外部提供のプロセス、製品、またはサービスが管理されていることを保証しなければなりません。これには、ICT 機器を回収のために送付する顧客などの外部プロバイダーとの情報セキュリティに関する適切な契約要件の実装が含まれます。12 この場合、組織は ICT 回収サービスを提供しており、機密情報または秘密情報が含まれている可能性のある顧客の ICT 機器の処理が含まれます。組織は、顧客の ICT 機器が安全に、かつ顧客の情報セキュリティ要件に従って取り扱われることを保証するプロセスを整備する必要があります。プロセスには、顧客の身元と承認の確認、機器の在庫と状態の確認、機器または顧客に関する情報を含むラベルやステッカーの除去または破棄、機器に保存されているデータの消去、実行したアクションと達成された結果の文書化などの手順が含まれる必要があります12 監査人が、サーバー名、IP アドレス、管理者パスワードがわかるステッカーが付いたベンチ上の 2 台のサーバーに気づいたという事実は、顧客の IT セキュリティに関連する入荷貨物の処理プロセスが効果的でないか、従われていないことを示しています。これは、顧客の情報またはシステムへの不正アクセス、開示、または変更のリスクをもたらす可能性があります。したがって、監査人は監査結果を記録し、顧客の IT セキュリティに関連する入荷貨物の処理プロセスを確認し、ISO 27001:2022 の条項 8.1.4 に適合していないかどうかを判断する必要があります12 その他のアクションは、次の理由により適切ではありません。

- * A. ICT マネージャーに情報セキュリティ インシデントを記録し、情報セキュリティ インシデント管理プロセスを開始するよう依頼することは適切ではありません。なぜなら、これは組織自身の情報やシステムに影響を与える情報セキュリティ インシデントではないからです。情報セキュリティ インシデントとは、事業運営を損ない、情報セキュリティを脅かす可能性が非常に高い、望ましくない、または予期せぬ情報セキュリティ イベントの 1 つまたは一連のものと定義されます。12 この場合、情報セキュリティ イベントは組織の情報やシステムではなく、顧客の情報やシステムに影響を与えます。したがって、組織は情報セキュリティ インシデント管理プロセスではなく、顧客の IT セキュリティに関連する入荷品の処理プロセスに従う必要があります。

* C. Recording what the auditor has seen in the audit findings, but taking no further action is not appropriate because this would not address the root cause or the impact of the issue. The auditor has a responsibility to verify the effectiveness and compliance of the organisation's information security management system, and to report any nonconformities or opportunities for improvement¹² Therefore, the auditor should check the process for dealing with incoming shipments relating to customer IT security, and determine whether there is a nonconformity with clause 8.1.4 of ISO 27001:2022.

* D. Raising a nonconformity against control 5.31 Legal, statutory, regulatory and contractual requirements is not appropriate because this control is not relevant to the issue. Control 5.31 requires the organisation to identify and comply with the legal, statutory, regulatory and contractual requirements that are applicable to the information security management system¹² In this case, the issue is not about the organisation's compliance with the legal, statutory, regulatory and contractual requirements, but about the organisation's control of the externally provided processes, products or services that are relevant to the information security management system. Therefore, the auditor should check the process for dealing with incoming shipments relating to customer IT security, and determine whether there is a nonconformity with clause 8.1.4 of ISO 27001:2022.

* E. Raising a nonconformity against control 8.20 'network security' (networks and network devices shall be secured, managed and controlled to protect information in systems and applications) is not appropriate because this control is not relevant to the issue. Control 8.20 requires the organisation to secure, manage and control its own networks and network devices to protect the information in its systems and applications¹² In this case, the issue is not about the organisation's network security, but about the organisation's control of the externally provided processes, products or services that are relevant to the information security management system. Therefore, the auditor should check the process for dealing with incoming shipments relating to customer IT security, and determine whether there is a nonconformity with clause 8.1.4 of ISO 27001:2022.

* F. Asking the auditee to remove the labels, then carry on with the audit is not appropriate because this would not address the root cause or the impact of the issue. The auditor should not interfere with the auditee's operations or suggest corrective actions during the audit, as this would compromise the auditor's objectivity and impartiality¹² The auditor should check the process for dealing with incoming shipments relating to customer IT security, and determine whether there is a nonconformity with clause 8.1.4 of ISO 27001:2022.

References:

1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1 2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

最新問題: 159

シナリオ8 :テッサ、マリク、マイケルは、セキュリティ、コンプライアンス、事業計画および戦略の分野で経験豊富な専門家で構成された独立監査チームを結成しました。彼らは、大手ウェブデザイン会社であるクラスタスの認証監査を実施する任務を負っています。これまでの監査業務において、彼らは公平性と客観性を含め、卓越した職業倫理を示してきました。今回、クラスタスはISO/IEC 27001認証を取得することで競争優位性を獲得できると確信しています。

監査チームリーダーのテッサは、豊富な監査経験と、IT関連問題、コンプライアンス、ガバナンスにおける非常に優れた実績を有しています。一方、マリクは組織計画とリスク管理のバックグラウンドを持ち、組織のセキュリティ管理とリスク許容度を包括的に分析し、組織内のリスクレベルを正確に評価することに長けています。また、マイケルは、厳格な標準化された手順に従い、セキュリティ管理の実践的な評価を実施することに熟練した経験豊富な専門家です。

必要な監査作業を終えた後、テッサは監査チームとの会議を招集した。彼らはマイケルの指摘事項の一つを分析し、客観的かつ正確な判断を下した。マイケルが指摘した問題は、会社の日常業務における軽微な法令違反であり、彼はそれがIT技術者によって引き起こされたと考えていた。そこで、経営陣が責任者の名前を尋ねた後、テッサは経営陣と面談し、法令違反の責任者を伝えた。明確化を図るため、テッサは監査最終日に報告会を開催した。この会議で、彼女は特定された不適合事項をクラスタス社の経営陣に報告した。しかし、テッサは、クラスタス社の認証監査報告書を簡潔にし、重要な所見を強調するために、不必要な証拠を記載しないように助言された。監査チームは、検討した証拠に基づき監査結論案を作成し、認証を与える前に組織の2つの領域を監査する必要があると判断した。これらの決定は被監査組織に提出されたが、被監査組織は監査結果を受け入れず、補足情報を要求した。被監査組織の意見にもかかわらず、監査人は既に認証を与えることを決定していたため、補足情報の受け入れを拒否した。被監査組織の上級管理職は、監査結論は現実を反映していないと主張したが、監査チームは自らの立場を堅持した。

上記のシナリオに基づいて、以下の質問に答えてください。

質問 :

監査報告書の作成および内容について、主に誰が責任を負うのか？

- A. 監査チームリーダー
- B. 監査チームメンバー
- C. 認証機関

Answer: A ([メッセージを残す](#))

包括的かつ詳細な解説 :

* A. 正解:

* ISO 19011:2018では、監査チームリーダーが監査報告書の作成と最終化に責任を負うと規定されています。

* B. 不正解:

チームメンバーは調査結果を提供するが、最終的な決定はリーダーが行う。

* C. 不正解:

* 認証機関は報告書を審査するが、作成は行わない。

関連規格参照：

* ISO 19011:2018 6.7.1項（監査報告書の作成及び承認）

最新問題: 160

問題：

哪種類型的審計要求受審計方 and 審計團隊在進行審計之前就遠端存取協議達成一致？

A. 虛擬

B. □部

C. 外部

Answer: (解答を表示する)

Comprehensive and Detailed In-Depth Explanation:

* A. Correct Answer:

* Virtual audits require predefined remote access protocols to ensure secure, authorized connections for data review.

* ISO 19011:2018 provides guidelines for virtual auditing security measures.

* B. Incorrect:

* Internal audits may use remote access, but agreement is not mandatory.

* C. Incorrect:

* External audits may involve remote access but do not require predefined agreements in all cases.

Relevant Standard Reference:

* ISO 19011:2018 Clause 6.4.10 (Remote and Virtual Auditing Procedures)

最新問題: 161

仮説：

情報セキュリティインシデント発生後、組織は包括的なバックアッププログラムを確立し、すべての重要データを定期的に自動的にオフサイトストレージにバックアップするようになりました。この際、組織はこの状況においてどの情報セキュリティ原則を適用したのでしょうか？

A. 誠実さ

B. 機密保持

C. 入手可能性

Answer: (解答を表示する)

包括的かつ詳細な徹底分析

CIAトライアド（機密性 完全性、可用性）は、情報セキュリティ原則の基礎となるものです。

可用性とは、必要なときにデータとサービスにアクセスできる状態を確保することです。定期的な自動バックアップとオフサイトストレージを導入することで、組織はセキュリティインシデント データ損失、サイバー攻撃、ハードウェア障害など）が発生した場合でも、重要なデータにアクセスできる状態を維持できます。これは、システムの回復力を確保するためにバックアップの維持とテストを重視するISO/IEC 27001:2022附属書A管理項目 A.8.13（情報バックアップ）に準拠しています。

データの完全性とは、データが改ざんされず正確であることを保証するものですが、バックアップはチェックサムや検証メカニズムが伴わない限り、それ自体ではデータの完全性を保証するものではありません。

最新問題: 162

シナリオ7 :Webvueは、コンピュータソフトウェアの開発、サポート、保守を専門とする日本を拠点とするテクノロジー企業です。Webvueは、さまざまなテクノロジー分野や企業向けにソリューションを提供しています。同社の主力サービスはCloudWebvueで、ストレージ、ネットワーク、仮想コンピューティングサービスを提供する包括的なクラウドコンピューティングプラットフォームであり、企業ユーザーと個人ユーザー向けに設計されています。CloudWebvueは、その柔軟性、拡張性、信頼性で高い評価を得ています。

Webvueは、ISO/IEC 27001認証の範囲にCloudWebvueのみを含めることを決定しました。そのため、フェーズ1とフェーズ2の監査は同時に実施されました。Webvueは、資産の機密性に対する厳格な管理を誇りとしています。CloudWebvueに保存されている情報を保護するために、適切な暗号化制御を使用しています。内部使用、制限付き、機密など、あらゆるレベルの情報は、クラウドに保存される前に固有のハッシュ値で暗号化されます。監査チームは、Keith、Sean、Layla、Sam、Tinaの5名で構成されました。ITおよび情報セキュリティ監査チームで最も経験豊富な監査員であるKeithが監査チームリーダーを務めました。彼の責任には、監査の計画と監査チームの管理が含まれていました。SeanとLaylaは、プロジェクト計画、ビジネス分析、ITシステム（ハードウェアとアプリケーション）に関する豊富な経験を持っています。彼らのタスクには、Webvueの内部システムとプロセスに基づいた監査計画の策定が含まれていました。一方、SamとTinaは最近学業を修了し、日々のタスクを処理しながら監査スキルを向上させる責任を負っていました。ISO/IEC 27001の附属書Aにおける暗号化の使用に関する管理項目8.24への準拠を関係者へのインタビューを通じて検証した結果、監査チームは、暗号化キーが当初、乱数ビット生成器（RGB）およびその他の鍵生成に関するベストプラクティスに基づいて生成されていたことを発見した。Webvueの暗号化ポリシーを確認した結果、インタビューで得られた情報は正確であると結論付けた。しかし、ポリシーに暗号化キーの使用方法和ライフサイクルが明記されていなかったため、これらのキーは引き続き使用されていた。Webvueと認証機関の間で後に合意された内容に基づき、監査チームは仮想監査を選択し、認証範囲と監査目標を満たすために、WebvueがISO/IEC 27001規格の管理要件8.11（データ匿名化）に準拠しているかどうかを検証することに重点を置きました。監査チームはCloudWebvueの内部データ保護プロセスをレビューし、同社がポリシーと規制基準をどのように遵守しているかに焦点を当てました。監査プロセスの一環として、監査チームリーダーのKeithは、Webvueの慣行の有効性を文書化および分析するために、関連文書と暗号化キー管理プログラムのスクリーンショットをキャプチャしました。Webvueはテストに生成されたテストデータを使用しています。しかし、品質保証マネージャーへのインタビューと部門のプロセスに基づく、リアルタイムのシステムデータが使用される場合もあります。これにより大量のデータが生成されますが、より正確な結果が得られます。テストデータの保護と管理は、監査中に暗号化プロセスをシミュレートしたWebvueの担当者によって検証されました。品質保証マネージャーへのインタビューで、キースは、セキュリティトレーニング部門の従業員が適切な手順に従っていないことを発見しました。この部門は監査範囲外でしたが、セキュリティトレーニング部門の不遵守は、監査範囲内のプロセス、特にCloudWebvueのデータセキュリティと暗号化の実践に影響を与える可能性があります。そのため、キースはこの発見を監査レポートに含め、被監査者に通知しました。

上記のシナリオに基づいて、以下の質問に答えてください。

質問：

シナリオ7に基づく、テストデータの使用が仕様に準拠しているかどうかを確認するために、どの監査手順が使用されましたか？

A. 文書情報レビュー

B. 裏付けとなる証拠

C. 技術検証

Answer: ([解答を表示する](#))

包括的かつ詳細な解説：

* C. 正解:

* 技術検証とは、制御装置を直接テストまたはシミュレーションすることを指します。

* Webvueの担当者が暗号化プロセスをシミュレーションし、テストデータのセキュリティ対策を確認した。

* A. 不正解:

文書レビューは受動的な作業であるのに対し、技術検証は能動的であり、リアルタイムの評価を含む。

* B. 不正解:

* 裏付けとは情報の相互確認のことであり、技術的検証とは実際の運用における管理体制のテストのことである。

関連規格参照：

* ISO 19011:2018 6.4.9項（監査における技術的検証）

最新問題: 163

ITサポートチームから以下のメールが届きます :ユーザー様、来週から、アカウントを引き続きご利用いただけるよう、以下の詳細を共有するためのスペースを確保するため、すべての非アクティブなメールアカウントを削除します。返信がない場合は、名前：

電子メールアドレス：

パスワード：

生年月日：

さらにサポートが必要な場合は、メールチームまでご連絡ください。ご協力ありがとうございました。

次のうち、最も適切な回答はどれですか？

A. メールを無視する

B. 回答としては、パスワードは誰とも共有すべきではない、というものでした。

C. これらのメールには返信せず、上司に報告してください。

Answer: C (メッセージを残す)

ITサポートチームから個人情報を要求するメールが届いた場合、最善の対応策は返信せず、上司に報告することです。このメールはフィッシング詐欺である可能性が高く、フィッシングとは、偽のメールやその他のメッセージを使って受信者を騙し、パスワード、クレジットカード番号、銀行口座情報などの機密情報を漏洩させるソーシャルエンジニアリングの一種です。フィッシングメールは、正規の組織や個人になりすまし、緊急性や好奇心を煽ることで、被害者を悪意のあるリンクをクリックさせたり、悪意のある添付ファイルを開かせたり、個人情報を提供させたりします。

ITサポートチームがメールでパスワードやその他の個人情報を尋ねることは、情報セキュリティポリシーとベストプラクティスに違反するため、決してあってはなりません。メールを無視したり、パスワードを誰にも共有すべきではないと返信したりしても、ITサポートチームや上司にフィッシング攻撃を知らせることができず、他のユーザーにも影響を与える可能性があるため、適切な対応とは言えません。メールを上司に報告することは、さらなる損害や情報漏洩を防ぐための責任ある行動です。ISO/IEC 27001:2022では、組織がフィッシングなどのソーシャルエンジニアリング攻撃のリスクと回避方法をユーザーに認識させるための啓発およびトレーニングプログラムを実施することを義務付けています (A.7.2.2項を参照)。参考文献 :CQI & IRCA認定ISO/IEC 27001:2022主任監査員トレーニングコース、ISO

/IEC 27001:2022 情報技術 - セキュリティ技術 - 情報セキュリティ管理システム - 要求事項、フィッシングとは何か？

最新問題: 164

ITサポートチームから以下のメールが届きます :ユーザー様、来週から、アカウントを引き続きご利用いただけるよう、以下の詳細を共有するためのスペースを確保するため、すべての非アクティブなメールアカウントを削除します。返信がない場合は、名前：

電子メールアドレス：

パスワード：

生年月日：

さらにサポートが必要な場合は、メールチームまでご連絡ください。ご協力ありがとうございました。

次のうち、最も適切な回答はどれですか？

A. メールを無視する

B. 回答としては、パスワードは誰とも共有すべきではない、というものでした。

C. これらのメールには返信せず、上司に報告してください。

Answer: C (メッセージを残す)

ITサポートチームから個人情報を要求するメールが届いた場合、最善の対応はメールに返信せず、上司に報告することです。このメールはフィッシング詐欺である可能性が高く、フィッシング詐欺とは、偽のメールやその他のメッセージを使って受信者を騙し、パスワード、クレジットカード番号、銀行口座情報などの機密情報を漏洩させるソーシャルエンジニアリングの一種です。フィッシングメールは、正規の組織や個人になりすまし、緊急性や好奇心を煽ることで、被害者を悪意のあるリンクをクリックさせたり、悪意のある添付ファイルを開かせたり、個人情報を提供させたりします。ITサポートチームがメールでパスワードやその他の個人情報を要求することは、情報セキュリティポリシーやベストプラクティスに違反するため、決してあってはなりません。メールを無視したり、「パスワードは誰にも教えない」と返信したりしても、ITサポートチームや上司にフィッシング詐欺の事実を知らせることができず、他のユーザーにも被害が及ぶ可能性があるため、適切な対応とは言えません。上司にメールを報告することは、さらなる被害や情報漏洩を防ぐための責任ある行動です。ISO/IEC 27001:2022 では、組織がフィッシングなどのソーシャルエンジニアリング攻撃のリスクと、それらを回避する方法についてユーザーに認識させるための啓発およびトレーニング プログラムを実施することを要求しています (条項 A.7.2.2 を参照)。参照: CQI および IRCA 認定 ISO/IEC 27001:2022 主任監査員トレーニング コース、ISO/IEC 27001:2022 情報技術 - セキュリティ技術 - 情報セキュリティ マネジメント システム - 要求事項、フィッシングとは？

最新問題: 165

仮説：

Northstormは、ユニークなヴィンテージおよびモダンなアクセサリーを取り扱うオンライン小売店です。当初は小規模な市場に参入しましたが、eコマース市場の拡大とともに成長を遂げてきました。Northstormはオンラインのみで事業を展開しており、効率的な決済処理、在庫管理、マーケティングツール、注文処理を実現しています。人気商品を優先的に仕入れ、補充、発送しています。

Northstormは従来、自社ウェブサイトホスティングし、ハードウェア、ソフトウェア、データ管理を含むインフラストラクチャを完全に制御することでIT運用を管理していました。しかし、このアプローチでは、応答性の高いインフラストラクチャが不足していたため、成長が阻害されていました。eコマースと決済システムを強化するため、Northstormは社内データセンターの拡張を選択し、3か月かけて2段階で拡張を完了しました。最初の段階では、コアサーバー、POSシステム、注文、請求、データベース、バックアップシステムをアップグレードしました。第2段階では、メール、決済、ウェブ機能の改善に取り組みました。さらに、この段階でNorthstormは、個人情報（PII）の管理者と処理者に関する国際標準を採用し、データ処理の安全性とグローバル規制への準拠を確保しました。

拡張にもかかわらず、ノースストームのデータセンターはアップグレード後も進化するビジネスニーズに対応できませんでした。この不備により、注文の優先順位付けの問題など、新たな課題が生じました。顧客からは優先的に処理された注文が届かないという報告があり、同社は迅速な対応に苦慮しました。これは主に、注文の優先順位付けと顧客とのやり取りをシミュレートするために設計されたアプリケーション「YouDecide」からの注文をメインサーバーが処理できなかったためです。このアプリケーションは、アップグレード時にインストールされた新しいオペレーティングシステム（OS）と互換性のない高度なアルゴリズムに依存していました。

Northstorm社は、緊急の互換性問題に直面し、適切な検証を行わずにアプリケーションを急いでパッチ適用した結果、セキュリティ上の脆弱性を抱えたバージョンをインストールしてしまいました。このセキュリティ上の脆弱性によりメインサーバーが影響を受け、同社のウェブサイトが1週間オフラインになる事態となりました。より信頼性の高いソリューションの必要性を認識した同社は、ウェブサイトのホスティングをeコマースプロバイダーにアウトソーシングすることを決定しました。移行に先立ち、セキュリティ強化のため、同社は製品所有権に関する機密保持契約を締結し、ユーザーアクセス権限の徹底的な見直しを実施しました。

シナリオ1に基づく予防および制御対策として適切なものはどれですか？

- A. 過去の知識に基づいて注文の優先順位を決定するアプリケーション。
- B. 機密保持契約書に署名する
- C. 社内データセンターの容量を拡張する

Answer: B (メッセージを残す)

包括的かつ詳細な徹底分析

予防的制御とは、セキュリティインシデントやリスクの発生を未然に防ぐために実施されるセキュリティ対策です。情報システムを事前に保護し、潜在的な脅威を軽減します。

- A. 過去の知識に基づいて注文の優先順位を付けるアプリケーションを使用する - これは業務効率化策ではありますが、セキュリティ対策ではありません。効率性は向上しますが、セキュリティ侵害やリスクを直接的に防止するものではありません。
- B. 機密保持契約の締結 — これは予防的な対策であり、外部委託先のサービスプロバイダーに移行する前に、機密性の高いビジネス情報が不正に開示されることを防ぎます。当事者を法的に機密保持義務に拘束することで、知的財産の盗難やデータの不正使用のリスクを軽減します。
- C. 社内データセンターの容量を拡張する - これは、インフラストラクチャの不足という問題に対処するものの、セキュリティ関連の脅威を防止するものではないため、是正措置または運用上の制御です。

最新問題: 166

您正在一家提供醫療保健服務的住宅療養院進行 ISMS 初始認證審核。審計計劃的下一步是召開末次會議。在最終審核小組會議上，身為審核組組長，您同意報告 2 項輕微不符合項和 1 項改進機會，如下：

Cosmic Certifications Limited				
Summary of audit findings:				
Opportunities for Improvement (OI)				
Item	Findings		Requirements	Follow-up
1.	The organisation should improve the overall awareness of information security incident management responsibility and process.		Clause 7.4 and Control A.5.24	N/A
Nonconformities (NCs)				
Item	Findings	Grade	Requirements	Follow-up
1.	During the audit on the outsourced process, sampling one of the outsourced service contracts with WeCare the medical device manufacturer found that ABC does not include personal data protection and legal compliance as part of the information security requirements in the contract.	Minor	Clause 4.2 and Control A.5.20	Corrective actions are required.
2.	During the audit on information security during the business continuity process, sampling one of the service continuity and recovery plans for the resident's healthy status monitoring service. The auditor found the recovery plan has not yet been tested.	Minor	Clause 8.1 and Control A.5.29	Corrective actions are required.
signed by Audit				
Team Leader				

在閉幕會議上，管理系統代表(MSR) 向您通報 ABC 將在未來 3 個月與 WeCare 醫療設備製造商合併的資訊。合併後該組織的名稱將是 ABC。他詢問是否可以將 WeCare 醫療器材生口地點納入後續審核，以便認證中將其納入。他表示 WeCare 已通過 ISO/IEC 27001:2022 認證。

選擇一個選項以正確回應 MSR 的請求。

- A. 建議需要對 WeCare 進行初步審核，但這可以與ABC 的後續審核結合起來
- B. 建議任何變更都會影響初始審核的認證範圍。該組織有責任在商定的時間範圍更新認證機構，以便就合併WeCare 做出決定。
- C. 建議沒有問題。如果WeCare能獲得其認證機構的同意，新業務可以立即納入認證範圍
- D. 建議最好延後認證流程並等待業務收購者完成

Answer: B (メッセージを残す)

According to ISO/IEC 27001 guidelines, any significant changes to the scope of the ISMS, such as a merger, must be communicated to the certification body. This ensures that the certification remains valid and that all locations and processes are included in the scope. The certification body will then decide the appropriate actions to incorporate the new entity into the existing certification.

References:

*ISO/IEC 27001 Lead Auditor Reference Materials

*PECB Candidate Handbook for ISO 27001 Lead Auditor

有効な **ISO-IEC-27001-Lead-Auditor-CN** 問題集は GoShiken.com が提供された合格しやすい ISO-IEC-27001-Lead-Auditor-CN 試験問題集！ GoShiken.com が最新の **ISO-IEC-27001-Lead-Auditor-CN** 試験問題集を提供しています。GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 問題集をゲットする人はこちら：
<https://www.goshiken.com/PECB/ISO-IEC-27001-Lead-Auditor-CN-mondaishu.html> (**41830%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: **167**

シナリオ 1: Fintive は、オンライン決済およびセキュリティ保護ソリューションの大手プロバイダーです。1999 年にカリフォルニア州サンノゼでトーマス・フィンによって設立された Fintive は、情報セキュリティの向上、不正行為の防止、および PII (個人情報注入) などのユーザー情報の保護を希望するオンライン企業にサービスを提供しています。Fintive の意思決定および運用プロセスは、過去の事例に基づいています。顧客データを収集し、分類し、分析します。このような複雑な分析を実行するには、大規模な人員が必要でした。しかし、長年にわたり、このような分析を容易にする技術も進歩してきました。現在、Fintive はチャットボットなどの最新ツールを使用してパターン分析を実行し、不正行為を即座に防止することを計画しています。このツールは、顧客サービスの向上にも役立ちます。

この最初のアイデアはソフトウェア開発チームに伝えられ、彼らはそれを支持してプロジェクトを担当することになった。彼らはチャットボットを既存のシステムに統合する作業を開始した。さらに、チームはチャットボットがチャットの問い合わせの85%に回答するという目標を設定した。

チャットボットの統合が成功すると、同社は直ちに顧客向けにリリースした。

しかし、チャットボットにはいくつか問題があるようだ。

トレーニング段階 (チャットボットがクエリパターンを「学習」する段階)において、テストが不十分であったり、サンプルデータが不足していたりするため、チャットボットはユーザーのクエリを解決して正しい回答を提供することができません。さらに、チャットボットが無効な入力 (奇妙なドットパターンや通常とは異なる文字など)を受け取ると、ランダムなファイルをユーザーに送信してしまいます。そのため、チャットボットは顧客のクエリに適切に対応できず、従来のカスタマーサポートはチャットによる問い合わせで手一杯になり、顧客の要望を解決することができなくなっています。

そのため、Fintiveはソフトウェア開発ポリシーを策定しました。このポリシーでは、ソフトウェアが社内で開発されたか外部委託されたかにかかわらず、オペレーティングシステムに実装する前にブラックボックステストを実施することを規定しています。

シナリオ1に基づく、チャットボットは無効な入力を受け取った際に、ユーザーにランダムなプロファイルを送信します。これにはどのような影響があるでしょうか？

- A. 機密情報の漏洩
- B. 評判の失墜
- C. サービスを提供できません

Answer: B ([メッセージを残す](#))

最新問題: **168**

場景 9 :Techmanic 是一家比利時公司，成立於1995 年，目前在布魯塞爾運作。它提供 IT 諮詢、軟體設計和硬體/軟體服務，包括部署和維護。該公司服務於公共服務、金融、電信、能源、醫療保健和教育等行業。作為一家以客戶為中心的公司，它優先考慮建立牢固的客戶關係並引領安全實踐。

Techmanic 已獲得 ISO/IEC 27001 認證一年，並對此認證感到自豪。在認證審核期間，審核員發現其ISMS 實施上存在一些不一致之處。由於觀察到的情況並不影響其 ISMS 實現預期結果的能力，因此在審計師遠端跟進根本原因分析和糾正措施後，Techmanic 獲得了認證。的遵守情況。認識持續改進的價值並從過去的評估中學習。Techmanic 實施了客戶先前的監督審計報告的做法。這種積極主動的方法不僅有助於識別和解決潛在的不合格情況，而且還旨在簡化 IT 諮詢領域的重新認證流程。

監督審核期間，發現了多處不符合項。ISMS 繼續滿足 ISO/IEC 27001*s 的要求，但根據客戶部稽核員的報告,Techmanic 未能解決與託管服務相關的不符合問題。此外，客戶部稽核報告存在多處不一致之處，這使人們對客戶部稽核師在託管服務審計過程中的獨立性產生了質疑。基於此，延期認證未獲核准。因此。Techmanic 請求轉移到另一個認證機構。同時，該公司向客戶發布聲明稱,ISO/IEC 27001 認證涵蓋 IT 服務以及託管服務。

根據上述情景，回答以下問題：

根據 ISO/IEC 17021-1，監督審核的目的為何？

- A. 評估合規性並授予初始認證
- B. 評估組織的財務績效
- C. 在審核期間保持對認證管理系統的信心

Answer: C ([メッセージを残す](#))

Relevant Standard Reference:

最新問題: 169

CMMとは何の略ですか？

- A. 能力成熟度マトリックス
- B. 能力成熟度マトリックス
- C. 能力成熟度モデル
- D. 有能で成熟したモデル

Answer: C (メッセージを残す)

能力成熟度モデル（CMM）は、効果的なソフトウェアプロセスの主要要素を記述するフレームワークです。ソフトウェア開発組織の成熟度を、初期段階から最適化段階まで5段階に分類しています。CMMIは、組織が現在のプロセス能力レベルを評価し、改善すべき領域を特定するのに役立ちます1。参考文献 :ISO/IEC 27001:2022 主任審査員 - IECB

最新問題: 170

シナリオ 5: Cobt。ロンドンを拠点とする保険会社で、商業、産業、生命保険など幅広い保険ソリューションを提供しています。Cobt は近年、顧客数が大幅に増加しています。取り扱うデータ量が膨大であるため、ISO/IEC 27001 認証を取得することで情報セキュリティに多くのメリットがもたらされ、継続的な改善への取り組みを示すことができると考えています。同社は定期的なリスク評価を的確に実施していますが、ISMS を導入すると日々の業務に大きな変化が生じます。リスク評価プロセス中に、組織の内部統制が重大な欠陥を検出または防止できなかったリスクが特定されました。同社はISMS導入のための方法論に従い、わずか数ヶ月で実用的なISMSを構築した。監査チームのメンバーにはそれぞれ責任が割り当てられた。サラは、Cobtが多様な商業および保険ソリューションを提供することで著しい事業拡大を遂げた一方で、被監査者の確保や協力、証拠へのアクセスといった点において、依然として一部のプロセスが手作業に依存していることを認めた。今回のケースでは、Cobtの拒否により、監査の信頼性および合理的な保証を提供できる能力について疑問が生じた。これに対し、サラは認証契約に署名する前に監査から撤退することを決定し、Cobtおよび認証機関にその旨を通知した。この決定は、監査原則の遵守と透明性の維持を確実にするためであり、これらの原則を堅持するという彼女の一貫した姿勢を示すものである。

上記のシナリオに基づいて、以下の質問に答えてください。

シナリオ5で説明されているサラの役割に基づくと、以下のうちどれが彼女の職務の一部とみなされるべきではないでしょうか？

- A. 監査チームのメンバーに責任を割り当てる
- B. 監査基準と目的を定義する
- C. 計画監査

Answer: A (メッセージを残す)

包括的かつ詳細な徹底分析

- A. 監査チームメンバーへの責任の割り当て（正解）これはサラの責任ではありません。認証機関が監査チームを割り当て、責任を定義し、独立性と客観性を確保します。
- B. 監査基準と目的の定義（適切な責任）- 監査チームリーダーであるサラは、ISO 19011（マネジメントシステムの監査に関する指針）に従って、監査基準と目的を確立する必要があります。
- C. 監査の計画（適切な責任）- 監査チームリーダーは、タイムラインやリソースの割り当てを含め、監査の計画に責任を負います。

関連規格参照：

ISO/IEC 27001:2022 条項9.2（内部監査）

最新問題: 171

組織 A 的審核員對供應商 B 進行審核。

- A. 與 A 中的其他相關經理分享調口結果
- B. 與 B 的資安經理分享調口結果
- C. 與 A 的供應商評估團隊分享調口結果
- D. 與 B 的其他客口分享調口結果
- E. 與 B 的認證機構分享調口結果

F. 與 B 中的其他相關經理分享調口結果

Answer: A,D (メッセージを残す)

According to the PECB Candidate Handbook¹, one of the principles of auditing is confidentiality, which means that auditors should respect the confidentiality of information obtained during the audit and not disclose it to unauthorized parties. The handbook also states that auditors should only report audit results to those who have a legitimate need to know, such as the client, the auditee, and the certification body. Therefore, sharing the findings with other relevant managers in A or B's other customers would be a breach of confidentiality, as they are not directly involved in the audit process or the information security management system of B. Sharing the findings with B's Information Security Manager or other relevant managers in B would be appropriate, as they are part of the auditee organization and responsible for the implementation and improvement of the ISMS. Sharing the findings with A's supplier evaluation team or B's certification body would also be acceptable, as they have a legitimate need to know the audit results for the purpose of supplier selection or certification, respectively. Reference: 1: PECB Candidate Handbook - ISO 27001 Lead Auditor, pages 7-8.

最新問題: 172

シナリオ2 :ナイト社は、米国カリフォルニア州北部を拠点とする電子機器メーカーで、ビデオゲーム機を開発しています。ナイト社は世界中に300人以上の従業員を抱えています。創業5周年を機に、同社は次世代ビデオゲーム機「G-Console」をグローバル市場向けに発売することを決定しました。G-Consoleは2021年の究極のメディアコンソールと位置づけられ、プレイヤーに最高のゲーム体験を約束します。

メインユニットパッケージには、VRヘッドセット、2つのゲームやその他のギフト。

長年にわたり、同社は誠実さ、正直さ、そして顧客への敬意を通して確固たる評判を築いてきました。この評判こそが、多くの熱心なゲーマーがKnightのGコンソールを発売と同時に手に入れたいと願った理由の一つです。ナイト社は顧客志向の企業であることに加えて、彼らの開発品質はゲーム業界で広く認められている。しかし、価格は妥当な範囲を超えて高額である。しかし、ナイト社の製品の品質は最高レベルであるため、ほとんどの忠実な顧客にとってこれは問題ではない。世界有数のビデオゲーム機開発企業であるナイト社は、悪意のある攻撃の標的となることも少なくありません。同社の情報管理システム（ISMS）は1年以上前から運用されており、財務部門と人事部門を除くナイト社の全部門を網羅しています。

最近、ナイト社の機密情報を含むファイルの一部がハッカーによって流出しました。ナイト社のインシデント対応チーム（IRT）は、直ちにシステム全体と事件の詳細の分析を開始しました。IRTは当初、ナイト社の従業員が脆弱なパスワードを使用していたため、不正なハッカーがアカウントに容易にアクセスできたのではないかと疑っていた。しかし、徹底的な調査の結果、ハッカーはファイル転送プロトコル（FTP）の通信を傍受することでアカウントにアクセスしていたことが判明した。

FTPは、アカウント間でファイルを転送するために使用されるネットワークプロトコルです。認証には平文のパスワードを使用します。この情報セキュリティインシデントの結果、ナイト社はIRTの助言に基づき、FTPをセキュアシェル（SSH）に置き換えることを決定した。これにより、通信を傍受した者は暗号化されたデータしか見ることはできなくなる。

これらの変更を受けて、ナイト社はリスク評価を実施し、管理策の導入によって同様の事象のリスクが最小限に抑えられたかどうかを検証した。この評価結果はISMSプロジェクトマネージャーによって承認され、新しい管理策の導入後のリスクレベルは同社のリスク許容度と一致していると判断された。

このシナリオに基づいて、以下の質問に教えてください。

シナリオ2に基づき、ISMSプロジェクトマネージャーはリスク評価の結果を承認しました。これは許容範囲内でしょうか？

- A. いいえ、リスク軽減後に残るリスクは、どの段階においても経営陣の承認を得る必要があります。
- B. いいえ、新しいISMS管理策を実施した後に残るリスクは、ISMSチームによって承認される必要があります。
- C. はい、リスク軽減後に残るリスクはすべてISMSプロジェクトマネージャーの承認を得る必要があります。

Answer: A (メッセージを残す)

ISO/IEC 27001の文脈では、リスクアセスメントの承認と、処理後の残存リスクレベルの受容は、通常、最高経営陣の責任となります。これは、最高経営陣が情報セキュリティマネジメントシステムとその結果に対して責任を負い、組織を代表してリスクを受け入れる権限を持っているためです¹²。参照：提供された情報は、ISO/IEC 27001のリスクアセスメントおよび処理プロセスの標準的な実践に基づいています。このプロセスでは、リスクの承認と受容における最高経営陣の役割が強調されています。

最新問題: 173

（2）-----を決定する際には、監査人は（1）-----を考慮する必要がある。

A. （1）標準要件、（2）監査基準

B. 1）監査リスク、2）監査目的

C. （1）違法行為に関連する罰則、（2）重要性

Answer: (解答を表示する)

監査人は、監査目標」を決定する際に「監査リスク」を考慮に入れるべきである。監査に伴うリスクを理解することで、目標を明確に定義することができ、監査が最も重要な懸念事項に焦点を当て、監査範囲と整合し、特定されたリスクに適切に対処できることが保証される。

最新問題: 174

シナリオ7 Lawsyは、ニュージャージー州とニューヨーク市にオフィスを構える大手法律事務所です。50名以上の弁護士を擁し、企業法務、知的財産、銀行業務、金融サービスといった分野で顧客に包括的な法的サービスを提供しています。同社は、情報セキュリティにおけるベストプラクティスの導入と技術革新への対応に注力することで、市場において確固たる地位を築いていると確信しています。

Lawsyは、過去2年間、ISMS（情報セキュリティマネジメントシステム）の厳格な導入、評価、および内部監査を実施してきた。

彼らは現在、知名度が高く信頼できる認証機関であるISMAに対し、ISO/IEC 27001認証の申請を行っている。

監査の第一段階では、監査チームは導入プロセス中に作成されたすべてのISMS文書をレビューした。

彼らはまた、経営陣によるレビューや内部監査の記録を精査し、評価した。

Lawsy社は、不適合に対して必要に応じて是正措置が講じられたことを示す証拠を提出し、これを受けて監査チームは内部監査担当者への聞き取り調査を実施した。この聞き取り調査により、内部監査計画と手順に関する詳細な理解が得られ、内部監査の適切性と頻度が検証された。

監査チームは、情報セキュリティポリシーやリスク評価基準などの戦略文書の検証を継続しました。情報セキュリティポリシーのレビュー中に、チームは、文書化された情報とガバナンスフレームワーク（すなわち情報セキュリティポリシー）を説明する手順との間に矛盾があることに気づきました。

従業員はノートパソコンを職場外に持ち出すことが許可されているものの、Lawsy社にはその使用に関する明確な手順が定められていません。社内規定にはノートパソコンの使用に関する一般的な情報しか記載されていません。同社は、ノートパソコンに保存されている情報の機密性と完全性を保護するために、従業員の常識に頼っています。この問題は、フェーズ1監査報告書に記載されています。

監査の第一段階が完了した後、監査チームリーダーは監査計画書を作成し、監査の目的、範囲、基準、および手順を明記した。

監査の第2段階では、監査チームは情報セキュリティポリシーを作成したサイバーセキュリティマネージャーにインタビューを行った。マネージャーは、Lawsy社が3ヶ月ごとに情報セキュリティに関する必須の研修と啓発コースを実施していることを指摘し、第1段階で指摘された問題点の妥当性を証明した。

面接後、監査チームは従業員研修記録50件のうち15件を精査し、Lawsy社が研修および意識向上に関するISO/IEC 27001の要件を満たしていると結論付けた。この結論を裏付けるため、監査チームは精査した従業員研修記録のコピーを作成した。

上記のシナリオに基づいて、以下の質問に答えてください。

監査チームは、調査した従業員の研修記録をコピーして、結論を裏付けました。監査チームは、この行動をとる前にローシーの承認を得るべきだったでしょうか？シナリオ7を参照してください。

A. はい。監査チームは、あらゆる状況において（メモを取ったり、文書をコピーしたりする場合も含め）、プロセスの存在を確認する際には、被監査者の承認を得る必要があります。

B. はい、被監査者が同意すれば、監査チームは監査中に確認した文書をコピーすることができます。

C. いいえ、監査チームは、文書が監査基準を満たしているかどうかを確認するために、文書をコピーする権利があります。

Answer: B (メッセージを残す)

はい、監査チームは文書をコピーする前にLawsyの承認を得る必要があります。これは、機密情報や秘密情報が含まれている可能性のある文書の複製について、被監査者が同意していることを確認するためのベストプラクティスです。監査担当者は情報を観察し記録することはできますが、信頼関係を維持し、機密保持契約を遵守するためには、文書のコピーには通常、明示的な許可が必要です。

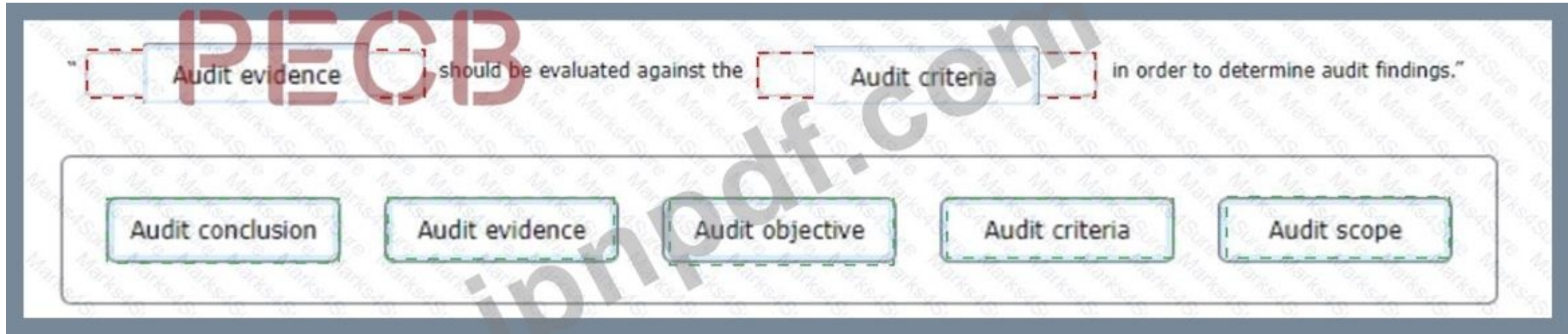
最新問題: 175

監査結果の生成に関して、次の文を最も適切に完成させる語を選択してください。

文を適切な単語で完成させるには、完成させたい空欄をタップして赤くハイライト表示し、下の選択肢から適切なテキストをタップしてください。または、選択肢を適切な空欄にドラッグすることもできます。



Answer:



Explanation:

監査結果を判断するためには、監査証拠を監査基準に照らして評価する必要がある。

監査証拠とは、監査人が監査プロセス中に取得した情報であり、監査意見または結論を形成するための根拠として使用されます12。監査証拠には、記録、文書、声明、観察、インタビュー、またはテスト結果が含まれます12。

監査基準とは、監査証拠と比較するための参照として使用される一連の方針、手順、基準、規制、または要件のことです12。監査基準は、ISO規格、業界のベストプラクティス、法的義務など、内部または外部の情報源から導き出すことができます12。

監査結果とは、監査証拠を評価し、監査基準13と比較するプロセスによって得られる結果です。監査結果は、監査基準が満たされている（適合か、満たされていない（不適合かを示すことができます。また、ベストプラクティスや改善の機会を特定することもできます13。

参考文献：

* ISO 19011:2022 マネジメントシステムの監査に関する指針

* ISO/IEC 27001:2022 情報技術—セキュリティ技術—情報セキュリティマネジメントシステム—要求事項

* 監査結果の構成要素 - 内部監査人協会

最新問題: 176

是正措置」とはどういう意味ですか？ 1つ選択してください。

- A. 不適合や事故の発生を防ぐための措置を講じる。
- B. 不適合や事故の原因を排除するための措置を講じる。
- C. 経営陣が不適合に対処するために講じた措置
- D. 不適合または事象を是正するための措置を講じる。

Answer: ([解答を表示する](#))

是正措置とは、発生した、または発生する可能性のある不適合や事象の根本原因を特定し、排除することで、それらの再発や発生を防止するプロセスです。是正措置はISO 27001の改善要件の一部であり、是正措置の特定、評価、実施、レビュー、文書化という標準的なワークフローに従います。

参考文献 :ISO 27001要求事項10.1に対する是正措置、不適合および是正措置の手順、PECB候補者ハンドブックISO 27001主任審査員（12ページ）

最新問題: 177

以下の記述のうち、文書レビューの目的を最も正確に説明しているのはどれですか？

- A. 文書管理システムが監査基準を満たしていないかどうかを明らかにし、監査報告書を裏付ける証拠を収集する。
- B. 文書管理システムが監査基準を満たしているかどうかを判断し、監査プロセスを支援するための調査結果を収集します。
- C. 記録に基づいて管理システムが監査基準を満たしているかどうかを判断し、オンサイト監査活動を支援するための情報を収集します。
- D. 管理システムが監査基準（ある場合）を満たしているかどうかを検出し、監査計画を裏付ける情報を決定する。

Answer: C ([メッセージを残す](#))

文書レビューとは、オンサイト監査活動の前に、マネジメントシステムに関連する文書化された情報を検証するプロセスです。文書レビューの目的は以下のとおりです。12

* 文書化されている範囲で、マネジメントシステムが監査基準に適合しているかどうかを判断する。つまり、文書がISOの要求事項と整合し、完全であり、準拠しているかどうかを確認する。

/IEC 27001およびその他の適用される規格または規制。

* オンサイト監査活動を支援するための情報を収集する。すなわち、マネジメントシステムの範囲、目的、プロセス、統制、リスク、機会を特定し、それに応じて監査方法、技術、リソースを計画する。

他の記述は正確ではありません。理由は以下のとおりです。

文書レビューは、マネジメントシステム全体の適合性または不適合性を明らかにするものではなく、文書化された情報のみを対象とするものです。マネジメントシステムの適合性または不適合性は、面談、観察、試験を含むオンサイト監査活動によって決定されます。12

* 文書レビューは、監査報告書やプロセスを裏付ける証拠や所見を収集するものではなく、オンサイト監査活動を裏付ける情報を収集するものです。証拠や所見はオンサイト監査活動中に収集され、その後文書化されて報告されます。12

文書レビューは、文書化されているマネジメントシステムの不適合を検出するものではなく、文書化された情報の適合性を判断するものです。マネジメントシステムの不適合は、マネジメントシステムのパフォーマンスと有効性を評価するオンサイト監査活動によって検出されます。12

* 文書レビューは、監査計画を裏付ける情報を特定するものではなく、オンサイト監査活動を裏付ける情報を収集するものです。監査計画は、監査範囲、目的、基準、およびプログラムに基づいて、文書レビューの前に作成されます。文書レビューは、監査計画の実施の一部です。12 参考文献:

1: ISO/IEC 27001:2022 リードオーディター（情報セキュリティマネジメントシステム）コース（CQIおよびIRCA認定トレーニング1）2: ISO/IEC 27001 リードオーディタートレーニングコース（PECB 2）

最新問題: 178

あなたは、地元の病院や官公庁などの大規模組織に輸送サービスを提供する国際物流組織の出荷部門でISMS監査を実施しています。荷物には通常、医薬品、生物学的サンプル、パスポートや運転免許証などの書類が含まれています。会社の記録を見ると、ラベルの住所が間違っていることや、15%のケースで1つの荷物に2つ以上の異なる住所のラベルが貼られていることなどが原因で、返品が大量に発生していることがわかります。あなたは輸送マネージャー（SM）の面接を行っています。

出荷前に商品の検査は行いましたか？

SM：明らかに破損している商品は、出荷前に担当スタッフが取り除きますが、利益率が非常に低いため、正式な検査プロセスを実施するのは経済的ではありません。

商品を返品した後、どのような措置を講じますか？

SM：これらの契約のほとんどは比較的少額なので、調査を行うよりも、ラベルを再印刷して個々の荷物を再送する方が簡単で便利だと考えています。

貴社が提起されたクレームは、ラベル表示プロセスに対する管理体制の不備により、ISO 27001:2022に準拠していません。

最終会議で、配送担当マネージャーは、自分の発言が誤解された可能性があるとして謝罪しました。彼は、正しいラベルが正しい荷物に貼られているかを自動的にチェックするバックエンドのITプロセスについて知らなかったため、ラベル貼付中に荷物が剥がれてしまうことを説明しました。そして、不適切な行為を撤回するようあなたに求めました。

監査チームリーダーとして、輸送マネージャーの依頼に対してあなたが取るべき正しい対応を表す3つの選択肢から選んでください。

- A. 輸送マネージャーに、彼の要望が監査報告書に含まれることを伝えてください。
- B. 監査人がより多くの時間を確保できるときに、経営陣が提供された新しい情報について話し合うことをお勧めします。
- C. 輸送管理者に、違反は軽微であり、直ちに是正する必要があることを通知してください。
- D. 審査チームのメンバーに、何が起こるべきだと考えているのか説明してもらってください。
- E. 彼にあなたの理解を伝え、不服従を撤回してください。
- F. 輸送マネージャーの正直なご意見に感謝しますが、不適合品を撤去するという提案は正しいアプローチではありません。
- G. 証拠の取得には非常に費用がかかるため、輸送管理者がこの違反を立証することを推奨します。
- H. 不適合項目が表示されるということは、修正が必要なより深刻なシステム障害の証拠です。

Answer: A,B,F (メッセージを残す)

- * A. 出荷マネージャーに、彼の要求が監査報告書に含まれることを伝えます。これは、監査報告書には、被監査者から提起された要求や異議を含め、監査に関連するすべての関連情報と証拠を文書化する必要があるためです。監査報告書には、監査の結論と勧告の根拠も記載する必要があります12。
- * B. 提供された新しい情報は、監査人がより多くの時間を確保できるようになったときに議論されることを経営陣に伝えます。これは、監査人が不完全または未検証の情報に基づいて性急な決定を下すべきではないためです。監査人は、新しい情報を体系的かつ客観的に検討および評価し、それが監査結果、不適合、または結論に影響を与えるかどうかを判断する必要があります12。
- * F. 出荷マネージャーの誠実さに感謝しつつも、不適合の取り下げは適切な対応ではないと助言する。これは、監査員は被監査者の協力と透明性を認め、感謝すべきであると同時に、専門家としての誠実さと独立性を維持すべきだからである。監査員は、不適合が誤って提起されたか、または効果的に修正され検証されたと確信しない限り、不適合を取り下げてはならない12。

参考文献：

- * ISO 19011:2022 マネジメントシステムの監査に関する指針
- * ISO/IEC 17021-1:2022 適合性評価－マネジメントシステムの監査及び認証を行う機関に対する要求事項－第1部：要求事項

最新問題: 179

あなたは、医療サービスを提供するABC（オーストラリアとカリフォルニア）の高齢者向け介護施設でISMS監査を実施しています。監査計画の次のステップは、ABCのモバイルアプリケーションの開発、サポート、およびライフサイクルプロセスの情報セキュリティを検証することです。監査中に、組織がモバイルアプリケーションの開発をCMMIレベル5、ITSM（ISO/IEC 20000-1）、およびBCMS（ISO 20000-1）の認証を取得している企業にアウトソーシングしていることがわかりました。

22301）と

ISMS（ISO/IEC 27001）の認証を取得しています。

ITマネージャーは、ソフトウェアセキュリティ管理プロセスについて説明しました。その概要は以下のとおりです。

モバイルアプリケーション開発においては、少なくとも「設計上のセキュリティ」と「事前定義されたセキュリティ」の原則を遵守すべきである。

以下の個人データ保護セキュリティ機能を含める必要があります。

アクセス制御。

個人データの暗号化には、鍵長256ビットの高次暗号化標準（AES）アルゴリズムが使用され、個人データは匿名化されます。

脆弱性のチェックを実施しましたが、セキュリティ上のバックドアは発見されませんでした。

最新のモバイルアプリケーションテストレポートをサンプルとしてご覧いただきました。詳細は以下のとおりです。

Target of Test: ABC's healthcare mobile app, version 1		Test results	Test summary
Security test			
Personal data encryption	Fail	Not able to perform the encryption.	
Personal data pseudonymisation	Fail	Not able to perform the pseudonymisation.	
Final approval:			
by: <i>Service Manager</i>			signed

ITマネージャーは、ソフトウェアセキュリティ管理手順に基づき、テスト結果は自身が承認する必要があると説明した。暗号化機能と匿名化機能は、システムとサービスのパフォーマンスを著しく低下させたため、テストに失敗した。この要件を満たすには、通常よりも150%多くのリソースが必要だった。サービスマネージャーは、アクセス制御が適切かつ許容範囲内であることに同意した。そのため、サービスマネージャーは承認書に署名した。監査結果を準備しています。正しい選択肢を選んでください。

- A. 不遵守 NC)。サービス管理者がソフトウェアセキュリティ管理手順を遵守していません。（第.1項、管理措置A.8.30に関連）
- B. 不適合 NC)が存在します。組織および開発者によって実施されたセキュリティテストが失敗しました。（第.1項、規制措置A.8.29に関連）
- C. 不適合なし NC)。サービスマネージャーはサービス提供を継続するという正しい判断を下しました。（第.1項、管理措置A.8.30に関連）
- D. 不適合 NC)があります。組織および開発担当者が受入試験を実施していません。（第.1項、規制措置A.8.29に関連）

Answer: A (メッセージを残す)

最新問題: 180

場景3 :NightCore是一家總部位於美國的跨國科技公司，專注於電子商務 雲端運算、數位串流媒體和人工智慧。在實施資訊安全管理系統 (ISMS) 8 個多月後，他們聘請了認證機構進行第三方審核，以獲得SO/IEC 27001 認證。認證機構成立了一個由七名審核員組成的團隊。傑克是最有經驗的審核員，被任命為審核組組長。多年來，他獲得了許多知名認證，例如SO/IEC 27001 首席審核員、CISA、CISSP 和 CISM。Jack 透過研究和評估 NightCore 實施的每項資訊安全要求和控制，對ISMS 審口的每個階段進行了全面分析。在第二階段審核期間。傑克發現了一些不合格項。在將購買的軟體許可證發票數量與軟體庫存進行比較後，傑克發現該公司的許多電腦一直在使用非法版本的軟體。他決定要求高階主管對這項違規行為做出解釋，看看他們是否意識到這一點。他的下一步是審計 NightCore 的 IT 部門。高層指派 NightCore 的系統管理員 Tom 擔任指導，陪伴Jack 和稽核團隊了解系統和數位資口基礎設施的口部運作。在採訪財務部的一名成員時，審計人員發現該公司最近向其一名顧問進行了一些不尋常的大額交易。收集有關交易的所有必要詳細資訊後。傑克決定直接訪問高階主管。在討論第一個不合格項時，高階主管告訴傑克，他們願意決定使用複製軟體而不是原始軟體，因為它更便宜Jack向NightCore的高層解釋口，使用非法版本的軟體違反了SO/IEC 27001和國家法律法規的要求。然而，他們似乎對此感到滿意。

監査から数か月後、ジャックは監査中に収集したナイトコアに関する情報の一部を、ナイトコアの競合他社に多額の金銭で売却した。

このシナリオに基づいて、以下の質問に答えてください。

シナリオ3によると。

- A. 付録A 5.1 情報セキュリティポリシー
- B. 付属書A 5.10 情報およびその他の関連資産の許容される使用
- C. 付属書A 5.32 知的財産権

Answer: C (メッセージを残す)

NightCoreは、違法なバージョンのソフトウェアを使用することで、ISO/IEC 27001の附属書A.8.1.1に規定されている知的財産権に関する規制を無視した。この規制では、組織記録の保護には、データまたはソフトウェアの形で保持されている知的財産および個人情報が含まれることが求められている。

最新問題: 181

あなたは経験豊富なISMS監査チームリーダーであり、監査員への研修と指導を行っています。監査員はリスクプロセスについて明確な理解が不足しているため、以下に詳述する各プロセスの例を示してほしいと依頼されました。

提供される各説明は、以下のリスク管理プロセスのいずれかに準拠している必要があります。

フォームに入力するには、入力したい空白部分をクリックして赤色でハイライト表示し、次に下の選択肢から適切なテキストをクリックしてください。または、各選択肢を適切な空白部分にドラッグすることもできます。

A process by which the nature of the risk is determined along with its probability and impact	
A process by which a risk is controlled at all stages of its life cycle by means of the application of organisational policies, procedures and practices	
A process by which a risk is recognised and described	
A process by which the impact and /or probability of a risk is compared against risk criteria to determine if it is tolerable	
A process by which the impact and/or probability of a risk is reduced by means of the application of controls	
A process by which a risk is passed to a third party, for example through obtaining appropriate insurance	

Risk transfer

Risk analysis

Risk identification

Risk management

Risk mitigation

Risk evaluation

Answer:

A process by which the nature of the risk is determined along with its probability and impact	Risk analysis
A process by which a risk is controlled at all stages of its life cycle by means of the application of organisational policies, procedures and practices	Risk management
A process by which a risk is recognised and described	Risk identification
A process by which the impact and /or probability of a risk is compared against risk criteria to determine if it is tolerable	Risk evaluation
A process by which the impact and/or probability of a risk is reduced by means of the application of controls	Risk mitigation
A process by which a risk is passed to a third party, for example through obtaining appropriate insurance	Risk transfer



Explanation:

process by which the nature of the risk is determined along with its probability and impact	Risk analysis
process by which a risk is controlled at all stages of its life cycle by means of the application of organisational policies, procedures and practices	Risk management
process by which a risk is recognised and described	Risk identification
process by which the impact and /or probability of a risk is compared against risk criteria to determine if it is tolerable	Risk evaluation
process by which the impact and/or probability of a risk is reduced by means of the application of controls	Risk mitigation
process by which a risk is passed to a third party, for example through obtaining appropriate insurance	Risk transfer

リスク分析とは、リスクの性質、発生確率、影響度を決定するプロセスです。リスク分析では、組織の情報セキュリティ目標や要件に影響を与える可能性のある事象や状況の発生確率と結果を推定します12。リスク分析には、定性的手法、定量的手法、またはその両方の組み合わせを使用できます12。

リスク管理とは、組織の方針、手順、慣行を適用することにより、リスクのライフサイクルのすべての段階でリスクを制御するプロセスです。リスク管理には、組織の情報セキュリティのパフォーマンスやコンプライアンスに影響を与える可能性のあるリスクの状況確立し、特定、分析、評価、対処、監視、およびレビューすることが含まれます12。リスク管理の目的は、リスクがタイムリーかつ効果的に特定および対処され、改善の機会が活用されるようにすることです12。

リスク識別とは、リスクを認識し、記述するプロセスです。リスク識別には、組織の情報セキュリティ目標または要件に影響を与える可能性のあるリスクの発生源、原因、事象、シナリオ、および潜在的な影響を特定し、文書化することが含まれます12。リスク識別には、ブレインストーミング、インタビュー、チェックリスト、アンケート、または履歴データなど、さまざまな手法を使用できます12。

リスク評価とは、リスクの影響や発生確率をリスク基準と比較し、許容できるかどうかを判断するプロセスです。リスク評価では、リスク分析の結果を、組織のリスク許容度、リスク耐性、リスク受容度を反映した事前定義された基準と比較します12。リスク評価には、ランキング、スコアリング、マトリックスなど、さまざまな方法を使用できます12。リスク評価は、適切なリスク対策オプションの優先順位付けと決定に役立ちます12。

リスク軽減とは、制御策を適用することによってリスクの影響や発生確率を低減するプロセスです。リスク軽減には、組織の情報セキュリティ目標や要件に影響を与える可能性のあるリスクを防止、軽減、移転、または受け入れるように設計された対策を選択して実施することが含まれます12。リスク軽減には、技術的、組織的、法的、物理的など、さまざまな種類の制御策が含まれる場合があります12。リスク軽減は、費用対効果分析と残存リスク評価に基づいて行う必要があります12。

リスク移転とは、適切な保険の取得などによって、リスクを第三者に移転するプロセスです。リスク移転には、リスクに対する責任または義務の一部または全部を、リスクを管理する能力や力量のある別の当事者と共有または移転することが含まれます12。リスク移転には、契約、合意、パートナーシップ、アウトソーシング、保険など、さまざまな方法があります12。リスク移転は、組織内の効果的なリスク管理の代替手段として使用すべきではありません12。

参考文献：

* ISO/IEC 27001:2022 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項

* ISO/IEC 27005:2022 情報技術－セキュリティ技術－情報セキュリティリスクマネジメント

有効な **ISO-IEC-27001-Lead-Auditor-CN** 問題集は GoShiken.com が提供された合格しやすい ISO-IEC-27001-Lead-Auditor-CN 試験問題集！ GoShiken.com が最新の **ISO-IEC-27001-Lead-Auditor-CN** 試験問題集を提供しています。GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 問題集をゲットする人はこちら:
<https://www.goshiken.com/PECB/ISO-IEC-27001-Lead-Auditor-CN-mondaishu.html> (418**30%OFF**問題集溶と正解付きで 30%w特別割引コード: **Freepdfdumps**)

最新問題: 182

あなたは、医療サービスを提供するABCという高齢者向け介護施設でISMS監査を実施しています。すべての入居者が、位置情報、心拍数、血圧をモニタリングするための電子リストバンドを装着していることに気づきました。リストバンドは、医療スタッフが入居者の健康状態を監視 分析するために、すべてのデータを自動的に人工知能 AI)クラウドサーバーにアップロードしていることが分かりました。

ISMSの適用範囲を確認するため、マネジメントシステム担当者 (MSR)にインタビューを行ったところ、ISMSの適用範囲にはアウトソーシングされたデータセンターも含まれると説明された。

ISMSの適用範囲を検証するために必要な監査証拠として、3つの選択肢を選んでください。

A. 被監査者は、施設および環境の安全性に関する居住者のニーズと期待を特定しました。

B. 被監査者はISO 9001認証を取得しています。

C. 被監査者は、医療サービスおよび患者データ処理に関する政府当局のニーズと期待を特定しました。

D. 被監査者は、住民の個人データを保護する方法に関する住民のニーズと期待を特定しました。

E. 被監査者は、快適な設備、医療専門家の能力、清潔な環境に関して、入居者のニーズと期待を特定しました。

F. 被監査者は、住民の医療サービスに対するニーズと期待を把握した。

G. AIクラウドサーバーが設置されているデータセンターとのITサービス契約

H. 被監査企業は、外部のソフトウェア会社からヘルスケアモニタリングアプリケーションを購入することを検討しています。

Answer: C,D,G (メッセージを残す)

ISO 27001:2022の4.3項によれば、組織は、内部および外部の問題、利害関係者の要求、および他の組織とのインターフェースと依存関係を考慮して、情報セキュリティマネジメントシステム (ISMS)の適用範囲を決定しなければならない。12 この場合、ISMSの適用範囲は、居住者のデータの医療監視と分析のための人工知能 AI)クラウドサーバーをホストするアウトソーシングされたデータセンターをカバーしている。したがって、ISMSの適用範囲を検証するために必要な監査証拠には、以下が含まれるべきである。

* 被監査機関は、医療サービスおよび患者データ処理に関する政府当局のニーズと期待を特定しました。これは外部の問題であり、ISMSの範囲に影響を与える利害関係者の要求事項です。被監査機関は、医療サービスおよび患者データの品質、安全性、プライバシーに関する関連法規を遵守する必要があるためです。12

* 被監査機関は、居住者の個人データをどのように保護すべきかに関する居住者のニーズと期待を特定しました。これは外部の問題であり、ISMSの範囲に影響を与える利害関係者の要求事項です。被監査機関は、電子リストバンドとAIクラウドサーバー12によって収集、処理、保存される居住者の個人データの機密性、完全性、可用性を確保する必要があるためです。

* 人工知能 AI)クラウドサーバーが設置されているデータセンターとのITサービス契約。これは、ISMSの範囲に影響を与える他の組織とのインターフェースおよび依存関係です。監査対象者は、ISMSに関連する外部提供のプロセス、製品、およびサービスを管理し、情報セキュリティに関連する適切な契約要件を実装する必要があります。12 次のオプションは、ISMSの範囲を検証するのに適切または十分ではありません。

* 被監査者は、施設および環境の安全性に関する居住者のニーズと期待を特定しました。これは外部の問題であり、利害関係者の要求事項ですが、情報セキュリティ12とは関係がないため、ISMSの範囲には影響しません。

* 被監査企業はISO 9001認証を取得しています。これは被監査企業の品質マネジメントシステムを示すものですが、情報セキュリティとは関係がないため、ISMSの範囲を検証するものではありません12

* 被監査者は、居住者の快適な施設、医療専門家の能力、清潔な環境に関するニーズと期待を特定しました。これらは外部の問題および利害関係者の要求事項ですが、情報セキュリティ12とは関係がないため、ISMSの範囲には影響しません。

* 被監査者は、住民の医療サービスに関するニーズと期待を特定しました。これらは外部の問題および利害関係者の要求事項ですが、情報セキュリティに特化したものではないため、ISMSの範囲を検証するものではありません。12

* 被監査企業は、外部ソフトウェア会社からヘルスケアモニタリングアプリを購入することを検討しています。これは将来的にISMSの範囲に影響を与える可能性のある変更ですが、まだ実装または管理されていないため、ISMSの現在の範囲を検証するものではありません。12 参考文献:

1: ISO/IEC 27001:2022 リードオーディター (情報セキュリティマネジメントシステム)コース (CQIおよびIRCA認定トレーニング1) 2: ISO/IEC 27001 リードオーディタートレーニングコース (PECB 2)

最新問題: 183

シナリオ9 :Techmanicは1995年に設立されたベルギーの企業で、現在はブリュッセルに拠点を置いています。ITコンサルティング、ソフトウェア設計、ハードウェア/ソフトウェアサービス（導入保守を含む）を提供しています。公共サービス、金融、通信、エネルギー、医療、教育などの業界にサービスを提供しています。顧客中心主義の企業として、顧客との強固な関係構築と最先端のセキュリティ対策を最優先事項としています。Techmanicは、ISO/IEC 27001認証を1年間保持していることを誇りに思っています。認証監査において、監査員はISMSの実装にいくつかの不整合を発見しました。しかし、発見された問題はISMSの意図された成果達成能力に影響を与えなかったため、監査員がリモートで根本原因分析と是正措置を実施した後、Techmanicは認証を取得しました。継続的な改善と過去の評価からの学習の価値を認識し、Techmanicは過去の監視監査レポートをレビューする慣行を導入しました。この積極的なアプローチは、潜在的な不適合を特定して対処するのに役立つだけでなく、ITコンサルティング分野における再認証プロセスを効率化することも目的としています。監視監査中に、複数の不適合が特定されました。内部監査員の報告書によると、ISMSは引き続きISO/IEC 27001*の要求事項を満たしていましたが、Techmanicはマネージドサービスに関連する不適合に対処していませんでした。さらに、内部監査報告書にはいくつかの矛盾があり、マネージドサービス監査における内部監査員の独立性について疑問が生じました。このため、認証の延長は承認されませんでした。そこで、Techmanicは別の認証機関への移管を申請しました。同時に、同社は顧客に対し、ISO/IEC 27001認証はITサービスとマネージドサービスの両方を対象としている旨の声明を発表しました。

上記のシナリオに基づいて、以下の質問に答えてください。

シナリオ9に基づき、監査人は監督監査期間中に延長監査を実施することを決定しました。この状況をどのように定義しますか？

- A. 監視監査中に拡張監査が実施されたため、許容範囲内です。
- B. 監査人は監査期間の延長を承認できないため、受け入れられません。
- C. 拡張監査は最初の認証監査の後にものみ実施されるため、受け入れられません。

Answer: (解答を表示する)

包括的かつ詳細な徹底分析

A. 正解：

ISO/IEC 17021-1では、拡張監査を監視監査と並行して実施することが認められています。

これにより、重複作業とコストを削減しつつ、法令遵守を維持できます。

B. 不正解：

認証機関は、延長監査を承認する権限を有する。

C. 不正解：

延長は2年目に限定されず、認証期間中のいつでも可能です。

関連規格参照：

最新問題: 184

以下の状況のうち、脅威となるのはどれですか？

- A. HackXは海賊版ソフトウェアを使用および配布しています。
- B. 情報セキュリティ研修は、組織のITチームのメンバーのみに提供されます。
- C. ハッカーがパスワードを解読して管理者アカウントを侵害しました。

Answer: C (メッセージを残す)

最新問題: 185

質問：

複数の監査テスト計画を組み合わせて使用する目的は何ですか？

- A. 複数の方法を用いて、基準およびガイドラインへの準拠を確認する。
- B. 組織のすべての領域が同じレベルで監査されるようにします。
- C. 頻繁な監査の必要性を軽減する

Answer: (解答を表示する)

包括的かつ詳細な解説：

* A. 正解:

複数の監査テスト計画を組み合わせることで、異なる視点や検証手法が適用され、監査の精度が向上します。

* ISO 19011:2018は、包括的な結果を確保するために、監査に対する多様なアプローチを推奨しています。

* B. 不正解:

* すべての分野が同等の監査を必要とするわけではなく、リスクに基づいた重点的な監査が望ましい。

* C. 不正解:

組織のニーズによっては、頻繁な監査が必要となる場合があります。

関連規格参照：

* ISO 19011:2018 6.4.3項（保証のための複数の監査試験方法の使用）

最新問題: **186**

審核方法可以與代表受審核方的個人互動，也可以不互動。下列哪兩種方法具有互動性？

A. 抽樣（例如口品）

B. 透過即時視訊串流觀察執行的工作

C. 與受審核方一起檢討清單

D. 檢口地方當局的法律合規性

E. 進行採訪

F. 分析審核前提供的文件

Answer: C,E ([メッセージを残す](#))

According to the PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, audit methods can be classified into two categories: with or without interaction with individuals representing the auditee (page 12).

Audit methods with interaction include reviewing checklists with auditee and conducting interviews, as they involve direct communication and feedback from the auditee. Audit methods without interaction include sampling (e.g. products), observing work performed via live video streaming, checking legal compliance with local authorities, and analysing documents provided in advance of the audit, as they do not require any dialogue or exchange with the auditee. References: PECB Candidate Handbook for ISO/IEC 27001 Lead Auditor, page 12.

最新問題: **187**

您是一位經驗豐富的 ISMS 審核團隊領導者。您目前正在對國際運輸組織進行第三方監督審核。您抽取了四份口部稽核報告，其中指出：

報告 1 - 審計員：詹姆斯先生

一年來，該組織在100 次中有 23 次未能滿足其承諾的交付日期。

分級 - 次要

矯正措施到期時間 :9 個月□。

報告 2 - 審計員：詹姆斯先生

1 月至 3 月期間，我們收到了125 起有關服務台團隊的投訴。客口指責他們粗魯且反應遲鈍。

分級 - 次要

矯正措施到期時間 :12 個月□。

報告 3 - 審計員：詹姆斯先生

上個月收到的 40 個客口訂單中，有38 個已正確處理。其餘 2 份中，一份缺簽名，一份缺日期

評分 -

更正期間 :3週□

報告 4 - 審計員：羅傑斯先生

在檢口的 30 份人事記錄中，發現26 份已完全填寫，而其餘4 份均缺少個人的開始日期。

分級 - 主要

更正期間 :1週

これらの報告書についてあなたが懸念している点を、以下の4つの選択肢のうちどれが表していますか？

- A. 法令遵守状況の調査が行われなかったことを懸念しています。
- B. その組織が基準を満たさない製品を格付けするための基準を持っているかどうかが気になります。
- C. レポート3に評価が記録されていないことが気になります。
- D. 審査員が情報セキュリティプロセスにしか注目しないのではないかと心配しています。
- E. 監査人が修正と是正措置の違いを理解していないのではないかと心配しています。
- F. 重大な不適合に対処するための措置は、軽微な不適合に対処するための措置よりも先に完了すべきなので、私は懸念しています。
- G. 監査人が内部監査の大部分を実施しているように見えることが懸念されます。
- H. 4つの報告書間で、不適合事項への対応期限が大きく異なっていたことを懸念しています。

Answer: B,C,E,H (メッセージを残す)

最新問題: 188

管理體系審核的目的是？選擇1

- A. 評估組織管理系統的性能
- B. 提升組織管理系統的性能
- C. 管理組織管理系統的性能
- D. 研究組織管理系統的性能

Answer: A (メッセージを残す)

A management system audit is a systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled. The audit criteria are a set of requirements that may include policies, procedures, standards, regulations, etc. The purpose of a management system audit is to evaluate the performance of an organisation's management system in terms of its effectiveness, efficiency, compliance, and improvement. A management system audit can also identify strengths, weaknesses, opportunities, and risks of the management system and provide recommendations for improvement.

最新問題: 189

あなたは経験豊富なISMS監査員で、現在、初めての認証監査を受けているISMS監査員をサポートしています。彼女は、組織の情報セキュリティ目標を監査する際に何を検証すべきかをあなたに尋ねます。あなたは監査チェックリストに含まれる項目について質問し、彼女は次のように答えます。

ISO/IEC 27001への準拠に関して、以下の回答のうち、あなたが特に懸念する3つの項目はどれですか？

2022年？

- A. 各情報セキュリティ目標を、その目標を達成するために理解する必要のある担当者にどのように伝えるかを検討します。
- B. 経営陣が今年の情報セキュリティ目標を策定したかどうかを確認します。策定していない場合は、計画通りにタスクが完了したかどうかを確認します。
- C. 情報セキュリティの目標が文書化されているか確認し、全員が何を達成する必要があるのか、どのように達成するのか、いつ達成するのかを理解していることを確認します。
- D. 情報セキュリティ目標を定期的に見直し、必要に応じてこれらの目標を変更または取り消すための適切な手順があるかどうかを確認します。
- E. 各目標に完了日が設定されているかどうか、また、達成日が設定されていない目標がないかを確認します。
- F. 各目標を達成するために必要な予算、人員、資材が決定されているかどうかを確認します。
- G. 情報セキュリティに関するすべての目標が測定可能かどうかを確認します。測定可能でない場合、組織は進捗状況を追跡できなくなります。

Answer: B,C,E (メッセージを残す)

情報セキュリティマネジメントシステム (ISMS)の確立、実施、維持、継続的改善に関する要求事項を規定するISO/IEC 27001:2022によると、6.2項では、組織は関連する機能およびレベルで情報セキュリティ目標を設定する必要があると規定されています1。目標は、情報セキュリティポリシーと整合していること、測定可能であること（可能な場合）、評価可能であること、監視されていること、伝達されていること、必要に応じて更新されていること1が求められます。したがって、ISMS監査員は、組織の情報セキュリティ目標を監査する際に、監査基準に従ってこれらの側面を検証する必要があります。

ISO/IEC 27001:2022への適合性に関して懸念が生じるISMS監査員研修生からの回答は以下の3つです。

経営陣が今年度の情報セキュリティ目標を決定したかどうかを確認します。決定していない場合は、このタスクが完了するように計画されているかどうかを確認します。この回答は、研修中の監査員が、経営幹部レベルだけでなく、関連する機能やレベルにおいても情報セキュリティ目標を設定する必要があることを認識していないことを示唆しているため、懸念を生じさせます。また、研修中の監査員が情報セキュリティ目標の決定の遅延や延期を容認する意思があることを示唆しており、これはISMSのパフォーマンスと有効性に影響を与える可能性があります。

情報セキュリティの目標が紙に書き出されているか確認し、達成すべきこと、その達成方法、達成期限を全員が明確に理解できるようにします。この回答は、研修中の監査担当者が、情報セキュリティの目標は紙に書き出すだけでなく、測定可能（可能であれば）または評価可能なものにすることが必要であることを認識していないことを示唆しているため、懸念を生じさせます。また、研修中の監査担当者が、電子記録やデジタル記録、ポスター、ニュースレターなど、情報セキュリティの目標を文書化および伝達するためのさまざまなメディアや形式の柔軟性と適合性を認識していないことも示唆しています。

各目標に完了日が設定されていること、および「達成期限」が設定されていない目標がないことを確認します。この回答は、研修中の監査担当者が、特定の期日までに完了するだけでなく、監視される情報セキュリティ目標を設定する必要があることを認識していないことを示唆しているため、懸念を生じさせます。また、研修中の監査担当者が、組織の内部または外部の状況に変化が生じた場合、あるいは新たなリスクや機会が生じた場合など、必要に応じて情報セキュリティ目標を更新する可能性と必要性を認識していないことも示唆しています。

ISMS監査員研修生からのその他の回答は許容範囲内であり、ISO/IEC 27001:2022への適合性に関して懸念事項はありません。例えば、各情報セキュリティ目標が、目標達成のためにその目標を認識する必要のある人々にどのように伝達されているかを確認することは、条項6.2の伝達面の検証に関連しています。情報セキュリティ目標を定期的に見直し、必要に応じて修正または取り消すためのプロセスが整備されていることを確認することは、条項6.2の更新面の検証に関連しています。各目標を達成するために必要な予算、人員、資材が決定されていることを確認することは、条項6.2の計画面の検証に関連しています。すべての情報セキュリティ目標が測定可能であることを確認すること。測定可能でない場合、組織は目標に対する進捗状況を追跡することができません。これは、条項6.2の測定可能性面の検証に関連しています。参照 :ISO/IEC 27001:2022 - 情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステム - 要求事項

最新問題: 190

目的、基準、範囲は、第三者機関によるISMS監査の重要な特徴です。監査の目的を構成する2つの質問はどれですか？

- A. 顧客のプロセスと機能を評価する
- B. ISO/IEC 27001の要求事項への準拠を評価する。
- C. 監査計画を完了する
- D. ISMSを導入しているサイトを確認する
- E. ISMSの適用範囲を定義する
- F. 組織効率の見直し

Answer: B,D ([メッセージを残す](#))

監査目的とは、顧客または認証機関が監査を通じて達成しようとする具体的な目標または目的のことです。監査目的とは、監査が何を達成しようとするかを明確にし、監査の計画と実施の基礎となるものです。監査目的は、監査の種類、範囲、基準によって異なる場合がありますが、明確で、測定可能で、達成可能なものでなければなりません。

第三者機関によるISMS監査の監査目的の例としては、以下のようなものがあります。

* ISO/IEC 27001の要求事項への適合性を評価する :この目的は、組織のISMSが、情報セキュリティマネジメントシステムの確立、実装、維持、および改善に関するベストプラクティスを規定するISO/IEC 27001規格の要求事項を満たしていることを監査が検証することを意味します。監査では、組織のISMSの文書、プロセス、管理策、およびパフォーマンスを、規格の条項および附属書Aの管理策に照らして評価します。

* ISMS運用拠点の確認 :この目的は、組織のISMSが、組織が事業を運営またはサービスを提供しているすべての関連拠点または場所を網羅していることを確認することです。監査では、ISMSの適用範囲が正確であり、組織の状況、目的、およびリスクと整合していることを検証します。

その他のフレーズは監査目的ではなく、むしろ次のとおりです。

* 顧客のプロセスと機能を評価する :これは監査の目的ではなく、組織のプロセスと機能が満たすべき監査基準または要件です。監査基準とは、監査証拠を比較して適合性または不適合性を判断するための基準です。監査基準には、ISO/IEC 27001の要求事項、顧客の要求事項、またはその他の適用可能な規格や規制が含まれる場合があります。

監査計画の実施 :これは監査の目的ではなく、監査人が監査中に実行するタスクまたは活動です。監査計画とは、目的、範囲、基準、スケジュール、役割、責任など、監査の取り決めや詳細を記述した文書です。監査人は、監査が効果的かつ効率的に実施されるよう、監査計画に従って実行する必要があります。

* ISMSの適用範囲を決定する :これは監査の目的ではなく、監査を実施するための前提条件またはインプットです。ISMSの適用範囲とは、組織内の情報セキュリティ管理システムの範囲と境界のことです。ISMSに含まれる、または除外されるプロセス、活動、場所、資産、および利害関係者を定義します。ISMSの適用範囲は、認証を申請する前、または監査を受ける前に組織によって決定される必要があります。

組織効率の見直し :これは監査の目的ではなく、監査を実施することで得られる可能性のある結果です。組織効率とは、組織が目標達成のためにリソースをどれだけ効果的に活用しているかを示す指標です。監査は、情報セキュリティ管理システムの強み、弱み、機会、脅威を特定することで、組織効率の見直しと改善に役立つ可能性があります。

参考文献：

* ISO/IEC 27001:2022 リードオーディター（情報セキュリティマネジメントシステム）の目的と内容は、Quality.orgおよびPECBによるものです。

* ISO 19011:2018 マネジメントシステムの監査に関する指針 [第5.3.1項]

最新問題: 191

メールアカウントを引き続き使用するには、名前、メールアドレス、パスワードを送信するように求めるメールが届きます。これらの情報を送信しないと、メールアカウントは無効になります。このシナリオは何を示しているでしょうか？

A. 人員に関連する脆弱性

B. 無許可の脅迫行為の種類

C. 脅威メッセージの種類に関する妥協

Answer: B ([メッセージを残す](#))

ここで説明したシナリオは、フィッシング攻撃の典型的な例です。フィッシング攻撃とは、攻撃者が電子通信において信頼できる組織になりすますソーシャルエンジニアリングの一種です。その目的は、個人を騙して機密情報を提供させることです。これは、攻撃者が個人情報への不正アクセスを試みるという点で、不正行為型の脅威に該当します。参考文献：⇒フィッシングを脅威として捉えるこの理解は、情報セキュリティ管理システムの原則と一致しており、フィッシング攻撃とその防止策を説明する資料によって裏付けられています。

最新問題: 192

シナリオ7 Lawsyは、ニュージャージー州とニューヨーク市にオフィスを構える大手法律事務所です。50名以上の弁護士を擁し、企業法務、知的財産、銀行業務、金融サービスといった分野で顧客に包括的な法的サービスを提供しています。同社は、情報セキュリティにおけるベストプラクティスの導入と技術革新への対応に注力することで、市場において確固たる地位を築いていると確信しています。

Lawsyは、過去2年間、ISMS（情報セキュリティマネジメントシステム）の厳格な導入、評価、および内部監査を実施してきた。

彼らは現在、知名度が高く信頼できる認証機関であるISMAに対し、ISO/IEC 27001認証の申請を行っている。

監査の第一段階では、監査チームは導入プロセス中に作成されたすべてのISMS文書をレビューした。

彼らはまた、経営陣によるレビューや内部監査の記録を精査し、評価した。

Lawsy社は、不適合に対して必要に応じて是正措置が講じられたことを示す証拠を提出し、これを受けて監査チームは内部監査担当者への聞き取り調査を実施した。この聞き取り調査により、内部監査計画と手順に関する詳細な理解が得られ、内部監査の適切性と頻度が検証された。

監査チームは、情報セキュリティポリシーやリスク評価基準などの戦略文書の検証を継続しました。情報セキュリティポリシーのレビュー中に、チームは、文書化された情報とガバナンスフレームワーク（すなわち情報セキュリティポリシー）を説明する手順との間に矛盾があることに気づきました。

従業員はノートパソコンを職場外に持ち出すことが許可されているものの、Lawsy社にはその使用に関する明確な手順が定められていません。社内規定にはノートパソコンの使用に関する一般的な情報しか記載されていません。同社は、ノートパソコンに保存されている情報の機密性と完全性を保護するために、従業員の常識に頼っています。この問題は、フェーズ1監査報告書に記載されています。

監査の第一段階が完了した後、監査チームリーダーは監査計画書を作成し、監査の目的、範囲、基準、および手順を明記した。

監査の第2段階では、監査チームは情報セキュリティポリシーを作成したサイバーセキュリティマネージャーにインタビューを行った。マネージャーは、Lawsy社が3ヶ月ごとに情報セキュリティに関する必須の研修と啓発コースを実施していることを指摘し、第1段階で指摘された問題点の妥当性を証明した。

面接後、監査チームは従業員研修記録50件のうち15件を精査し、Lawsy社が研修および意識向上に関するISO/IEC 27001の要件を満たしていると結論付けた。この結論を裏付けるため、監査チームは精査した従業員研修記録のコピーを作成した。

上記のシナリオに基づいて、以下の質問に答えてください。

Lawsy社は、職場外でのノートパソコンの使用に関する手順を定めておらず、ノートパソコンに保存された情報の機密性を保護するために従業員の常識に頼っている。これは以下のことを示唆している。

A. 異常

B. 不適合品

C. 一貫性

Answer: B ([メッセージを残す](#))

Lawsy社は、職場外でのノートパソコンの使用を許可しているにもかかわらず、具体的な使用手順を定めていないため、規格不適合となります。ISO/IEC 27001では、セキュリティ管理策と管理プロセスを明確に定義、文書化、実施することが求められています。従業員の一般的な知識だけに頼ることは、モバイルワークやテレワークに伴う情報セキュリティリスクの管理に関する規格の要件を満たしません。

参照規格 :ISO/IEC 27001:2013、A.6.2項 (モバイルデバイスおよびテレワークの管理)

最新問題: 193

あなたは、医療サービスを提供するABCという名の高齢者向け介護施設で、ISMS（情報セキュリティマネジメントシステム）監査を受けています。

審核計劃の下一步是驗證 ABC 醫療保健行動應用程式開發、支援和生命週期流程的資訊安全性。在審核過程中，您了解到該組織將行動應用程式開發外包給了經過CMMI 5 級、ITSM (ISO/IEC 20000-1)、BCMS (ISO 22301) 和ISMS (ISO/IEC 27001) 認證的專業軟體開發組織。

IT經理介紹了軟體安全管理流程，並將流程總結如下：

行動應用程式開發至少應採用「設計安全」和「預設安全」原則。應具備以下個人資料保護安全功能：

存取控制。

個人資料加密，即高階加密標準 (AES) 演算法，金鑰長度256位元；個人資料假名化

已檢口漏洞，無安全後門

您採樣最新的行動應用測試報告 - 參考 ID :0098，詳細資訊如下：

Target of Test: ABC’s healthcare mobile app, version 1	Test results	Test summary
Performance test		
Response time	GOOD	Sampling 20 users, aged between 15-20, all of them feel good about the response time.
Useability and user interface	GOOD	Sampling 20 users, aged between 15-20, all of them feel good about the user interface, size of the text, and colour.
Security test		
Access control (username and password)	PASS	Compliance with the organisation’s information security policy, unique username and minimal 12 digits password (with Capital/Lower case, numbers, symbols combination)
Access control – One-time-password (OTP)	PASS	The mobile app generates an 8-digit OTP and sends it to an authorised user’s mobile phone via SMS, as a second factor of identity authentication.

Personal data encryption	Fail	Not able to perform the encryption.
Personal data pseudonymization	Fail	Not able to perform the pseudonymization.
Final approval:		
by: Service Manager		signed

您想進一步調口其他領域以收集更多審計證據。選擇三個不會出現在您的審核追蹤中的選項。

- A. 收集更多證據， 了解居民家庭成員為安裝ABC 的醫療保健行動應用程式支付的費用。（與第.2條相關）
- B. 透過在手機上下載並測試行動應用程式來收集更多證據。（與控制A.8.1 相關）
- C. 收集更多證據以確定 ABC 醫療保健行動應用程式的使用者數量。（與第.2條相關）
- D. 收集更多有關組織如何執行個人資料處理測試的證據。（與控制措施A.5.34 相關）
- E. 收集更多有關組織業務連續性政策的證據。（與控制措施A.5.30 相關）
- F. 收集更多有關組織在選擇外部服務提供者時如何管理資訊安全的證據。（與控制措施A.5.19 相關）
- G. 收集更多有關開發人員如何培訓其口品支援人員的證據。（與第.2條相關）
- H. 收集更多證據來驗證開發人員的 CMMI Level 5、ITSM (ISO/IEC 20000-1)、BCMS (ISO22301) 和 ISMS (ISO/IEC 27001) 認證。（與控制措施A.5.21 相關）

Answer: (解答を表示する)

The three options that will not be in your audit trail are A, C, and H. These options are either not relevant to the information security of ABC's healthcare mobile app development, support, and lifecycle process, or not within the scope of your audit. The amount of money that residents' family members pay to install the app (A) and the number of users of the app are not related to the information security aspects or objectives of the ISMS1. The verification of the developer's certifications (H) is not your responsibility as an ISMS auditor, as you should rely on the competence and impartiality of the certification bodies that issued them2. The other options are relevant and within the scope of your audit, as they relate to the security functions, testing, policies, and procedures of the mobile app development, support, and lifecycle process13. References: 1: ISO /IEC 27001:2022, Information technology - Security techniques - Information security management systems - Requirements, Clause 4.2 \n2: ISO/IEC 27006:2022, Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems, Clause 4.1 \n3: PECB Certified ISO/IEC 27001 Lead Auditor Exam Preparation Guide, Domain 5: Conducting an ISO/IEC 27001 audit

最新問題: 194

あなたは、医療サービスを提供するABC オーストラリアとカリフォルニア)の高齢者向け介護施設でISMS監査を実施しています。監査計画の次のステップは、ABCのモバイルアプリケーションの開発、サポート、およびライフサイクルプロセスの情報セキュリティを検証することです。監査中に、組織がモバイルアプリケーションの開発をCMMIレベル5、ITSM (ISO/IEC 20000-1)、およびBCMS (ISO 20000-1)の認証を取得している企業にアウトソーシングしていることがわかりました。22301)とISMS (ISO/IEC 27001)の認証を取得しています。ITマネージャーは、ソフトウェアセキュリティ管理プロセスについて説明しました。その概要は以下のとおりです。モバイルアプリケーション開発においては、少なくとも 設計上のセキュリティ」と 事前定義されたセキュリティ」の原則を遵守すべきである。以下の個人データ保護セキュリティ機能を含める必要があります。アクセス制御。個人データの暗号化には、鍵長256ビットの高次暗号化標準 (AES)アルゴリズムが使用され、個人データは匿名化されます。

脆弱性のチェックを実施しましたが、セキュリティ上のバックドアは発見されませんでした。
最新のモバイルアプリケーションテストレポートをサンプルとしてご覧いただきました。詳細は以下のとおりです。

Target of Test: ABC's healthcare mobile app, version 1		Test results	Test summary
Security test			
Personal data encryption		Fail	Not able to perform the encryption.
Personal data pseudonymisation		Fail	Not able to perform the pseudonymisation.
Final approval:			
Signed			

IT Service Manager
ITマネージャーは、ソフトウェアセキュリティ管理手順に基づき、テスト結果は自身が承認する必要があると説明した。暗号化機能と匿名化機能は、システムとサービスのパフォーマンスを著しく低下させたため、テストに失敗した。この要件を満たすには、通常よりも150%多くのリソースが必要だった。サービスマネージャーは、アクセス制御が適切かつ許容範囲内であることに同意した。そのため、サービスマネージャーは承認書に署名した。
監査結果を準備しています。正しい選択肢を選んでください。

- A. 不適合 (NC)が存在します。組織および開発者によって実施されたセキュリティテストが失敗しました。
(第1項、規制措置A.8.29に関連)
- B. 不遵守 (NC)。サービス管理者がソフトウェアセキュリティ管理手順を遵守していません。(第1項、管理措置A.8.30に関連)
- C. 不適合なし (NC)。サービスマネージャーはサービス提供を継続するという正しい判断を下しました。
(第1項、管理措置A.8.30に関連)
- D. 不適合 (NC)が存在します。組織および開発担当者は受入試験を実施していません。
(第1項、規制措置A.8.29に関連)

Answer: B (メッセージを残す)

最新問題: 195

- 以下の記述のうち、文書レビューの目的を最もよく表しているのはどれですか？
- 記録管理システムが監査基準を満たしているかどうかを判断し、監査報告書を裏付ける証拠を収集する。
- A. 記録された管理システムが監査基準を満たしているかどうかを判断し、監査プロセスを支援するために結果を収集します。
- B. 管理システム（記録部分が監査基準を満たしているかどうかを判断し、オンサイト監査活動を支援するための情報を収集します。
- C. 監査基準に基づいて、管理システムに記録されている不適合項目を検出し、監査プログラムをサポートする情報を特定します。

Answer: C (メッセージを残す)

文書レビューとは、オンサイト監査活動の前に、マネジメントシステムに関連する文書化された情報を検証するプロセスです。文書レビューの目的は以下のとおりです。12

* 文書化されている範囲で、マネジメントシステムが監査基準に適合しているかどうかを判断する。つまり、文書がISOの要求事項と整合し、完全であり、準拠しているかどうかを確認する。

1/IEC 27001およびその他の適用される規格または規制。

* オンサイト監査活動を支援するための情報を収集する。すなわち、マネジメントシステムの範囲、目的、プロセス、統制、リスク、機会を特定し、それに応じて監査方法、技術、リソースを計画する。

他の記述は正確ではありません。理由は以下のとおりです。

文書レビューは、マネジメントシステム全体の適合性または不適合性を明らかにするものではなく、文書化された情報のみを対象とするものです。マネジメントシステムの適合性または不適合性は、面談、観察、試験を含むオンサイト監査活動によって決定されます。12

* 文書レビューは、監査報告書やプロセスを裏付ける証拠や所見を収集するものではなく、オンサイト監査活動を裏付ける情報を収集するものです。証拠や所見はオンサイト監査活動中に収集され、その後文書化されて報告されます。12

文書レビューは、文書化されているマネジメントシステムの不適合を検出するものではなく、文書化された情報の適合性を判断するものです。マネジメントシステムの不適合は、マネジメントシステムのパフォーマンスと有効性を評価するオンサイト監査活動によって検出されます。12

* 文書レビューは、監査計画を裏付ける情報を特定するものではなく、オンサイト監査活動を裏付ける情報を収集するものです。監査計画は、監査範囲、目的、基準、およびプログラムに基づいて、文書レビューの前に作成されます。文書レビューは、監査計画の実施の一部です。12 参考文献:

1: ISO/IEC 27001:2022 リードオーディター（情報セキュリティマネジメントシステム）コース（CQIおよびIRCA認定トレーニング1）2: ISO/IEC 27001 リードオーディタートレーニングコース（PECB 2）

最新問題: 196

シナリオ4 :そのブランドプロモーション会社は、米国で最も有名な企業のいくつかと取引のあるマーケティング会社です。

社内コスト削減のため、Branding社は2年以上にわたり、ソフトウェア開発とITヘルプデスク業務をTechvology社にアウトソーシングしています。Techvology社は、Branding社のソフトウェア、ネットワーク、ハードウェアに関する要件を管理するために必要な専門知識を有しています。Branding社は情報セキュリティマネジメントシステム（ISMS）を導入し、ISO/IEC 27001認証を取得しており、高い情報セキュリティ基準を維持するという強い意志を示しています。Branding社は、アウトソーシング先のTechvology社の業務がISO/IEC 27001のセキュリティ要件を満たしていることを確認するため、定期的に監査を実施しています。

前回の監査では、ブランディングの監査チームは監査対象となるプロセスと監査計画を特定しました。テックボロジーが過去1年間に2件の情報セキュリティインシデントを報告したことを踏まえ、証拠に基づくアプローチを採用しました。監査は、これらのインシデントへの対応を評価し、アウトソーシング契約の条件を遵守していることを確認することに重点を置いています。監査は、提供されたサービスがブランディングの期待と確立された基準を満たしているかどうかを評価するために、テックボロジーのアウトソーシング業務の品質を監視する方法を包括的にレビューすることから始まりました。監査人はまた、テックボロジーが両当事者間の契約上の要件を遵守していることを確認しました。これには、情報セキュリティ対策を含むすべての側面を遵守していることを確認するために、アウトソーシング契約の条件を徹底的にレビューすることが含まれます。

さらに、今回の監査では、Techvologyのアウトソーシング業務およびその他の組織を管理するためのガバナンスプロセスについても厳格な評価が行われました。このステップはブランドプロモーションにとって非常に重要であり、アウトソーシング契約に伴う潜在的なリスクを軽減するための適切な管理および監督メカニズムが確立されているかどうかを確認するのに役立ちます。

監査担当者は、Techvology社の全階層の従業員に聞き取り調査を行い、インシデント対応記録を分析した。Techvology社は、従業員に対しインシデント管理に関する意識向上トレーニングを実施していたことを示す記録も提出した。収集した情報に基づき、監査担当者は、2件のサイバーセキュリティインシデントはいずれも従業員の能力不足が原因であると推測した。そのため、監査担当者は、関係する従業員の人事ファイルへのアクセスを要求し、関連する経験、資格、トレーニング記録などの能力を確認した。

ブランディング社の監査担当者は、入手した証拠の妥当性を厳密に評価し、受け取った記録の信頼性を損なったり、矛盾させたりする可能性のある証拠に対して常に警戒を怠りませんでした。テックボロジー社の監査においても、監査担当者はこの原則を遵守し、インシデント対応記録を厳密に評価するとともに、様々なレベルや職務の従業員に対して詳細なインタビューを実施しました。彼らはテックボロジー社の担当者の発言を鵜呑みにするのではなく、インシデント管理プロセスに関する主張を裏付ける具体的な証拠を求めました。

上記のシナリオに基づいて、以下の質問に答えてください。

質問 :

シナリオ4の最後の段落は、どの監査原則を説明していますか？

A. リスクベースのアプローチ

B. フェアディスプレイ

C. 専門家としての懐疑心

Answer: C (メッセージを残す)

包括的かつ詳細な解説 :

* C. 正解:

専門家としての懐疑心とは、証拠に疑問を投げかけ、主張を検証し、憶測を避けることを意味する。

監査担当者は証拠の妥当性を厳密に評価し、Techvology社が行った主張が具体的な証拠によって裏付けられていることを確認した。

* A. 不正解:

リスクベース監査では高リスク領域を優先しますが、この段落では主張と証拠の検証に焦点を当てています。

* B. 不正解:

* 公正な提示は調査結果の正確な報告を保証するが、この段落は報告ではなく証拠への疑問に焦点を当てている。

関連規格参照 :

* ISO 19011:2018 第4項（監査の原則：職業的懐疑心）

有効な **ISO-IEC-27001-Lead-Auditor-CN** 問題集は GoShiken.com が提供された合格しやすい ISO-IEC-27001-Lead-Auditor-CN 試験問題集！ GoShiken.com が最新の **ISO-IEC-27001-Lead-Auditor-CN** 試験問題集を提供しています。GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 問題集をゲットする人はこちら：
<https://www.goshiken.com/PECB/ISO-IEC-27001-Lead-Auditor-CN-mondaishu.html> (**41830%OFF**問題集溶と正解付きで **30%**w 特別割引コード: **Freepdfdumps**)

最新問題: **197**

ビジネスプロセスのPDCAサイクルにおける 検査」の部分に適切なフレーズは次のうちどれか2つはどれですか？

- A. 改善する
- B. 経営変革
- C. 検証トレーニング
- D. ターゲットをリセット
- E. 情報セキュリティポリシーの更新
- F. 審査プロセス

Answer: C,F ([メッセージを残す](#))

ビジネスプロセスのPDCAサイクルにおける チェック」に該当する2つのフレーズは次のとおりです。

- C. トレーニングの検証
- F. 監査プロセス

C. このフレーズはPDCAサイクルの チェック」に適用されます。なぜなら、実行」フェーズで実施されたトレーニング活動の有効性を測定および評価することが含まれるからです。トレーニングは、ISO 27001:20221の7.2項で要求されている情報セキュリティ意識、教育、および能力の重要な側面です。トレーニングを検証することで、組織はスタッフが情報セキュリティに関連する役割と責任を果たすために必要な知識、スキル、および行動を習得したかどうかを評価できます。トレーニングを検証することで、組織はトレーニングプログラムのギャップや弱点を特定し、改善策を計画することもできます。

F. このフレーズは、PDCA サイクルの チェック」に適用されます。なぜなら、実行」フェーズで実装されたプロセスのパフォーマンスと適合性を調査およびレビューすることが含まれるからです。監査は、客観的な証拠を入手し、それを評価して監査基準がどの程度満たされているかを判断するための体系的で独立した文書化されたプロセスです。2 監査プロセスは、組織が情報セキュリティの目標と要件が満たされているかどうか、情報セキュリティ管理が効果的かつ効率的であるかどうか、情報セキュリティリスクが適切に管理されているかどうかを確認するのに役立ちます。監査プロセスはまた、組織が不適合や改善の機会を特定し、是正措置または予防措置を計画するのにも役立ちます。

参照：

1 :ISO/IEC 27001:2022 - 情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステム - 要求事項、7.2項 2 :ISO 19011:2018 - マネジメントシステムの監査に関する指針、3.2項

最新問題: **198**

認証機関が認証を付与するかどうかを決定する際に、認証報告書に記載する必要のない結論は次のうちどれですか？

- A. 重大な不適合に対して組織が講じた是正措置は承認されました。
- B. 組織は、情報セキュリティ管理システムに適用されるすべての法律およびその他の要件を完全に遵守しています。
- C. 軽微な不適合に関する是正措置に対処するための計画が承認されました。
- D. 認証範囲を満たしています

Answer: ([解答を表示する](#))

認証機関が認証付与を決定する際に必要としない監査報告書の結論は、組織がISMSに適用されるすべての法的要件およびその他の要件を完全に遵守しているというものです。これは、認証機関が組織の法的遵守を検証する権限も責任も持たないためです。これはISO/IEC 27001:2022の範囲外です。認証機関は、組織のISMSが規格の要件に適合しているかどうかのみを評価します。規格の要件には、ISMSに関連する法的要件およびその他の要件を特定および評価するプロセスの確立が含まれます。組織は、自らの法的遵守を確保し、要求された場合は認証機関にその遵守の証拠を提供する責任があります。参照 ⇒ ISO/IEC 27001:2022、条項

6.1.3; ISO/IEC 27006:2022、条項9.2.2.4; PECB候補者ハンドブックISO 27001主任審査員、29ページ。

最新問題: 199

以下のうち、第1段階の第三者監査の主な目的を最もよく表しているのはどれですか？

- A. 監査チームをクライアントに紹介する。
- B. 組織の調達状況を理解する
- C. 第2段階レビューの赤レベルを決定する
- D. 組織が法律を遵守しているかどうかを確認する
- E. 独立監査報告書を作成する
- F. 組織の顧客を理解する

Answer: C ([メッセージを残す](#))

ステージ 1 第三者監査の主な目的は、ステージ 2 監査の準備状況を判断することです。ステージ 1 監査は、組織の ISMS 文書、範囲、コンテキスト、および目的を評価し、ステージ 2 監査の前に対処する必要のある主要なギャップまたは不適合を特定する予備評価です。ステージ 1 監査では、監査計画フェーズで行われるため、監査チームをクライアントに紹介しません。ステージ 1 監査では、ステージ 2 監査で行われるため、組織の法的コンプライアンスをチェックしません。ステージ 1 監査では、ステージ 2 監査後に行われるため、独立した監査レポートを作成しません。参照: : CQI & IRCA ISO 27001:2022 主任監査員コース ハンドブック、70 ページ。: ISO/IEC 27001 主任監査員 - PECB、23 ページ。

最新問題: 200

次のうち、第2段階の第三者監査の主な目的を最もよく表しているのはどれですか？

- A. 認証準備状況の確認
- B. 組織が法律を遵守しているかどうかを確認する
- C. 基準を満たさない状況を特定する
- D. 組織の管理システムを理解する

Answer: C ([メッセージを残す](#))

ステージ2の第三者監査の主な目的は、組織のマネジメントシステムの実施状況と有効性を評価し、規格12の要求事項に対する不適合を特定することです。その他の選択肢は、ステージ1監査の目的 A、D) または監査範囲の特定側面 B) のいずれかです。参照 :1 :ISO/IEC 27006:2022、情報技術ーセキュリティ技術ー情報セキュリティマネジメントシステムの監査および認証を提供する機関に対する要求事項、条項9.2 \n2 :PECB認定ISO/IEC 27001主任監査員試験準備ガイド、ドメイン4 :ISO/IEC 27001監査の準備

最新問題: 201

下列哪兩個短語是與第一方審核相關的 目標」？

- A. 應用國際標準
- B. 為認證機構準備審核報告
- C. 確認管理系統的範圍準確
- D. 按時完成審核
- E. 應用監理要求
- F. 更新管理策略

Answer: ([解答を表示する](#))

A first-party audit is an internal audit conducted by the organization itself or by an external party on its behalf. The objectives of a first-party audit are to: 12 Confirm the scope of the management system is accurate, i.e., it covers all the processes, activities, locations, and functions that are relevant to the information security objectives and requirements of the organization.
Update the management policy, i.e., review and revise the policy statement, roles and responsibilities, and objectives and targets of the information security management system (ISMS) based on the audit findings and feedback.
The other phrases are not objectives of a first-party audit, but rather:

国際規格の適用: これは ISMS の要件であり、監査の目的ではありません。ISMS は ISO/IEC 27001 規格およびその他の適用可能な規格または規制に準拠する必要があります 12 認証機関向けの監査レポートの作成: これは第三者監査の活動であり、第一者監査ではありません。第三者監査は、ISMS の適合性と有効性を検証し、適合証明書を発行するために独立した認証機関によって実施される外部監査です 12 監査を期限内に完了する: これはパフォーマンス指標であり、監査の目的ではありません。監査は計画された期間と予算内で完了する必要がありますが、これは監査の主な目的ではありません 12 規制要件の適用: これは ISMS の要件でもあり、監査の目的ではありません。ISMS は、情報セキュリティに関する組織の法的義務および契約上の義務を遵守する必要があります 12 参照:

1: ISO/IEC 27001:2022 リードオーディター（情報セキュリティマネジメントシステム）コース（CQIおよびIRCA認定トレーニング1）2: ISO/IEC 27001 リードオーディタートレーニングコース（REC B 2）

最新問題: 202

シナリオ6 :Sinvestmentは、住宅保険、商業保険、生命保険を提供する保険会社です。同社はノースカロライナ州で設立されましたが、近年、ヨーロッパやアフリカを含む他の地域にも事業を拡大しています。Sinvestmentは、業界における適用法令を遵守し、情報セキュリティインシデントの発生を防止することに尽力しています。同社はISO/IEC 27001に基づく情報セキュリティマネジメントシステム（ISMS）を導入し、ISO/IEC 27001認証の申請を行っています。

認証機関は、監査を実施するために2名の監査員を任命した。監査員はSinvestment社と機密保持契約を締結した後、監査を開始した。まず、ISMS適用範囲記述書、情報セキュリティポリシー、内部監査報告書など、必要な標準文書を精査した。Sinvestment社は文書作成手順を確立していると述べていたものの、すべての文書が同じ形式ではなかったため、精査は容易ではなかった。

その後、監査チームはSinvestmentの経営幹部に対し、ISMS導入におけるそれぞれの役割を理解するため、複数回のインタビューを実施した。監査の第1段階におけるすべての活動は、Sinvestmentからの要請による現地での文書および情報レビューを除き、リモートで実施された。

この段階で、監査担当者は情報セキュリティ研修および啓発プログラムに関する文書を一切発見できなかった。質問に対し、Sinvestmentの担当者は、全従業員に情報セキュリティ研修コースを提供していると述べた。監査の第1段階により、監査チームはSinvestmentの業務内容とISMS（情報セキュリティマネジメントシステム）について包括的な理解を得ることができた。

第2段階監査は、第1段階監査の3週間後に実施されました。監査チームは、マーケティング部門（監査範囲外において、従業員のアクセス権限を管理するための適切な手順が欠如していることを確認しました。従業員のアクセス権限の管理はISO/IEC 27001の要件であり、既に会社の情報セキュリティポリシーにも含まれているため、この問題は監査報告書に記載されました。さらに、第2段階監査において、監査チームはSinvestmentがユーザーアクティビティをログに記録していないことを確認しました。

同社の手順書には「ユーザー活動を記録したログは保存し、定期的に確認する必要がある」と記載されているが、同社はそのような手順を実施している証拠を一切提示していない。

監査活動全体を通して、監査員は観察、インタビュー、文書化された情報のレビュー、分析、および技術的検証を通じて情報と証拠を収集しました。監査チームはフェーズ1とフェーズ2の両方から得られたすべての監査結果を分析し、肯定的な認証勧告を発行することを決定しました。

上記のシナリオに基づいて、以下の質問に教えてください。

監査チームは、Sinvestment社の要請に基づき、Sinvestment社の現地で文書を精査しました。これは許容範囲内でしょうか？

A. はい、Sinvestmentは、文書審査プロセス中にサイトから文書が削除されないよう要求する権利を有します。

B. いいえ、Sinvestmentは文書レビューをどこで実施するかを決定することはできません。なぜなら、最初のレビュー段階の前に機密保持契約が締結されているからです。

C. いいえ、オンサイトとオフサイトの活動を組み合わせると、審査プロセスに悪影響を与える可能性があります。

Answer: A (メッセージを残す)

はい、Sinvestmentが文書情報のレビューをオンサイトで実施するよう要求することは問題ありません。特に機密情報の管理と守秘義務の確保のため、Sinvestmentは文書を社外に持ち出すことを禁止する権利を有しており、これはISO/IEC 27001で求められるセキュリティ管理に合致するものです。

最新問題: 203

複数の監査テスト計画を組み合わせる目的は何ですか？

A. 複数の方法を用いて、基準およびガイドラインへの準拠を確認する。

B. 組織のすべての領域が平等な監査の対象となるようにしてください。

C. 頻繁な監査の必要性を軽減する

Answer: A (メッセージを残す)

包括的かつ詳細な徹底分析

A. 正解：

複数の監査テスト計画を組み合わせることで、異なる視点や検証手法が適用され、監査の精度が向上する。
ISO 19011:2018は、包括的な結果を確保するために、監査に対する多様なアプローチを推奨しています。

B. 不正解：

すべての分野が同等の監査を必要とするわけではなく、リスクに基づいた監査が望ましい。

C. 不正解：

組織のニーズによっては、頻繁な監査が必要となる場合もある。

関連規格参照：

最新問題: 204

あなたは、医療サービスを提供する高齢者向け介護施設でISMS監査を実施しています。監査計画の次のステップは、情報セキュリティインシデント管理プロセスを検証することです。ITセキュリティマネージャーは、情報セキュリティインシデント管理手順を提示し、そのプロセスがISO/IEC 27035-1:2016に基づいていることを説明しました。

文書を確認すると、「情報セキュリティ上の脆弱性、インシデント、または事象は、発見後1時間以内に連絡担当者（PoC）に報告しなければならない」という記述が見つかります。従業員に聞き取り調査を行ったところ、「脆弱性、インシデント、および事象」の意味について、従業員間で認識のずれがあることが判明しました。

イベント追跡システムから過去6か月間のイベント報告記録のサンプルを抽出しました。結果は以下の表にまとめられています。

Type of report	Description	Resolution/Recovery Actions	Resolution/ Recovery Time
Information security weakness, report ID: 056	The human resources manager's mobile phone was hacked by ransomware, asking for \$1000 to unlock (decrypt) the data	IT department suggests the person shall pay the ransom to unlock the phone. No further action is needed.	24 hours
Information security weakness, report ID: 078	The medical staff's company mobile phone (with patient data) was hacked by ransomware, asking for \$5000 to unlock (decrypt) the data	IT department suggests the company shall pay the ransom to unlock the company phone. No further action is needed.	24 hours
Information security event, report ID: 090	The cloud server does not respond and healthcare monitoring stops for 8 hours.	IT department reboots the cloud server remotely. No further action is needed.	24 hours
Information security incident, report ID: 012	The cloud server does not respond and healthcare monitoring stops for 48 hours.	IT department reboots the cloud server remotely. No further action is needed.	24 hours

監査証拠をさらに収集するために、他の領域についても調査を進めたいと考えています。監査証拠に表示されないオプションを2つ選択してください。

A. より多くの従業員にインタビューを行い、報告プロセスに対する彼らの理解度を把握することで、より多くの証拠を集める。

（管理措置A.6.8に関連）

B. 会社が携帯電話とデータのロックを解除するために、どのように、そしていつ身代金を支払ったか（クレジットカードや銀行振込など）に関する証拠をさらに収集する。（管理措置A.5.26に関連）

C. 人事部長が個人活動データ（クレジットカードや銀行振込など）のロックを解除するために、どのように、そしていつ身代金を支払ったのかに関するさらなる証拠を収集する。（管理措置A.5.26に関連）

D. 組織がインシデント復旧時間をどのように決定しているかについて、より多くの証拠を収集する。（管理措置A.5.27に関連）

E. 組織が事件後、それ以上の措置は不要と判断した理由を説明するため、さらなる証拠を収集する。（管理措置A.5.26に関連）

F. インシデント復旧手順に関するさらなる証拠を収集する。（管理措置A.5.26に関連）

Answer: B,C (メッセージを残す)

- *C. 人事部長が個人用モバイルデータのロック解除のために身代金をどのように、いつ支払ったか クレジットカード、銀行振込など)について、より多くの証拠を収集する。(管理策5.26に関連)これは、組織のインシデント管理プロセスの監査には関連しません。人事部長の個人用電話と、その電話に対するランサムウェア攻撃への対処方法は、ISMS監査の範囲外です。組織は個人用デバイスについて責任を負いません。
- *B. 会社の携帯電話とデータのロックを解除するために、会社が身代金をどのように、いつ支払ったか クレジットカード、銀行振込など)について、より多くの証拠を収集する。(管理策5.26に関連) 一見関連性があるように見えるが、これは身代金の支払い方法に焦点を当てている。根本的な問題は、組織が身代金を支払ったこと自体であり、これは一般的にインシデント対応におけるベストプラクティスではない。監査では、なぜこのような決定がなされたのか、また代替ソリューション データのバックアップ、デバイスの消去と復元など)が検討されたかどうかに焦点を当てるべきである。
- 他の選択肢が重要な理由：
- *A. 報告プロセスに関する理解度について、より多くの職員にインタビューを行い、証拠をさらに収集する。(管理策6.8に関連)これは、 弱点、事象、およびインシデント」の理解における認識のずれに直接対処するものであり、適切なインシデント報告にとって極めて重要です。
- *D. 組織がインシデント復旧時間をどのように決定したかについて、より多くの証拠を収集する。(管理策5.27に関連)これは、恣意的で全てのインシデントに適切ではない可能性のある24時間復旧時間の根拠を調査するものです。
- *E. 組織が事件後、それ以上の措置は不要と判断した経緯について、より多くの証拠を収集する。(管理策5.26に関連)これは、事件対応の適切性、特に身代金支払い後の予防措置の欠如を検証するものである。
- *F. インシデント復旧手順に関する証拠をさらに収集する。(管理策5.26に関連)これは、実際の手順を検証し、その有効性とベストプラクティスとの整合性を評価するものです。

最新問題: 205

ITマネージャーがあなたに近づき、会社のリスク管理プロセスを変更するのを手伝ってほしいと頼んできたとき、あなたはちょうど組織の予定されていた情報セキュリティ監査を完了したばかりです。彼は他のマネージャーが理解しやすいように現在のドキュメントを更新しようとしています、あなたの議論から、彼がいくつかの重要な用語を混同していることが明らかです。あなたは彼に、それぞれの記述に適切なリスク用語を当てはめるように依頼しました。正解は何でしょうか？

The strategy chosen to respond to a specific information security risk	
The effect of uncertainty on information security objectives	
The requirements against which information security risks are evaluated	
A definition of the overall level of information security risk that is considered to be tolerable	

This is a definition of information security risk

This is a definition of information security risk criteria

This is a definition of information security risk acceptance criteria

This is a definition of information security risk treatment

Answer:

The strategy chosen to respond to a specific information security risk	This is a definition of information security risk treatment
The effect of uncertainty on information security objectives	This is a definition of information security risk
The requirements against which information security risks are evaluated	This is a definition of information security risk criteria
A definition of the overall level of information security risk that is considered to be tolerable	This is a definition of information security risk acceptance criteria

This is a definition of information security risk

This is a definition of information security risk criteria

This is a definition of information security risk acceptance criteria

This is a definition of information security risk treatment

最新問題: 206

監査担当者は一定の知識とスキルを備えている必要がありますが、監査チームリーダーはさらにいくつかの追加的な知識とスキルを備えている必要があります。以下のリストから、監査チームリーダーのみに当てはまる項目を2つ選択してください。

- A. 計画レビュー
- B. リスクベースの監査手法を理解し、適用する
- C. 適切なサンプリング手法を適用する
- D. 監査に提供されたリソースを効果的に活用する
- E. 被監査者の文化や社会面を理解する
- F. 収集した情報の関連性と正確性を検証する。

Answer: A,D (メッセージを残す)

PECB候補者ハンドブック1によると、監査チームリーダーは監査担当者と比較して、以下の追加的な知識とスキルを備えている必要がある。

監査計画の作成、監査チームメンバーへの作業割り当て、および活動の調整を含む監査の計画立案

監査に提供される人員、時間、予算、設備などのリソースを効果的に活用する。

監査プロセスを管理する。これには、開始会議と終了会議の主導、監査チームの指揮、紛争の解決、監査目標の達成の確保などが含まれる。

監査報告書および監査結果を確認し、承認する。

*監査全体を通してクライアントおよびその他の関係者とコミュニケーションをとる。参考資料: 1: PECB 候補者ハンドブック - ISO 27001 主任監査員、9-10 ページ。

最新問題: 207

ISMSにおける情報セキュリティリスク評価プロセスの正しい順序を選択してください。

手順を完了するには、入力したい空白部分をクリックして赤色でハイライト表示し、次に下のオプションから該当するテキストをクリックしてください。または、オプションを適切な空白部分にドラッグすることもできます。

1.

2.

3.

4.

To complete the sequence click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the options to the appropriate blank section.

Identify the information security risks Evaluate the information security risks Analyse the information security risks Establish information security criteria

Answer:

1.

2.

3.

4.

To complete the sequence click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the options to the appropriate blank section.

Identify the information security risks Evaluate the information security risks Analyse the information security risks Establish information security criteria

Explanation:

1.

2.

3.

4.

情報セキュリティマネジメントシステム（ISMS）の規格であるISO 27001:2022によると、情報セキュリティリスク評価プロセスの正しい手順は以下のとおりです。

- * 情報セキュリティ基準を確立する
- * 情報セキュリティリスクを特定する
- 情報セキュリティリスクを分析する
- * 情報セキュリティリスクを評価する

最初のステップは、情報セキュリティ基準を確立することです。これには、リスク評価方法、リスク受容基準、およびリスク評価基準が含まれます。これらの基準は、組織がどのようにリスク評価を実施するか、どのレベルのリスクが許容されるか、そしてリスクをどのように比較し、優先順位付けするかを定義します。

第2段階は、情報セキュリティリスクを特定することです。これには、ISMSに関連する資産、脅威、脆弱性、および既存の対策を特定することが含まれます。組織はまた、各リスクシナリオの潜在的な影響と発生確率を特定する必要があります。

第3段階は、情報セキュリティリスクの分析です。これには、第1段階で設定した基準に基づいて、各リスクシナリオのリスクレベルを推定することが含まれます。組織は、不確実性の原因とリスク推定の信頼度も考慮する必要があります。

第4段階は、情報セキュリティリスクを評価することです。これには、推定リスクレベルをリスク許容基準と比較し、リスクが許容範囲内であるか、または対策が必要かを判断することが含まれます。組織は、リスク評価基準とISMSの目的に基づいて、リスクの優先順位付けを行うべきである。

参照 :ISO 27001:2022 条項 6.1.2 情報セキュリティリスク評価、ISO 27001 リスク評価

リスク対策：完全ガイド - Advisera、ISO 27001 リスク評価 :7ステップガイド - IT Governance UK Blog

最新問題: 208

あなたは、医療サービスを提供するヨーロッパの高齢者向け介護施設ABCでISMS監査を実施しています。監査計画の次のステップは、継続的改善プロセスの有効性を検証することです。

監査の結果、入居者の家族のほとんど（90%）が、中国農業銀行のヘルスケアモバイルアプリを通じて、WeCare医療機器の宣伝広告を週に1回、メールとSMSで受け取っていたことが明らかになった。彼らは全員、収集した個人データを、ABCとのサービス契約に明記されているケアや治療以外の目的でマーケティングやその他の目的で使用することに反対していた。彼らは、ABCが入居者とその家族の個人情報を無関係の第三者に開示していると強く疑う根拠があり、苦情を申し立てた。

サービスマネージャーは、調査の結果、これらの苦情はすべて法令違反に該当する問題であると判断されたと述べた。

不適合および是正管理手順（文書参照ID :ISMS_L2_10.1、バージョン1）に従って、是正措置が計画され、実施されました。

間違っている項目を書き留めてください。後ほどご連絡いたします。文を最も適切に完成させる単語を選択してください。

"When reviewing the _____ of action taken in response to a _____, an auditor seeks evidence of _____ that will _____ recurrence of the issue."

To complete the sentence with the best words, click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

repair

assurance

responsibility

effectiveness

nonconformity

prevent

change

problem

Answer:

“When reviewing the effectiveness of action taken in response to a nonconformity, an auditor seeks evidence of change that will prevent recurrence of the issue.”

To complete the sentence with the best words, click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

repair

assurance

responsibility

effectiveness

nonconformity

prevent

change

problem

Explanation:

この文を完成させる方法の一つは次のとおりです。

不適合への対応として講じられた措置の有効性を審査する際、監査員は問題の再発を防止するための変更の証拠を探します。」ISO/IEC 27001:2022、10.1項によれば、組織はISMSのパフォーマンスと有効性を評価し、方針と目標が組織の戦略的方向性と整合していることを確認し、ISMSの意図された成果を達成するための措置を講じることによって、ISMSの適合性、妥当性、有効性を継続的に改善しなければなりません。継続的な改善を実現する方法の1つは、不適合を特定して是正し、その原因を排除して再発を防止するための措置を講じることです。

したがって、是正措置の有効性をレビューする際には、監査人は、組織が不適合の根本原因を分析し、ISMSに適切な変更を実施し、変更によって望ましい改善が実現し、問題の再発が防止されたことを検証した証拠を探す必要がある。参考文献：

- * ISO/IEC 27001:2022、10.1項、不適合および是正措置
- * ISO/IEC 27001:2022、第10.2項、継続的改善
- * PECB候補者ハンドブック ISO 27001主任審査員、19ページ、監査プロセス
- * PECB候補者ハンドブック ISO 27001主任審査員、21ページ、監査結果

最新問題: 209

仮説：

Northstormは、ユニークなヴィンテージおよびモダンなアクセサリーを取り扱うオンライン小売業者です。小規模な市場からスタートしましたが、eコマース市場の拡大とともに成長を遂げてきました。Northstormは完全にオンラインで運営されており、効率的な決済処理、在庫管理、マーケティングツール、配送プロセスを実現しています。また、人気商品を優先的に入荷、補充、発送するシステムを採用しています。

Northstormは従来、ウェブサイトのホスティングと、ハードウェア、ソフトウェア、データ管理を含むインフラストラクチャの完全な制御によってIT運用を管理してきました。しかし、このアプローチではインフラストラクチャの応答性が不十分であったため、成長が阻害されていました。eコマースと決済システムを改善するため、Northstormは社内データセンターの拡張を選択し、3か月かけて2段階で拡張を完了しました。第1段階では、コアサーバー、POSシステム、注文システム、請求システム、データベース、バックアップシステムをアップグレードしました。第2段階では、メール、決済、ウェブ機能の改善に重点を置きました。さらに、この段階でNorthstormは、個人情報（PII）の管理者および処理者に関する国際標準を採用し、データ処理方法が安全で信頼性が高く、グローバルな規制に準拠していることを保証しました。

拡張にもかかわらず、ノースストームのデータセンターはアップグレード後も進化するビジネスニーズに対応できませんでした。この不備により、注文の優先順位付けの問題など、一連の新たな課題が発生しました。顧客からは優先的に処理された注文が届かないという報告があり、同社は迅速な対応に苦慮しました。これは主に、注文の優先順位付けや顧客対応のシミュレーションに使用されるアプリケーション「YouDecide」からの注文をメインサーバーが処理できなかったことが原因でした。このアプリケーションは、アップグレード時にインストールされた新しいオペレーティングシステムと互換性のない高度なアルゴリズムに依存していました。

緊急の互換性問題に直面したNorthstormは、十分な検証を行わずにアプリケーションを急いでパッチ適用した結果、改ざんされたバージョンがインストールされてしまいました。このセキュリティ脆弱性によりメインサーバーが影響を受け、同社のウェブサイトが1週間ダウンしました。より信頼性の高いソリューションの必要性を認識した同社は、ウェブサイトのホスティングをeコマースサービスプロバイダーにアウトソーシングすることを決定しました。移行を完了する前に、同社は製品所有権に関する機密保持契約を締結し、セキュリティ強化のためにユーザーアクセス権限の包括的な見直しを実施しました。

質問：
シナリオ1に基づき、Northstormはユーザーのアクセス権限を確認しました。これはどのような種類のセキュリティ制御で、どのような機能を持つのでしょうか？

- A. 探偵と管理者
- B. 矯正と管理
- C. 法律とテクノロジー

Answer: A ([メッセージを残す](#))

包括的かつ詳細な解説：

セキュリティ対策は、種類（管理的・技術的・物理的）と機能（予防的・検出的・是正的）によって分類できる。

- * A. 検出的および管理的 - 正解。アクセス権限の確認は、手続き上のセキュリティ対策（ポリシーの適用や監査など）を伴うため、管理的統制です。また、ユーザー権限を監査および検証することで、不適切なアクセスや不正アクセスを特定するのに役立つため、検出的統制でもあります。
 - * B. 是正かつ管理的 - 不適切。ユーザーアクセス権限の確認は問題を修正するのではなく、潜在的な不正アクセスを検出するものである。また、管理的ではなく、事務的な行為である。
 - * C. 法的小および技術的 - ユーザーアクセス権限の確認は、法的または技術的な制御ではなく、管理ポリシーに基づくアクションであるため、これは誤りです。
- これは、不正アクセスを防止し、セキュリティポリシーを徹底するために、ユーザーアクセスを定期的に見直すことを義務付けているISO/IEC 27001:2022附属書A管理A.5.18（アクセス権限）に準拠しています。

最新問題: 210

選出最能完成句子的單字：

Select the word that best completes the sentence:

"A purpose of retaining documented information is to conformity with the requirements of a management system standard."

To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

demonstrate

audit

maintain

certify

Answer:

Select the word that best completes the sentence:

"A purpose of retaining documented information is to conformity with the requirements of a management system standard."

To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

Explanation:

"A purpose of retaining documented information is to conformity with the requirements of a management system standard."

The word that best completes the sentence is "demonstrate". According to ISO/IEC 27001:2022, Clause 7.5, the organization shall retain documented information as evidence of the performance of the processes and the conformity of the products and services with the requirements¹. The purpose of retaining documented information is to demonstrate conformity with the requirements of the management system standard, not to maintain, audit, or certify it. References: 1: ISO/IEC 27001:2022, Information technology - Security techniques - Information security management systems - Requirements, Clause 7.5

最新問題: 211

あなたは、医療サービスを提供するABC オーストラリアとカリフォルニア)の高齢者向け介護施設でISMS監査を実施しています。監査計画の次のステップは、ABCのモバイルアプリケーションの開発、サポート、およびライフサイクルプロセスの情報セキュリティを検証することです。監査中に、組織がモバイルアプリケーションの開発をCMMIレベル5およびITSM ISO/IEC 20000-) 認証企業にアウトソーシングしていることがわかりました。

1) BCMS ISO 22301)およびISMS ISO/IEC 27001)の認証を取得済み。

ITマネージャーは、ソフトウェアセキュリティ管理プロセスについて説明しました。その概要は以下のとおりです。

モバイルアプリケーション開発においては、少なくとも 設計セキュリティ」と デフォルトセキュリティ」の原則を遵守する必要があります。また、以下の個人データ保護セキュリティ機能を含めるべきです。

アクセス制御。

個人データの暗号化には、鍵長256ビットの高次暗号化標準 AES)アルゴリズムが使用され、個人データは匿名化されます。

脆弱性のチェックを実施しましたが、セキュリティ上のバックドアは発見されませんでした。

最新のモバイルアプリケーションテストレポートをサンプルとしてご覧いただきました。詳細は以下のとおりです。

Target of Test: ABC’s healthcare mobile app, version 1	Test results	Test summary
Security test		
Personal data encryption	Fail	Not able to perform the encryption.
Personal data pseudonymisation	Fail	Not able to perform the pseudonymisation.
Final approval:		
by: <i>Service Manager</i> 		

あなたはITマネージャーに、個人データの暗号化と匿名化のテストが失敗したにもかかわらず、なぜ組織がまだモバイルアプリを使用しているのかを尋ねます。さらに、サービスマネージャーにはそのようなテストを承認する権限があるのでしょうか？

ITマネージャーは、ソフトウェアセキュリティ管理手順によれば、テスト結果は彼によって承認される必要があると説明した。

暗号化機能と匿名化機能は、システムとサービスのパフォーマンスを著しく低下させたため、導入に失敗しました。この要件を満たすには、さらに150%のリソースが必要となります。サービスマネージャーは、アクセス制御が適切かつ許容範囲内であることに同意しました。そのため、サービスマネージャーは承認に署名しました。

監査結果を準備しています。正しい選択肢を選んでください。

- A. 不適合事項なし (NC)。サービスマネージャーはサービス提供を継続するという正しい判断を下しました。
(第1項、管理措置A.8.30に関連)
- B. 不適合 (NC)が存在します。組織および開発担当者は受入試験を実施していません。
(第1項、規制措置A.8.29に関連)
- C. 不適合 (NC)が存在します。組織および開発者によって実施されたセキュリティテストが失敗しました。
(第1項、規制措置A.8.29に関連)
- D. 不遵守 (NC)。サービス管理者がソフトウェアセキュリティ管理手順を遵守していません。(第1項、管理措置A.8.30に関連)

Answer: D (メッセージを残す)

正解はDです。不適合 (NC)が発生しています。サービスマネージャーはソフトウェアセキュリティ管理手順を遵守していません (条項1、管理A.8.30に関連)。ソフトウェアセキュリティ管理手順に従ってテスト結果を承認すべきだったのは、サービスマネージャーではなくITマネージャーです。サービスマネージャーがセキュリティテストの失敗を受け入れるという決定は、組織が採用した「設計によるセキュリティ」および「デフォルトによるセキュリティ」の原則にも違反しています。他の選択肢は、誤りか無関係です。組織と開発者は受け入れテストを実施しましたが、失敗しました (B、C)。サービスマネージャーがサービスを継続するという決定は、不適合を正当化するものではありません (A)。参照 :1 :ISO/IEC 27001:2022、情報技術 - セキュリティ技術 - 情報セキュリティ管理システム - 要求事項、条項8.1 \n2 :PECB認定ISO/IEC 27001主任監査員試験準備ガイド、ドメイン5 :ISO/IEC 27001監査の実施

有効な **ISO-IEC-27001-Lead-Auditor-CN** 問題集は GoShiken.com が提供された合格しやすい ISO-IEC-27001-Lead-Auditor-CN 試験問題集！ GoShiken.com が最新の **ISO-IEC-27001-Lead-Auditor-CN** 試験問題集を提供しています。GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 問題集をゲットする人はこちら：
<https://www.goshiken.com/PECB/ISO-IEC-27001-Lead-Auditor-CN-mondaishu.html> (418**30%OFF**問題集溶と正解付きで **30%**w特別割引コード: **Freepdfdumps**)

最新問題: 212
監査リソースを説明するために、次の文を最も適切に完成させる語句を選択してください。

“Audit resources include the resources to complete the audit programme as well as personnel to achieve the audit objectives.”

To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

certification technological competent management backup essential

Answer:

“Audit resources include the resources to complete the audit programme as well as personnel to achieve the audit objectives.”

To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

certification technological competent management backup essential

参照：
ISO 19011:2018 - マネジメントシステムの監査に関する指針、5.3項 PECB候補者ハンドブック ISO 27001主任監査員、19ページ

最新問題: 213

シナリオ6 :Sinvestmentは、住宅保険、商業保険、生命保険を提供する保険会社です。同社はノースカロライナ州で設立されましたが、近年、ヨーロッパやアフリカを含む他の地域にも事業を拡大しています。Sinvestmentは、業界における適用法令を遵守し、情報セキュリティインシデントの発生を防止することに尽力しています。同社はISO/IEC 27001に基づく情報セキュリティマネジメントシステム（ISMS）を導入し、ISO/IEC 27001認証の申請を行っています。

認証機関は、監査を実施するために2名の監査員を任命した。監査員はSinvestment社と機密保持契約を締結した後、監査を開始した。まず、ISMS適用範囲記述書、情報セキュリティポリシー、内部監査報告書など、必要な標準文書を精査した。Sinvestment社は文書作成手順を確立していると述べていたものの、すべての文書が同じ形式ではなかったため、精査は容易ではなかった。

その後、監査チームはSinvestmentの経営幹部に対し、ISMS導入におけるそれぞれの役割を理解するため、複数回のインタビューを実施した。監査の第1段階におけるすべての活動は、Sinvestmentからの要請による現地での文書および情報レビューを除き、リモートで実施された。

この段階で、監査担当者は情報セキュリティ研修および啓発プログラムに関する文書を一切発見できなかった。質問に対し、Sinvestmentの担当者は、全従業員に情報セキュリティ研修コースを提供していると述べた。監査の第1段階により、監査チームはSinvestmentの業務内容とISMS（情報セキュリティマネジメントシステム）について包括的な理解を得ることができた。

第2段階監査は、第1段階監査の3週間後に実施されました。監査チームは、マーケティング部門（監査範囲外において、従業員のアクセス権限を管理するための適切な手順が欠如していることを確認しました。従業員のアクセス権限の管理はISO/IEC 27001の要件であり、既に会社の情報セキュリティポリシーにも含まれているため、この問題は監査報告書に記載されました。さらに、第2段階監査において、監査チームはSinvestmentがユーザーアクティビティをログに記録していないことを確認しました。

同社の手順書には「ユーザー活動を記録したログは保存し、定期的に確認する必要がある」と記載されているが、同社はそのような手順を実施している証拠を一切提示していない。

監査活動全体を通して、監査員は観察、インタビュー、文書化された情報のレビュー、分析、および技術的検証を通じて情報と証拠を収集しました。監査チームはフェーズ1とフェーズ2の両方から得られたすべての監査結果を分析し、肯定的な認証勧告を発行することを決定しました。

ISO/IEC 27001の要求事項によれば、企業はユーザー活動を記録するログプログラムを導入している証拠を提出する必要がありますか？シナリオ6を参照してください。

- A.** はい、ユーザーのアクティビティを記録したイベントログは保存し、定期的に確認する必要があります。
- B.** いいえ、このプロセスの実施は標準的な要件ではないからです。
- C.** いいえ、弊社はこの手順の実施を推奨しているだけです。

Answer: A ([メッセージを残す](#))

はい、ISO/IEC 27001規格によれば、企業はユーザー活動のログ記録に関する手順の実施状況を示す証拠を提出する必要があります。この要件は、イベントが記録され、定期的にレビューされることを保証し、セキュリティインシデントの検出と防止を支援するために不可欠です。

参照規格 :ISO/IEC 27001:2013、A.12.4項（記録および監視）

最新問題: **214**

シナリオ2 :ナイト社は、米国カリフォルニア州北部を拠点とする電子機器メーカーで、ビデオゲーム機を開発しています。ナイト社は世界中に300人以上の従業員を抱えています。創業5周年を機に、同社は次世代ビデオゲーム機「G-Console」をグローバル市場向けに発売することを決定しました。G-Consoleは2021年の究極のメディアコンソールと位置づけられ、プレイヤーに最高のゲーム体験を約束します。

メインユニットパッケージには、VRヘッドセット、2つのゲームやその他のギフト。

長年にわたり、同社は誠実さ、正直さ、そして顧客への敬意を通して確固たる評判を築いてきました。この評判こそが、多くの熱心なゲーマーがKnightのGコンソールを発売と同時に手に入れたいと願った理由の一つです。

ナイト社は顧客志向の企業であることに加えて、

彼らの開発品質はゲーム業界で広く認められている。しかし、価格は妥当な範囲を超えて高額である。

しかし、ナイト社の製品の品質は最高レベルであるため、ほとんどの忠実な顧客にとってこれは問題ではない。

世界有数のビデオゲーム機開発企業であるナイト社は、悪意のある攻撃の標的となることも少なくありません。同社の情報管理システム（ISMS）は1年以上前から運用されており、財務部門と人事部門を除くナイト社の全部門を網羅しています。

最近、ナイト社の機密情報を含むファイルの一部がハッカーによって流出しました。ナイト社のインシデント対応チーム（IRT）は、直ちにシステム全体と事件の詳細の分析を開始しました。

IRTは当初、ナイト社の従業員が脆弱なパスワードを使用していたため、不正なハッカーがアカウントに容易にアクセスできたのではないかと疑っていた。しかし、徹底的な調査の結果、ハッカーはファイル転送プロトコル（FTP）の通信を傍受することでアカウントにアクセスしていたことが判明した。

FTPは、アカウント間でファイルを転送するために使用されるネットワークプロトコルです。認証には平文のパスワードを使用します。

この情報セキュリティインシデントの結果、ナイト社はIRTの助言に基づき、FTPをセキュアシェル（SSH）に置き換えることを決定した。これにより、通信を傍受した者は暗号化されたデータしか見ることはできないようになる。

これらの変更を受けて、ナイト社はリスク評価を実施し、管理策の導入によって同様の事象のリスクが最小限に抑えられたかどうかを検証した。この評価結果はISMSプロジェクトマネージャーによって承認され、新しい管理策の導入後のリスクレベルは同社のリスク許容度と一致していると判断された。

このシナリオに基づいて、以下の質問に答えてください。

FTPは認証に平文パスワードを使用します。以下はFTPサーバーの例です。

- A.** 脆弱性
- B.** リスク
- C.** 脅威

Answer: A ([メッセージを残す](#))

FTP認証に平文パスワードを使用することは、攻撃者によって悪用される可能性のある脆弱性であるため、脆弱性となります。平文パスワードはネットワークスニファや中間者攻撃によって容易に傍受される可能性があり、重大なセキュリティリスクとなります¹。参考文献 ≡ この説明は、情報セキュリティ分野における脆弱性の理解、特にFTPなどのネットワークプロトコルとその関連リスクに関する理解と一致しています。

最新問題: **215**

監査報告書に関する以下の4つの記述のうち、正しいものはどれですか？

- A.** 監査報告書は、監査チームのコメントに基づいて監査チームリーダーが作成する必要があります。

- B. 監査報告書には、監査計画を含めるか、監査計画を参照する必要があります。
- C. 監査報告書は、その内容が不都合な場合もあるため、まず組織の最高経営陣に送付すべきです。
- D. 監査報告書は、特に機密扱いと明記されていない限り、広く配布するのに適しているとみなすべきである。
- E. 監査報告書には不適合事項のみを記載すべきである。
- F. 監査報告書は合意された期間内に作成されるべきです。
- G. 不要になった監査報告書は、組織の一般廃棄物の一部として処分することができます。
- H. 監査報告書は必ずクライアントによって確認され、日付が記入され、承認」の署名がなされるべきです。

Answer: A,B,F,H (メッセージを残す)

ISO/IEC 27001 主任審査員向け PECB 候補者ハンドブックによると、監査報告書は、監査証拠の収集と分析を担当する監査チームリーダーが監査チームからの意見を取り入れて作成する必要があります1。監査報告書には、監査の目的、範囲、基準、および方法論の基礎となる監査計画を含めるか、または参照する必要があります2。さらに、監査報告書は、監査プログラム管理の一部であり、監査結果のタイムリーな伝達を保証するため、合意された期間内に作成する必要があります3。加えて、監査報告書は常にクライアントによってレビューされ、日付が記入され、承認済み」として署名される必要があります。これは、監査の完了と監査結果および結論に関する正式な合意を確認するためです4。

他の記述が誤りである理由は以下のとおりです。

監査報告書は、その内容が不都合な場合があるため、監査の公平性と機密性が損なわれる可能性があるため、組織の経営陣に最初に送付すべきではありません。監査報告書は、監査プログラムの手順と監査計画に従って配布する必要があります。

監査報告書は、特に機密扱いと明記されていない限り、一般に公開するのに適していると考えるべきではありません。これは、監査の機密保持義務および個人情報の保護に違反するからです。

監査報告書は機密文書として扱い、権限のある関係者のみと共有すべきである。

監査報告書は、不適合を証明するだけでなく、監査の範囲と価値を限定するものであってはならない。

監査報告書には、法令遵守状況、改善の機会、優良事例、および監査で指摘された事項も記載されるべきである。

不要になった監査報告書は、組織の一般廃棄物として廃棄してはなりません。これは、監査の機密性および情報セキュリティにリスクをもたらすためです。監査報告書は、監査プログラムの手順および適用される法的要件に従って、保管、廃棄、または破棄する必要があります。

1: ISO/IEC 27001 主任審査員候補者ハンドブック、32 ページ、セクション 4.4.32: ISO/IEC 27001 主任審査員候補者ハンドブック、33 ページ、セクション 4.4.43: ISO 27001 主任審査員候補者ハンドブック /IEC 27001 主任審査員、31 ページ、セクション 4.4.14: PECB 候補者ハンドブック ISO/IEC 27001 主任審査員、34 ページ、セクション 4.4.55: PECB 候補者ハンドブック ISO/IEC 27001 主任審査員、24 ページ、セクション 4.3.1. : PECB 候補者ハンドブック ISO/IEC 27001 主任審査員、33 ページ、セクション 4.4.4. : PECB 候補者ハンドブック ISO/IEC 27001 主任審査員、24 ページ、セクション 4.3.1. : PECB 候補者ハンドブック ISO/IEC 27001 主任審査員、33 ページ、セクション 4.4.4. : PECB 候補者ハンドブック ISO/IEC 27001 主任審査員、32 ページ、セクション 4.4.3. : PECB ISO/IEC 27001主任審査員候補者ハンドブック、ページ 33、セクション4.4.4. : ISO/IEC 27001主任審査員向けPECB候補者ハンドブック、24ページ、セクション4.3.1. : PECB ISO/IEC 27001 主任審査員候補者ハンドブック、34 ページ、セクション 4.4.5。

最新問題: 216

シナリオ 4: Branding は、米国で最も著名な企業と提携しているマーケティング会社です。内部コストを削減しています。Branding は 2 年以上にわたり、ソフトウェア開発と IT サポートデスク業務を Techvology にアウトソーシングしています。Techvology は、ブランドのソフトウェア、ネットワーク、ハードウェア要件を管理するために必要な専門知識を備えています。Branding は情報セキュリティ管理システム (ISMS) を導入し、ISO/IEC 27001 認証を取得しており、情報セキュリティの高い基準を維持するというコミットメントを示しています。アウトソーシング業務のセキュリティが ISO/IEC 27001 認証要件を満たしていることを確認するために、テクノロジーの監査を積極的に行っています。

前回の監査において、ブランドの監査チームは監査対象となるプロセスと監査計画を策定しました。彼らは証拠に基づいたアプローチを採用し、特にTechvologyが過去1年間に報告した2件の情報セキュリティインシデントをあらゆる側面から考慮に入れました。

さらに、今回の監査では、Techvologyのアウトソーシング業務およびその他の組織を管理するためのガバナンスプロセスについても厳密に評価しました。このステップは、アウトソーシング契約に伴う潜在的なリスクを軽減するための適切な統制および監督メカニズムが存在するかどうかを確認するため、ブランドプロモーションにとって非常に重要です。

監査担当者は、Techvology社の全階層の従業員にインタビューを行い、インシデント解決記録を分析しました。さらに、Techvology社は、従業員向けにインシデント管理に関する啓発会議を実施したことを示す記録を証拠として提出しました。収集した情報に基づき、監査担当者は、両方のサイバーセキュリティインシデントは従業員の能力不足が原因であると予測しました。そのため、監査担当者は、関連する経験、資格、研修記録など、従業員の能力を示す証拠を確認するため、関係従業員の人事ファイルへのアクセスを要求しました。

ブランディング社の監査担当者は、入手した証拠の妥当性を厳密に評価し、受け取った記録の信頼性を否定したり疑わせたりする可能性のある証拠に対して常に警戒を怠りませんでした。テックボロジー社の監査においても、監査担当者はこの方針を堅持し、インシデント解決記録を厳密に評価するとともに、様々なレベルや職務の従業員に対して徹底的なインタビューを実施しました。テックボロジー社の担当者の発言を鵜呑みにするのではなく、インシデント管理プロセスに関する担当者の主張を裏付ける具体的な証拠を求めたのです。

上記のシナリオに基づいて、以下の質問に答えてください。

シナリオ4の最後の段落は、どの監査原則を説明していますか？

A. リスクベースのアプローチ

B. フェアディスプレイ

C. 職業的懐疑主義

Answer: [\(解答を表示する\)](#)

専門家としての懐疑心とは、証拠に疑問を投げかけ、主張を検証し、憶測を避けることを意味する。

監査担当者は証拠の妥当性を厳密に評価し、Techvology社が行った主張が具体的な証拠によって裏付けられていることを確認した。

A. 不正解：

リスクベース監査は高リスク領域を優先するが、この段落では主張と証拠の検証に焦点を当てている。

B. 不正解：

公正な提示は調査結果の正確な報告を保証するが、この段落は報告ではなく、証拠への疑問に焦点を当てている。

関連規格参照：

Explanation:

包括的かつ詳細な徹底分析

最新問題: 217

ACTで行っていること - PDCAサイクルから

A. プロセスパフォーマンスを継続的に監視するための対策を講じる

B. プロセスパフォーマンスを継続的に改善するための行動をとる

C. プロセスパフォーマンスを継続的に監視するための対策を講じる

D. スタッフのパフォーマンスを継続的に改善するための行動をとる

Answer: B ([メッセージを残す](#))

PDCAサイクルの「実行」フェーズでは、「チェック」フェーズの結果に基づいてプロセスがレビューおよび評価されます。このフェーズで行われるアクションは、問題の根本原因に対処し、是正措置と予防措置を実施し、プロセス文書を更新することによって、プロセスのパフォーマンスを継続的に改善することを目的としています。1 参照: ISO/IEC 27001:2022 リードオーディター (情報セキュリティマネジメントシステム) | CQI | IRCA

最新問題: 218

情境 3

NightCore是一家總部位於美國的跨國科技企業，專注於電子商務、雲端運算、數位串流媒體和人工智慧(AI)。在實施資訊安全管理系統(ISMS)一年多後，NightCore委託一家認證機構進行ISO/IEC 27001認證審核。

認証機関は5名の監査員からなるチームを編成し、ジャックがチームリーダーを務めた。ジャックは、リスク管理、情報セキュリティ対策、インシデント管理における豊富な監査経験で知られている。

彼のスキルは監査の原則とプロセスに高度に合致しており、監査範囲を効果的に理解し、関連する基準を適用することが可能です。ジャックはまた、ナイトコアの組織構造、ミッション、経営慣行、および事業活動に適用される法的・規制上の要件についても深い理解を示しました。

監査チームは、信頼性が高く再現性のある結論を体系的に導き出すために、合理的な監査手法に従います。チームは、ある程度検証可能な情報のみが有効な証拠とみなされることを認識しています。監査プロセスにおいて、まれに特定の情報の検証が困難な場合や検証可能性が低い場合、監査人は専門的な判断に基づいて、そのような証拠の信頼性を評価し、信憑性を判断します。

監査中、監査担当者は、NightCoreの情報セキュリティ管理システム（ISMS）の運用計画と管理に関する所見とレビューメモを記録しました。また、NightCoreの情報インベントリおよび関連資産に関する所見も記録しました。さらに、ネットワークサービス接続を保護するために実装されたファイアウォール構成についてもレビューを行いました。

審査プロセスが最終段階に入るにつれ、NightCoreが最高水準の情報セキュリティを維持するという強い意志がますます明らかになってきています。ISO/IEC 27001認証は容易に取得可能であり、NightCoreはこの認証を取得することで、テクノロジー業界における評判をさらに高めることができるでしょう。

質問

NightCoreの監査において、監査担当者は、運用計画、資産目録、ファイアウォール構成など、情報セキュリティ管理システム（ISMS）の運用における主要分野に重点を置きました。監査担当者は、NightCoreの監査中にどのような種類の証拠を収集しましたか？

A. 分析と文献的証拠

B. 物理的および技術的証拠

C. 数学的証拠

Answer: B ([メッセージを残す](#))

監査人は主に物的証拠と技術的証拠を収集したため、選択肢Bが正解となる。

物理的および技術的証拠とは、システム、構成、運用方法の直接観察、ならびに組織環境内の有形または技術的要素の検査を通じて得られた証拠を指します。

このシナリオでは、監査担当者はファイアウォールの設定を確認し、運用計画および管理活動を検証し、情報および関連資産のインベントリを検査しました。ファイアウォールの設定は、直接確認および検証できるシステム設定とセキュリティメカニズムを含むため、技術的証拠の明確な例です。資産インベントリは文書化されていますが、その正確性と完全性を確認するために、物理的またはシステムレベルの検査によって検証されることがよくあります。運用計画および管理の観察には、プロセスが実際にどのように実行されるかを目撃することが含まれており、これも物理的または技術的な証拠となります。

選択肢Aは、分析的証拠および文書的証拠は主に報告書、指標、傾向分析、またはシステムを直接検査しない公式文書を含むため、誤りです。一部の文書はレビューされましたが、このシナリオでは運用および技術的制御の検査と観察が重視されています。選択肢Cは、数学的証拠はISO規格で認められた監査証拠のカテゴリではないため、誤りです。

ISO 19011は、特に技術的および運用上の管理策の有効性を評価する際に、観察と検査を監査証拠収集の有効な方法として認めています。したがって、今回の監査で収集された証拠は、物理的証拠および技術的証拠に分類するのが最も適切です。

最新問題: 219

質問

ABCマニュファクチャリング社は、規制の厳しい化学業界で事業を展開しています。同社は内部統制を確立していますが、業界の複雑さゆえに、情報セキュリティマネジメントシステム（ISMS）が不十分となる可能性のある多くの課題が存在します。

この状況はどのようなリスクを示唆していますか？

A. 固有のリスク

B. リスク管理

C. リスクの検出

Answer: A ([メッセージを残す](#))

このシナリオは内在リスクを表しており、選択肢Aが正解です。内在リスクとは、内部統制の有効性とは無関係に、プロセス、システム、または組織がその性質、環境、または複雑さゆえにエラーや障害を起こしやすい性質を指します。

ABCマニュファクチャリング社は、高度に規制され複雑な化学産業において事業を展開しています。このような環境では、当然ながら複雑な規制要件、危険物、そして厳格なコンプライアンス義務が伴います。これらの特性は、たとえ内部統制が存在していても、業界の複雑さゆえにエラーやISMS（情報セキュリティマネジメントシステム）の欠陥が発生する可能性を高めます。これこそが、固有リスクの本質的な特徴です。

選択肢Bは誤りです。統制リスクとは、内部統制が問題の防止や発見に失敗する可能性を指します。このシナリオでは、統制は実施されていますが、リスクは統制の不備ではなく、業界自体の複雑さから生じています。選択肢Cも誤りです。発見リスクとは、監査人が監査中に既存の問題を発見できる能力に関するものであり、組織の運用環境に関するものではありません。

ISO/IEC 27001監査においては、監査の重点と深度を計画する上で、内在リスクを理解することが不可欠です。規制の厳しい業界は、その複雑さとコンプライアンス要件の高さから、必然的に内在リスクも高くなります。したがって、このシナリオは明らかに内在的なリスクを示している。

最新問題: 220

為了驗證是否符合 ISO/IEC 27001 附錄 A 控制措施 8.15 記錄，審核小組驗證了伺服器日誌樣本，以確定它們是否可以編輯或刪除使用了哪種審計程序？

- A. 分析
- B. 取樣
- C. 觀察

Answer: A ([メッセージを残す](#))

The audit procedure used here is "analysis." The audit team analyzed server logs to verify if they can be edited or deleted, focusing on evaluating the logs' properties and the controls over their manipulation to ensure they comply with ISO/IEC 27001 requirements.

最新問題: 221

第三者監視監査を実施している際に、監査チームの別のメンバーから説明を求められました。そのメンバーは、組織におけるコントロール5.7 脅威インテリジェンス」の適用状況を評価するよう依頼されています。彼らは、これが ISO/IEC 2022年版で導入された新しいコントロールの1つであることを認識しています。

27001では、適切な監査管理を確保したいと考えています。

彼らは審査プロセスを支援するためのチェックリストを作成しており、計画されている活動が管理要件に準拠していることをあなたに確認してもらいたいと考えています。

以下の選択肢のうち、効果的な監査証拠を表しているのはどれですか？（3）

- A. 脅威インテリジェンスの生成という任務が、組織の内部監査チームに割り当てられるようにします。
- B. 組織のリスク評価プロセスが効果的な脅威インテリジェンスから始まるようにします。
- C. 全従業員が脅威を報告することの重要性を理解できるよう、上級管理職と話し合います。
- D. 現在の脅威情報収集体制の有効性について経営陣に適切な情報を提供するための措置が講じられるよう徹底します。
- E. 組織に完全に文書化された脅威インテリジェンスプロセスがあるかどうかを確認します。
- F. 組織の情報資産の機密性、完全性、可用性を保護するために、脅威インテリジェンスが積極的に使用されているかどうかを調査します。
- G. 情報セキュリティ上の脅威に関連する情報を収集・評価し、脅威インテリジェンスを生成する方法について検討します。
- H. 脅威インテリジェンスの生成において、内部情報源と外部情報源が使用されているかどうかを判断します。

Answer: D,F,G ([メッセージを残す](#))

These three options represent valid audit trails for control 5.7, as they are aligned with the control's requirements and objectives. According to the web search results from my predefined tool, control 5.7 requires organisations to collect and analyse information relating to information security threats and use that information to take mitigation actions¹². The control also specifies that threat intelligence should be relevant, perceptive, contextual, and actionable, and that it should be used to prevent, detect, or respond to threats³⁴.

Therefore, the auditor should verify how the organisation collects, analyses, and produces threat intelligence, how it uses threat intelligence to protect its information assets, and how it monitors and evaluates the effectiveness of its threat intelligence arrangements. The other options are not valid audit trails, as they are either irrelevant, incorrect, or incomplete. For example:

*The task of producing threat intelligence is not assigned to the organisation's internal audit team, but to the person or team responsible for the ISMS, such as the information security manager or the information security committee⁵.

*The organisation's risk assessment process does not begin with effective threat intelligence, but with the identification of the context, scope, and objectives of the ISMS. Threat intelligence is an input for the risk identification and analysis, but not the starting point of the risk assessment process.

*Speaking to top management to make sure all staff are aware of the importance of reporting threats is not sufficient to audit the control, as it does not address how the organisation collects, analyses, and produces threat intelligence, nor how it uses it to take mitigation actions. The auditor should also speak to the staff involved in the threat intelligence process, and review the relevant documents and records.

*Checking that the organisation has a fully documented threat intelligence process is not enough to audit the control, as it does not verify the implementation and effectiveness of the process. The auditor should also observe the process in action, and examine the outputs and outcomes of the process.

*Determining whether internal and external sources of information are used in the production of threat intelligence is a partial audit trail, as it only covers one aspect of the control. The auditor should also assess the quality, reliability, and relevance of the sources, and how the information is analysed and used.

References: = 1: ISO 27001:2022 Annex A 5.7 - Threat Intelligence - ISMS.online¹²: ISO 27001 Annex A

5.7 Threat Intelligence - High Table²³: ISO/IEC 27001:2022 Information technology - Security techniques

最新問題: 222

あなたは経験豊富なISMS監査チームリーダーで、監査員の研修を指導しています。あなたは彼女に一連の質問をすることで、今後の監査に関する彼女の理解度を確かめることにしました。以下はあなたの質問と彼女の回答です。

彼女はどの4つの質問に正しく答えたか？

- A. Q: その後の監査では、新たな不適合を発見すべきでしょうか？ A: はい。
- B. 質問: その後の監査で、法令違反の問題が効果的に解決されていることを保証すべきでしょうか？ 回答: はい。
- C. 質問: 合意された改善の機会と是正措置は、フォローアップレビューで考慮されるべきでしょうか？
年
- D. Q: フォローアップ監査の目的は、是正措置、是正対策、および改善機会の完了を確認することですか？ A: はい。
- E. Q: すべてのレビューにフォローアップレビューが必要ですか？ A: いいえ。
- F. Q: その後の監査の結果は、最初に不適合を特定した監査チームリーダーに報告すべきでしょうか？ A: はい。
- G. Q: フォローアップ監査の結果を監査クライアントに報告すべきですか？ A: いいえ。
- H. Q: 必要に応じて、後続のレビューの結果を別の後続のレビューとして使用できますか？ A: はい。

Answer: B,D,E,H ([メッセージを残す](#))

フォローアップ監査、特に情報セキュリティマネジメントシステム (ISMS) の文脈におけるフォローアップ監査の理解と、ISO 19011:2018で提供されるガイドラインに基づき、研修中の監査員が正しく回答した質問は以下の4つです。

B: 質問: フォローアップ監査では、不適合が効果的に対処されたことを確認する必要がありますか？ 回答: はい、その通りです。フォローアップ監査の主な目的は、前回の監査で特定された不適合が効果的に対処され、講じられた是正措置が適切かつ効果的であることを確認することです。

D: Q: フォローアップ監査の目的は、是正措置、是正対策、および改善機会の完了を確認することですか？ A: はい。フォローアップ監査は、是正措置および是正対策の完了と有効性を確認することを目的としています。また、初回監査で特定された改善機会の実施状況も検討する場合があります。

E: Q: すべての監査でフォローアップ監査は必須ですか？ A: いいえ。これは正しいです。フォローアップ監査は、すべての監査で自動的に必須となるわけではありません。通常、フォローアップ監査は、以前の監査で不適合やその他の重大な問題が特定され、是正措置の実施状況と有効性を検証する必要がある場合に実施されます。

H: Q: フォローアップ監査の結果、必要に応じてさらにフォローアップ監査を実施することは可能ですか？ A: はい。これは起こり得る結果です。フォローアップ監査で是正措置が十分に効果を発揮していないことが判明した場合、または新たな問題が特定された場合は、再度フォローアップ監査を実施する必要があるかもしれません。

研修中の監査員が提供したその他の回答には、説明や修正が必要です。例えば、フォローアップ監査は主に以前に特定された不適合と是正措置に焦点を当てますが、新たな不適合が発見された場合は、それを特定することもあります A)。改善の機会は、是正措置に焦点を絞ったフォローアップ監査よりも、通常監査の範囲内でより重視されます C)。また、フォローアップ監査の結果は、透明性と説明責任を確保するため、通常は監査チームリーダーと監査依頼者の両方に報告されるべきです FとG)。

研修中の監査員が正しく回答した 4 つの質問は、B、D、E、および H です。これらの質問と回答は、ISO 19011:2018、6.712 項に規定されているフォローアップ監査の定義と目的と一致しています。フォローアップ監査は、前回の監査の結果として講じられた是正措置の完了と有効性を検証するために実施されます (B、D)。フォローアップ監査はすべての監査で必須ではありませんが、監査プログラム、監査クライアント、またはその他の利害関係者によって要求される場合があります (E)。是正措置が満足のいくものでない場合、または合意された期間内に完了しない場合は、フォローアップ監査の結果、別のフォローアップ監査が実施される可能性があります (H)。その他の質問と回答は、不正確または無関係です。フォローアップ監査は、新たな不適合を特定しようとするべきではありません。これは、フォローアップ監査の目的ではないためです (A)。フォローアップ監査では、合意された改善の機会と是正措置の両方を考慮する必要があります。これらはどちらも前回の監査の結果です。フォローアップ監査の結果は、監査依頼者だけでなく、前回の監査を実施した監査チームリーダー F、G) などの関係者にも報告する必要があります。参考文献 :1 ISO

19011:2018、マネジメントシステムの監査に関するガイドライン、第6.7項 \n2: PECB認定ISO/IEC 27001主任監査員試験準備ガイド、ドメイン6 ISO/IEC 27001監査の終了

最新問題: 223

礼儀正しい訪問者が、訪問者IDを持たずに歩き回っています。従業員として、以下の例外を除き、以下の対応を取る必要があります。

- A. 挨拶をしてコーヒーを提供する
- B. 受付に電話して、訪問者の状況を伝えてください。
- C. 彼に挨拶して、どうしたのか尋ねてください。
- D. 彼を目的地まで護衛する

Answer: A (メッセージを残す)

従業員として、訪問者IDを持たずにうろついている訪問者を見かけた場合、挨拶をしてコーヒーを勧める以外に、以下の対応を取るべきです。挨拶をしてコーヒーを勧めるのは、訪問者の身元や目的を確認せずに歓迎したり支持したりしていると受け取られる可能性があるため、適切な行動ではありません。また、訪問者に信頼を得たり、親切心につけ込んだりする機会を与えてしまう可能性もあります。受付に電話して訪問者について知らせるのは適切な行動です。担当者が状況を把握し、訪問者が承認され登録されていることを確認できるからです。挨拶をして用件を尋ねるのは適切な行動です。訪問者の存在と意図に対する関心と好奇心を示すことができるからです。目的地まで案内するのは適切な行動です。訪問者が一人でうろつき、許可されていないエリアや情報にアクセスするのを防ぐことができるからです。参考文献: : CQI & IRCA ISO 27001:2022 主任審査員コースハンドブック、42 ページ。 : [ISO/IEC 27001 主任審査員 - PECB]、15 ページ。

最新問題: 224

あなたは経験豊富なISMS監査チームリーダーであり、ISMS監査員への研修と指導を行っています。彼らは外部プロバイダーを評価し、以下の活動を含むチェックリストを作成するよう依頼されました。彼らは、提案された行動が適切であることを確認するために、あなたにそのチェックリストをレビューするよう依頼しました。彼らが参加を求められた監査は、データセンターに対する第三者機関による監査でした。データセンターの運営主体は、より広範な通信グループの一員です。グループ内の各データセンターは、それぞれ独自のISMS（情報セキュリティマネジメントシステム）を運用し、独自の認証情報を保有しています。ISO/IEC 27001:2022における外部プロバイダーの要件に関する3つのオプションから選択してください。

- A. 他のデータセンターが、たとえ同じ通信グループに属していても、外部サプライヤーとみなされるかどうかを確認します。
- B. 外部プロバイダーが、自社の製品またはサービスの使用から生じるリスクを組織に通知するための書面による手順を整備していることを確認します。
- C. 私は、組織が情報の機密性、完全性、およびアクセス可能性を保護するために重要だと特定した各プロセスについて、外部のバックアッププロバイダーを確保するようにします。
- D. 外部から提供される製品やサービスを監査する必要があるため、監査活動は外部から提供されるプロセスに限定します。
- E. 組織が外部プロバイダーのパフォーマンスを定期的に監視、レビュー、評価することを確実にします。
- F. 組織がISMSに関して外部プロバイダーとコミュニケーションを取る必要性を判断していることを確認します。
- G. 私は、経営陣が外部および内部のISMSプロセスを提供する担当者に役割と責任を割り当てるようにします。
- H. 私は、組織が外部委託業者をランク付けし、業務の大部分を最も評価の高い業者に割り当てるようにします。

Answer: A,B,E (メッセージを残す)

* A. 他のデータセンターは、同じ通信グループに属していても、外部プロバイダーとして扱われていることを確認します。これは、ISO 27001:2022の8.1.4項で、組織は情報セキュリティマネジメントシステムに関連する外部提供のプロセス、製品、またはサービスが管理されていることを確認する必要があると規定されているため適切です。外部提供のプロセス、製品、またはサービスとは、組織との関係の程度に関わらず、外部の当事者によって提供されるものです。したがって、同じ通信グループ内の他のデータセンターは、外部プロバイダーとして扱われ、他の外部プロバイダーと同様の管理を受ける必要があります12

* B. 外部プロバイダーが、製品またはサービスの使用から生じるリスクを組織に通知するための文書化されたプロセスを整備していることを確認します。これは、ISO 8.1.4 項に基づき適切です。

27001:2022では、組織は外部プロバイダーとの間で情報セキュリティに関する適切な契約要件を導入することが求められています。契約要件の一つとして、外部プロバイダーが、セキュリティインシデント、脆弱性、組織の情報セキュリティに影響を与える可能性のある変更など、製品やサービスの使用から生じるあらゆるリスクを組織に通知する義務を課すことが挙げられます。外部プロバイダーは、そのような通知がタイムリーかつ正確で完全であることを保証するための文書化されたプロセスを整備しておく必要があります。12

* E. 組織が外部プロバイダーのパフォーマンスを定期的に監視、レビュー、評価することを確実にします。これは、ISO 27001:2022の8.1.4項で、組織が外部から提供されるプロセス、製品、またはサービスのパフォーマンスと有効性を監視、レビュー、評価することが求められているため適切です。組織は、外部プロバイダーの成果物と活動の適合性と適切性を測定および検証し、必要に応じてフィードバックと改善策を提供するプロセスを整備する必要があります。組織はまた、監視、レビュー、評価の結果の記録を保持する必要があります12

* F. 組織がISMSに関して外部プロバイダーとコミュニケーションを取る必要性を判断していることを確認します。これは、ISO 27001:2022の7.4.2項で、組織が外部プロバイダーとのコミュニケーションを含め、情報セキュリティマネジメントシステムに関連する内部および外部コミュニケーションの必要性を判断することが求められているため適切です。組織は、そのようなコミュニケーションの目的、内容、頻度、方法、および責任を定義し、それが情報セキュリティポリシーおよび目標と一致していることを確認する必要があります。組織はまた、コミュニケーションの実施の証拠として、コミュニケーションの文書化された情報を保持する必要があります12 ISO 27001に従って外部プロバイダーを評価するには、次の活動は適切ではありません。

2022年:

* C. 組織が情報の機密性、完全性、およびアクセス可能性の維持に不可欠であると特定した各プロセスについて、予備の外部プロバイダーを確保するようにします。これは適切ではありません。ISO 27001:2022では、組織が各重要プロセスについて予備の外部プロバイダーを持つことを要求していないためです。組織は、外部プロバイダーの障害または中断に備えて、緊急時対応計画またはバックアップソリューションを用意することを選択できますが、これは必須要件ではありません。組織は、外部プロバイダーに関連するリスクと機会を評価し、適切な対応策を決定する必要があります。これには、予備の外部プロバイダーを持つことが含まれる場合も含まれない場合もあります。12

* D. 外部提供のプロセスに監査活動を限定します。外部提供の製品やサービスを監査する必要がないためです。これは適切ではありません。ISO 27001:2022の8.1.4項では、組織は情報セキュリティマネジメントシステムに関連する外部提供のプロセス、製品、またはサービスを管理する必要があると規定されているからです。外部提供の製品やサービスには、組織の情報セキュリティに影響を与える可能性のあるソフトウェア、ハードウェア、データ、クラウドサービスなどが含まれる場合があります。したがって、監査活動は、該当する場合、外部提供のプロセスと製品またはサービスの両方を対象とする必要があります12

* G. 私は、経営陣が外部ISMSプロセスと内部ISMSプロセスを提供する者に対して役割と責任を割り当てていることを確認します。これは適切ではありません。ISO 27001:2022の5.3項では、経営陣は組織内の情報セキュリティ管理システムの役割と責任を割り当てる必要があり、外部プロバイダーに対して割り当てる必要はないと規定されているからです。外部プロバイダーは、組織に提供するプロセス、製品、またはサービスについて、自らの役割と責任を割り当てる責任があります。組織は、外部プロバイダーがその役割と責任について十分な能力と認識を持ち、組織の情報セキュリティ要件を遵守する契約上の義務を負っていることを確認する必要があります12

* H. 組織が外部プロバイダーをランク付けし、最も評価の高いプロバイダーに業務の大部分を割り当てるようにします。これは適切ではありません。ISO 27001:2022 では、組織が外部プロバイダーをランク付けしたり、そのようなランク付けに基づいて業務を割り当てたりすることを要求していないためです。組織は、外部プロバイダーのパフォーマンスと有効性を評価および比較することを選択できますが、これは必須要件ではありません。組織は、組織に関連する情報セキュリティ基準と目標に基づいて、外部プロバイダーを選択して使用する必要があります。12 参考文献:

1: ISO/IEC 27001:2022 リードオーディター（情報セキュリティマネジメントシステム）コース（CQIおよびIRCA認定トレーニング1）2: ISO/IEC 27001 リードオーディタートレーニングコース（PECB 2）

最新問題: 225

監査チームのリーダーたちは、今年初めに実施した第三者機関による監督監査に続き、フォローアップ監査を計画している。彼らは、是正措置を検討する前に、修正が必要な不適合事項を確認することにした。

以下の説明に基づき、監視中に特定された不適合に対する是正措置として適切なものはどれですか？ 4つ選択）

- A. 顧客データサービス供給契約に不足していた署名を追加しました。
- B. 新システム導入時に顧客に送付されなかったソフトウェアインストールガイドが公開されました。
- C. 日付エラーを修正した新しいネットワークスイッチ購入注文
- D. 規定の手順に従ってバックアップを実行できなかったデータセンターの従業員は、再研修を受けた。
- E. ハードドライブ HD302 (赤色 (破棄予定) ではなく緑色 (使用可能) で色分け) がシステムから取り外されました。
- F. 予定されていた経営レビューが欠席したため、総支配人が優先順位を上げて、特定の日に年2回開催することに決定しました。
- G. 製品輸送に関する文書化された手順は、配送チームがこの活動をどのように実行しているかを反映していませんでした。そのため、手順は書き直され、チームはそれに応じてトレーニングを受けました。
- H. 組織は適合性表を維持できず、その更新責任を最高技術責任者に再割り当てしました。

Answer: A,B,C,E (メッセージを残す)

ISO/IEC 27001 主任審査員向け PECB 候補者ハンドブックによると、是正とは、再作業、修理、交換など、検出された不適合を排除するための措置です 1。A、B、C、E の例は、署名の欠落、ガイドの欠落、日付の誤り、カラーコードの誤りなど、不適合の原因となったエラーや欠陥を修正するため、是正です。その他の例 (D、F、G、H) は、不十分なトレーニング、計画の不備、文書化の不備、責任の不明確さなど、不適合の根本原因に対処するため、是正措置です 2。参考文献: 1:

ISO/IEC 27001 主任審査員のための PECB 候補者ハンドブック、35 ページ、セクション 4.5.12: ISO/IEC 27001 主任審査員のための PECB 候補者ハンドブック、36 ページ、セクション 4.5.2。

最新問題: 226

あなたは経験豊富な監査チームリーダーであり、監査員の研修を指導する立場にあります。

貴社チームは現在、外部顧客のためにデータを保管する組織に対し、第三者監視監査を実施しています。訓練を受けた監査担当者は、適合性声明書（SoA）に記載され、現場で実施されている組織内統制をレビューする任務を負っています。

研修を希望する監査担当者にレビューしてもらいたい管理項目を、以下のリストから4つ選択してください。

- A. 荷積みエリアへの出入り口通路
- B. 電力ケーブルとデータケーブルはどのように建物内に引き込まれますか？
- C. 情報セキュリティに関する意識向上、教育、トレーニング
- D. 人員の確認とチェック。
- E. 情報資産目録の作成と維持
- F. 現場監視カメラおよび入退室管理システムの運用
- G. 機器メンテナンスの手配
- H. 組織の事業継続計画

Answer: A,B,F,G (メッセージを残す)

ISMSの物理的側面に関連するリストにある4つの管理策は以下のとおりです。

- * 荷積み場への出入り
- * 電力ケーブルとデータケーブルが建物に引き込まれる方法
- * 敷地内のCCTVおよびドア制御システムの運用
- * 組織の機器保守に関する取り決め

これらの管理策は、ISO 27001附属書Aから派生したものであり、ISMSに適用できる情報セキュリティ管理策の包括的なリストを提供しています。リストにあるその他の管理策は、ISMSの組織的、法的、または人的側面に関連するものであり、これらも重要ですが、この質問の焦点ではありません。

ISMS監査ガイドライン2によれば、研修中の監査員は、物理的統制を以下の方法で確認する必要があります。

- * SoAを確認して、適用されるコントロールとその実装状況を特定する
- * 関係するスタッフや管理職にインタビューを行い、彼らが統制を理解し、関与していることを確認する。
- * 物理的および環境的条件を観察し、制御の存在と有効性を確認する
- * 関連する文書や記録を調査して、管理策の遵守状況とパフォーマンスを検証します。これが試験の準備に役立つことを願っています。

有効な **ISO-IEC-27001-Lead-Auditor-CN** 問題集は GoShiken.com が提供された合格しやすい ISO-IEC-27001-Lead-Auditor-CN 試験問題集！ GoShiken.com が最新の **ISO-IEC-27001-Lead-Auditor-CN** 試験問題集を提供しています。GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 問題集をゲットする人はこちら：
<https://www.goshiken.com/PECB/ISO-IEC-27001-Lead-Auditor-CN-mondaishu.html> (418**30%OFF**問題集溶と正解付きで 30%w特別割引コード: **Freepdfdumps**)

最新問題: 227

質問：

次のうち、経営管理を最も適切に定義しているのはどれですか？

- A. 人事管理に関連する統制には、従業員研修、経営陣によるレビュー、内部監査が含まれます。
- B. 職務分掌、職務ローテーション、職務記述書、承認プロセスなど、組織構造に関連する統制。
- C. ファイアウォール、警報システム、監視カメラ、侵入検知システム（IDS）などの技術の使用に関連する制御措置。

Answer: A (メッセージを残す)

包括的かつ詳細な解説：

- * 管理統制（管理統制とも呼ばれる）には、効果的なセキュリティガバナンスを確保するためのポリシー、手順、プロセスが含まれます。これらの統制には、研修、内部監査、セキュリティ意識向上プログラム、および経営陣によるレビューが含まれます。これらは、ISO/IEC 27001:2022 附属書 A 統制 A.5.2（情報セキュリティの役割と責任）および A.5.3（職務分掌に準拠しています）。
- * B. 組織構造の統制は、職務の分離や職務のローテーションに関係するため、純粋な管理統制というよりは構造的な統制である。
- * C. 技術的制御には、ファイアウォール、IDS、その他のセキュリティメカニズムが含まれ、これらは管理上の措置ではなく技術的な措置です。

最新問題: 228

選出最能完成句子的單字：

Select the words that best complete the sentence:

“The purpose of a third-party audit is to _____ an organisation’s _____ to inform _____ decision.”

To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

approve

inspect

a compliance

an accreditation

products

evaluate

management system

a certification

processes

Answer:

Select the words that best complete the sentence:

“The purpose of a third-party audit is to **evaluate** _____ an organisation’s **management system** to inform _____ decision.”

To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

approve

inspect

a compliance

an accreditation

products

evaluate

management system

a certification

processes

最新問題: 229

フィッシングとは、どのような種類の情報セキュリティインシデントですか？

- A. 個人的な問題
- B. ハッカー/突破攻撃
- C. 技術的な脆弱性
- D. 訴訟事件

Answer: B (メッセージを残す)

フィッシングは、クラッカー／ハッカー攻撃に分類される情報セキュリティインシデントの一種です。
フィッシングとは、偽のメールやその他のメッセージを使って受信者を騙し、パスワード、クレジットカード番号、銀行口座情報などの機密情報を漏洩させる詐欺行為の一種です。フィッシングメールは、正規の組織や個人になりすまし、緊急性や好奇心を煽ることで、被害者を悪意のあるリンクをクリックさせたり、悪意のある添付ファイルを開かせたり、個人情報を提供させたりします。

フィッシングは、個人情報の盗難、金銭的損失、データ漏洩、マルウェア感染、その他の損害につながる可能性があるため、情報セキュリティに対する一般的かつ深刻な脅威です。ISO/IEC 27001:2022では、組織がフィッシングなどのソーシャルエンジニアリング攻撃のリスクと回避方法をユーザーに認識させるための啓発およびトレーニングプログラムを実施することを義務付けています A.7.2.2項参照)。参考文献 :CQIおよびIRCA認定ISO/IEC 27001:2022 主任監査員トレーニングコース、ISO/IEC 27001:2022 情報技術 - セキュリティ 技術 - 情報セキュリティ管理システム - 要求事項、フィッシングとは？

最新問題: 230

あなたは経験豊富な監査チームリーダーであり、監査員の研修を指導する立場にあります。

貴チームは現在、外部顧客のためにデータを保管する組織に対し、第三者監視監査を実施しています。訓練を受けた監査担当者は、適合性報告書 \$oA)に記載され、現場で実施されている人事管理体制を検証する任務を負っています。

研修を希望する監査担当者にレビューしてもらいたい管理項目を、以下のリストから4つ選択してください。

- A. 機密保持および機密保持契約
- B. マルウェア対策の実装方法
- C. 情報セキュリティに関する意識向上、教育、トレーニング
- D. リモートワーク体制
- E. 人員の確認とチェック。
- F. 現場監視カメラおよび入退室管理システムの運用
- G. 組織の情報削除に関する取り決め
- H. 組織の事業継続計画

Answer: A,C,D,E ([メッセージを残す](#))

研修中の監査員が確認すべき、リストにある4つの統制事項は以下のとおりです。

*

A. 機密保持契約および秘密保持契約 :この管理策では、機密情報にアクセスするすべての従業員、契約業者、および第三者が、当該情報の機密性と完全性を保護する義務を負う適切な契約に署名することを組織が保証する必要があります。これは、外部顧客のためにデータを保管する組織にとって特に重要であり、顧客の情報資産を保護し、契約上の義務を遵守するという組織の姿勢を示すものです。

* C. 情報セキュリティに関する意識向上、教育、および研修 :この管理策では、組織の情報システムおよび情報資産にアクセスするすべての従業員、契約業者、および第三者に対し、定期的かつ適切な情報セキュリティに関する意識向上、教育、および研修を提供することが求められます。これは、彼らが自身の役割と責任、情報セキュリティに関する方針と手順、潜在的な脅威とリスク、および情報セキュリティインシデントの防止と対応に関するベストプラクティスを確実に理解するために不可欠です。

* D. リモートワーク体制 :この管理策では、組織はテレワーク、モバイルワーク、在宅勤務などのリモートワーク体制に伴う情報セキュリティリスクを管理するためのポリシーと手順を確立し、実施する必要があります。これには、承認されたデバイス、アプリケーション、ネットワーク、暗号化および認証方法、バックアップおよび復旧手順、報告および監視メカニズムなど、リモートワークの条件と要件を定義することが含まれます。これは、外部クライアントのためにデータを保存する組織にとって重要です。なぜなら、従業員の場所や使用するデバイスに関係なく、情報セキュリティレベルが維持されることが保証されるからです。

* E. 人員の身元確認 :この管理策では、組織の情報システムおよび情報資産にアクセスするすべての従業員、契約業者、および第三者の経歴、資格、および照会先について、適切な身元確認を実施することが求められます。これは、彼らの身元、適性、および信頼性を確認するため、また、組織および顧客の情報セキュリティを損なう可能性のある、権限のない者や悪意のある者の雇用を防止するために必要です。

最新問題: 231

シナリオ6

Sinvestmentは、住宅保険、商業保険、生命保険など、さまざまな保険プランを提供する保険会社です。もともと北カリフォルニアで設立された同社は、ヨーロッパやアフリカを含む他の地域にも事業を拡大しています。Sinvestmentは事業の成長に加え、業界の関連法規制を遵守し、情報セキュリティインシデントを防止することにも尽力しています。同社はISO規格に基づいた情報セキュリティマネジメントシステム (SMS)を導入しています。

本製品はIEC 27001規格に準拠しており、認証申請中です。

認証機関は監査チームを任命し、監査を実施させた。監査チームはSinvestment社と機密保持契約を締結した後、業務を開始した。監査の第一段階におけるすべての活動は現地で実施されたが、Sinvestment社の要請により、アーカイブ情報のレビューはリモートで実施された。

監査チームはまず、情報セキュリティマネジメントシステム（ISMS）の適用範囲記述書、情報セキュリティポリシー、内部監査報告書などの必要文書をレビューする第1段階監査を実施しました。記録された情報の評価は、主にその内容と管理プロセスに基づいて行われました。

さらに、監査担当者は、情報セキュリティ研修および啓発プログラムに関する文書が不完全で、重要な詳細情報が欠落していることを発見した。これについて質問された際、Sinvestmentの経営陣は、同社は全従業員に情報セキュリティ研修コースを提供したと述べた。

監査の第2段階は、第1段階から3週間後に実施された。監査チームは、マーケティング部門（監査範囲外において、従業員のアクセス権限を管理する手順が欠如していることを発見した。

従業員のアクセス権限の管理はISO/IEC 27001の要件の一つであり、会社の情報セキュリティポリシーにも組み込まれているため、この問題は監査報告書に含められました。

質問

シナリオ6に基づくと、監査チームは市場部門のアクセス制御手順で発見された不備を監査報告書に含めるべきでしょうか？

A. はい、監査報告書にはすべての監査結果を含める必要があります。

B. いいえ、それは監査対象企業の代表者にのみ伝えられるべきです。

C. いいえ、マーケティング部門の活動は情報セキュリティ管理システムに潜在的なリスクをもたらさないからです。

Answer: A (メッセージを残す)

監査チームが発見された不備を監査報告書に含めることは適切であり、選択肢Aが正解です。ISO/IEC 17021-1およびISO 19011では、監査対象部門が正式に監査範囲に記載されているかどうかに関わらず、監査基準への適合性に関連するすべての所見を報告することが監査員に求められています。重要なのは、その問題がISMSの要求事項または方針に関連しているかどうかです。

このシナリオでは、アクセス権限管理はSinvestment社の情報セキュリティポリシーに明示的に含まれており、ISO/IEC 27001の中核的な要件となっています。マーケティング部門におけるアクセス制御手順の欠如は、ISMS要件の実装における弱点を示しています。マーケティング部門は監査対象範囲には含まれていませんでしたが、監査員はISMS全体の有効性に悪影響を及ぼす可能性のある状況を認識することができました。

選択肢Bは、問題を非公式に伝えるだけでは透明性と追跡可能性が損なわれるため、誤りです。監査報告書には、調査結果の完全かつ正確な記録が記載されていなければなりません。選択肢Cも、マーケティング部門は特に保険業界において個人データや機密情報を頻繁に取り扱うため、ISMS（情報セキュリティマネジメントシステム）のリスクとなる可能性が明らかに高いため、誤りです。

監査人は、関連する調査結果を客観的かつ漏れなく報告することが求められます。したがって、この問題を監査報告書に含めることは適切でした。

最新問題: 232

シナリオ4

SendPayは、代理店や金融機関のネットワークを通じてグローバルな送金サービスを提供する金融サービス会社です。市場参入間もないSendPayは、高品質なサービスの提供に尽力しており、昨年ローンチした手数料無料のデジタルプラットフォームでは、スマートフォンやノートパソコンを使っていつでもどこでも送金・受金が可能です。当時、SendPayはソフトウェア開発業務を外部チームに委託しており、そのチームが同社の技術インフラも管理していました。

同社は最近、情報セキュリティマネジメントシステム（ISMS）を導入してから約1年後、ISO/IEC 27001認証の申請を行った。

監査において、監査人はSendPayのアウトソーシング事業、特にアウトソーシング会社が担当するソフトウェア開発と技術インフラの保守に重点を置いた。

彼らは、アウトソーシング業務の品質を監視するためのSendPayのプロセスをレビューおよび評価する構造化されたアプローチを採用した。これには、同社が契約上の義務を履行していることの確認、アウトソーシング先の雇用に関する適切な管理手順の確保、およびアウトソーシング契約の予期された、または予期せぬ終了に対するSendPayの対応の評価が含まれていた。

しかしながら、監査人は、SendPayの契約書にはアウトソーシング契約の予期せぬ解除の可能性が十分に考慮されていないことを、慎重に指摘した。さらに、SendPayが任命した技術専門家が監査人を支援し、監査対象のアウトソーシング活動に関する専門知識と経験を提供した。

監査チームは、情報セキュリティ管理システム（ISMS）が定められた目標を達成していることを確認するため、従業員がISMSに関する研修を受けた時間数を算出しました。また、監査中に抽出したサンプルに基づいて情報セキュリティインシデントの平均解決時間を算出し、SendPayのインシデント管理の実践状況を把握しました。さらに、監査担当者は監査中に収集した証拠の信頼性を評価しました。監査証拠の信頼性に影響を与えるいくつかの要因を考慮しました。例えば、監視ビデオは写真よりも客観的な証拠となります。時間的要素も信頼性に重要な役割を果たし、取引記録などの仕組みは証拠の信頼性を高めることができます。

SendPayは、業務効率と拡張性を向上させるためにクラウドプラットフォームを利用しています。しかし、リソースの制約により、監査人は監査プロセス中にSendPayに対しクラウド活動の一覧を提供するよう求めず、代わりにSendPayの声明に依拠しました。

質問

シナリオ4に基づくと、アウトソーシングされた業務の監査において、関係者全員が関与することは許容されるのでしょうか？

A. はい、すべての関係者の参加は容認できると考えています。

B. いいえ、技術専門家の関与は受け入れられません。

C. いいえ、観察者は1人だけで良いです。

Answer: A ([メッセージを残す](#))

シナリオ4で説明されているすべての関係者の関与は許容範囲内であり、マネジメントシステムの監査に関するISO 19011:2018のガイダンスに合致しているため、選択肢Aが正解です。ISO 19011では、監査チーム以外にも、技術専門家、ガイド、オブザーバー、被監査企業の代表者など、さまざまな参加者が監査に関与する可能性があることを認めており、ただし、それぞれの役割が明確に定義され、管理されていることが条件となります。

この事例では、SendPay社が任命した技術専門家が、アウトソーシングされたソフトウェア運用および技術インフラに関する専門知識を提供することで、監査担当者を支援しました。これはISO 19011で明確に認められており、監査担当者自身が十分に持ち合わせていない専門知識が必要な場合に、技術専門家の活用が認められています。技術専門家の役割は、監査チームに専門知識を提供することであり、監査結果に影響を与えたり、監査担当者の判断を代替したりすることではありません。

選択肢Bは誤りです。ISO 19011は技術専門家の関与を禁止していません。むしろ、アウトソーシングされたIT運用やクラウドベースのサービスなど、複雑または高度な技術分野の監査においては、技術専門家の関与が推奨されています。選択肢Cも誤りです。オブザーバーのみの参加に限定すると、監査員はアウトソーシングされた業務を効果的に評価するために必要な技術的知見を得ることができません。

監査チームのリーダーが監査プロセスを管理し、独立性と客観性を確保する限り、監査人、被監査企業の代表者、および技術専門家の関与は適切である。

したがって、この監査にすべての関係者が関与することは、ISO監査原則の下で許容される。

最新問題: **233**

リストを使用する利点を説明する選択肢を2つ選んでください。

A. 各レビューで同じリストが使用されるため、レビューは不要です。

B. 指定された面接対象者を制限する

C. 関連する監査追跡への準拠を確保する

D. 監査計画が確実に実施されるようにする

E. レビュー時間を短縮

F. 必要であればリストを変更しないでください。

Answer: C,D ([メッセージを残す](#))

チェックリストは、監査人が監査の目的と範囲に関連する情報を収集し、検証するのに役立つツールです。チェックリストには、次のような利点があります。

関連する監査証拠が確実に追跡されるようにする :チェックリストは、監査対象基準の適合性または不適合性を裏付ける証拠の出所を特定し、追跡するのに役立ちます。また、監査の重要な側面を見落としたり、漏らしたりすることを防ぐのにも役立ちます。

監査計画の確実な実施 :チェックリストは、監査担当者が監査計画に従って作業を進めるのに役立ちます。監査計画には、監査の目的、範囲、基準、スケジュール、役割、責任など、監査の手順と詳細が記載されています。また、監査担当者が時間とリソースを効果的かつ効率的に管理するのにも役立ちます。

その他の選択肢はチェックリストを使用する利点ではなく、むしろ次の点である。

同じチェックリストをレビューせずにすべての監査に使用すること :これはチェックリストを使用する際の欠点であり、硬直的で非効率的な監査アプローチにつながる可能性があります。チェックリストは、監査対象者および監査基準の状況、リスク、変更点を考慮して、各監査に合わせてカスタマイズおよび調整する必要があります。また、チェックリストの妥当性と関連性を確保するために、定期的にレビューおよび更新する必要があります。

インタビュー対象者を指名された関係者に限定すること :これはチェックリストを使用する際の欠点であり、監査の範囲と深さを制限してしまう可能性があります。チェックリストは、監査担当者が監査にとって貴重な証拠や洞察を提供する可能性のある他の関係者や情報源にインタビューすることを妨げるものであってはなりません。チェックリストはガイドとして使用すべきであり、制約として使用すべきではありません。

監査期間の短縮 :これは必ずしもチェックリストを使用する利点とは限りません。なぜなら、被監査企業のISMSの複雑さ、規模、成熟度、証拠の入手可能性と質、監査員の能力と経験、監査員と被監査企業間の協力とコミュニケーションのレベルなど、さまざまな要因に左右されるからです。チェックリストは効率性と組織性を向上させることで監査期間の短縮に役立つ可能性がありますが、より多くの証拠や検証を必要とすることで監査期間が長くなる可能性もあります。

必要に応じてチェックリストから逸脱しないこと :これはチェックリストを使用する際の欠点であり、表面的な、あるいは不完全な監査につながる可能性があります。チェックリストは、監査中に発生した問題や懸念事項 (チェックリストに記載されていないものであっても) を監査担当者が調査・検討することを妨げるものであってはなりません。チェックリストはあくまで補助的なものであり、代替物として使用すべきではありません。

参照 :

ISO/IEC 27001:2022 主任審査員 (情報セキュリティマネジメントシステム)の目的と内容は Quality.org および PECB から引用。ISO 19011:2018 マネジメントシステムの監査に関するガイドライン [セクション 6.2.2]

最新問題: 234

シーン2：

1990年代に設立されたClinicは、心臓関連疾患の治療と複雑な手術を専門とする医療機器メーカーです。ヨーロッパに本社を置き、患者と医療従事者にサービスを提供しています。Clinicは、治療計画の個別化、治療結果のモニタリング、機器機能の向上を目的として患者データを収集しています。データセキュリティの強化と信頼性の構築のため、ClinicはISO/IEC 27001に基づく情報セキュリティマネジメントシステム（ISMS）を導入しています。当クリニックは、内部の問題、インターフェース、内部活動と外部委託活動間の依存関係、および利害関係者の期待のみを考慮して、ISMSの範囲を決定します。この範囲は綿密に文書化され、いつでも確認できるようになっています。ISMSを定義するにあたり、当クリニックは、研究開発、患者データ管理、顧客サポートといった主要部門内の主要プロセスに焦点を当てることを選択しました。当初は困難もありましたが、クリニックはISMSの導入と、独自のニーズに合わせた安全管理策の策定に尽力しました。プロジェクトチームは、ISO/IEC 27001の附属書Aに記載されている特定の管理策を除外する一方で、業界固有の管理策を追加して安全性を強化しました。チームは、内部要因と外部要因に基づいてこれらの管理策の適合性を評価し、最終的に、管理策の選択と導入の根拠を詳細に記した包括的な適合性宣言書（SoA）を作成しました。認証取得に向けた準備が進むにつれ、チームリーダーに任命されたブライアンは、自主的なリスク評価手法を採用し、会社の戦略的な課題とセキュリティ対策を特定して評価した。この積極的なアプローチにより、クリニックのリスク評価が目標と使命に合致することが保証された。

シナリオ2に基づく、クリニックのISMSの範囲は正しく定義されているでしょうか？

- A. いいえ、クリニックは外部の問題も考慮する必要があります。
- B. はい、クリニックのISMSの範囲は正しく定義されています。
- C. いいえ、クリニックは除外事項とその理由もISMSに含める必要があります。

Answer: A (メッセージを残す)

包括的かつ詳細な徹底分析

- A. 正解: ISO/IEC 27001 条項 4.1 (組織とその特性の理解) シナリオでは、クリニックは内部の問題のみを考慮し、規制要件、業界標準、サイバーセキュリティの脅威などの外部要因を評価しなかったとされています。
- B. 誤り：外部要因が考慮されていないため、範囲が完全には正しくありません。
- C. 誤り：除外事項の正当化は、ISMSの適用範囲記述書ではなく、SoA（適用範囲記述書）が必要となる。

最新問題: 235

場景 7 Lawsy 是一家領先的律師事務所，在新澤西州和紐約市設有辦公室。它擁有 50 多名律師，為商業法、智慧財產權、銀行和金融服務領域的客戶提供完善的法律服務。他們相信，由於他們致力於實施資訊安全最佳實踐並跟上技術發展的步伐，他們在市場上佔據了有利的地位。

Lawsy 已經嚴格實施、評估和進行 ISMS 內部審核兩年了。

現在，他們已向知名且可信賴的認證機構SMA申請ISO/IEC 27001認證。

在第一階段審核期間，審核小組審核了實施過程中所建立的所有ISMS 文件。

他們還審核和評估了管理審核和內部審計的記錄。

Lawsy 提交了證據記錄，表明在必要時對不合格項採取了糾正措施，因此審核組約談了內部審核員訪談透過提供對內部稽核計畫和程序的詳細了解，驗證了內部稽核的充分性和頻率。

審計小組繼續驗證戰略文件，包括資訊安全政策和風險評估標準。在資訊安全政策審核期間，團隊注意到描述治理框架（即資訊安全政策）的記錄資訊與程序之間存在不一致。

儘管允許員工將筆記型電腦帶到工作場所之外，但Lawsy 並沒有製定有關在這種情況下使用筆記型電腦的程序。此政策僅提供有關筆記型電腦使用的一般資訊。該公司依靠員工的常識來保護筆記型電腦中儲存的資訊的機密性和完整性。該問題已記錄在第一階段審計報告中。

完成第一階段審核後，審核組長準備了審核計劃，其中規定了審核目標範圍、標準和程序。

在第二階段審核期間，審核小組約談了資安經理，資安經理起草了資訊安全政策。他透過指出 Lawsy 每三個月舉辦一次強制性資訊安全培訓和意識課程來證明第一階段中確定的問題的合理性。

面談後，審核小組檢查了15 份員工培訓記錄（共50 份），得出的結論是awsy 符合 ISO/IEC 27001 有關培訓和意識的要求。為了支持這個結論，他們影印了檢查過的員工訓練記錄。

根據上述場景，回答以下問題：

審核員是否應在審核完成後將員工訓練記錄的副本存檔？請參閱場景 7。

- A. 否，文件副本通常不會儲存為審核記錄
- B. はい、監査契約書に記載されているとおり、監査人は文書のコピーを所持しています。

C. はい、審査プロセス中に作成されたすべての文書情報は、審査記録として保管する必要があります。

Answer: A (メッセージを残す)

いいえ、監査計画で特に要求され合意されている場合を除き、ファイルのコピーは一般的に監査記録として保管されません。監査記録には通常、監査人が作成したメモや所見が含まれ、被監査者のファイルのコピーは含まれません。ただし、これらが不可欠であり、被監査者によって明示的に許可されている場合はこの限りではありません。

最新問題: 236

貴社は現在、ISO/IEC 27001:2022認証の取得を目指しています。あなたは先日、内部ISMS監査員の資格を取得しました。ICTマネージャーは、あなたの新たな知識を活用して、情報セキュリティインシデント管理プロセスの設計を支援してもらいたいと考えています。

彼は計画策定プロセスにおける以下の段階を特定し、それらがどのような順序で行われるべきかを確認するようあなたに依頼しました。

Step 1	Incident logging
Step 2	
Step 3	
Step 4	
Step 5	
Step 6	
Step 7	
Step 8	Incident closure

To complete the sequence, click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the options to the appropriate blank section.

Incident prioritisation – classify the incident as critical, high, medium, low

Task creation and management – identification and coordination of work needed to resolve the incident

SLA management and escalation – ensure any service level agreements are adhered to whilst resolution is being implemented. If a breach looks likely, escalate to secure more resources

Incident resolution – a temporary workaround or permanent resolution has been identified

Incident assignment – incident is passed to the individual best suited to resolve it

Incident categorisation – determine whether the incident is a hardware issue, network issue or software issue

Answer:

Step 1	Incident log	
Step 2		Incident categorisation – determine whether the incident is a hardware issue, network issue
Step 3		Incident prioritisation – classify the incident as critical, high, medium, low
Step 4		
Step 5		SLA management and escalation – ensure any service level agreements are adhered to whilst resolution is being implemented. If a
Step 6		Incident resolution – a temporary workaround or permanent resolution has been identified
Step 7		
Step 8	Incident closure	

To complete the sequence, click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the options to the appropriate blank section.

Incident prioritisation – classify the incident as critical, high, medium, low

Task creation and management – identification and coordination of work needed to resolve the incident

SLA management and escalation – ensure any service level agreements are adhered to whilst resolution is being implemented. If a breach looks likely, escalate to secure more resources

Incident resolution – a temporary workaround or permanent resolution has been identified

Incident assignment – incident is passed to the individual best suited to resolve it

Incident categorisation – determine whether the incident is a hardware issue, network issue or software issue

Explanation:

ステップ 1 = インシデントのログ記録 ステップ 2 = インシデントの分類 ステップ 3 = インシデントの優先順位付け ステップ 4 = インシデントの割り当て ステップ 5 = タスクの作成と管理 ステップ 6 = SLA の管理とエスカレーション ステップ 7 = インシデントの解決 ステップ 8 = インシデントのクローズ 情報セキュリティインシデント管理プロセスの各段階の順序は、インシデント、イベント、脆弱性に対して迅速、効果的、かつ秩序だった対応を保証する論理的な順序に従う必要があります。また、この順序は、ISO/IEC 27001:2022 および ISO が提供するベストプラクティスとガイダンスにも準拠している必要があります。

/IEC 27035:2022。したがって、以下の順序が推奨されます。

* ステップ 1 = インシデントの記録: このステップでは、発生日時、発生源、説明、影響、報告者など、潜在的なインシデント、イベント、または脆弱性の詳細を記録します。このステップは、インシデントの追跡可能な記録を提供し、その後の分析と対応を容易にするために重要です。このステップは、情報セキュリティのインシデント、イベント、および脆弱性の管理に関する責任と手順を組織が確立することを要求する ISO/IEC 27001:2022 の管理策 A.16.1.1 に関連しています。このステップは、インシデント、イベント、および脆弱性の記録方法に関するガイダンスを提供する ISO/IEC 27035:2022 の条項 6.2 にも関連しています。

* ステップ 2 = インシデントの分類: このステップでは、ハードウェアの問題、ネットワークの問題、ソフトウェアの問題など、インシデント、イベント、または脆弱性の種類と性質を判断します。このステップは、インシデントを分類し、適切な解決担当者またはチームに割り当てるために重要です。このステップは、組織が情報セキュリティのイベントと脆弱性を適切な管理チャネルを通じてできるだけ迅速に報告することを要求する ISO/IEC 27001:2022 の管理策 A.16.1.2 に関連しています。このステップは、インシデント、イベント、および脆弱性を分類する方法に関するガイダンスを提供する ISO/IEC 27035:2022 の条項 6.3 にも関連しています。

* ステップ 3 = インシデントの優先順位付け: このステップでは、インシデント、イベント、または脆弱性の深刻度と緊急度を評価し、それを重大、高、中、または低に分類します。このステップは、インシデントの優先順位付けと、対応に必要なリソースと時間の割り当てに重要です。このステップは、組織が定義された基準に従って情報セキュリティイベントと脆弱性を評価し、優先順位付けすることを要求している ISO/IEC 27001:2022 の管理策 A.16.1.3 に関連しています。このステップは、インシデント、イベント、および脆弱性の優先順位付け方法に関するガイダンスを提供する ISO/IEC 27035:2022 の条項 6.4 にも関連しています。

* ステップ 4 = インシデントの割り当て: このステップでは、スキル、知識、および可用性に基づいて、インシデント、イベント、または脆弱性を解決するのに最も適した個人またはチームにインシデント、イベント、または脆弱性を引き渡します。

この手順は、インシデントが適切な担当者またはチームによって処理され、遅延や混乱を避けるために重要です。この手順は、組織が合意された手順に従って、情報セキュリティインシデントおよび脆弱性にタイムリーに対応することを要求する ISO/IEC 27001:2022 の管理策 A.16.1.4 に関連しています。また、この手順は、インシデント、イベント、および脆弱性の割り当て方法に関するガイダンスを提供する ISO/IEC 27035:2022 の条項 6.5 にも関連しています。

* ステップ5＝タスクの作成と管理: このステップでは、根本原因分析の実施、ソリューションのテスト、変更の実装、アクションの文書化など、インシデント、イベント、または脆弱性を解決するために必要な作業を特定し、調整します。このステップは、インシデントが効果的かつ効率的に解決され、アクションが追跡および管理されることを保証するために重要です。このステップは、情報セキュリティのイベントや脆弱性から得られた教訓を組織に適用して是正措置および予防措置を講じることを要求する ISO/IEC 27001:2022 の管理策 A.16.1.5 に関連しています。このステップは、インシデント、イベント、および脆弱性に対するタスクの作成と管理方法に関するガイダンスを提供する ISO/IEC 27035:2022 の条項 6.6 にも関連しています。

* ステップ6＝SLA の管理とエスカレーション: このステップでは、解決策の実施中にサービスレベル契約 (SLA) が遵守されていることを確認し、違反が発生する可能性が高い場合または発生した場合は、インシデントを上位の権限またはサポートレベルにエスカレーションします。このステップは、インシデントが合意された時間枠と品質内で解決され、逸脱や問題が伝達され対処されることを保証するために重要です。このステップは、ISO の管理 A.16.1.6 に関連しています。

ISO/IEC 27001:2022では、組織が情報セキュリティ上のインシデントや脆弱性を、必要に応じて関連する内部および外部の関係者に伝達することが求められています。この手順は、インシデント、イベント、脆弱性に関するSLA およびエスカレーションの管理方法に関するガイダンスを提供するISO/IEC 27035:2022の6.7項にも関連しています。

* ステップ7＝インシデント解決 :このステップでは、インシデント、イベント、または脆弱性を解決するために、一時的な回避策または恒久的な解決策を適用し、情報および情報処理施設の正常な動作を復旧します。このステップは、インシデントが完全に満足いく形で解決され、情報セキュリティが望ましいレベルまで回復されることを保証するために重要です。

この手順は、ISO/IEC 27001:2022の管理策A.16.1.7に関連しています。この管理策では、組織が情報セキュリティインシデントおよび脆弱性の原因を特定し、それらの再発または発生を防止するための措置を講じることを求めています。また、この手順は、インシデント、イベント、および脆弱性を解決する方法に関するガイダンスを提供するISO/IEC 27035:2022の条項6.8にも関連しています。

* ステップ8＝インシデントのクローズ: このステップでは、インシデント、イベント、または脆弱性が満足に解決され、すべてのアクションが完了して文書化されたことを確認した後、それらをクローズします。この手順は、インシデントが正式に解決され、それ以上の対応が不要であることを確認するために重要です。この手順は、情報セキュリティインシデントと脆弱性、および講じた措置に関する証拠を収集し文書化することを組織に求めるISO/IEC 27001:2022の管理策A.16.1.8に関連しています。また、この手順は、インシデント、イベント、および脆弱性を解決する方法に関するガイダンスを提供するISO/IEC 27035:2022の条項6.9にも関連しています。

参考文献：

* ISO/IEC 27001:2022、情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項1

* PECB候補者ハンドブック ISO/IEC 27001主任審査員2

* ISO 27001:2022 主任審査員 - PECB3

* ISO 27001:2022認定ISMS主任監査員 - Jisc4

* ISO/IEC 27001:2022 主任審査員移行研修コース5

* ISO 27001 - 情報セキュリティ主任監査員コース - PwCトレーニングアカデミー6

* ISO/IEC 27035:2022、情報技術－セキュリティ技術－情報セキュリティインシデント管理

最新問題: 237

シナリオ9 :Techmanicは1995年に設立されたベルギーの企業で、現在はブリュッセルに拠点を置いています。同社はITコンサルティング、ソフトウェア設計、ハードウェアおよびソフトウェアサービス（導入保守を含む）を提供しています。サービス対象分野は、公共サービス、金融、通信、エネルギー、医療、教育など多岐にわたります。顧客中心主義を掲げるTechmanicは、顧客との強固な関係構築を重視し、最先端のセキュリティ対策の導入に尽力しています。

Techmanic は ISO/IEC 27001 認証を取得してから 1 年が経過し、この認証を誇りに思っていました。認証監査中に、監査員は同社の情報セキュリティ管理システム (ISMS) の実装にいくつかの矛盾を発見しました。特定された問題は ISMS が意図した結果を達成する能力に影響を与えなかったため、監査員がリモートで根本原因分析と是正措置を実施した後、Techmanic は認証を取得しました。同年、同社はサービス一覧にホスティングサービスを追加し、この分野をカバーするように認証範囲を拡大するよう申請しました。監査を担当した監査員は申請を承認し、監視監査中に拡張監査を実施することを Techmanic に通知しました。Techmanic は、ISMS の継続的な有効性と ISO/IEC 27001 への準拠を確認するために監視監査を受けました。監視監査の目的は、最近追加されたホスティングサービスを含む Techmanic のセキュリティ対策が、認証の厳格な要件にシームレスに整合していることを確認することでした。監査担当者は、特にITコンサルティング分野において、再認証プロセス中に前回の監視監査報告書の調査結果を戦略的に活用し、追加の再認証監査を回避することを目指しました。これは、継続的な改善の価値と、過去の評価から学ぶ能力を示すものです。

Techmanicは、過去の監査報告書をレビューする取り組みを実施しています。この積極的なアプローチは、潜在的な不適合事項の特定と解決に役立つだけでなく、ITコンサルティング業界における再認証プロセスの効率化も目指しています。

監視監査において、いくつかの不適合事項が確認されました。情報セキュリティマネジメントシステム (ISMS)は、引き続きISO/IEC規格に準拠しています。

TechmanicはISO/IEC 27001*規格の要件を満たしていましたが、内部監査員は、同社がマネージドサービスに関連する不適合を解決できていないと報告しました。さらに、内部監査報告書にはいくつかの矛盾点があり、マネージドサービス監査プロセスにおける内部監査員の独立性について疑問が生じました。このため、Techmanicは拡張認証を取得できませんでした。そこで、同社は別の認証機関に申請しました。同時に、同社は顧客に対し、ISO/IEC 27001認証はITサービスとマネージドサービスの両方を対象としているとの声明を発表しました。

上記のシナリオに基づいて、以下の質問に教えてください。

質問：

監査担当者は、是正措置を遠隔で監視した後、Techmanic社が認証を取得することを推奨しました。これは妥当でしょうか？

A. はい、軽微な不適合がいくつか見つかったため、監査員はリモートで是正計画のフォローアップを行うことができます。

B. いいえ、監査報告書に不適合事項が含まれているため、フォローアップ監査を実施する必要があります。

C. いいえ、延長が申請されているため、現地監査のフォローアップ作業を実施する必要があります。

Answer: A ([メッセージを残す](#))

包括的かつ詳細な解説：

* A. 正解:

* 軽微な不適合については、監査員が是正措置を確認できる限り、遠隔でのフォローアップも許容されます。

* ISO/IEC 17021-1:2015では、是正措置の有効性が実証できる場合に、遠隔でのフォローアップが認められています。

* B. 不正解:

* フォローアップは必須ですが、軽微な問題の場合はリモート検証でも構いません。

* C. 不正解:

重大な不適合がない限り、現地でのフォローアップは必須ではありません。

関連規格参照：

* ISO/IEC 17021-1:2015 9.6.8項（リモート監査フォローアップ）

最新問題: **238**

次のうち、第2段階監査の目的を最もよく表しているのはどれですか？

A. 組織が法律を遵守しているかどうかを確認してください。

B. 監査計画が実施されていることを確認する。

C. 管理システムの実施状況を評価する

D. 組織のプロセスを理解する

Answer: C ([メッセージを残す](#))

ステージ2監査の目的は、ISO/IEC 27001:2022の要求事項および組織独自のポリシーと手順に従って、マネジメントシステム（この場合はISMS）の実装を評価することです。ステージ2監査では、ISMSの有効性とパフォーマンスに関する証拠を収集するとともに、組織の管理策の適合性と適切性を検証します。また、ステージ2監査では、組織が情報セキュリティ目標を達成し、情報セキュリティリスクを管理する能力も評価します。参照 :ISO/IEC 27006:2022、9.2.2.2項、PECB候補者ハンドブックISO 27001主任監査員、28ページ。

最新問題: **239**

シーン8 :テス

1. マリクとマイケルは、セキュリティ、コンプライアンス、事業計画および戦略の分野における独立した資格を有する専門家で構成された監査チームです。彼らは、大手ウェブデザイン会社であるクラスタス社に対し、認証監査を実施しました。監査中、彼らは公平性と客観性を含む卓越した職業倫理を示しました。今回、クラスタス社は、ISO/IEC 27001認証を取得できれば、一歩リードできると確信しています。

監査チームリーダーのテッサは、監査に関する専門知識を有し、IT関連の問題、コンプライアンス、ガバナンスにおいて非常に優れた実績を持っています。マリクは、組織計画とリスク管理のバックグラウンドを持ち、組織のセキュリティ管理とリスク許容度に対する包括的かつ分析的なアプローチに基づき、組織内のリスクレベルを正確に把握することに長けています。一方、マイケルは、厳格な標準化された手順に従って実施される管理評価を通じて、実践的なセキュリティに関する専門知識を有しています。

必要な監査活動を実施した後、テッサは監査チーム会議を開始し、そこでマイケルの発見事項の1つを分析して、その問題について客観的かつ正確な決定を下しました。マイケルが遭遇した問題は、組織の日常業務における些細な問題であり、彼はそれがIT技術者によって引き起こされたと考えていました。そこで、テッサは上級管理職と面談し、責任者の名前を尋ねた後、誰が責任を負うべきかを伝えました。明確化と理解を促進するため、テッサは監査最終日に最終会議を招集しました。この会議で、彼女は発見された不適合をクラスタスの経営陣に報告しました。しかし、テッサはクラスタスの認証監査報告書に不必要な証拠を記載しないように助言され、報告書が簡潔で主要な発見事項に焦点を当てたものになるようにしました。

監査チームは、検討した証拠に基づき監査結論案を作成し、認定を与える前に組織の2つの分野を監査する必要があると判断した。これらの決定は後に被監査組織に提出されたが、被監査組織は調査結果を受け入れず、追加情報を要求した。被監査組織の意見にもかかわらず、監査人は既に認定勧告を受け入れることを決定していたため、追加情報は受け入れなかった。被監査組織の上級管理職は、監査結論は事実を反映していないと主張したが、監査チームは決定を維持した。

上記のシナリオに基づいて、以下の質問に答えてください。

最終会議で指摘された法令違反点に関して、テッサは何をすべきでしょうか？

A. 各不適合について、組織への潜在的な影響を含め、詳細な分析を提供してください。

B. 重大な不適合項目のみ

C. 議論は常に、関連する標準条項と整合させてください。

Answer: A ([メッセージを残す](#))

包括的かつ詳細な徹底分析

A. 正解：

ISO 19011:2018では、監査員はすべての不適合事項について、適切な理解と是正措置計画の策定を確実にするために、十分な詳細と背景情報を提供しなければならないと規定している。

不適合事項を十分に説明しないと、効果的な是正措置が講じられない可能性がある。

B. 不正解：

透明性を確保するため、軽微な不適合事項も提示しなければならない。

C. 不正解：

標準条項に準拠することは必要だが、詳細な分析の方がより重要である。

関連規格参照：

ISO 19011:2018 6.6.2項（最終会議における監査結果の提示）

最新問題: **240**

質問

ISO/IEC 27001認証監査において、監査チームリーダーは確立された監査のベストプラクティスに従わなかった。さらに、情報セキュリティマネジメントシステム (ISMS)の複雑な領域を評価するために必要な専門知識が不足していたため、監査結果は不十分であった。監査報告書は提出されたものの、監査の一部に不備が見られ、規定の手順に完全に準拠していなかった。

不法行為訴訟において、このような状況はどの程度の法的責任に相当するのでしょうか？

A. 全般的な損失

B. 重大な過失

C. 故障なし

Answer: ([解答を表示する](#)**)**

このシナリオは通常の過失に該当するため、選択肢Aが正解となります。通常の過失とは、個人が同様の状況下で合理的に期待される注意、能力、または勤勉さを発揮しなかった場合に発生します。ISO/IEC 27001認証監査においては、たとえ危害を加える意図がなかったとしても、確立された監査手順、ベストプラクティス、または能力要件に従わなかった場合が含まれます。

このシナリオでは、監査チームリーダーが確立されたベストプラクティスに従わず、特定の複雑なISMS分野に関する十分な専門知識を欠いていました。これらの欠点により、監査範囲が不十分となり、最適な結果が得られませんでした。しかし、監査は実施され、調査結果も報告されており、無謀な無視、故意の不正行為、または意図的な義務違反の兆候はありません。この区別は、過失の重大性を評価する際に重要です。

重大な過失とは、義務付けられた監査要件を故意に無視したり、能力を欠いたまま意図的に監査を実施したり、結果に対して無謀な無関心を示したりといった、認められた基準からの重大な逸脱を示す証拠を必要とする。本件では、その基準は満たされていない。同様に、手続き上の不備や能力不足の存在は明らかに何らかの過失を示しているため、選択肢Cも誤りである。

ISO 19011:2018は、監査員の能力、適切な職業上の注意、および監査原則の遵守を重視している。

これらの期待に応えられなかったことは過失に当たるが、この場合は重大な過失ではなく、通常の過失の範囲内にとどまる。

最新問題: 241

予備認証監査の第1段階を完了し、第2段階の準備を進めた後、被監査組織は監査チームリーダーに対し、組織が最近取得した2つの拠点を監査対象に含めたい旨を通知した。

この情報を踏まえて、監査チームリーダーにはどのような行動を取ることを期待しますか？

- A. 両拠点でリモートレビューの第一段階を完了するために、ビデオ会議プラットフォームを使用するよう手配してください。
- B. フェーズ2レビューの期間を延長し、追加のサイトを含める。
- C. 被監査部門の監査チームリーダーに通知し、要求を受け入れるよう指示する。
- D. レビュープログラムを管理する担当者に通知するために、他のサイトに関する情報を入手する。

Answer: (解答を表示する)

ISO/IEC 27001 主任監査員のための PECB 候補者ハンドブックによると、監査チームリーダーは、監査の目的、範囲、基準、期間、リソース、およびリスクに影響を与える可能性があるため、監査プログラムを管理する担当者に知らせるために、追加のサイトに関する情報を入手する必要があります。監査チームリーダーはまた、監査計画を見直し、被監査者および監査クライアントと協議して必要な調整を行う必要があります 1。参照: 1: ISO/IEC 27001 主任監査員のための PECB 候補者ハンドブック、27 ページ、セクション 4.3.2.2。

有効な **ISO-IEC-27001-Lead-Auditor-CN** 問題集は GoShiken.com が提供された合格しやすい ISO-IEC-27001-Lead-Auditor-CN 試験問題集！ GoShiken.com が最新の **ISO-IEC-27001-Lead-Auditor-CN** 試験問題集を提供しています。GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 問題集をゲットする人はこちら:
<https://www.goshiken.com/PECB/ISO-IEC-27001-Lead-Auditor-CN-mondaishu.html> (41830%OFF問題集溶と正解付きで 30%w特別割引コード: **Freepdfdumps**)

最新問題: 242

シナリオ3 :NightCoreは、電子商取引、クラウドコンピューティング、デジタルストリーミングメディア、人工知能を専門とする米国拠点の多国籍テクノロジー企業です。情報セキュリティマネジメントシステム (ISMS)を導入してから8か月以上が経過した時点で、ISO/IEC 27001認証を取得するために、第三者監査を行う認証機関を雇いました。

認証機関は7名の監査員からなるチームを編成した。その中で最も経験豊富なジャックが監査チームリーダーに任命された。彼は長年にわたり、ISO/IEC 27001主任監査員、CISA、CISSP、CISMなど、数々の権威ある資格を取得している。

ジャックは、NightCoreが実施しているすべての情報セキュリティ要件と管理策を調査 評価することで、ISMS監査の各段階について包括的な分析を実施しました。監査の第2段階で、ジャックはいくつかの不適合項目を発見しました。購入したソフトウェアライセンスの請求書の数とソフトウェアの在庫を比較した結果、会社のコンピュータの多くが違法バージョンのソフトウェアを使用していたことが判明しました。彼は、この違反について経営陣に説明を求め、彼らがこの違反を認識していたかどうかを確認することにしました。次のステップとして、NightCoreのIT部門を監査することにしました。経営陣は、NightCoreのシステム管理者であるトムをジャックと監査チームのメンターに任命し、システムとデジタル資産インフラストラクチャの内部構造を理解できるように支援しました。

監査担当者は財務部門の担当者への聞き取り調査の中で、同社が最近、あるコンサルタント会社と異常に高額な取引を行っていたことを発見した。取引に関する必要な詳細情報をすべて収集した後、ジャックは上級幹部に直接聞き取り調査を行うことにした。

最初のコンプライアンス違反に関する話し合いの中で、経営陣はジャックに対し、ソフトウェアのコピーの方が安価であるため、オリジナル版の代わりにコピー版を使用しても構わないと伝えた。ジャックはナイトコアの経営陣に対し、違法なバージョンのソフトウェアを使用することはISO/IEC 27001規格および国内法規に違反すると説明した。しかし、経営陣はこれに納得したようだった。

監査から数か月後、ジャックは監査中に収集したナイトコアに関する情報の一部を、ナイトコアの競合他社に多額の金銭で売却した。

このシナリオに基づいて、以下の質問に答えてください。

ISO/IEC 27001は、組織が国内の法律や規制を遵守することを義務付けていますか？

- A. はい、ただし、関連する法的要件や契約上の要件を具体的に示す必要はありません。
- B. いいえ、この基準では、組織が国の法律や規制を遵守すべきかどうかは明示的に規定されていません。
- C. はい、適用法規の遵守はISO/IEC 27001の要件です。

Answer: ([解答を表示する](#))

ISO/IEC 27001では、組織は情報セキュリティに関するものを含め、適用される法律、法令、規制、および契約上の要件を遵守することが求められています。これらの要件は、組織のISMSの一部として特定、文書化され、常に最新の状態に維持されなければなりません。

参照 :ISO/IEC 27001:2013規格、6.1.3項（情報セキュリティ要求事項）

最新問題: **243**

シナリオ4 :SendPayは、代理店や金融機関のネットワークを通じてサービスを提供する金融会社です。主なサービスの1つは、国際送金です。新会社であるSendPayは、顧客に最高品質のサービスを提供することに尽力しています。同社は国際取引を取り扱うため、顧客には身元情報、取引の理由、取引を完了するために必要なその他の詳細情報などの個人情報を提供する必要があります。そのため、SendPayは、潜在的な情報セキュリティの脅威を検出、調査、対応することを含め、顧客情報を保護するためのセキュリティ対策を実施しています。安全なサービスを提供するという同社の取り組みは、ISMSの導入にも反映されており、同社はこれに多大な時間とリソースを投資しています。

昨年、SendPayはスマートフォンやノートパソコンなどの電子機器を介して追加料金なしで通貨取引ができるデジタルプラットフォームを立ち上げました。このプラットフォームを通じて、SendPayの顧客はいつでもどこでも資金を送受信できます。このデジタルプラットフォームは、SendPayの業務効率化と事業拡大に貢献しました。当時、SendPayはソフトウェア事業を外部委託していたため、このプロジェクトは外部委託会社のソフトウェア開発チームによって完成されました。

同チームはSendPayの技術インフラの維持管理も担当している。

最近、同社は情報セキュリティマネジメントシステム（ISMS）を導入してから約1年後、ISO/IEC 27001認証の申請を行った。同社は、その基準を満たす認証機関と契約を締結した。その後まもなく、認証機関はSendPayのISMSを監査するために4名の監査員からなるチームを任命した。

監査中に、以下の状況が発見されました。

1. 外部委託していたソフトウェア会社が、SendPayとの契約を事前の通知なしに解除しました。その結果、SendPayは社内でサービスを直ちに復旧することができず、5日間の業務中断が発生しました。監査担当者は、SendPayの担当者に対し、契約解除が発生した場合の対応計画を示す証拠を求めました。担当者は書面による証拠は提出しませんでした。監査中に、SendPayの経営陣が、同様の事態が再び発生した場合にすぐにサービスを提供できる他の2つのソフトウェア開発会社を特定したと監査担当者に伝えました。
2. ソフトウェア開発会社に委託された業務が監視されていたという証拠はなかった。SendPayの担当者は監査人に対し、ソフトウェア開発会社とは定期的に連絡を取り合い、潜在的な変更があれば適切に通知していたと改めて説明した。
3. ファイアウォールのテスト中に異常は発見されませんでした。監査担当者は、ファイアウォールの構成をテストして、これらのサービスが提供するセキュリティレベルを判断しました。パケットアナライザーを使用してファイアウォールポリシーをテストし、送受信パケットをリアルタイムで検査しました。

このシナリオに基づいて、以下の質問に教えてください。

3つ目の事例として、監査担当者がSendPayネットワークに実装されているファイアウォールの設定を自らテストしたケースがあります。この事例をどのように説明しますか？シナリオ4を参照してください。

- A.** 許容範囲内ですが、技術的プロセスの動作を検証するための技術的証拠が必要です。
- B.** 不適切。監査員はシステムまたは機器構成のテストを観察するだけでよく、システム自体をテストしてはならない。
- C.** 不合格。ファイアウォールの設定は、システムの動作に影響を与える可能性があるため、監査期間中はテストすべきではありません。

Answer: ([解答を表示する](#))

ISMS監査において、監査担当者がファイアウォールなどの技術的制御をテストし、これらのプロセスの運用状況と有効性を検証することは、許容されるだけでなく、多くの場合必要不可欠です。このような実践的なテストは、セキュリティ対策の有効性を示す具体的かつ技術的な証拠となります。

参照 :ISO/IEC 27001:2013規格、A.13項（通信セキュリティ）、ISO 19011:2018、マネジメントシステムの監査に関するガイドライン

最新問題: **244**

組織は、アプリケーションが自動更新される際に、更新版のソースコードをチェックしないことが多い。そのため、アプリケーションが不正な改変を受ける可能性がある。これは、メッセージ配信に影響を与える可能性のある潜在的な脆弱性となる。

A. 脅威、2) 機密保持

B. リスク、2) 可用性

C. 脆弱性、2) 完全性

Answer: C (メッセージを残す)

脆弱性とは、情報システム、システムセキュリティ手順、内部統制、または実装における弱点であり、脅威の発生源によって悪用される可能性があるものです。この場合、更新されたアプリケーションのソースコードをチェックしないと、不正な変更につながる可能性があり、情報の完全性に影響を与える可能性のある脆弱性となります。ここでいう完全性とは、情報の正確性と完全性を指します。

参考文献: = この説明は、情報セキュリティ管理システムの一般原則およびISMS ISO/IEC 27001主任監査員のトレーニングおよび認証プログラムで通常扱われる内容と一致しており、脆弱性とその情報セキュリティ属性（完全性など）への影響の理解が含まれます。

最新問題: 245

將正確的責任與第二方審核的每位參與者配對：

Match the correct responsibility with each participant of a second-party audit:

Responsibility	Audit Participant
Prepares the audit report	
Prepares audit checklists for use during the audit	
Supports an auditor and provides feedback on their experience	
Follows-up on audit findings within an agreed timeframe	
Provides an independent account of the audit but does not participate in the audit	
Escorts the auditors but does not participate in the audit	

To complete the table click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop each option to the appropriate blank section.

Audit Team Leader

Auditor in training

Auditor

Auditee

Guide

Observer

Answer:

Match the correct responsibility with each participant of a second-party audit:

Responsibility	Audit Participant
Prepares the audit report	Audit Team Leader
Prepares audit checklists for use during the audit	Auditor
Supports an auditor and provides feedback on their experience	Auditor in training
Follows-up on audit findings within an agreed timeframe	Auditee
Provides an independent account of the audit but does not participate in the audit	Observer
Escorts the auditors but does not participate in the audit	Guide

To complete the table click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop each option to the appropriate blank section.

Audit Team Leader

Auditor in training

Auditor

Auditee

Guide

Observer

Responsibility	Audit Participant
Prepares the audit report	Audit Team Leader
Prepares audit checklists for use during the audit	Auditor
Supports an auditor and provides feedback on their experience	Auditor in training
Follows-up on audit findings within an agreed timeframe	Auditee
Provides an independent account of the audit but does not participate in the audit	Observer
Escorts the auditors but does not participate in the audit	Guide

最新問題: 246

あるマーケティング代理店が、情報セキュリティマネジメントシステム（ISMS）の導入の一環として、リスク評価手法を開発しました。これは許容範囲内でしょうか？

- A. はい、ISO/IEC 27001に準拠したリスク評価方法であればどれでも使用できます。
- B. はい、ただし、リスク評価方法が一般的に認められているリスク評価方法と一致している場合に限りです。
- C. いいえ、ISMSを導入するには、ISO/IEC 27001で規定されているリスク評価方法を使用する必要があります。

Answer: [\(解答を表示する\)](#)

包括的かつ詳細な徹底分析

ISO/IEC 27001は、特定のリスク評価方法を規定するのではなく、リスク評価に関する一般的な要件を定めています。組織は、以下の条件を満たす限り、独自のリスク評価方法を開発することができます。

情報セキュリティに対するリスクと影響を特定する。

リスクを評価するためのリスク基準を定義する。

組織の状況に基づいて、リスク対策計画を実施する。

A. 正解：

ISO/IEC 27001の6.1.2項（情報セキュリティリスク評価）では、組織は独自のリスク評価方法を定義できると規定されている。

このアプローチは、体系的で、測定可能であり、事業目標と整合していなければならない。

B. 不正解：

組織は、そのアプローチがISOの要件を満たしている限り、OCTAVE、MEHARI、EBIOSなどの認知された方法論を使用する必要はありません。

C. 不正解：

ISO/IEC 27001は、特定のリスク評価方法を義務付けているわけではなく、一貫性のある体系的なアプローチを用いることのみを求めている。

関連規格参照：

ISO/IEC 27001:2022 6.1.2項（情報セキュリティリスク評価プロセス）

最新問題: **247**

定性的証拠と定量的証拠の主な違いは何ですか？

A. 定性的証拠は監査基準を決定するために関連のあるサンプル分析から得られるのに対し、定量的証拠は定量化できない情報の分析から得られる。

B. 定性的証拠は、プロセスや統制が監査基準を満たしているかどうかを評価することに焦点を当てており、定量的証拠は、業務プロセスが完全に機能し、効果的であるかどうかを判断することを目的としています。

C. 定性的証拠は母集団全体を推定するために使用され、定量的証拠は特定のプロセスが要求される基準を満たしているかどうかを評価することに焦点を当てています。

Answer: B ([メッセージを残す](#))

包括的かつ詳細な徹底分析

B. 正解：

定性的証拠は、記述的データ、観察データ、およびインタビューに基づくデータに基づいて、プロセスが監査基準に準拠しているかどうかを評価する。

定量的証拠とは、数値データ（例えば、指標、統計、または業績指標）を用いて、プロセスが機能的かつ効果的であるかどうかを評価する手法である。

A. 不正解：

定性的証拠はサンプリングに限定されず、定量的証拠は測定可能なデータに基づいている。

C. 不正解：

定性的な証拠は人口を推定するものではなく、主観的かつ記述的なものである。

関連規格参照：

ISO 19011:2018 6.4.7項（監査証拠の種類：定性的証拠と定量的証拠）

最新問題: **248**

シナリオ 1: Fintive は、オンライン決済およびセキュリティ保護ソリューションの大手プロバイダーです。1999 年にカリフォルニア州サンノゼでトーマス・フィンによって設立された Fintive は、情報セキュリティの向上、不正行為の防止、および PII (個人情報注入) などのユーザー情報の保護を希望するオンライン企業にサービスを提供しています。Fintive の意思決定および運用プロセスは、過去の事例に基づいています。顧客データを収集し、分類し、分析します。このような複雑な分析を実行するには、大規模な人員が必要でした。しかし、長年にわたり、このような分析を容易にする技術も進歩してきました。現在、Fintive はチャットボットなどの最新ツールを使用してパターン分析を実行し、不正行為を即座に防止することを計画しています。このツールは、顧客サービスの向上にも役立ちます。

この最初のアイデアはソフトウェア開発チームに伝えられ、彼らはそれを支持してプロジェクトを担当することになった。彼らはチャットボットを既存のシステムに統合する作業を開始した。さらに、チームはチャットボットがチャットの問い合わせの85%に回答するという目標を設定した。

チャットボットの統合が成功すると、同社は直ちに顧客向けにリリースした。

しかし、チャットボットにはいくつか問題があるようだ。

トレーニング段階 チャットボットがクエリパターンを 学習」する段階)において、テストが不十分であったり、サンプルデータが不足していたりするため、チャットボットはユーザーのクエリを解決して正しい回答を提供することができません。さらに、チャットボットが無効な入力（奇妙なドットパターンや通常とは異なる文字など）を受け取ると、ランダムなファイルをユーザーに送信してしまいます。そのため、チャットボットは顧客のクエリに適切に対応できず、従来のカスタマーサポートはチャットによる問い合わせで手一杯になり、顧客の要望を解決することができなくなっています。

そのため、Fintiveはソフトウェア開発ポリシーを策定しました。このポリシーでは、ソフトウェアが社内で開発されたか外部委託されたかにかかわらず、オペレーティングシステムに実装する前にブラックボックステストを実施することを規定しています。

このシナリオに基づいて、以下の質問に答えてください。

チャットボットは、ユーザーの問い合わせを解決し、正しい回答を提供するために、問い合わせパターンを 学習」する必要がある。

どのような種類の技術がこれを実現できるのか？

- これ？
- A. 人工知能
 - B. クラウドコンピューティング
 - C. 機械学習

Answer: (解答を表示する)

機械学習は人工知能の一分野であり、アルゴリズムと統計モデルを用いて、明示的なプログラミングなしに、経験やデータに基づいてシステムが特定のタスクにおけるパフォーマンスを時間とともに向上させることを可能にする技術です。このシナリオにおいては、機械学習はチャットボットがクエリのパターンから学習し、適切な回答を提供することを可能にする技術となります。

最新問題: 249

あなたは経験豊富なISMS監査員で、ICTリサイクルサービスを提供する組織の第三者監査を担当しています。この組織は、会社が不要になったICT機器を処理し、修理・再利用するか、安全に廃棄処分します。

部屋の隅にあるベンチの上に2台のサーバーが置いてあるのに気づきます。どちらにもサーバー名、IPアドレス、管理者パスワードが書かれたステッカーが貼られています。ICTマネージャーにこれらの品物について尋ねると、それらは昨日、長年の顧客から届いた荷物の一部だと教えてくれます。

あなたはどのような行動を取るべきでしょうか？

- A. 管理措置5.31 法的、規制的、コンプライアンスおよび契約上の要件」において、不遵守項目が特定されました。
- B. レビュー対象者にタグを削除してもらい、その後レビューを続けてください。
- C. 監査結果を記録し、顧客のITセキュリティに関連する入荷貨物の処理プロセスをレビューする。
- D. ICTマネージャーに情報セキュリティインシデントを記録してもらい、情報セキュリティインシデント管理プロセスを開始してください。
- E. 管理措置8.20 ネットワークセキュリティ」ネットワークおよびネットワーク機器は、システムおよびアプリケーション内の情報を保護するために保護、管理、制御されるべきである)への不遵守が発見されました。
- F. レビュー結果に表示された内容を記録し、それ以上の行動は取らない。

Answer: C (メッセージを残す)

最新問題: 250

以下の選択肢の中から、第三者監査チームの責任者が全面的に担当するオプションを選択してください。

- A. 監査チームメンバーの選定
- B. 監査チーム用のチェックリストを作成する
- C. 認証機関の代理として
- D. マネジメントシステムにおける不適合を特定する

Answer: (解答を表示する)

正確な抜粋より：

Aの説明（監査チームリーダーの単独責任）：

監査チームリーダーは、監査チームが監査を効果的に実施し、その目的を達成するために必要な能力とリソースを備えていることを最終的に保証する責任を負います。これには、監査範囲を網羅するために、個々の能力、業界経験、語学力などを考慮し、適切なチームメンバーを選定するという重要な任務が含まれます。認証機関が監査員の候補者リストを提供する場合がありますが、特定の監査における具体的な選定は、チームが目的に適していることを保証するチームリーダーの責任です。

参照：

ISO/IEC 17021-1:2015、7.3項 監査チーム」:この項では、監査チームを編成するための要件を詳述しています。具体的には、7.3.2項 監査チームの選定」には、 認証機関は、必要に応じて、監査チームリーダーおよび技術専門家を 含む監査チームを、特定の監査のために選定する」と規定されています。認証機関が 選定」するとはいえ、実際には、監査チームリーダーが監査のニーズに基づいてチームメンバーを選定する権限を委任されるか、あるいは直接責任を負い、認証機関が正式に承認することがよくあります。チームリーダーがチーム構成に直接関与することは、監査の有効性にとって非常に重要です。これは、チームリーダーの意見や承認なしに、個々のチームメンバーや認証機関内の管理職に完全に委任することはできない業務です。

B（単独責任ではない）の説明：

監査チームリーダーは監査チェックリストのレビュー、指導、承認を行うのは当然ですが、詳細なチェックリストの作成は、チーム内の有能な監査員であれば誰でも、あるいは認証機関の中央部門が行うことも可能です。これはチームリーダーだけの専任業務ではありません。

参照：

ISO 19011:2018（マネジメントシステムの監査に関する指針）6.4.3項 監査のための文書化された情報の準備」:この項では、監査チームはチェックリストなどの文書化された情報を監査のために準備する必要があると述べています。これは監査チームリーダーのみの責任であるとは明記されていません。

C（単独責任ではない）の説明：

監査チームリーダーは監査中、主要な権限と責任を負い、認証機関の代表者としての役割を担いますが、監査チームのメンバー全員が認証機関の専門性、倫理、および手続きを遵守することが求められます。したがって、 認証機関を代表して行動する」ことは、最終的な責任はリーダーが負うものの、監査チーム全体の共同責任となります。

参照：

ISO/IEC 17021-1:2015、第4項 原則」：認証活動に関わるすべての担当者に適用される、公平性、能力、責任などの原則を概説しています。

ISO 19011:2018、第5項 監査の原則」：倫理的行動 適切な職業上の注意、独立性などの原則は、すべての監査員に適用されます。

D（単独責任ではない）の説明：

不適合を特定することは、チームのすべての監査員の基本的な責任です。各監査員は、担当区域における文書化された情報の確認、インタビューの実施、プロセスの観察を通して、監査基準に照らして不適合を特定し、報告することが求められます。その後、チームリーダーがこれらの不適合をレビュー、統合し、適切な分類と文書化を確実に実施しますが、不適合を特定するのはチームリーダーだけではありません。

参照：

ISO 19011:2018、6.4.8項 監査活動の実施」には、 適合および不適合の証拠を収集する必要がある」と記載されています。これはすべての監査員が実施する活動です。

ISO 19011:2018、6.4.9項 監査情報の識別と記録」： 監査結果、

記録しなければならない。」これはすべての監査人に適用されます。

最新問題: 251

シナリオ7 :Webvue。日本に本社を置くWebvueは、コンピュータソフトウェアの開発、サポート、保守を専門とするテクノロジー企業です。Webvueは、様々なテクノロジーおよびビジネス分野にわたるソリューションを提供しています。同社の主力サービスは、ストレージ、ネットワーク、仮想コンピューティングサービスを提供する包括的なクラウドコンピューティングプラットフォームであるCloudWebvueです。企業ユーザーと個人ユーザーの両方に対応するように設計されたCloudWebvueは、その柔軟性、拡張性、信頼性で高い評価を得ています。

Webvue は ISO/IEC 27001 認証範囲に CloudWebvue のみを含めることを決定しました。そのため、フェーズ 1 とフェーズ 2 の監査が同時に実施されました。Webvue は、CloudWebvue に保存されている情報を保護するために適切な暗号化制御を使用するなど、厳格な資産の機密性を誇りにしています。機密レベルや内部使用かどうかに関わらず、すべての情報は、クラウドに保存される前に、対応する固有のハッシュ値で最初に暗号化されます。Sean、Lyra、Sam、Tin a. Keith は、IT および情報セキュリティ監査チームで最も経験豊富な監査員であり、監査チームを率いています。彼の責任には、監査チームの計画と管理が含まれます。この慣行はまだ開発中でした。Webvue の暗号化ポリシーをレビューした後、インタビュー中に得られた情報は本物であると結論付けました。ただし、ポリシーでは暗号化キーの使用と有効期間について規定されていなかったため、暗号化キーはまだ使用されていました。

Webvueと認証機関の間でその後締結された合意に基づき、監査チームは仮想監査を選択し、認証範囲と監査目標を満たすためにWebvueがISO/IEC 27001管理基準8.11「データマスキング」に準拠していることを検証することに特化しました。監査チームはCloudWebvue内のデータ保護に関わるプロセスを検証し、同社がポリシーと規制基準をどのように遵守しているかに焦点を当てました。このプロセスの一環として、監査チームリーダーのキースは、Webvueの慣行の有効性を文書化および分析するために、関連文書と暗号化キー管理手順のスクリーンショットを撮影しました。

Webvueはテスト目的で生成されたテストデータを使用しています。しかし、QA部門マネージャーへのインタビューと同部門の手順に基づき、リアルタイムのシステムデータが使用される場合があることが判明しました。このような場合、大量のデータが生成され、より正確な結果が得られます。テストデータは保護および管理されており、これは監査中にWebvueの担当者が行った暗号化プロセスのシミュレーションによって検証されました。監査の範囲外ではありますが、セキュリティトレーニング部門のコンプライアンス違反は、監査範囲内のプロセス、特にCloudWebvue内のデータセキュリティと暗号化の実践に影響を与える可能性があります。そのため、Keithはこの調査結果を監査レポートに含め、被監査者に通知しました。

上記のシナリオに基づいて、以下の質問に教えてください。

シナリオ7によると、テストデータの使用が要件を満たしているかどうかを確認するために、どの監査手順が使用されますか？

A. 記録情報の確認

B. 確認

C. 技術検証

Answer: C (メッセージを残す)

包括的かつ詳細な徹底分析

C. 正解：

技術検証とは、制御装置を直接テストまたはシミュレーションすることである。

Webvueの担当者が暗号化プロセスをシミュレーションし、テストデータのセキュリティ対策を確認した。

A. 不正解：

文書レビューは受動的なプロセスであるのに対し、技術検証は能動的であり、リアルタイムの評価を含む。

B. 不正解：

裏付けとは情報の相互確認のことであり、技術的検証とは実際の運用における管理体制のテストである。

関連規格参照：

最新問題: 252

三元系成分を結合させている接着剤はどれですか？

A. 旅程

B. 人物

C. コラボレーション

D. テクノロジー

Answer: D (メッセージを残す)

トライアドとは、情報セキュリティの3つの要素、すなわち機密性、完全性、可用性を指します3。テクノロジーは、このトライアドを結びつける接着剤のようなものであり、不正アクセス、改ざん、損失から情報を保護するための様々な制御と対策を実施する手段を提供します3。参考文献 :ISO

/IEC 27001:2022 主任審査員研修コース - BSI

最新問題: 253

情境 5 :Data Grid Inc. 是一家知名公司，為整個資訊科技基礎設施提供安全服務。它提供網路安全軟體，包括端點安全、防火牆和防毒軟體。二十年來，Data Grid Inc. 透過先進的口品和服務幫助多家公司保護其網路安全。Data Grid Inc. 在資訊和網路安全領域享有盛譽，決定獲得ISO/IEC 27001 認證，以更好地保護其口部和客口資口並獲得競爭優勢。

Data Grid Inc. 任命了審計團隊，該團隊同意審計任務的條款。此外，Data Grid Inc.明確了審核範圍，明確了審核標準，並建議在五天口結束審核。由於Data Grid Inc.員工人數眾多，流程複雜，審計小組拒口Data Grid Inc.在五天口進行審計的提議。Data Grid Inc.堅稱他們計劃在五天口完成審核，因此雙方同意在規定的時間口進行審核。審計小組遵循基於風險的審計方法。

為了獲得主要業務流程和控制的概述， 審計團隊存取了流程描述和組織圖表。他們無法對 IT 風險和控制進行更深入的分析， 因為他們對IT 基礎架構和應用程式的存取受到限制。然而， 審計小組表示，Data Grid Inc. 的 ISMS 出現重大缺陷的風險很低， 因為該公司的大部分流程都是自動化的。因此， 他們透過詢問Data Grid Inc. 的代表以下問題來評估 ISMS 整體上符合標準要求：

*如何定義和指派 IT 和 IT 控制的職責？

*Data Grid Inc. 如何評估控制措施是否達到了預期效果？

*Data Grid Inc. 採取了哪些控制措施來保護操作環境和資料免受惡意軟體的侵害？

*是否實施了與防火牆相關的控制？

Data Grid Inc. 的代表提供了充分且適當的證據來解決所有這些問題。

審計組長起草審計結論並向Data Grid Inc. 的最高管理階層報告。

儘管審核員推薦Data Grid Inc.進行認證， 但Data Grid Inc.與認證機構之間在審核目標方面口生了誤解。Data Grid Inc. 表示， 儘管審計目標包括確定潛在改進的領域， 但審計團隊並未提供此類資訊。

根據該場景， 回答以下問題：

如何避免認證機構和 Data Grid Inc. 之間口生誤解？

請參閱場景 5。

A. 驗證審核報價

B. 簽署認證協議

C. 定義審核計劃

Answer: ([解答を表示する](#))

Signing the certification agreement, which should clearly outline the audit objectives, scope, and responsibilities, would help prevent misunderstandings between the certification body and Data Grid Inc. A well-defined agreement ensures both parties have a clear understanding of what the audit will entail and what outputs are expected.

References: ISO/IEC 27006:2015, Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems

最新問題: **254**

あなたは、医療サービスを提供する高齢者向け介護施設で、ISMS（情報セキュリティマネジメントシステム）の初回認証監査を実施しています。監査計画の次のステップは、最終会議を開催することです。最終監査チーム会議において、監査チームリーダーとして、あなたは以下のとおり、2件の軽微な不適合と1件の改善機会を報告することに同意しました。

Cosmic Certifications Limited				
Summary of audit findings:				
Opportunities for Improvement (OI)				
Item	Findings		Requirements	Follow-up
1.	The organisation should improve the overall awareness of information security incident management responsibility and process.		Clause 7.4 and Control A.5.24	N/A
Nonconformities (NCs)				
Item	Findings	Grade	Requirements	Follow-up
1.	During the audit on the outsourced process, sampling one of the outsourced service contracts with WeCare the medical device manufacturer found that ABC does not include personal data protection and legal compliance as part of the information security requirements in the contract.	Minor	Clause 4.2 and Control A.5.20	Corrective actions are required.
2.	During the audit on information security during the business continuity process, sampling one of the service continuity and recovery plans for the resident's healthy status monitoring service. The auditor found the recovery plan has not yet been tested.	Minor	Clause 8.1 and Control A.5.29	Corrective actions are required.
signed by Audit				
Team Leader				

最終会議で被監査者に提示する、監査プロジェクトマネージャーの提案オプションを選択してください。

- A. 提案された是正措置計画を承認した後、認証を受けることをお勧めします。
- B. 6ヶ月以内に包括的な見直しを行うことをお勧めします。
- C. 3ヶ月以内に部分的な見直しを行うことをお勧めします。
- D. 調査結果は、監視監査から1年以内に結論を出すことが推奨されます。

Answer: (解答を表示する)

*軽微な不適合：特定された不適合は軽微なものであり、情報セキュリティマネジメントシステム (ISMS)に重大なリスクをもたらすものではありません。集中的な是正措置により容易に修正できると考えられます。

*改善の機会：これは不適合ではなく、ISMSを強化するための提案です。直ちに是正措置を講じる必要はありませんが、組織の継続的改善活動の中で対処すべき事項です。

*初回認証：これは初回認証監査であるため、組織は特定された不適合事項に対処する取り組み姿勢を示すことが求められます。部分監査では、不適合が指摘された特定の領域に焦点を当てたフォローアップを行い、それらが適切に対処されたことを確認します。

他の選択肢が適さない理由：

*A. 提案された是正措置計画を承認した後、認証を推奨する：認証は目標ではありますが、是正措置の有効性を検証する前に認証を推奨するのは時期尚早です。

*B. 6か月以内に全面的な再監査を実施することを推奨します。これは軽微な不適合に対しては範囲が広すぎます。全面的な再監査は通常、重大な不適合またはシステム上の問題に対して実施されます。

*D. 1年後のサーベイランス監査で指摘事項を解消することを推奨する：これは不適合事項に対処するには長すぎる期間である。ISMSへの取り組みを示すためには、迅速な是正措置が必要である。

要約すると、3か月以内に部分監査を実施することを推奨することは、組織が是正措置を実施する時間を確保することと、その有効性をタイムリーに検証することとのバランスを適切にとっています。このアプローチはISO 27001の原則に合致しており、組織の認証取得に向けた取り組みを支援します。

シナリオ 5: Cobt はロンドンに拠点を置く保険会社で、幅広い商業保険、産業保険、生命保険ソリューションを提供しています。近年、Cobt の顧客基盤は大幅に拡大しています。大量のデータを処理する必要性から、同社は情報セキュリティを確保し、継続的な改善への取り組みを示すために ISO/IEC 27001 認証を取得することを決定しました。同社はすでに日常的なリスク評価の実施に熟練していましたが、情報セキュリティマネジメントシステム (ISMS) の導入により、日常業務に大きな変化が生じました。リスク評価プロセス中に、組織の内部統制が重大な欠陥を検出または防止できなかったというリスクが特定されました。同社は情報セキュリティマネジメントシステム (ISMS) 導入のための方法論に従い、わずか数か月で機能的なISMSを確立しました。ISMSの導入が成功した後、CobtはISO/IEC 27001認証を申請しました。経験豊富な監査員であるサラが監査のリーダーに任命されました。サラは監査依頼書を綿密に分析した後、監査チームのリーダーとしての責任を引き受け、すぐにCobtに関する一般的な情報の収集を開始しました。彼女は監査基準と目標を策定し、監査計画を立て、監査チームのメンバーに責任を割り当てました。サラは、Cobtが多様なビジネスおよび保険ソリューションを提供することで大幅な事業拡大を達成したものの、依然として一部のプロセスが手作業に依存していることを認識していた。そのため、彼女はまず、同社が情報セキュリティリスクをどのように管理しているかについての情報を収集することに重点を置いた。サラはCobtの担当者に連絡を取り、当初合意した監査内容の1つである、オフサイトレビューのためのリスク管理関連情報へのアクセスを要請した。しかし、Cobtは後に、そのような情報は外部から入手するには機密性が高すぎるとして拒否した。この拒否は、特に被監査企業の協力と証拠の入手可能性に関して、監査の実現可能性について懸念を引き起こした。さらに、Cobtは監査計画に疑問を呈し、同社が行った最近の変更が適切に反映されていないと述べた。同社は、監査中に実施される業務は当初の範囲にのみ適用され、監査範囲の最新の変更は網羅されていないと指摘した。サラはまた、拒否された情報が監査の目的にとって重要であることを考慮し、この状況の重大性を評価した。こうした状況において、Cobtの拒否は、監査の完全性および合理的な保証を提供できる能力について疑問を投げかけるものであった。以上のことから、サラは認証契約に署名する前に監査から撤退することを決定し、Cobtおよび認証機関にその旨を通知した。この措置は、審査原則が遵守され、透明性が維持されることを確実にするとともに、これらの原則に対する彼女の揺るぎないコミットメントを示すことを目的としている。

上記のシナリオに基づいて、以下の質問に教えてください。

- 質問：
- シナリオ5に基づき、コプト社は監査計画が監査範囲の最近の変更を正確に反映していないと指摘しています。サラはこの状況でどうすべきでしょうか？
- A. 監査範囲は監査対象となる活動の状況と重要性を反映するため、監査計画はCobtの要求に従って修正されました。
 - B. Cobtは既存の技術に最近変更があった場合にのみ監査範囲の変更を要求できるため、当初の範囲内で監査を継続してください。
 - C. 監査計画は、Cobt、Sarah、および認証機関が監査範囲の変更について合意に達した場合にのみ変更できます。

Answer: (解答を表示する)

包括的かつ詳細な解説：

- * C. 正解：監査範囲の変更は、被監査者、監査員、および認証機関の承認を得なければなりません。これにより、公平性が確保され、監査計画に関するISO 19011ガイドラインへの準拠が維持されます。
- * A. 誤り：監査スケジュールは、Cobtの要求のみで変更することはできません。承認が必要です。
- * B. 誤り：監査の範囲は技術的な変更に限らず、組織的および手続き的な変更も含まれます。

関連規格参照：

- * ISO 19011:2018 5.5.2項（監査範囲およびスケジュールの決定）

最新問題: 256

以下のうち、第1段階監査の主な目的を説明しているのはどれですか？

- A. 第2段階の準備状況を判断する。
- B. 組織が法律を遵守しているかどうかを確認する
- C. 組織の理解
- D. 監査計画を作成する

Answer: A (メッセージを残す)

ステージ1監査の主な目的は、組織のISMS文書の適切性と有効性を評価し、ISMSの導入と運用が検証されるステージ2監査に向けて組織が準備できているかどうかを判断することです。ステージ1監査では、ISMSの範囲、目的、および背景を検証するとともに、ステージ2監査の前に対応する必要のある懸念事項や不適合事項を特定します。

参考文献：

- * ISO/IEC 27001:2022 リードオーディター（情報セキュリティマネジメントシステム）の目的と内容は、Quality.orgおよびPECBによるものです。
- * ISO/IEC 27006:2015 情報技術－セキュリティ技術－情報セキュリティマネジメントシステムの監査及び認証を行う機関に対する要求事項 セクション7.3.1

有効な **ISO-IEC-27001-Lead-Auditor-CN** 問題集は GoShiken.com が提供された合格しやすい ISO-IEC-27001-Lead-Auditor-CN 試験問題集！ GoShiken.com が最新の **ISO-IEC-27001-Lead-Auditor-CN** 試験問題集を提供しています。GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 問題集をゲットする人はこちら：
<https://www.goshiken.com/PECB/ISO-IEC-27001-Lead-Auditor-CN-mondaishu.html> (418**30%OFF**問題集溶と正解付きで **30%**w特別割引コード: **Freepdfdumps**)

最新問題: **257**

あなたは、顧客向けにウェブサイトを設計する組織の第三者監査を実施する経験豊富な監査チームリーダーです。現在、その組織の適合性に関する声明書をレビューしています。

ISO/IEC 27001の要求事項によれば、適合性に関する記述について、以下の2つの記述のうち正しいものはどれですか？

- A. 組織的選択除外に関するあらゆる統制についての説明のみが必要です。
- B. 健康状態に関する声明は、組織の最高経営陣が所有し、修正します。
- C. ISO/IEC 27001への準拠を目指す組織は、適合性に関する声明書を発行する必要があります。
- D. 適合性に関する記述は、少なくとも年に一度見直さなければならない。
- E. 適合性に関する声明書に付属書Aの管理策を含めるか除外するかを理由を説明する必要があります。
- F. 適合性に関する声明は、経営陣によるレビューの際に見直されなければならない。

Answer: C,E ([メッセージを残す](#))

最新問題: **258**

あなたは、医療サービスを提供する高齢者向け介護施設で、ISMS（情報セキュリティマネジメントシステム）の初回認証監査を実施しています。監査計画の次のステップは、最終会議を開催することです。最終監査チーム会議において、監査チームリーダーとして、あなたは以下のとおり、2件の軽微な不適合と1件の改善機会を報告することに同意しました。

Cosmic Certifications Limited				
Summary of audit findings:				
Opportunities for Improvement (OI)				
Item	Findings		Requirements	Follow-up
1.	The organisation should improve the overall awareness of information security incident management responsibility and process.		Clause 7.4 and Control A.5.24	N/A
Nonconformities (NCs)				
Item	Findings	Grade	Requirements	Follow-up
1.	During the audit on the outsourced process, sampling one of the outsourced service contracts with WeCare the medical device manufacturer found that ABC does not include personal data protection and legal compliance as part of the information security requirements in the contract.	Minor	Clause 4.2 and Control A.5.20	Corrective actions are required.
2.	During the audit on information security during the business continuity process, sampling one of the service continuity and recovery plans for the resident's healthy status monitoring service. The auditor found the recovery plan has not yet been tested.	Minor	Clause 8.1 and Control A.5.29	Corrective actions are required.
signed by Audit				
Team Leader				

最終会議において、マネジメントシステム担当者（MSR）は、ABC社が今後3ヶ月以内に医療機器メーカーのWeCare社と合併することをあなたに伝えました。合併後の組織名はABC社となります。担当者は、WeCare社の医療機器製造拠点を今後の認証監査に含めることができるかどうかを尋ねました。また、WeCare社は既にISO/IEC 27001:2022認証を取得していると述べました。

MSRからの要求に適切に対応するためのオプションを選択してください。

- A. WeCareは初回審査を受けることが推奨されますが、これはABCによるその後の審査と組み合わせることも可能です。
- B. 初回監査では、認証範囲に影響を与える変更については、事前に確認しておくことをお勧めします。組織は、WeCareとの合併に関する決定を円滑に進めるため、合意された期間内に認証機関に最新情報を提供する責任があります。
- C. その提案は正しいです。WeCareが認証機関から承認を得ることができれば、新規事業者もすぐに認証対象に含めることができます。
- D. 認証プロセスを延期し、事業買収者が完了するまで待つことをお勧めします。

Answer: B (メッセージを残す)

ISO/IEC 27001のガイドラインによれば、合併など、ISMSの適用範囲に重大な変更が生じた場合は、認証機関に通知する必要があります。これにより、認証の有効性が維持され、すべての拠点とプロセスが適用範囲に含まれることが保証されます。認証機関は、新しい組織を既存の認証に組み込むための適切な措置を決定します。

参照：

* ISO/IEC 27001 主任審査員向け参考資料

シナリオ2 :ナイト社は、米国カリフォルニア州北部を拠点とする電子機器メーカーで、ビデオゲーム機を開発しています。ナイト社は世界中に300人以上の従業員を抱えています。創業5周年を機に、同社は次世代ビデオゲーム機「G-Console」をグローバル市場向けに発売することを決定しました。G-Consoleは2021年の究極のメディアコンソールと位置づけられ、プレイヤーに最高のゲーム体験を約束します。

メインユニットパッケージには、VRヘッドセット、2つのゲームやその他のギフト。

長年にわたり、同社は誠実さ、正直さ、そして顧客への敬意を通して確固たる評判を築いてきました。この評判こそが、多くの熱心なゲーマーがKnightのGコンソールを発売と同時に手に入れたいと願った理由の一つです。

ナイト社は顧客志向の企業であることに加えて、

彼らの開発品質はゲーム業界で広く認められている。しかし、価格は妥当な範囲を超えて高額である。

しかし、ナイト社の製品の品質は最高レベルであるため、ほとんどの忠実な顧客にとってこれは問題ではない。

世界有数のビデオゲーム機開発企業であるナイト社は、悪意のある攻撃の標的となることも少なくありません。同社の情報管理システム（ISMS）は1年以上前から運用されており、財務部門と人事部門を除くナイト社の全部門を網羅しています。

最近、ナイト社の機密情報を含むファイルの一部がハッカーによって流出しました。ナイト社のインシデント対応チーム（IRT）は、直ちにシステム全体と事件の詳細の分析を開始しました。

IRTは当初、ナイト社の従業員が脆弱なパスワードを使用していたため、不正なハッカーがアカウントに容易にアクセスできたのではないかと疑っていた。しかし、徹底的な調査の結果、ハッカーはファイル転送プロトコル（FTP）の通信を傍受することでアカウントにアクセスしていたことが判明した。

FTPは、アカウント間でファイルを転送するために使用されるネットワークプロトコルです。認証には平文のパスワードを使用します。

この情報セキュリティインシデントの結果、ナイト社はIRTの助言に基づき、FTPをセキュアシェル（SSH）に置き換えることを決定した。これにより、通信を傍受した者は暗号化されたデータしか見ることはできないようになる。

これらの変更を受けて、ナイト社はリスク評価を実施し、管理策の導入によって同様の事象のリスクが最小限に抑えられたかどうかを検証した。この評価結果はISMSプロジェクトマネージャーによって承認され、新しい管理策の導入後のリスクレベルは同社のリスク許容度と一致していると判断された。

このシナリオに基づいて、以下の質問に教えてください。

シナリオ2に基づく、ISMSの適用範囲はナイト社の財務部門と人事部門には適用されません。これは許容範囲内でしょうか？

A. いいえ、ISMS の範囲にはすべての組織単位とプロセスを含める必要があります。

B. はい、ISMSの適用範囲は組織全体、または組織内の特定の部門のみを含むことができます。

C. はい、ISMSは情報セキュリティに直接影響を与える可能性のあるプロセスと資産にのみ適用する必要があります。

Answer: B ([メッセージを残す](#))

最新問題: 260

シナリオ9

CloudFortは、ネットワークセキュリティ、クラウドコンピューティング、仮想化ソリューションを提供する小規模なインターネット企業です。同社は最近、ISO/IEC 27001規格に基づく情報セキュリティマネジメントシステム（ISMS）認証を取得し、認知度を大幅に向上させるとともに、CloudFortの事業運営の成熟度を証明しました。

CloudFortは、内部監査を通じて、セキュリティ管理と情報セキュリティマネジメントシステム（ISMS）の全体的な有効性と効率性を継続的に見直し、改善しています。同社の規模と客観性を高める必要性を考慮し、経営陣は、監査対象業務からの独立性を確保し、ISMSの継続的な改善のための助言サポートを提供するために、内部監査機能を外部委託することを決定しました。

初回認証監査の完了後、同社はデータストレージソリューション専門の新部門を設立しました。この部門では、データセンター向けに最適化されたルーターやスイッチに加え、ネットワーク仮想化やネットワークセキュリティ機器といったソフトウェアベースのネットワーク機器を提供しています。新部門の設立に伴い、CloudFortはリスク評価プロセスと内部監査を開始しました。内部監査の結果、新たなプロセスと管理体制の有効性と効率性が確認されました。

新設部署がISO/IEC 27001の要件を完全に満たしていることを確認した後、経営陣は同部署を認証範囲に含めることを決定しました。そして、同部署のプロセスとセキュリティ対策が統合情報セキュリティマネジメントシステム（ISMS）に完全に準拠していることを保証するため、認証範囲の拡大を求める申請書を認証機関に提出しました。

最初の認証監査から1年後、認証機関はCloudFortの情報セキュリティマネジメントシステム（ISMS）の2回目の監査を実施しました。この監査の目的は、CloudFortのISMSがISO/IEC 27001規格の特定の要件を満たしているかどうかを判断し、ISMSの継続的な改善を確保することでした。監査チームは、認証されたISMSが規格の要件を満たしていることを確認しました。しかし、新設された部署によって導入された変更は、マネジメントシステム全体の運用方法に大きな影響を与え、既存のプロセスと管理の更新が必要となりました。

さらに、CloudFortは認証範囲の拡大を申請したにもかかわらず、新設部門が情報セキュリティマネジメントシステム（ISMS）に与える影響について、認証機関にタイムリーな最新情報を提供できなかった。そのため、CloudFortの認証は停止された。

質問

CloudFort社から、認証範囲を拡張して新たな部門を含めるよう要請がありました。この状況をどのように分類しますか？シナリオ9を参照してください。

A. 受け入れられません。拡張機能は初期認証範囲に含めるべきであり、大規模な再認証プロセスが実行されない限り、後から追加すべきではありません。

B. 許容範囲内。多くの被監査者は、最初の認証時に狭い範囲を定義し、その後、翌年以降に延長を申請することができる。

C. 範囲を拡大するには組織全体の監査を再度行う必要があるため、受け入れられません。

Answer: B (メッセージを残す)

この状況は許容範囲内であり、選択肢Bが正解です。ISO/IEC 17021-1およびISO/IEC 27006では、認証を受けた組織が初回認証後に認証範囲の拡張を申請することが明示的に認められています。組織が当初は限定的または縮小された範囲で認証を開始し、ISMSの成熟、事業規模の拡大、または新設部門の設立に伴って後から範囲を拡大することは一般的であり、完全に認められています。

ISO/IEC 27001では、組織全体を最初の認証範囲に含めることは義務付けられていません。その代わりに、認証範囲が明確に定義され、文書化され、管理されていることが求められます。CloudFortは新しい部門を設立した際、リスク評価と内部監査を適切に開始し、その後、認証機関に正式に認証範囲の拡張を申請しました。これは、ISOの要求事項への準拠と、優れたISMSガバナンスを示しています。

選択肢Aは誤りです。なぜなら、認証機関が変更内容がISMSを根本的に変えるほど広範囲に及ぶと判断しない限り、スコープの拡張には全面的な再認証監査は必要ないからです。選択肢Cも誤りです。スコープの拡張は、組織全体の完全な再監査を自動的に必要とするものではありません。認証機関は通常、新しいスコープ要素と既存のISMSとの相互作用を対象とした、焦点を絞った拡張監査を実施します。

シナリオ9における認証停止は、スコープ拡張要求が不適切だったためではなく、CloudFortが新設部門の影響に関する十分な情報を認証機関にタイムリーに提供しなかったために発生した。スコープ拡張を要求する行為自体は適切かつ許容範囲内であった。

最新問題: **261**

您是一位經驗豐富的 ISMS 審核團隊領導，為培訓中的審核員提供指導。今天課程的主題是根據ISO/IEC 27001:2022的要求進行資訊安全風險管理。

您為班級提供一系列活動。然後，您要求全班將這些活動按照它們在標準中出現的順序進行排序。

他們應該向您報告的正確順序是什麼？

1st

2nd

3rd

4th

5th

6th

To complete the sequence click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the options to the appropriate blank section.

Create and maintain information security risk criteria

Identify the risks that need to be considered when planning for the information security management system

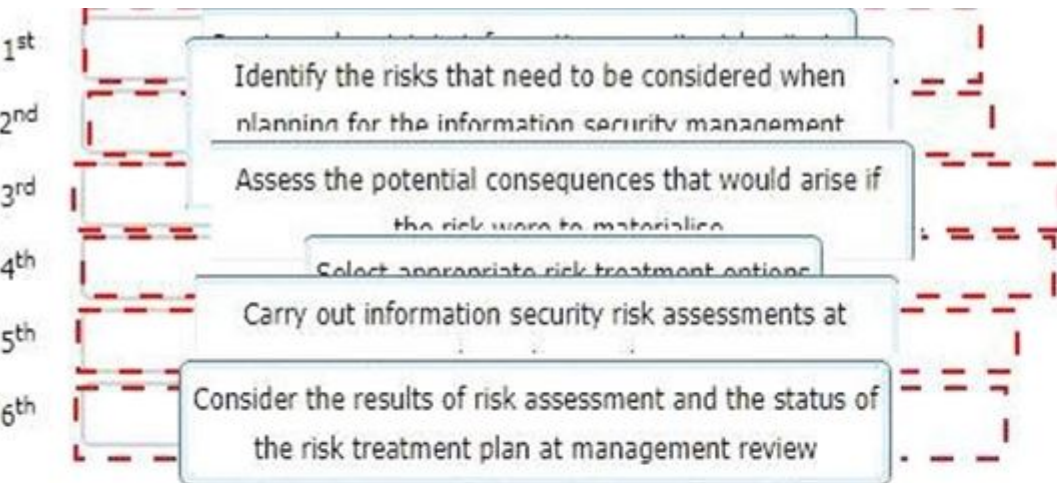
Assess the potential consequences that would arise if the risk were to materialise

Select appropriate risk treatment options

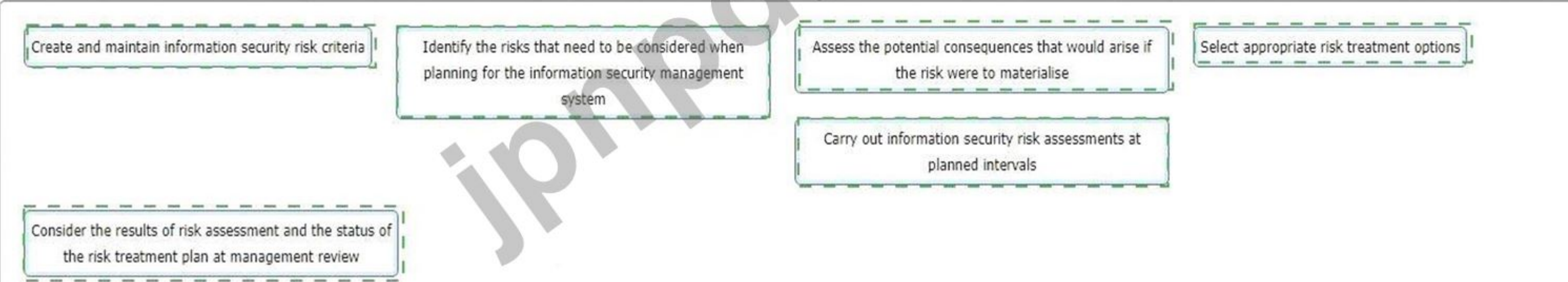
Carry out information security risk assessments at planned intervals

Consider the results of risk assessment and the status of the risk treatment plan at management review

Answer:



To complete the sequence click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the options to the appropriate blank section.



Explanation:



The correct sequence of activities for the management of information security risk in accordance with the requirements of ISO/IEC 27001:2022 is as follows:

1st: Create and maintain information security risk criteria 2nd: Identify the risks that need to be considered when planning for the information security management system 3rd: Assess the potential consequences that would arise if the risk were to materialise 4th: Select appropriate risk treatment options 5th: Carry out information security risk assessments at planned intervals 6th: Consider the results of risk assessment and the status of the risk treatment plan at management review This sequence is based on the information security risk management process described in ISO/IEC 27001:

2022 clause 6.1, which includes the following activities:

- * establishing and maintaining information security risk criteria;
- * ensuring that repeated information security risk assessments produce consistent, valid and comparable results;

- * identifying the information security risks;
- * analyzing the information security risks;
- * evaluating the information security risks;
- * treating the information security risks;
- * accepting the information security risks and the residual information security risks;
- * communicating and consulting with stakeholders throughout the process;
- * monitoring and reviewing the information security risks and the risk treatment plan.

References:

ISO/IEC 27001:2022, clause 6.1

[PECB Candidate Handbook ISO/IEC 27001 Lead Auditor], pages 14-15

ISO 27001 Risk Management in Plain English

最新問題: **262**

質問

監査の範囲と基準は誰が決定するのか？

A. 監査チームリーダー

B. 被監査者との協議後、監査チームは

C. 認証機関

Answer: C ([メッセージを残す](#))

正解は認証機関です。なぜなら、ISO/IEC 17021-1では、監査範囲と監査基準の設定責任は、監査チームや被監査者ではなく、認証機関に明確に割り当てられているからです。

認証機関は、認証プロセスを管理し、一貫性、公平性、および認定要件への準拠を確保する責任を負います。

監査範囲は、認証監査の対象となる組織単位、場所、活動、プロセスなど、監査の範囲を定義します。監査基準は、ISO/IEC 27001の要求事項、法的義務、内部ISMSポリシーなど、適合性を評価するためのポリシー、手順、要求事項のセットを定義します。監査チームリーダーは、定義された範囲内で監査を実施する方法を計画することはできますが、監査範囲自体を決定することはできません。

選択肢Aは誤りです。監査チームリーダーの役割は、監査の実施を管理し、監査計画を作成し、監査活動を調整することであり、正式な範囲や基準を設定することではありません。選択肢Bも誤りです。被監査組織を理解し、範囲の実現可能性を確認するためには、被監査組織との協議が必要ですが、最終的な権限は認証機関にあります。

この責任の分離により、独立性が確保され、組織が認証の範囲に不当な影響を与えることを防ぐことができます。したがって、認証機関は監査範囲と監査基準を定める主体となります。

最新問題: **263**

シナリオ7 :Lawtsyは、ニュージャージー州とニューヨーク市にオフィスを構える大手法律事務所です。50名以上の弁護士を擁し、企業法務、知的財産、銀行業務、金融サービスといった分野で顧客に包括的な法的サービスを提供しています。同社は、情報セキュリティにおけるベストプラクティスの導入と技術革新への対応に注力することで、市場において確固たる地位を築いていると確信しています。

Lawtsyは、過去2年間、ISMS（情報セキュリティマネジメントシステム）の厳格な導入、評価、および内部監査を実施してきた。

彼らは現在、知名度が高く信頼できる認証機関であるISMAに対し、ISO/IEC 27001認証の申請を行っている。

監査の第一段階では、監査チームは導入プロセス中に作成されたすべてのISMS文書をレビューした。

彼らはまた、経営陣によるレビューや内部監査の記録を精査し、評価した。

Lawtsy社は、不適合に対して必要に応じて是正措置が講じられたことを示す証拠を提出し、これを受けて監査チームは内部監査担当者への聞き取り調査を実施した。この聞き取り調査により、内部監査計画と手順に関する詳細な理解が得られ、内部監査の適切性と頻度が検証された。

監査チームは、情報セキュリティポリシーやリスク評価基準などの戦略文書の検証を継続しました。情報セキュリティポリシーのレビュー中に、チームは、文書化された情報とガバナンスフレームワーク（すなわち情報セキュリティポリシー）を説明する手順との間に矛盾があることに気づきました。

従業員はノートパソコンを職場外に持ち出すことが許可されているものの、Lawtsy社にはその使用に関する明確な手順が定められていません。社内規定にはノートパソコンの使用に関する一般的な情報しか記載されていませ

ん。同社は、ノートパソコンに保存されている情報の機密性と完全性を保護するために、従業員の常識に頼っています。この問題は、フェーズ1監査報告書に記載されています。

監査の第一段階が完了した後、監査チームリーダーは監査計画書を作成し、監査の目的、範囲、基準、および手順を明記した。

監査の第2段階では、監査チームは情報セキュリティポリシーを作成したサイバーセキュリティマネージャーにインタビューを行った。マネージャーは、Lawtsy社が3ヶ月ごとに情報セキュリティに関する必須の研修と啓発コースを実施していることを指摘し、第1段階で指摘された問題点の妥当性を証明した。

面接後、監査チームは従業員研修記録50件のうち15件を精査し、Lawtsy社が研修および意識向上に関するISO/IEC 27001の要件を満たしていると結論付けた。この結論を裏付けるため、監査チームは精査した従業員研修記録のコピーを作成した。

上記のシナリオに基づいて、以下の質問に教えてください。

監査チームは、従業員の研修記録50件のうち15件を調査した結果、Lawtsy社は研修および意識向上に関するISO/IEC 27001の要件を満たしていると結論付けました（シナリオ7に記載）。

A. 監査人

B. サンプルング

C. サンプルサイズ

Answer: (解答を表示する)

このシナリオでは、サンプルサイズに関連するリスクが生じます。従業員50名の研修記録のうち15名のみを調査した場合、ISO/IEC 27001の研修および意識向上に関する要件に対する組織全体の遵守状況を十分に代表するものではない可能性があります。このサンプルサイズでは、組織全体に関する一般的な結論を導き出すには不十分であるリスクがあります。

最新問題: 264

あなたは、地元の病院や官公庁などの大規模組織に輸送サービスを提供する国際物流組織の出荷部門でISMS監査を実施しています。荷物には通常、医薬品、生物学的サンプル、パスポートや運転免許証などの書類が含まれています。会社の記録を見ると、ラベルの住所が間違っていることや、15%のケースで1つの荷物に2つ以上の異なる住所のラベルが貼られていることなどが原因で、返品が大量に発生していることがわかります。あなたは輸送マネージャー（\$M）の面接を行っています。

出荷前に商品の検査は行いましたか？

SM：明らかに破損している商品は、出荷前に担当スタッフが取り除きますが、利益率が非常に低いため、正式な検査プロセスを実施するのは経済的ではありません。

商品を返品した後、どのような措置を講じますか？

SM：これらの契約のほとんどは比較的小額なので、調査を行うよりも、ラベルを再印刷して個々の荷物を再送の方が簡単で便利だと考えています。

不適合事項が特定されました。この状況に基づき、被監査者が今後の監査において実施すべき、附属書Aに記載されている管理策のうち、3つを選択してください。

A. 5.11 資産収益率

B. 5.13 情報タグ

C. 5.3 職務分担

D. 5.32 知的財産権

E. 5.34 プライバシーと個人識別情報（PII）の保護

F. 5.6 特殊利益団体とのつながり

G. 6.3 情報セキュリティに関する意識向上、教育および研修

H. 6.4 懲戒手続き

Answer: B (メッセージを残す)

フォローアップ監査を実施する際に、被監査企業が実施していることを期待する附属書Aの3つの管理策は以下のとおりです。

B. 5.13 情報のラベリング

E. 5.34 プライバシーと個人識別情報（PII）の保護 G. 6.3 情報セキュリティの意識向上、教育、トレーニング B. この管理策では、組織が情報資産を情報分類体系に従ってラベル付けし、それに応じて取り扱うことが求められます 12. この管理策は、ラベルの宛先間違いや荷物の誤った宛先への送付を防ぎ、情報資産の機密性、完全性、可用性を損なうことを回避するのに役立つため、監査対象者にとって重要です。情報資産に正しくラベルを貼ることで、監査対象者は、それらが意図した受取人に届けられ、不正アクセス、使用、開示から保護されることも保証できます。

E. この管理策では、組織が処理する個人識別情報（PII）の個人のプライバシーと権利を保護し、適用される法的義務および契約上の義務を遵守することが求められます 13. この管理策は、入居者の個人データが供給業者によって不正に使用されることを防ぐのに役立つため、被監査者にとって重要です。不正使用は、入居者とその家族のプライバシーと権利を侵害し、被監査者を法的リスクや評判リスクにさらす可能性があります。また、被監査者は、入居者とその家族のPIIを保護することで、信頼と満足度を高め、苦情や紛争を回避することもできます。

G. この管理策では、組織はすべての従業員と契約社員が情報セキュリティポリシー、それぞれの役割と責任、および関連する情報セキュリティ手順と管理策を認識していることを確認する必要があります14。この管理策は、被監査組織にとって重要です。なぜなら、被監査組織が従業員の情報セキュリティ文化と行動を改善し、情報セキュリティインシデントにつながる可能性のある人的ミスや過失を減らすのに役立つからです。被監査組織は、従業員に情報セキュリティに関する意識向上、教育、トレーニングを提供することで、従業員の能力とパフォーマンスを向上させ、情報セキュリティプロセスと管理策の有効性と効率性を確保することもできます。

参照：

1: ISO/IEC 27001:2022 - 情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステム - 要求事項、附属書A 2: ISO/IEC 27002:2022 - 情報技術 - セキュリティ技術 - 情報セキュリティ管理策の実施基準、8.2.1項 3: ISO/IEC 27002:2022 - 情報技術 - セキュリティ技術 - 情報セキュリティ管理策の実施基準、18.1.4項 4: ISO/IEC 27002:2022 - 情報技術 - セキュリティ技術 - 情報セキュリティ管理策の実施基準、7.2.2項

最新問題: 265

あなたは、医療サービスを提供する高齢者向け介護施設でISMS監査を受けています。監査計画の次のステップは、適合性声明書（SoA）に必要な管理策が含まれていることを確認することです。

あなたは最新のSoA（バージョン5）文書を確認し、ソースコードのアクセス制御（A.8.4）のサンプルを参照しています。そして、外部委託先のソフトウェア開発者から受け取ったABCヘルスケアモバイルアプリケーションのソースコードを、組織がどのように保護できるかを理解したいと考えています。

ITセキュリティマネージャーは、受け取ったソースコードはSCMシステムで検査され、その完全性とセキュリティが確保されると説明した。ソフトウェアの閲覧と更新は、許可されたユーザーのみが行うことができる。システムはチェックインとチェックアウトのアクティビティを自動的に記録します。バージョン管理もシステムによって自動的に行われます。

SCM上で合計10個のユーザーアカウントを発見しました。それらはすべてIT部門のものでした。人事部長に確認したところ、ユーザーの1人であるスコットは9か月前に退職していたことが判明しました。SCMシステム管理者は、スコットが最後にソースコードをチェックアウトしたのは1か月前であることを確認しました。彼は、セキュリティエリア内のローカルネットワーク上の承認済みデスクトップを使用していました。あなたはユーザーのログアウト手順を確認しましたが、そこには「管理者は、退職が承認された時点で、関連するICTシステムおよび/またはデバイスからユーザーアカウントと権限が直ちに無効化されるようにしなければならない」と記載されています。ユーザーScottにはログアウト記録がありません。

ITセキュリティマネージャーは、スコットは優秀なソフトウェアエンジニアであり、元同僚であり、友人だったと説明した。

退職後も、彼は毎月オフィスに戻り、ソースコードの保守サポートを提供し続けていました。そのため、SCM上の彼のアカウントは今も残っています。私たちはスコットのことをよく知っています。入社時にすべての身元調査に合格しています。ですから、彼が外部プロバイダーになったからといって、追加の情報セキュリティ要件に同意する必要はないと考えました。」

監査結果を準備しています。正しい選択肢を3つ選んでください。

A. 不適合（NC）が存在します。スコットは、介護施設（外部プロバイダー）との新たな関係に関連する適用可能な情報セキュリティ要件について通知を受けるべきでした。しかし、ITセキュリティマネージャーは、これが行われなかったことを確認しました。これは管理策A.5.20に準拠していません。

B. 不適合（NC）が存在します。組織のアクセス制御体制が効果的に機能していませんでした。組織に雇用されていない人物が介護施設のICTシステムにアクセスできていたためです。これは管理措置A.5.15に準拠していません。

C. 法令違反（NC）が存在します。ITセキュリティマネージャーは、スコットのユーザーアカウントがSCMから削除されたことを確認せず、また、スコットの退職後にユーザーのログアウトプロセスを完了しませんでした。これは条項9.1および管理措置A.5.15に準拠していません。

D. 不適合（NC）が存在します。操作手順が十分に文書化されていません。そのため、SCMシステム管理者はユーザーアカウントを即座に削除することができません。これは条項9.1および管理A.5.37に準拠していません。

E. 不適合（NC）が存在します。組織には、システムツールを使用してソースコードへのアクセスとバージョン管理を行う方法を規定する文書化された手順がありません。これは、条項9.1および管理A.8.4に準拠していません。

F. 法令違反（NC）が存在します。組織は、スコットが毎月短期間しかアカウントを再利用していなかったため、アカウントを開いたままにしておくことに関連するセキュリティリスクを特定できませんでした。これはセクション8.2に準拠していません。

G. 不適合事項が存在します（NC）。SCMはオープンソースのシステムソフトウェアです。セキュリティ上の問題があり、ソースコードへのアクセスやバージョン管理には使用できません。これは条項9.1および管理A.8.4に準拠していません。

H. 不適合（NC）が存在します。SCMはソースコードのチェックイン/チェックアウト活動を自動的に記録します。問題が発生した場合、チームはそれを追跡できない可能性があります。これは条項9.1および管理A.8.4に準拠していません。

Answer: (解答を表示する)

正解の選択肢は以下のとおりです。

不適合（NC）があります。組織のアクセス制御の仕組みが効果的に機能しておらず、組織に雇用されていない人物が介護施設のICTシステムにアクセスすることを許可されています。これは制御A.5.15に準拠していません。B）：この選択肢が正しいのは、制御A.5.15では、組織が安全なログオン手順を実装し、ユーザーのアクセス権限を管理することが求められているからです。組織は、承認されたユーザーのみがICTシステムにアクセスでき、ユーザーの

ステータスが変更されたときにアクセス権限が取り消されるか変更されるようにする必要があります。9か月前に退職したスコットがSCMにアクティブなアカウントを持ち、ソースコードをチェックアウトできるという事実は、アクセス制御の仕組みの失敗と制御A.5.15への不適合を示しています。

不適合 (NC)があります。IT セキュリティ マネージャーは、Scott のユーザー アカウントが SCM から削除されたことを確認せず、退職後にユーザー登録解除プロセスを完了しませんでした。これは、条項 9.1 および管理 A.5.15 に適合しません。：このオプションは正しいです。条項 9.1 では、組織が ISMS のパフォーマンスと有効性を監視、測定、分析、評価することを要求しています。組織は、ISMS の要件と目標が満たされていること、および ISMS が継続的に改善されていることを検証するためのプロセスと指標を持つ必要があります。組織はまた、監視と測定の結果が文書化され、伝達されることを保証する必要があります。IT セキュリティ マネージャーがユーザー登録解除手順に従わず、Scott の例外を文書化または伝達しなかったという事実は、監視と測定プロセスの失敗と、条項 9.1 および管理 A.5.15 への不適合を示しています。

不適合 (NC)があります。組織は、スコットが月に短期間だけ再雇用されたにもかかわらず、彼のアカウントを開いたままにしておくことに関連するセキュリティリスクを特定できませんでした。これは条項8.2に準拠していません。F) この選択肢は正しいです。条項8.2では、組織が情報セキュリティリスク管理プロセスを確立し、維持することが求められています。組織は、情報セキュリティリスクを特定し、リスクを分析および評価し、リスク基準とリスク処理オプションに従ってリスクを処理する必要があります。また、組織は、リスクとリスク処理計画を定期的に監視およびレビューし、結果を文書化する必要があります。組織が、スコットのSCMおよびソースコードへのアクセスに関連するセキュリティリスク（情報の不正な開示、変更、または削除など）を特定しなかったという事実は、リスク管理プロセスの失敗と条項8.2への不適合を示しています。

最新問題: 266

あなたは経験豊富なISMS監査チームリーダーであり、監査員の研修や初回監査報告書の作成を支援します。

研修中に監査担当者が監査報告書の内容に関連する用語を理解しているかどうかを確認したい場合は、以下の例を示すことで確認できます。

研修中、各事例について、監査員に活動を説明するのに適切な用語は何かを尋ね、活動と説明を一致させるように指示します。

An auditor using a copy of ISO/IEC 27001:2022 to check that its requirements are met	
An auditor’s note that the auditee is not adhering to its’ clear desk policy	
An auditor making a decision regarding the auditee’s conformity or otherwise to criteria	
An auditor examining verifiable records relevant to the audit process	

To complete the table, click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop each option to the appropriate blank section.

This example relates to the identification of an audit finding

This example relates to relates to the collection of audit evidence

This example relates to the use of audit criteria to determine conformity or nonconformity

This description relates to the determination of an audit conclusion

Answer:

An auditor using a copy of ISO/IEC 27001:2022 to check that its requirements are met	This example relates to the use of audit criteria to determine conformity or nonconformity
An auditor’s note that the auditee is not adhering to its’ clear desk policy	This example relates to the identification of an audit finding
An auditor making a decision regarding the auditee’s conformity or otherwise to criteria	This description relates to the determination of an audit conclusion
An auditor examining verifiable records relevant to the audit process	This example relates to relates to the collection of audit evidence

To complete the table, click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop each option to the appropriate blank section.

This example relates to the identification of an audit finding

This example relates to the use of audit criteria to determine conformity or nonconformity

This description relates to the determination of an audit conclusion

This example relates to relates to the collection of audit evidence

最新問題: 267

您是經驗豐富的 ISMS 審核團隊領導，指導審核員進行培訓。她詢問您審核報告中不合格項的分級。您決定透過詢問她以下哪四個陳述是正確的來測試她的知識。

- A. 重大不符合項目可能需要現場跟進
- B. 不合格項必須僅使用術語「嚴重」或「輕微」進行分級
- C. 解決重大不合格問題所採取的行動通常比解決輕微不合格問題所採取的行動更為實質性
- D. 非常輕微的不符合項應重新評級為改進機會
- E. 幾個輕微不符合項可以歸為一個主要不符合項
- F. 不合格品的分級必須在首次會議上向受審核方解釋
- G. 受審核方始終負責確定不合格品的分級標準
- H. 可以將不合格項分級以表示其重要性

Answer: (解答を表示する)

The four statements that are true are:

- *Major nonconformities may be subject to on-site follow up
- *The action taken to address major nonconformities is typically more substantial than the action taken to address minor nonconformities
- *Several minor nonconformities can be grouped into a major nonconformity
- *Nonconformities may be graded to indicate their significance

According to ISO 19011:2018, a nonconformity is the non-fulfilment of a requirement1. Nonconformities may be graded to indicate their significance, based on the criteria established by the audit programme or the audit client2. The grading of nonconformities may use different terms or levels, such as major, minor, critical, etc., depending on the nature and context of the audit3. However, some common definitions of major and minor nonconformities are:

- *A major nonconformity is a nonconformity that affects the ability of the management system to achieve its intended results, or that represents a significant breakdown of the management system4. Major nonconformities may require immediate corrective action and on-site follow up by the auditor to verify their closure5.
- *A minor nonconformity is a nonconformity that does not affect the ability of the management system to achieve its intended results, or that represents an isolated lapse of the management system4. Minor nonconformities may require corrective action within a specified time frame and off-site verification by the auditor to confirm their closure5.

The action taken to address nonconformities depends on the severity and impact of the nonconformity, and the risk of recurrence or escalation. Typically, the action taken to address major nonconformities is more substantial than the action taken to address minor nonconformities, as it may involve identifying and eliminating the root cause of the problem, implementing preventive measures, and monitoring the effectiveness of the solution. Several minor nonconformities can be grouped into a major nonconformity if they are related to the same requirement, process, or area, and if they indicate a systemic failure or a significant risk to the management system. The auditor should use professional judgment and evidence-based approach to decide whether to group or report nonconformities individually.

The other statements are false, based on the guidance of ISO 19011:2018. For example:

- *Option B is false, because nonconformities can be graded using different terms or levels, depending on the criteria established by the audit programme or the audit client2. The terms 'major' and 'minor' are not mandatory or universal, but rather examples of possible grading levels3.
- *選択肢Dは誤りです。なぜなら、非常に軽微な不適合は改善の機会として再評価されるべきではなく、依然として要求事項1を満たしていないことを示す不適合として報告されるべきだからです。改善の機会とは、マネジメントシステムのパフォーマンスや有効性を向上させるための提案であり、不適合や要求事項ではありません。
- *選択肢Fは誤りです。不適合の評価は、開始会議で被監査者に説明する必要はなく、監査結果と結論が提示され議論される終了会議で説明する必要があります。開始会議は、監査の目的、範囲、基準、方法の概要を提供し、監査の手配と手順を確認することを目的としています。
- *オプションGは誤りです。なぜなら、不適合の評価基準を決定する責任は、必ずしも被監査者にあるのではなく、被監査者およびその他の関係者と協議の上、監査プログラムまたは監査クライアントにあるからです。被監査者は、不適合に対処するための是正措置を講じ、その完了と有効性の証拠を提供する責任があります。

参照文献: 1: ISO 19011:2018、3.13; 2: ISO 19011:2018、6.6.2; 3: ISO 19011:2018、6.6.3; 4: ISO監査結果:不適合 - AUVA認証1; 5: 附属書III:不適合等級 - FSSC2; : ISO

27001認証 - 重大な不適合と軽微な不適合 - Advisera3; : 不適合への対処と解消に関するガイダンス - SADCAS4; : ISO 19011:2018、6.2; : ISO 19011:2018、3.14; :

ISO 19011:2018、6.7; : ISO 19011:2018、6.4; : ISO 19011:2018、6.7.2; : ISO 19011:2018; : ISO 19011:2018; :

ISO 19011:2018; : ISO 19011:2018; : ISO 19011:2018; : [ISO 19011:2018]; : [ISO 19011:2018]; : [ISO

19011:2018]; : [ISO 19011:2018]; : [ISO 19011:2018]; : [ISO 19011:2018]

最新問題: 268

シナリオ6 :Cyber ACryptは、マルウェア対策やデバイスセキュリティ、資産ライフサイクル管理、デバイス暗号化などのエンドポイント保護サービスを提供するサイバーセキュリティ企業です。同社は、情報セキュリティマネジメントシステム (ISMS)がISO/IEC 27001規格に準拠していることを検証し、優れたサイバーセキュリティへの取り組みを示すため、指定された監査チームリーダーであるジョンが主導する厳格な監査プロセスを受けました。監査業務を引き受けたジョンは、監査計画とチームの役割を概説するための会議をすぐに開催しました。この段階は、チームを監査の目的と範囲に合わせる上で非常に重要でした。しかし、Cyber ACryptのスタッフとの最初のブリーフィングでは、監査の範囲と目的についての理解に大きなギャップがあることが明らかになり、社内での準備上の潜在的な課題が示されました。監査の第1段階の開始に伴い、チームは現場活動の準備を行いました。彼らは、Cyber ACryptの情報セキュリティポリシーと運用手順を含む文書をレビューし、各文書が標準形式に準拠し、作成者識別情報、作成日、バージョン番号、承認日が含まれていることを確認しました。さらに、監査チームは、各文書に、関連する標準条項で要求される情報が含まれていることを確認しました。この段階で、タスクの実行を記述した文書の詳細な監査は不要であることが明らかになり、プロセスが合理化され、チームは重要な領域に集中することができました。現場活動の段階では、チームはCyber ACryptのポリシーの管理責任を評価しました。この徹底的なレビューは、継続的な改善と情報セキュリティマネジメントシステム (ISMS) 要件への準拠を確保することを目的としていました。その後、監査成果の第1段階に関する文書において、監査チームは調査結果を詳細に記述し、第1段階の目標達成に関する結論を強調しました。この文書は、監査チームとCyberACryptが予備的な監査結果と注意が必要な領域を理解する上で非常に重要でした。

監査チームは、主要な関係者への聞き取り調査も実施することにした。この措置は、経営システムがISO規格に準拠しているかどうかを検証するための信頼できる監査証拠を収集することを目的としていた。

/IEC 27001 の要求事項。サイバー ACrypt のあらゆるレベルのステークホルダーとのコミュニケーションにより、監査チームは貴重な視点を得ることができ、情報セキュリティ マネジメント システム (ISMS) の実装と有効性についての理解を深めることができました。

第1段階の監査報告書では、いくつかの重要な問題点が明らかになりました。適用範囲宣言書（SoA）および情報セキュリティマネジメントシステム（ISMS）ポリシーには、リスク評価の不備、アクセス制御の不備、定期的なポリシー見直しの欠如など、複数の点で不備がありました。これを受け、CyberACryptはこれらの不備に対処するため、直ちに行動を起こしました。迅速な対応と戦略文書の改訂は、同社のコンプライアンスに対する強いコミットメントを示すものでした。

監査チームのネットワークセキュリティに関する知識不足を補うために招集された技術専門家は、リスク評価手法の欠陥を特定し、ネットワークアーキテクチャをレビューする上で重要な役割を果たしました。これには、ファイアウォール、侵入検知・防御システム、その他のネットワークセキュリティ対策の評価、およびCyber ACryptが外部および内部の脅威をどのように検知、対応、復旧しているかの評価が含まれていました。ジョンの指導の下、技術専門家は監査結果をCyber ACryptの担当者に伝えました。しかし、監査チームは、専門家が被監査企業からコンサルティング料を受け取っていたため、専門家の客観性が損なわれた可能性があるとして指摘しました。監査プロセス中の技術専門家の行動を考慮し、監査チームリーダーは認証機関とこの件について話し合うことにしました。

上記のシナリオに基づいて、以下の質問に答えてください。

質問：

監査チームは、監査の第一段階において、どの活動を正しく実施できなかったか？

- A. 情報セキュリティ戦略と運用手順をレビューに組み込み、オンサイトイベントの準備を行います。
- B. サイバー暗号化ポリシーに対する経営陣の責任を評価するために、オンサイト活動を実施する。
- C. 関連する証拠や裏付けとなる文書が含まれていなかったため、第1段階の監査結果は記録されませんでした。

Answer: C ([メッセージを残す](#))

包括的かつ詳細な解説：

* C. 正解:

監査チームは調査結果を文書化したが、このシナリオでは十分な裏付けとなる証拠が含まれていたかどうかは確認できない。

* ISO 19011:2018では、監査結果を適切に文書化し、証拠に基づいて正当化することが求められています。

証拠を文書化しないと、監査の信頼性が低下する。

* A. 不正解:

監査に備えて方針や手順を見直すことは、適切な手順です。

* B. 不正解:

* ISMS準拠に関する経営陣の責任を評価することは、ステージ1における必須ステップです。

関連規格参照：

* ISO/IEC 27001:2022 条項9.2（内部監査）

* ISO 19011:2018 6.5.3項（監査文書化要求事項）

最新問題: 269

予備認証監査の第1段階を完了し、第2段階の準備を進めた後、被監査組織は監査チームリーダーに対し、組織が最近取得した2つの拠点を監査対象に含めたい旨を通知した。

この情報を踏まえて、監査チームリーダーにはどのような行動を取ることを期待しますか？

- A. フェーズ2レビューの期間を延長し、追加のサイトを含める。
- B. 認証機関に通知するための追加ウェブサイトから情報を取得する。
- C. 両拠点でリモートレビューの第一段階を完了するために、ビデオ会議プラットフォームを使用するよう手配する。
- D. 監査担当者に、要求は受け入れられるが、第1段階の監査全体をやり直す必要があることを通知する。

Answer: B ([メッセージを残す](#))

マネジメントシステムの監査および認証を提供する機関の要求事項を規定するISO/IEC 17021-1によれば、認証機関は、認証の範囲、組織の規模と複雑さ、活動に伴うリスクなどの要素に基づいて、監査時間と監査チームの構成を決定するための基準を確立する必要がある2。したがって、被監査者が最初の認証監査のステージ1を完了した後、監査範囲を2つの追加サイトを含むように拡張することを要求した場合、監査チームリーダーは追加サイトに関する情報を入手して認証機関に通知し、認証機関が範囲の変更をレビューして承認し、監査時間と監査チームをそれに応じて調整できるようにする必要がある2。他の選択肢は、この状況で監査チームリーダーが取るべき適切な行動ではない。たとえば、認証機関に通知せずにステージ2監査の長さを延長して追加サイトを含めることは、認証機関の手順とポリシーに違反する可能性がある。ビデオ会議プラットフォームを使用して2つのサイトのリモー

トステージ1監査を完了するように手配することは、サイトの性質と場所によっては実現不可能または効果的ではない可能性がある。また、被監査対象者に対し、要求は受け入れられるものの、ステージ1の監査を全面的にやり直す必要がある旨を通知することは、ステージ12以降、被監査対象者のISMSに大きな変更がない場合には、必ずしも必要または合理的ではない可能性がある。参照 ISO/IEC 17021-1:2015 - 適合性評価 - マネジメントシステムの監査及び認証を提供する機関に対する要求事項 - パート1：要求事項

最新問題: 270

下列哪兩項敘述是正確的？

- A. 實施 ISMS 的好處主要來自於資訊安全風險的降低
- B. 認證 ISMS 的好處是獲得政府機構的合同
- C. ISMS 的目的在於應用風險管理流程來維護資訊安全
- D. ISMS 的目的在於證明符合監管要求

Answer: (解答を表示する)

The benefits of implementing an ISMS are not limited to a reduction in information security risks, but also include improved business performance, customer satisfaction, legal compliance, and stakeholder confidence. The benefit of certifying an ISMS is not only to obtain contracts from governmental institutions, but also to demonstrate the organisation's commitment to information security to other potential customers, partners, and regulators. The purpose of an ISMS is to apply a risk management process for preserving information security, which means identifying, analysing, evaluating, treating, monitoring, and reviewing the information security risks that the organisation faces. The purpose of an ISMS is not to demonstrate compliance with regulatory requirements, but rather to ensure that the organisation meets its own information security objectives and obligations.

Reference:

ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) objectives and content from Quality.org and PECB ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements [Section 0.1] and [Section 1]

最新問題: 271

以下のフレーズのうち、ファーストパーティレビューに関連する 目的」に該当するものはどれですか？ 2つ選択可）

- A. 国際基準の適用
- B. 認証機関向け監査報告書の作成
- C. 管理システムの適用範囲の正確性を確認する
- D. 期限内にレビューを完了してください。
- E. 申請監督要件
- F. 更新管理戦略

Answer: C,F (メッセージを残す)

第一者監査とは、組織自身または組織に代わって外部機関が実施する内部監査のことです。第一者監査の目的は以下のとおりです。12

- * 管理システムの範囲が正確であることを確認します。つまり、組織の情報セキュリティの目的と要件に関連するすべてのプロセス、活動、場所、および機能を網羅していることを確認します。
- * 監査結果とフィードバックに基づいて、情報セキュリティマネジメントシステム (ISMS) の方針声明、役割と責任、目的と目標を見直し、改訂するなど、管理方針を更新する。

その他のフレーズは、第一者監査の目的ではなく、むしろ次のとおりです。

- * 国際規格の適用 :これはISMSの要件であり、監査の目的ではありません。ISMSはISO/IEC 27001規格およびその他の適用される規格または規制に準拠する必要があります12
- * 認証機関向け監査報告書の作成 :これは第三者監査の活動であり、第一者監査ではありません。第三者監査とは、ISMSの適合性と有効性を検証し、適合証明書を発行するために、独立した認証機関によって実施される外部監査です。12
- * 監査を期限内に完了する :これは業績指標であり、監査の目的ではありません。監査は計画された期間と予算内で完了する必要がありますが、これは監査の主要な目的ではありません12
- * 規制要件の適用: これはISMSの要件でもあり、監査の目的ではありません。ISMSは、情報セキュリティに関する組織の法的小および契約上の義務を遵守する必要があります12 参考文献:
1: ISO/IEC 27001:2022 リードオーディター（情報セキュリティマネジメントシステム）コース（CQIおよびIRCA認定トレーニング1）2: ISO/IEC 27001 リードオーディタートレーニングコース（PECB 2）

有効な **ISO-IEC-27001-Lead-Auditor-CN** 問題集は GoShiken.com が提供された合格しやすい ISO-IEC-27001-Lead-Auditor-CN 試験問題集！ GoShiken.com が最新の **ISO-IEC-27001-Lead-Auditor-CN** 試験問題集を提供しています。GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 問題集をゲットする人はこちら:
<https://www.goshiken.com/PECB/ISO-IEC-27001-Lead-Auditor-CN-mondaishu.html> (**41830%OFF**問題集溶と正解付きで **30%**w特別割引コード: **Freepdfdumps**)

最新問題: **272**

シナリオ6 :Cyber ACryptは、マルウェア対策とデバイスセキュリティ、資産ライフサイクル管理、およびデバイス暗号化を提供することでエンドポイント保護を実現するサイバーセキュリティ企業です。ISO/IEC 27001に準拠したISMSの検証と、サイバーセキュリティにおける卓越性への取り組みを示すため、同社は指定された監査チームリーダーであるジョンが主導する綿密な監査プロセスを受けました。監査業務を引き受けたジョンは、すぐに監査計画とチームの役割を概説するための会議を組織した。彼らは、情報セキュリティポリシーや運用手順を含むCyberACryptの文書を精査し、すべての文書が基準を満たし、作成者情報、作成日、バージョン番号、承認日などの標準化された形式になっていることを確認した。この徹底的なレビューは、継続的な改善とISMS要件への準拠が必要な領域を特定することを目的としていた。この文書は、監査チームとCyberACryptが初期監査結果と注意が必要な領域を理解する上で非常に重要であった。監査チームは、主要な関係者へのインタビューも実施することに決定しました。この決定の目的は、マネジメントシステムがISO/IEC 27001の要求事項に準拠しているかどうかを検証するための信頼できる監査証拠を収集することでした。CyberACryptのあらゆるレベルの関係者に対話することで、監査チームは貴重な洞察を得るとともに、ISMSの導入状況と有効性について理解を深めることができました。第1段階の監査報告書では、いくつかの重要な懸念事項が明らかになりました。適用範囲宣言書 \$oA)およびISMSポリシーには、リスク評価の不備、アクセス制御の不足、定期的なポリシー見直しの欠如など、複数の点で不備がありました。これを受け、CyberACryptはこれらの不備に対処するため、直ちに行動を起こしました。迅速な対応と戦略文書の改訂は、コンプライアンス達成への強いコミットメントを示すものでした。監査チームのサイバーセキュリティに関する知識のギャップを埋めるために導入された技術専門家は、リスク評価方法論の欠陥を特定し、ネットワークアーキテクチャをレビューする上で重要な役割を果たしました。これには、ファイアウォール、侵入検知および防御システム、その他のサイバーセキュリティ対策の評価、ならびにCyber ACryptが外部および内部の脅威をどのように検知、対応、復旧するかの評価が含まれます。ジョンの監督の下、技術専門家は監査結果をCyber ACryptの担当者に伝えました。しかし、監査チームは、被監査企業からコンサルティング料を受け取ったため、専門家の客観性が損なわれた可能性があることを発見しました。監査プロセス中の技術専門家の行動を考慮し、監査チームリーダーはこの問題を認証機関と話し合うことにしました。

上記のシナリオに基づいて、以下の質問に答えてください。

文書情報の評価に使用される基準のうち、監査チームによってまだ検証されていないものはどれですか？ シナリオ6を参照)

- A. 情報の内容を記録します
- B. 情報記録のフォーマット
- C. 文書情報管理プログラム

Answer: **C** ([メッセージを残す](#))

包括的かつ詳細な徹底分析

C. 正解：

シナリオ6では、監査チームが文書の内容と形式をレビューしたと述べているが、文書管理手順の評価については言及していない。

ISO/IEC 27001では、文書化された情報の管理手順を見直すことが求められています。

A. 不正解：

文書の内容は、ISO/IEC 27001の条項に準拠しているかどうかについてレビューされた。

B. 不正解：

監査チームは、すべての文書が標準化された形式であることを確認した。

関連規格参照：

ISO/IEC 27001:2022 条項7.5（文書化された情報に関する要求事項）

最新問題: **273**

シナリオ6 :Cyber ACryptは、マルウェア対策とデバイスセキュリティ、資産ライフサイクル管理、およびデバイス暗号化を提供することでエンドポイント保護を実現するサイバーセキュリティ企業です。ISO/IEC 27001に準拠したISMSの検証と、サイバーセキュリティにおける卓越性への取り組みを示すため、同社は指定された監査チームリーダーであるジョンが主導する綿密な監査プロセスを受けました。

監査業務を引き受けたジョンは、すぐに監査計画とチームの役割を概説するための会議を組織した。彼らは、情報セキュリティポリシーや運用手順を含むCyberACryptの文書を精査し、すべての文書が基準を満たし、作成者情報、作成日、バージョン番号、承認日などの標準化された形式になっていることを確認した。この徹底的なレビューは、継続的な改善とISMS要件への準拠が必要な領域を特定することを目的としていた。この文書は、監査チームとCyberACryptが初期監査結果と注意が必要な領域を理解する上で非常に重要であった。

監査チームは、主要な関係者へのインタビューも実施することに決定しました。この決定の目的は、マネジメントシステムがISO/IEC 27001の要求事項に準拠しているかどうかを検証するための信頼できる監査証拠を収集することでした。CyberACryptのあらゆるレベルの関係者に対話することで、監査チームは貴重な洞察を得るとともに、ISMSの導入状況と有効性について理解を深めることができました。

第1段階の監査報告書では、いくつかの重要な懸念事項が明らかになりました。適用範囲宣言書（SoA）およびISMSポリシーには、リスク評価の不備、アクセス制御の不足、定期的なポリシー見直しの欠如など、複数の点で不備がありました。これを受け、CyberACryptはこれらの不備に対処するため、直ちに行動を起こしました。迅速な対応と戦略文書の改訂は、コンプライアンス達成への強いコミットメントを示すものでした。

監査チームのサイバーセキュリティに関する知識のギャップを埋めるために導入された技術専門家は、リスク評価方法論の欠陥を特定し、ネットワークアーキテクチャをレビューする上で重要な役割を果たしました。これには、ファイアウォール、侵入検知および防御システム、その他のサイバーセキュリティ対策の評価、ならびにCyber ACryptが外部および内部の脅威をどのように検知、対応、復旧するかの評価が含まれます。ジョンの監督の下、技術専門家は監査結果をCyber ACryptの担当者に伝えました。しかし、監査チームは、被監査企業からコンサルティング料を受け取ったため、専門家の客観性が損なわれた可能性があることを発見しました。監査プロセス中の技術専門家の行動を考慮し、監査チームリーダーはこの問題を認証機関と話し合うことにしました。

上記のシナリオに基づいて、以下の質問に答えてください。

監査の第一段階において、監査チームはどの活動を正しく実施できなかったか？

A. 情報セキュリティポリシーや運用手順の確認を含め、オンサイトイベントの準備を行う。

B. サイバー暗号ポリシーの管理責任を評価することにより、現場活動を実施する。

C. 監査結果の第一段階が記録されておらず、関連する証拠や裏付けとなる文書が含まれていませんでした。

Answer: C ([メッセージを残す](#))

包括的かつ詳細な徹底分析

C. 正解：

監査チームは調査結果を文書化したが、このシナリオでは十分な裏付けとなる証拠が含まれていたかどうかは確認できない。

ISO 19011:2018では、監査結果を適切に文書化し、証拠に基づいて正当化することが求められています。

証拠を文書化しないと、監査の信頼性が低下する。

A. 不正解：

監査に備えて方針や手順を見直すことは、適切な手順である。

B. 不正解：

ISMS（情報セキュリティマネジメントシステム）のコンプライアンスに関する経営陣の責任を評価することは、ステージ1における必須の手順です。

関連規格参照：

ISO/IEC 27001:2022 条項9.2（内部監査）

最新問題: 274

リストを使用する利点を説明する選択肢を2つ選んでください。

A. 各レビューで同じリストが使用されるため、レビューは不要です。

B. 指定された面接対象者を制限する

C. 関連する監査追跡への準拠を確保する

D. 監査計画が確実に実施されるようにする

E. レビュー時間を短縮

F. 必要であればリストを変更しないでください。

Answer: C,D ([メッセージを残す](#))

チェックリストは、監査人が監査の目的と範囲に関連する情報を収集し、検証するのに役立つツールです。チェックリストには、次のような利点があります。

* 関連する監査証拠が確実に追跡されるようにする :チェックリストは、監査対象基準の適合性または不適合性を裏付ける証拠の出所を特定し、追跡するのに役立ちます。また、監査の重要な側面を見落としたり、漏らしたりすることを防ぐのにも役立ちます。

監査計画の確実な実施 :チェックリストは、監査担当者が監査計画に従って作業を進めるのに役立ちます。監査計画には、監査の目的、範囲、基準、スケジュール、役割、責任など、監査の手順と詳細が記載されています。また、監査担当者が時間とリソースを効果的かつ効率的に管理するのにも役立ちます。

その他の選択肢はチェックリストを使用する利点ではなく、むしろ次の点である。

* 見直しを行わずにすべての監査で同じチェックリストを使用すること :これはチェックリストを使用する際の欠点であり、硬直的で非効率な監査アプローチにつながる可能性があります。チェックリストは、監査対象者および監査基準の状況、リスク、変更点を考慮して、個々の監査に合わせてカスタマイズおよび調整する必要があります。また、チェックリストの妥当性と関連性を確保するために、定期的に見直しと更新を行う必要があります。

* インタビュー対象者を指名された関係者に限定すること :これはチェックリストを使用する際の欠点であり、監査の範囲と深さを制限してしまう可能性があります。チェックリストは、監査担当者が監査にとって貴重な証拠や洞察を提供する可能性のある、その他の関連関係者や情報源にインタビューすることを妨げるものであってはなりません。

チェックリストは、制約としてではなく、あくまでも指針として使用すべきです。

監査期間の短縮 :これは必ずしもチェックリストの使用による利点とは限りません。被監査企業のISMSの複雑さ、規模、成熟度、証拠の入手可能性と質、監査員の能力と経験、監査員と被監査企業間の協力とコミュニケーションのレベルなど、さまざまな要因に左右されるからです。チェックリストは効率性と組織性を向上させることで監査期間の短縮に役立つ場合もありますが、より多くの証拠や検証が必要となることで監査期間が長くなる可能性もあります。

* 必要に応じてチェックリストから逸脱しないこと :これはチェックリストを使用する際の欠点であり、表面的な、あるいは不完全な監査につながる可能性があります。チェックリストは、監査中に発生した問題や懸念事項（チェックリストに含まれていない場合でも）を監査担当者が調査・検討することを妨げるものであってはなりません。チェックリストはあくまで補助的なものであり、代替となるものではありません。

参考文献 :

* ISO/IEC 27001:2022 リードオーディター（情報セキュリティマネジメントシステム）の目的と内容は、Quality.orgおよびPECBによるものです。

* ISO 19011:2018 マネジメントシステムの監査に関する指針 [6.2.2項]

最新問題: 275

您詢問 IT 經理，為什麼組織仍在使用行動應用程序，而個人資料加密和假名化測試卻失敗了？此外，服務經理是否有權批准測試

IT經理解釋口，根據軟體安全管理程序，測試結果應由他批准加密和假名功能失敗的原因是這些功能嚴重降低了系統和服務效能。需要額外 150% 的資源來滿足這一點。服務經理同意存取控制足夠好並且可以接受。這就是服務經理簽署批准書的原因。

您對醫務人員的手機進行採樣，發現安裝了ABC 的醫療保健移動應用程序，版本1.01。你發現1.01版本沒有測試記錄。

IT經理解釋口，由於勒索軟體攻擊頻繁，外包行動應用開發公司對受測軟體進行了免費小幅更新，並對更新後的軟體進行了緊急發布，並口頭保證不會對安全造成任何影響

以他20年的資訊安全經驗來看，沒有必要重新測試

您正在準備審核結果 請選擇兩個正確的選項。

A. 不存在不合格項 (NC)。IT 經理證明他完全有能力。（與第2條相關）

B. 存在不合格項 (NC)。IT 經理不遵守軟體安全管理程序。（與第8.1 條相關，控制措施A.8.30）

C. 存在不合格項 (NC)。組織不控制計劃的變更並審計非預期變更的後果。（與第1條相關）

D. 還有改進的機會 (OI)。該組織根據其提供的免費服務的範圍選擇外部服務提供者。（與第8.1 條相關，控制措施A.5.21）

E. 不存在不合格項 (NC)。IT 經理展現了良好的領導能力。（與條款相關

5.1，控制5.4）

F. 還有改進的機會 (OI)。IT 經理應根據適當的測試做出是否繼續提供服務的決定。（與第8.1 條相關，控制措施A.8.30）

Answer: (解答を表示する)

ISO 27001:2022 附屬書 A 管理 8.30 によれば、組織は、情報セキュリティ管理システムに関連する外部提供のプロセス、製品、またはサービスが管理されていることを保証しなければなりません。これには、コードの所有権と知的財産権をカバーするライセンス契約の開発と締結、および附屬書 A 8.25 および 8.29 に従った安全な設計とコーディングに関連する適切な契約要件の実装が含まれます。12 この場合、組織と開発者はセキュリティ テストを実施しましたが、失敗しました。これは、附屬書 A 8.29 の安全な設計とコーディングの要件が満たされていないことを示しています。IT マネージャーは、暗号化と匿名化機能がシステムとサービスのパフォーマンスを低下させたため失敗したこと、そしてこれをカバーするために追加の 150% のリソースが必要であることを説明しています。しかし、これは、ソフトウェア セキュリティ管理手順に従ってテストを承認する権限を持たないサービス マネー

ジャーによるテスト結果の受け入れを正当化するものではありません。サービスマネージャーは、プロセスの責任者であるITマネージャーと協議し、不適合および是正措置の処理手順に従うべきでした。アクセス制御のみに基づいてサービスを継続するというサービスマネージャーの決定は、モバイルアプリによって処理される個人データの機密性、完全性、および可用性を損なうリスクに組織をさらすことになります。したがって、条項8.1、管理A.8.30に不適合 (NC)があります。

ISO 27001:2022 条項 8.1 によれば、組織は情報セキュリティ要件を満たすために必要なプロセスを計画、実装、管理し、条項 8.1 で決定されたアクションを実行する必要があります。

6.1. 組織は、計画された変更を管理し、意図しない変更の結果をレビューし、必要に応じて悪影響を軽減するための措置を講じるものとする。12 この場合、組織は、頻繁なランサムウェア攻撃に対応して外部委託の開発者が提供したマイナーアップデートである、モバイルアプリのバージョン 1.0 からバージョン 1.01 への計画された変更を管理していなかった。IT マネージャーは、開発者が更新されたソフトウェアの緊急リリースを実行し、セキュリティ機能に影響はないと口頭で保証したと説明している。

しかしながら、これだけでは、変更が適切に評価、テスト、文書化され、展開前に承認されることを保証するには不十分です。ITマネージャーは、変更管理プロセスと手順に従い、更新されたソフトウェアがセキュリティ要件を満たし、新たな脆弱性やリスクを導入していないことを検証する必要があります。ITマネージャーが20年間の情報セキュリティ経験と開発者の口頭保証に頼ることは、ソフトウェアの再テストを省略する正当な根拠にはなりません。したがって、条項8.1に不適合 (NC)があります。

参考文献：

1: ISO/IEC 27001:2022 リードオーディター（情報セキュリティマネジメントシステム）コース（CQIおよびIRCA認定トレーニング1）2: ISO/IEC 27001 リードオーディタートレーニングコース（RECB 2）

最新問題: 276

あなたは経験豊富なISMS監査チームリーダーです。第三者監視監査の実施中に、被監査対象者がISO/IEC 27001リスクマネジメント要件を理解しているかどうかをテストすることにしました。

あなたは彼女に一連の質問をし、彼女の答えは「それは本当です」か「それは間違いです」のどちらかです。次の記述のうち、彼女が「それは本当です」と答えるべき4つの記述はどれですか？

- A. リスク評価の結果は保管しなければならない。
- B. リスク特定。情報セキュリティリスクの深刻度を判断するために使用されます。
- C. ISO/IEC 27001は、リスク管理に対する一般的なアプローチを提供します。
- D. 組織は、特定された各ビジネスリスクに対してリスク管理計画を策定しなければならない。
- E. 組織は、情報セキュリティリスクを排除するために、リスク管理プロセスを導入する必要があります。
- F. 組織のリスク管理プロセスの最初の段階は、情報セキュリティリスク評価であるべきです。
- G. リスク評価は毎月実施すべきである。
- H. 重大な変更の後にはリスク評価を実施すべきである。

Answer: A,C,D,H (メッセージを残す)

ISO/IEC 27001 のリスク管理要件によれば、次の 4 つの記述は正しいです。12 リスク評価の結果は保持されなければなりません。これは、ISO/IEC 27001:2022 の 8.2.3 項で、組織が情報セキュリティリスク評価プロセスとその結果の文書化された情報を保持することを要求しているためです。12 ISO/IEC 27001 は、リスク管理の概要アプローチを提供します。これは、ISO/IEC 27001:2022 の 6.1.2 項で、リスク基準の設定、リスクの評価、リスクへの対処、リスクの監視とレビューを含む情報セキュリティリスク管理プロセスの一般的な手順が規定されているためです。12 組織は、特定されたすべてのビジネスリスクに対してリスク対処計画を作成する必要があります。これは、ISO/IEC 27001:2022 の条項 6.1.3 で、組織が許容できないリスクに対処するために講じる措置、責任、予定日、および必要なリソースを定義するリスク処理計画を作成することが要求されているためです 12 リスク評価は、重大な変更の後に実施する必要があります。これは、ISO/IEC 27001:2022 の条項 8.2.4 で、組織が計画された間隔で、または重大な変更が発生したときにリスク評価を見直して更新することが要求されているためです 12 ISO/IEC 27001 のリスク管理要件によると、次の 4 つの記述は誤りです。

リスク識別は、情報セキュリティリスクの重大度を判断するために使用されます。これは誤りです。リスク識別は、情報セキュリティリスク管理プロセスに関連する資産、脅威、脆弱性、および既存の制御を特定するために使用されます。情報セキュリティリスクの重大度は、リスクシナリオの可能性と影響を評価するリスク分析によって決定されます。12 組織は、情報セキュリティリスクを排除するためにリスク処理プロセスを運用する必要があります。これは誤りです。組織は、情報セキュリティリスクを処理するために、回避、移転、軽減、または受容の 4 つのオプションから選択できます。組織は、すべての情報セキュリティリスクを排除する必要はなく、リスク基準に従って受け入れられないものだけを排除すればよいのです。12 組織のリスク管理プロセスの最初のフェーズは、情報セキュリティリスク評価であるべきです。これは誤りです。組織のリスク管理プロセスの最初のフェーズは、リスク管理ポリシー、目的、範囲、役割、責任、および基準を定義するリスク管理フレームワークを確立することです。情報セキュリティリスク評価は、リスク管理プロセスの 2 番目のフェーズです。12 リスク評価は、毎月実施する必要があります。これは誤りです。ISO/IEC 27001では、リスク評価を実施する固定頻度は定められていません。組織は、リスク許容度、リスクプロファイル、運用状況に基づいて、リスク評価の見直しと更新の適切な間隔を決定する必要があります。12 参照:

1: ISO/IEC 27001:2022 リードオーディター（情報セキュリティマネジメントシステム）コース（CQIおよびIRCA認定トレーニング1）2: ISO/IEC 27001 リードオーディタートレーニングコース（RECB 2）

最新問題: 277

あなたは経験豊富なISMS監査チームリーダーです。訓練を受けた監査員から、実施する必要のある監査の種類について確認するため、あなたに連絡がありました。

以下の監査の種類と説明を照合してください。

フォームに入力するには、入力したい空白部分をクリックして 「In fed」をハイライト表示し、下のオプションから適切なテキストをクリックしてください。または、各オプションを対応する空白部分にドラッグすることもできます。

1. Also known as a first party audit, this type of audit involves an organisation auditing itself

2. A third party audit which assesses an organisation's conformity with every clause of a Standard

3. An audit whose scope requires the assessment of two or more Standards

4. An audit carried out at a single auditee by two or more auditing organisations

5. An audit carried out to verify the effectiveness of corrections, corrective action, and agreed opportunities for improvement

6. An audit forming part of a programme of certification body audits in which elements of the auditees' information system management system will be examined

A joint audit

A surveillance audit

An internal audit

A combined audit

A follow-up audit

A certification audit

Answer:

1. Also known as a first party audit, this type of audit involves an organisation auditing itself

2. A third party audit which assesses an organisation's conformity with every clause of a Standard

3. An audit whose scope requires the assessment of two or more Standards

4. An audit carried out at a single auditee by two or more auditing organisations

5. An audit carried out to verify the effectiveness of corrections, corrective action, and agreed opportunities for improvement

6. An audit forming part of a programme of certification body audits in which elements of the auditees' information system management system will be examined

An internal audit

A certification audit

A combined audit

A joint audit

A follow-up audit

A surveillance audit

A joint audit

A surveillance audit

An internal audit

A combined audit

A follow-up audit

A certification audit

Explanation:

1. Also known as a first party audit, this type of audit involves an organisation auditing itself

2. A third party audit which assesses an organisation's conformity with every clause of a Standard

3. An audit whose scope requires the assessment of two or more Standards

4. An audit carried out at a single auditee by two or more auditing organisations

5. An audit carried out to verify the effectiveness of corrections, corrective action, and agreed opportunities for improvement

6. An audit forming part of a programme of certification body audits in which elements of the auditees' information system management system will be examined

An internal audit

A certification audit

A combined audit

A joint audit

A follow-up audit

A surveillance audit

最新問題: 278

文を最も適切に完成させる単語を選びなさい。

単語一つで文を完成させるには、完成させたい空白部分をクリックして赤くハイライト表示し、表示されるオプションから「アプリテキスト」をクリックします。または、オプションを適切な空白部分にドラッグすることもできます。

"An accredited certification assures the of the .

 (Ctrl) ▾

Answer:

"An accredited certification assures the of the .

 (Ctrl) ▾

Explanation:

監査チームの能力と認証機関による決定 マネジメントシステムの監査および認証を提供する機関の要求事項を規定するISO/IEC 17021-1によれば、認定認証とは、認証機関が認定機関によって、その能力、公平性、およびパフォーマンス能力を実証するために、認められた基準に基づいて評価されたことを意味します1。したがって、認定認証は、ISO 19011およびISO/IEC 27001:2022に従って監査を実施する監査チームの能力、および監査証拠と調査結果に基づいて認証を付与または維持する認証機関による決定を保証します2。参照 :ISO/IEC

17021-1:2015 - 適合性評価 - マネジメントシステムの監査及び認証を提供する機関に対する要求事項 - 第 1 部 : 要求事項 ISO/IEC 27001:2022 主任審査員 (情報セキュリティマネジメントシステム)| CQI | IRCA

最新問題: 279

下列哪兩個選項不參與第一方審核？

- A. 認證機構審核員
- B. 來自認證機構的審核小組
- C. 經過CQI及IRCA認證的審核員
- D. 諮詢機構的審核員
- E. 接受過 CQI 和 IRCA 計畫訓練的審核員
- F. 在組織中接受過訓練的審核員

Answer: A,B ([メッセージを残す](#))

A first-party audit is an internal audit in which the organization's own staff or contractors check the conformity and effectiveness of the ISMS. A certification body auditor and an audit team from an accreditation body are external auditors who conduct audits for the purpose of certification or accreditation. They do not participate in a first-party audit, but rather in a third-party audit. Reference: First & Second Party Audits - operational services, The ISO 27001 Audit Process | Blog | OneTrust, The ISO 27001 Audit Process | A Beginner's Guide - IAS USA

最新問題: 280

場景 7 Lawsy 是一家領先的律師事務所， 在新澤西州和紐約市設有辦公室。它擁有 50 多名律師， 為商業法、智慧財口權、銀行和金融服務領域的客口提供完善的法律服務。他們相信， 由於他們致力於實施資訊安全最佳實踐並跟上技術發展的步伐， 他們在市場上佔據了有利的地位。

Lawsy 已經嚴格實施、評估和進行 ISMS 口部審核兩年了。

現在， 他們已向知名且口得信賴的認證機構SMA申請ISO/IEC 27001認證。

在第一階段審核期間， 審核小組審口了實施過程中所建立的所有ISMS 文件。

他們還審口和評估了管理審口和口部審計的記錄。

Lawsy 提交了證據記錄， 表明在必要時對不合格項採取了糾正措施， 因此審核組約談了口部審核員訪談透過提供對口部稽核計畫和程序的詳細了解， 驗證了口部稽核的充分性和頻率。

審計小組繼續驗證戰略文件， 包括資訊安全政策和風險評估標準。在資訊安全政策審口期間， 團隊注意到描述治理框架（即資訊安全政策）的記錄資訊與程序之間存在不一致。

儘管允許員工將筆記型電腦帶到工作場所之外， 但Lawsy 並沒有製定有關在這種情況下使用筆記型電腦的程序。此政策僅提供有關筆記型電腦使用的一般資訊。該公司依靠員工的常識來保護筆記型電腦中儲存的資訊的機密性和完整性。該問題已記錄在第一階段審計報告中。

完成第一階段審核後， 審核組長準備了審核計劃， 其中規定了審核目標範圍、標準和程序。

在第二階段審核期間， 審核小組約談了資安經理， 資安經理起草了資訊安全政策。他透過指出 Lawsy 每三個月舉辦一次強制性資訊安全培訓和意識課程來證明第一階段中確定的問題的合理性。

面談後， 審核小組檢口了15 份員工培訓記錄（共50 份）， 得出的結論是awsy 符合 ISO/IEC 27001 有關培訓和意識的要求。為了支持這個結論， 他們影印了檢口過的員工訓練記錄。

根據上述場景， 回答以下問題：

審計小組複印了所檢口的員工培訓記錄以支持他們的結論。審計團隊在採取此行動之前是否應該獲得 Lawsy 的批准？請參口場景 7。

A. 是的。審核小組在驗證所有情況下流程的存在時（包括做筆記和影印文件時）應獲得受審核方的批准。

B. 是的， 如果受審核方同意， 審核小組可以影印審核期間觀察到的文件。

C. 不可以， 審核小組有權影印文件， 以驗證某份文件是否符合審核標準。

Answer: B (メッセージを残す)

Yes, the audit team should obtain approval from Lawsy before photocopying documents. This is a best practice to ensure that the auditee agrees to the duplication of documents, which might contain sensitive or confidential information. Although auditors can observe and note down information, copying documents typically requires explicit permission to maintain trust and ensure compliance with confidentiality agreements. References: ISO 19011:2018, Guidelines for auditing management systems

最新問題: 281

あなたは、医療サービスを提供する介護施設の情報セキュリティ管理システム（ISMS）監査を実施しています。

監査計画の次のステップは、情報セキュリティインシデント管理プロセスを検証することです。

ITセキュリティマネージャーは、情報セキュリティインシデント管理手順（文書参照：ISMS_L2_16、バージョン4）について説明します。

文書を精査している際に、「情報セキュリティ上の脆弱性、インシデント、またはインシデントは、発見後1時間以内に担当者（PoC）に報告しなければならない」という記述に気づきました。従業員への聞き取り調査の結果、脆弱性、インシデント、またはインシデント」という表現の意味について、従業員間で認識のずれがあることが判明しました。

ITセキュリティマネージャーは、6か月前に「情報セキュリティの取り扱い」に関するオンライン研修ワークショップが開催されたと説明した。回答者全員がワークショップに参加し、レポート作成演習とコース評価に合格した。監査証拠をさらに収集するために、他の領域についても調査したいと考えています。有効な監査証拠の範囲外となる項目を3つ選択してください。

A. 情報セキュリティ障害発生時に情報セキュリティを維持するために、情報セキュリティインシデントが発生する領域を隔離する方法に関する証拠をさらに収集する（制御A.5.29に関連）

B. 適切な経路を通じて情報セキュリティインシデントを報告する方法に関する証拠をさらに収集する（管理策A.6.8に関連）

C. 組織が情報セキュリティインシデント対応訓練をどのように実施し、その有効性をどのように評価しているかについて、より多くの証拠を収集する。（7.2項に関連）

- D. 組織が情報セキュリティインシデントから学び、改善していく方法を示すための証拠をさらに収集する。（管理策A.5.27に関連）
- E. 組織が脆弱性監視を担当する連絡窓口（PoC）をどのように管理しているかについて、より多くの証拠を収集する。（セクション8.1に関連）
- F. 組織が事業継続計画をどのようにテストしているかについて、より多くの証拠を収集する。（管理策A.5.30に関連）
- G. 情報セキュリティポリシーに適切な用語と定義が含まれているかどうかを判断するために、さらなる証拠を収集する。（管理項目B.32に関連）
- H. ISO 27035（情報セキュリティインシデント管理）を内部監査基準として使用すべきかどうかを判断するために、さらなる証拠を収集する。（8.13項に関連）

Answer: E,G,H (メッセージを残す)

有効な監査証拠とはみなされない3つの選択肢は以下のとおりです。

組織が脆弱性を監視する連絡窓口（PoC）をどのように管理しているかについて、より多くの証拠を収集する。（条項8.1に関連）

情報セキュリティポリシーに用語と定義が含まれているかどうかについて、さらに証拠を収集してください。
（管理項目B.32に関連）

*ISO 27035（情報セキュリティインシデント管理）が内部監査基準として使用されているかどうかを判断するために、より多くの証拠を収集してください。（8.13項に関連）これらのオプションは、監査の焦点である情報セキュリティインシデント管理プロセスに直接関連していないため、有効な監査証拠ではありません。監査証拠は、監査の目的、範囲、および基準に関連している必要があり、監査結果と結論を裏付ける十分かつ信頼できる証拠を提供する必要があります1。

オプションEは無効です。PoCは情報セキュリティインシデント管理プロセスの一部ではなく、情報セキュリティインシデントを適切な当局に報告およびエスカレーションする責任を負う役割だからです2。監査証拠は、組織がPoCをどのように管理するかではなく、PoCがこの機能をどのように実行するかに焦点を当てるべきです。

オプションGは無効です。なぜなら、用語と定義は情報セキュリティインシデント管理プロセスの一部ではなく、組織の情報セキュリティの目的、原則、責任を定義する高レベルの文書である情報セキュリティポリシーの一部だからです3。監査証拠は、情報セキュリティポリシーに用語と定義が含まれているかどうかではなく、情報セキュリティポリシーがどのように伝達、実装、レビューされているかに焦点を当てるべきです。

オプションHは無効です。ISO 27035は情報セキュリティインシデント管理プロセスの一部ではなく、情報セキュリティインシデントを管理するためのベストプラクティスを提供するガイダンス文書だからです4。監査証拠は、組織がISO/IEC 27001の要件をどのように遵守しているかに焦点を当てるべきです。

情報セキュリティインシデント管理に関する2022年の基準であり、内部監査基準としてISO 27035を使用しているかどうかではない。

その他の選択肢は、情報セキュリティインシデント管理プロセスに関連しているため、有効な監査証拠であり、プロセスの適合性と有効性を評価するための有用な証拠を提供できます。例えば、次のようになります。

*オプションAは、情報セキュリティインシデントが発生した領域を隔離および検疫するための手順を確立し、さらなる損害を防ぎ、証拠を保全することを組織に求める管理策A.5.29に関連しているため、有効です。監査証拠では、組織がこれらの手順をどのように実装およびテストしているか、また、障害発生時に情報セキュリティの継続性をどのように確保しているかについての証拠を収集する必要があります。

*オプションBは、情報セキュリティイベントや脆弱性を報告するためのメカニズムを確立し、それらが組織内の適切なレベルにタイムリーに伝達されることを保証することを組織に求める管理策A.6.8に関連しているため、有効です。監査証拠には、組織がこれらのメカニズムをどのように定義して使用しているか、また報告プロセスをどのように監視およびレビューしているかについての証拠を収集する必要があります。

*オプションCは、組織が管理下にあるすべての人に情報セキュリティの意識向上、教育、トレーニングを提供し、これらの活動の有効性を評価することを義務付ける条項7.2に関連しているため有効です。監査証拠には、組織が情報セキュリティのトレーニングニーズをどのように特定するか、トレーニングをどのように提供および記録するか、学習成果とフィードバックをどのように測定するかについての証拠を収集する必要があります。

*オプションDは、組織が情報セキュリティインシデントから学び、再発防止または影響軽減のための是正措置を実施することを要求する管理A.5.27に関連しているため、有効です8。

監査証拠には、組織が情報セキュリティインシデントの根本原因と結果をどのように分析し文書化しているか、是正措置をどのように特定し実施しているか、そしてこれらの措置の有効性をどのように検証しているかに関する証拠を収集する必要がある。

*オプションFは、重大な情報セキュリティインシデントが発生した場合に情報および情報処理施設が利用可能であることを保証するため、組織が事業継続計画を策定および維持することを義務付ける管理策A.5.30に関連しているため有効です9。監査証拠には、組織が事業継続計画をどのように策定および更新するか、計画をどのようにテストおよびレビューするか、計画について関係者にどのように伝達およびトレーニングするかについての証拠を収集する必要があります。

参考文献：

- 1: ISO 19011:2018、6.2;
- 2: ISO/IEC 27001:2022、A.6.8.1;
- 3: ISO/IEC 27001:2022、5.2;
- 4 :ISO/IEC 27035:2016、序論；
- 5: ISO/IEC 27001:2022、A.5.29;

- 6: ISO/IEC 27001:2022、A.6.8;
- 7: ISO/IEC 27001:2022、7.2;
- 8: ISO/IEC 27001:2022、A.5.27;
- 9: ISO/IEC 27001:2022、A.5.30;
- 10: ISO 19011:2018;
- 11: ISO/IEC 27001:2022;
- 12: ISO/IEC 27001:2022;
- 13: ISO/IEC 27035:2016;
- 14: ISO/IEC 27001:2022;
- 15: ISO/IEC 27001:2022;
- 16: ISO/IEC 27001:2022;
- 17: ISO/IEC 27001:2022;
- 18: ISO/IEC 27001:2022

最新問題: 282

文を最も適切に完成させる単語を選びなさい。

文を適切な単語で完成させるには、完成させたい空欄をタップして赤くハイライト表示し、下の選択肢から適切なテキストをタップしてください。または、選択肢を適切な空欄にドラッグすることもできます。

It is the sole responsibility of a third-party audit team leader to .

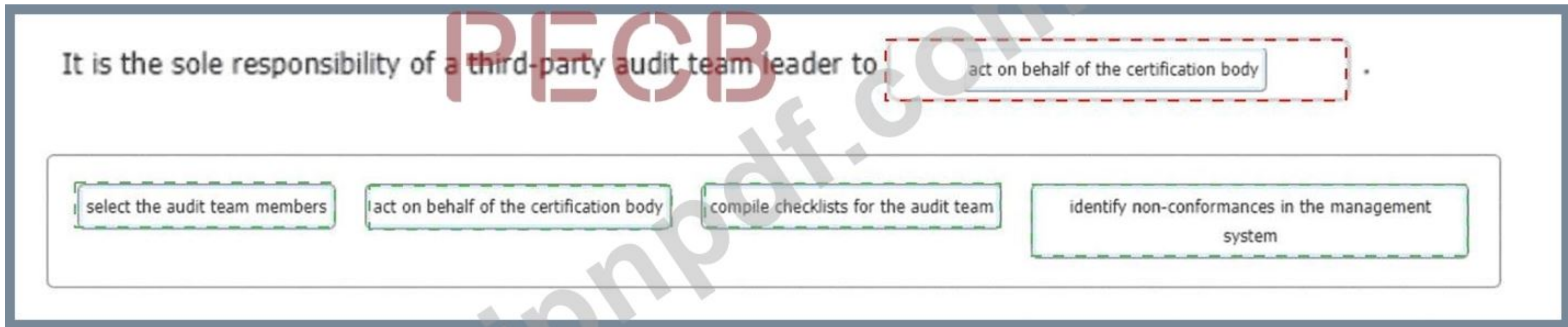
select the audit team members

act on behalf of the certification body

compile checklists for the audit team

identify non-conformances in the management system

Answer:



Explanation:

It is the sole responsibility of a third-party audit team leader to act on behalf of the certification body .

- * 第三者監査チームリーダーとは、認証機関など、他の組織に認証または認定サービスを提供する外部組織に代わって監査を実施する監査チームを率いる人物です12。
 - 第三者監査チームリーダーの主な責任の1つは、認証機関の代理として行動することであり、これは監査プロセス中に認証機関の利益、方針、手順を代表することを意味します12。
 - 認証機関の代理として行動するには、監査依頼者および被監査者とのコミュニケーション、監査の計画と実施、監査結果の報告と評価、認証または認定の決定に関する勧告を行うことが含まれます12。
 - * 認証機関の代理として行動する場合、監査プロセス全体を通して職業上の誠実さ、公平性、機密保持、および能力を維持することも求められます12。
- 参考文献：
- * ISO 19011:2022 マネジメントシステムの監査に関する指針
 - * ISO/IEC 17021-1:2022 適合性評価—マネジメントシステムの監査及び認証を行う機関に対する要求事項—第1部：要求事項

最新問題: 283

CMMとは何の略ですか？

- A. 能力成熟度マトリックス
- B. 能力成熟度マトリックス
- C. 能力成熟度モデル
- D. 有能で成熟したモデル

Answer: (解答を表示する)

能力成熟度モデル（CMM）は、効果的なソフトウェアプロセスの主要要素を記述するフレームワークです。ソフトウェア開発組織の成熟度を、初期段階から最適化段階まで5段階に分類しています。CMMIは、組織が現在のプロセス能力レベルを評価し、改善すべき領域を特定するのに役立ちます1。参照：ISO/IEC 27001:2022 主任審査員 - IECB

最新問題: 284

ISMSの適用範囲に関する以下の選択肢のうち、正しいものはどれですか？

- A. ISMSの適用範囲は記録情報として提供されるべきである。
- B. ISMSの範囲は継続的な改善を保証するものでなければならない。
- C. ISMSの範囲は、組織の戦略的方向性と整合していなければなりません。

Answer: A (メッセージを残す)

ISO/IEC 27001によると、ISMSの適用範囲は定義され、文書化されなければなりません。この文書には、情報セキュリティマネジメントシステムの範囲と適用範囲を含める必要があり、これにより、ISMSの対象となる情報、場所、および資産を明確にすることができます。

最新問題: 285

あるサイバーセキュリティ企業が、機密ファイルへのアクセスを許可された担当者のみに限定するアクセス制御ソフトウェアを導入しました。この場合、同社はどのような種類の制御を導入したのでしょうか？

- A. 予防と対策
- B. 探偵制御
- C. 補正制御

Answer: (解答を表示する)

包括的かつ詳細な徹底分析

- A. 予防的制御- 正解。アクセス制御ソフトウェアは、認証および認可メカニズムを適用することにより、不正アクセスを防止するように設計されています。これは、ISO/IEC 27001:2022 附属書A 制御A.5.18 (アクセス権限)に準拠しています。
- B. 検出制御は不正アクセス試行を識別してログに記録しますが、不正アクセスを防止するものではありません。
- C. 是正措置は、セキュリティインシデントが発生した後に実施されます。

最新問題: 286

シナリオ1

Fintiveは、オンライン決済およびセキュリティソリューションを専門とする大手セキュリティサービスプロバイダーです。1999年にトーマス・フィンによってカリフォルニア州サンノゼで設立されたFintiveは、情報セキュリティの向上、不正行為の防止、個人情報 (PII)などのユーザー情報の保護を目指すオンラインビジネスを支援しています。

Fintiveの意思決定および業務プロセスは、過去の事例に基づいており、顧客データを収集し、事例ごとに分類し、分析する。

当初、Fintiveはこのような複雑な分析を行うために多数の従業員を必要としていた。

しかし、技術の進歩に伴い、同社はチャットボットという最新ツールを活用してパターン分析を行い、リアルタイムで不正行為を防止できることに気づきました。このツールは顧客サービスの向上にも役立ちます。

当初のアイデアはソフトウェア開発チームに伝えられ、彼らはこの取り組みを支持し、プロジェクトのリーダーに任命された。彼らはチャットボットを既存のシステムに統合し始め、チャットボットの目標として、チャットによる問い合わせの85%に回答することを設定した。

チャットボットの統合に成功した後、同社はそれを顧客向けにリリースしました。しかし、チャットボットにはいくつかの問題が発生しました。トレーニング段階でのテスト不足とサンプルデータの不足 (クエリパターンを学習するために使用されるべきデータ)が原因で、チャットボットはユーザーのクエリに効果的に応答できませんでした。さらに、無効な入力 (一般的でないピリオドや特殊文字など)に遭遇すると、ランダムなファイルをユーザーに送信してしまうという問題もありました。

そのため、チャットボットは顧客からの問い合わせに効果的に対応することができず、従来のカスタマーサービス担当者の負担を増大させ、顧客の要望に対応することを不可能にしてしまう。

潜在的なリスクを認識したFintiveは、一連の新たな対策を実施することを決定しました。これらの対策には、包括的な監査ログの有効化、異常なアクティビティを検知する自動アラートシステムの設定、定期的なアクセスレビューの実施、およびシステム動作の異常監視が含まれます。その目的は、不正アクセス、エラー、または不審なアクティビティを迅速に特定し、重大な損害が発生する前に潜在的な問題を速やかに検知 調査することでした。

質問

シナリオ1に基づき、Fintiveは特定された問題に対してどのような対策を実施しましたか？

- A. 予防
- B. 探偵
- C. 訂正

Answer: B (メッセージを残す)

正確な抜粋より：

1. 制御タイプの定義 (ISO準拠の理解)

情報セキュリティ管理において：

予防的対策は、事故の発生を未然に防ぐために設計されています。

- * 検知制御は、インシデントや異常が発生した後、または発生時に、それらを特定および検出するように設計されています。
- * 是正措置は、問題が検出された後にそれを修正するために設計されています。

2. Fintiveが実施した管理策の分析

このシナリオでは、Fintiveが以下の制御策を実装したことが明記されています。

- * 包括的な監査ログ
- * 異常な活動を検知する自動アラートシステム
- * 定期的なアクセス審査
- * システムの動作を監視し、異常を検出する

これらのコントロールはすべて、以下の目的で設計されています。

- * 不正アクセスを検出
- * エラーを検出する
- * 不審な活動を検出する
- * 検出後に調査を有効にする

これは、予防的または是正的な対策ではなく、検出的な対策に直接関連するものです。

3. ISO/IEC 27002:2022 - 精密な制御アライメント

実施された管理策は、附属書Aの技術的および組織的な検出管理策に準拠しており、以下のものが含まれる。

- * A.8.15 - ログ記録

ログ記録により、セキュリティイベントの検出と調査が可能になります。

- * A.8.16 - モニタリング活動

監視は、異常な動作や潜在的なセキュリティインシデントを検出するために使用されます。

- * A.5.18 - アクセス権限（定期的な見直し）

アクセスレビューは、不適切または過剰なアクセスを検出します。

これらの制御機能は、チャットボットの誤動作を防ぐものでも、直接的に修正するものでもありません。問題を検出して、適切な対策を講じられるようにするためのものです。

4. 他の選択肢が間違っている理由

- * A. Preventive - IncorrectPreventive controls would include secure coding practices, input validation, sandboxing, or improved testing before release. These were not the controls described.
- * C. Corrective - IncorrectCorrective controls would involve fixing the chatbot logic, retraining the model, or disabling unsafe features. The scenario explicitly focuses on detection and monitoring, not correction.

Auditor Conclusion

Fintive implemented detective controls to identify unauthorized access, errors, and suspicious activity arising from the chatbot's behaviour. This is consistent with ISO/IEC 27001:2022 risk treatment and monitoring requirements.

有効な **ISO-IEC-27001-Lead-Auditor-CN** 問題集は GoShiken.com が提供された合格しやすい ISO-IEC-27001-Lead-Auditor-CN 試験問題集！ GoShiken.com が最新の **ISO-IEC-27001-Lead-Auditor-CN** 試験問題集を提供しています。GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com ISO-IEC-27001-Lead-Auditor-CN 問題集をゲットする人はこちら：
<https://www.goshiken.com/PECB/ISO-IEC-27001-Lead-Auditor-CN-mondaishu.html> (418**30%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 287

あなたは経験豊富なISMS監査チームリーダーで、監査員の研修を指導しています。あなたは彼女に一連の質問をすることで、今後の監査に関する彼女の理解度を確かめることにしました。以下はあなたの質問と彼女の回答です。

彼女はどの4つの質問に正しく答えたか？

A. Q: その後の監査では、新たな不適合を発見すべきでしょうか？ A: はい。

- B.** 質問: その後の監査で、法令違反の問題が効果的に解決されていることを保証すべきでしょうか？ 回答: はい。
- C.** 質問: 合意された改善の機会と是正措置は、フォローアップレビューで考慮されるべきでしょうか？
- 年
- D.** Q: フォローアップ監査の目的は、是正措置、是正対策、および改善機会の完了を確認することですか？ A: はい。
- E.** Q: すべてのレビューにフォローアップレビューが必要ですか？ A: いいえ。
- F.** Q: その後の監査の結果は、最初に不適合を特定した監査チームリーダーに報告すべきでしょうか？ A: はい。
- G.** Q: フォローアップ監査の結果を監査クライアントに報告すべきですか？ A: いいえ。
- H.** Q: 必要に応じて、後続のレビューの結果を別の後続のレビューとして使用できますか？ A: はい。

Answer: ([解答を表示する](#))

フォローアップ監査、特に情報セキュリティマネジメントシステム (ISMS) の文脈におけるフォローアップ監査の理解と、ISO 19011:2018で提供されるガイドラインに基づき、研修中の監査員が正しく回答した質問は以下の4つです。

- B. 質問 :フォローアップ監査は、不適合が効果的に対処されたことを確認するために行うべきですか？ 回答 :はい。これは正しいです。フォローアップ監査の主な目的は、以前の監査で特定された不適合が効果的に対処され、講じられた是正措置が適切かつ効果的であることを確認することです。
- D. 質問 :フォローアップ監査の目的は、是正措置、是正対策、および改善機会の完了を確認することですか？ 回答 :はい。フォローアップ監査は、是正措置および是正対策の完了と有効性を確認することを目的としています。また、初回監査で特定された改善機会の実施状況も検討する場合があります。
- E. Q: すべての監査でフォローアップ監査は必須ですか？ A: いいえ。これは正しいです。フォローアップ監査は、すべての監査で自動的に必須となるわけではありません。通常、フォローアップ監査は、以前の監査で不適合やその他の重大な問題が特定され、是正措置の実施状況と有効性を検証する必要がある場合に実施されます。
- H. Q: フォローアップ監査の結果、必要に応じてさらにフォローアップ監査を実施することは可能ですか？ A: はい。これは起こり得る結果です。フォローアップ監査で是正措置が十分に効果を発揮していないことが判明した場合、または新たな問題が特定された場合は、別のフォローアップ監査を実施する必要があるかもしれません。

研修中の監査員が提供したその他の回答には、説明や修正が必要です。例えば、フォローアップ監査は主に以前に特定された不適合と是正措置に焦点を当てますが、新たな不適合が発見された場合は、それを特定することもあります A)。改善の機会は、是正措置に焦点を絞ったフォローアップ監査よりも、通常監査の範囲内でより重視されます C)。また、フォローアップ監査の結果は、透明性と説明責任を確保するため、通常は監査チームリーダーと監査依頼者の両方に報告されるべきです FとG)。

研修中の監査員が正解した4つの質問は、B、D、E、Hです。

これらの質問と回答は、ISO 19011:2018、6.712項に規定されているフォローアップ監査の定義と目的に合致しています。フォローアップ監査は、前回の監査の結果として講じられた是正措置の完了と有効性を検証するために実施されます B、D)。フォローアップ監査はすべての監査で必須ではありませんが、監査プログラム、監査クライアント、またはその他の利害関係者によって要求される場合があります E)。是正措置が不十分であるか、合意された期間内に完了していない場合、フォローアップ監査の結果は、別のフォローアップ監査となる可能性があります K)。その他の質問と回答は、不正確または無関係です。フォローアップ監査は、新たな不適合を特定しようとするべきではありません。これは、フォローアップ監査の目的ではないためです A)。フォローアップ監査では、合意された改善の機会と是正措置の両方を考慮する必要があります。これらはどちらも前回の監査の結果です。フォローアップ監査の結果は、監査依頼者だけでなく、前回の監査を実施した監査チームリーダー F、G)などの関係者にも報告する必要があります。参照 :1 :ISO 19011:2018、マネジメントシステムの監査に関するガイドライン、6.7項 2 :PECB認定ISO/IEC 27001主任監査員試験準備ガイド、ドメイン6 :ISO/IEC 27001監査の終了

最新問題: 288

シナリオ7 :Lawtsyは、ニュージャージー州とニューヨーク市にオフィスを構える大手法律事務所です。50名以上の弁護士を擁し、企業法務、知的財産、銀行業務、金融サービスといった分野で顧客に包括的な法的サービスを提供しています。同社は、情報セキュリティにおけるベストプラクティスの導入と技術革新への対応に注力することで、市場において確固たる地位を築いていると確信しています。

Lawtsyは、過去2年間、ISMS（情報セキュリティマネジメントシステム）の厳格な導入、評価、および内部監査を実施してきた。

彼らは現在、知名度が高く信頼できる認証機関であるISMAに対し、ISO/IEC 27001認証の申請を行っている。

監査の第一段階では、監査チームは導入プロセス中に作成されたすべてのISMS文書をレビューした。

彼らはまた、経営陣によるレビューや内部監査の記録を精査し、評価した。

Lawtsy社は、不適合に対して必要に応じて是正措置が講じられたことを示す証拠を提出し、これを受けて監査チームは内部監査担当者への聞き取り調査を実施した。この聞き取り調査により、内部監査計画と手順に関する詳細な理解が得られ、内部監査の適切性と頻度が検証された。

監査チームは、情報セキュリティポリシーやリスク評価基準などの戦略文書の検証を継続しました。情報セキュリティポリシーのレビュー中に、チームは、文書化された情報とガバナンスフレームワーク（すなわち情報セキュリティポリシー）を説明する手順との間に矛盾があることに気づきました。

従業員はノートパソコンを職場外に持ち出すことが許可されているものの、Lawtsy社にはその使用に関する明確な手順が定められていません。社内規定にはノートパソコンの使用に関する一般的な情報しか記載されていません。同社は、ノートパソコンに保存されている情報の機密性と完全性を保護するために、従業員の常識に頼っています。この問題は、フェーズ1監査報告書に記載されています。

監査の第1段階が完了した後、監査チームリーダーは監査計画書を作成し、監査の目的、範囲、基準、および手順を概説した。

監査の第2段階では、監査チームは情報セキュリティポリシーを作成したサイバーセキュリティマネージャーにインタビューを行った。マネージャーは、Lawtsy社が3ヶ月ごとに情報セキュリティに関する必須の研修と啓発コースを実施していることを指摘し、第1段階で指摘された問題点の妥当性を証明した。

面接後、監査チームは従業員研修記録50件のうち15件を精査し、Lawtsy社が研修および意識向上に関するISO/IEC 27001の要件を満たしていると結論付けた。この結論を裏付けるため、監査チームは精査した従業員研修記録のコピーを作成した。

上記のシナリオに基づいて、以下の質問に教えてください。

シナリオ7に基づく、Lawtsyはレビューの第2段階を開始する前に何をすべきでしょうか？

A. 第1段階監査の結果は、品質監査に使用されます。

B. コンプライアンスを検証するために組み合わせることができる監査テストプログラムを定義します。

C. 認証機関と監査計画を確認し、承認する。

Answer: C ([メッセージを残す](#))

ステージ2監査を開始する前に、Lawtsyは認証機関と監査計画を確認し、合意する必要があります。これにより、両者がステージ2監査の目的、範囲、手順について合意し、期待値を一致させ、より円滑な監査プロセスを実現できます。

最新問題: **289**

ISMSの標準的な定義は何ですか？

A. これは、組織の評判の実装、確立、レビュー、運用、維持などのビジネス目標を達成するために設計された情報セキュリティシステムのアプローチです。

B. 情報セキュリティ意識を確立、実施、運用、監視、レビュー、維持、および改善するための全社的な事業目標。

C. 組織の情報セキュリティを確立、実装、運用、監視、レビュー、維持、改善するというビジネス目標を達成するために使用されるプロジェクトベースのアプローチ。

D. 組織のビジネス目標を達成するために、組織の情報セキュリティを確立、実装、運用、監視、レビュー、維持、改善するための体系的なアプローチ。

Answer: ([解答を表示する](#)**)**

ISMSの標準的な定義は、組織の情報セキュリティを確立、実装、運用、監視、レビュー、維持、改善して事業目標を達成するための体系的なアプローチです。この定義はISO/IEC 27001:2022の3.17項に示されており、ISMSの主要な構成要素と目的を説明しています。ISMSは継続的な改善を必要とする継続的なプロセスであるため、プロジェクトベースのアプローチではありません。ISMSは組織の目標をサポートするマネジメントシステムであるため、企業全体の事業目標ではありません。ISMSは組織の状況、リスク、コントロール、パフォーマンスを包含するより広範な概念であるため、情報セキュリティの体系的なアプローチではありません。参考文献 :CQI & IRCA ISO

27001:2022主任監査員コースハンドブック、15ページ。ISO

/IEC 27001:2022、条項3.17。

最新問題: **290**

シナリオ9 :UpNetはISO/IEC 27001認証を取得したインターネット企業です。

ISO/IEC 27001認証取得以来、当社の認知度は著しく向上しました。この認証は、UpNefsの事業運営の成熟度と、広く認知され受け入れられている規格への準拠を証明するものです。

しかし、認証はそこで終わりではありません。UpNetは、内部監査を通じて、セキュリティ管理とISMS全体の有効性および効率性を継続的に見直し、強化しています。経営陣は専任の内部監査チームを雇用することに消極的だったため、内部監査機能を外部委託することにしました。この形式の内部監査は、独立性と客観性を確保し、ISMSの継続的な改善のための助言サポートを提供します。

最初の認証監査後まもなく、同社はデータおよびストレージ製品を専門とする新部門を設立した。この部門では、データセンター向けに最適化されたルーターやスイッチ、ネットワーク仮想化やネットワークセキュリティ機器などのソフトウェアベースのネットワーク機器を提供している。これにより、既にISMS認証の対象となっていた他の部門の業務にも変更が生じた。

そのため、UpNetはリスク評価プロセスと内部監査を開始しました。内部監査の結果に基づき、同社は既存および新規のプロセスと管理体制の有効性と効率性を確認しました。

新設された部署がISO/IEC 27001の要件を満たしていたため、経営陣は認証範囲に含めることを決定しました。UpNetは、会社全体を対象とするISO/IEC 27001認証を取得したことを発表しました。

最初の認証監査から1年後、認証機関はUpNefsのISMS（情報セキュリティマネジメントシステム）に対する別の監査を実施した。

この監査は、UpNefsのISMSが規定のISO/IEC 27001の要求事項に準拠しているかどうかを判断し、ISMSの継続的な改善を確保することを目的としていました。監査チームは、認証済みのISMSが引き続き規格の要求事項を満たしていることを確認しました。しかしながら、新設された部署はマネジメントシステムのガバナンスに大きな影響を与えており、さらに認証機関にはこれらの変更について一切通知されていませんでした。そのため、UpNefsの認証は一時停止されました。

上記のシナリオに基づいて、以下の質問に教えてください。

シナリオ9の最後の段落で説明されている監査の種類は何ですか？

A. 監督と監査

B. 内部監査

C. 再認証監査

Answer: A (メッセージを残す)

シナリオ9の最後の段落で説明されている監査は、サーベイランス監査です。この種の監査は、認証を受けたISMSが最初の認証後も規格の要件を満たし続けていることを確認するために定期的 to 実施されます。

最新問題: 291

シナリオ6 :Cyber ACryptは、マルウェア対策やデバイスセキュリティ、資産ライフサイクル管理、デバイス暗号化などのエンドポイント保護サービスを提供するサイバーセキュリティ企業です。同社は、情報セキュリティマネジメントシステム (ISMS) がISO/IEC 27001規格に準拠していることを検証し、優れたサイバーセキュリティへの取り組みを示すため、指定された監査チームリーダーであるジョンが主導する厳格な監査プロセスを受けました。監査業務を引き受けたジョンは、監査計画とチームの役割を概説するための会議をすぐに開催しました。この段階は、チームを監査の目的と範囲に合わせる上で非常に重要でした。しかし、Cyber ACryptのスタッフとの最初のブリーフィングでは、監査の範囲と目的についての理解に大きなギャップがあることが明らかになり、社内での準備上の潜在的な課題が示されました。監査の第1段階の開始に伴い、チームは現場活動の準備を行いました。彼らは、Cyber ACryptの情報セキュリティポリシーと運用手順を含む文書をレビューし、各文書が標準形式に準拠し、作成者識別情報、作成日、バージョン番号、承認日が含まれていることを確認しました。さらに、監査チームは、各文書に、関連する標準条項で要求される情報が含まれていることを確認しました。この段階で、タスクの実行を記述した文書の詳細な監査は不要であることが明らかになり、プロセスが合理化され、チームは重要な領域に集中することができました。現場活動の段階では、チームはCyber ACryptのポリシーの管理責任を評価しました。この徹底的なレビューは、継続的な改善と情報セキュリティマネジメントシステム (ISMS) 要件への準拠を確保することを目的としていました。その後、監査成果の第1段階に関する文書において、監査チームは調査結果を詳細に記述し、第1段階の目標達成に関する結論を強調しました。この文書は、監査チームとCyberACryptが予備的な監査結果と注意が必要な領域を理解する上で非常に重要でした。

監査チームは、主要な関係者への聞き取り調査も実施することにした。この措置は、経営システムがISO規格に準拠しているかどうかを検証するための信頼できる監査証拠を収集することを目的としていた。

IEC 27001 の要求事項。サイバー ACrypt のあらゆるレベルのステークホルダーとのコミュニケーションにより、監査チームは貴重な視点を得ることができ、情報セキュリティ マネジメント システム (ISMS) の実装と有効性についての理解を深めることができました。

第1段階の監査報告書では、いくつかの重要な問題点が明らかになりました。適用範囲宣言書 (SoA) および情報セキュリティマネジメントシステム (ISMS) ポリシーには、リスク評価の不備、アクセス制御の不備、定期的なポリシー見直しの欠如など、複数の点で不備がありました。これを受け、CyberACryptはこれらの不備に対処するため、直ちに行動を起こしました。迅速な対応と戦略文書の改訂は、同社のコンプライアンスに対する強いコミットメントを示すものでした。

監査チームのネットワークセキュリティに関する知識不足を補うために招集された技術専門家は、リスク評価手法の欠陥を特定し、ネットワークアーキテクチャをレビューする上で重要な役割を果たしました。これには、ファイアウォール、侵入検知 防御システム、その他のネットワークセキュリティ対策の評価、およびCyber ACryptが外部および内部の脅威をどのように検知、対応、復旧しているかの評価が含まれていました。ジョンの指導の下、技術専門家は監査結果をCyber ACryptの担当者に伝えました。しかし、監査チームは、専門家が被監査企業からコンサルティング料を受け取っていたため、専門家の客観性が損なわれた可能性がある と指摘しました。監査プロセス中の技術専門家の行動を考慮し、監査チームリーダーは認証機関とこの件について話し合うことにしました。

上記のシナリオに基づいて、以下の質問に教えてください。

質問：

シナリオ6に基づく to 、監査チームによって監査の第1段階におけるインタビューの目的は適切に設定されていたでしょうか？

A. はい、このインタビューの目的は、マネジメントシステムがISO/IEC 27001の要求事項に準拠しているかどうかを確認するための監査証拠を収集することです。

B. いいえ、インタビューの目的がマネジメントシステムの主要業績評価指標 (KPI) と一致していなかったため、監査の有効性が低下しました。

C. いいえ、このインタビューの目的は、被監査者が直面している課題を完全に理解することです。

Answer: A ([メッセージを残す](#))

包括的かつ詳細な解説：

* A. 正解:

* 監査面談の主な目的は、ISO/IEC 27001への準拠を確認することです。

* ISO 19011:2018では、インタビューは監査証拠を収集する方法の一つであると規定されています。

* B. 不正解:

* KPIは業績測定に関係するが、インタビューはコンプライアンスの検証に重点を置く。

* C. 不正解:

* ビジネス上の課題を理解することは二次的なものであり、主な目的はISO/IEC 27001への準拠検証です。

関連規格参照：

* ISO 19011:2018 6.4.6項（監査における面接技法）

最新問題: **292**

あなたは監査プロジェクトの管理、および特定のプロジェクトにおける監査チームの規模と構成の決定を担当します。考慮すべき要素を2つ選択してください。

* 監査範囲と基準

A. 顧客関係

B. 監査チームが監査目標を達成するために必要な総合的な能力

C. 監査チームリーダーの資格

D. 監査費用

E. 被監査者が希望する期間

Answer: ([解答を表示する](#))

12の総合的な能力：

監査範囲と監査基準：監査範囲とは、監査の対象となる場所、プロセス、機能、期間など、監査の範囲と境界を定義するものです。監査基準とは、監査証拠を比較する際の参照基準として使用される一連のポリシー、手順、標準、または要件のことです。監査範囲と監査基準は、監査の複雑さと規模を決定し、ひいては監査の関連するすべての側面を網羅するために必要な監査員の数と専門知識に影響を与えます。

* 監査目的を達成するために必要な監査チームの総合的な能力：監査チームは、監査を効果的かつ効率的に実施し、信頼できる監査結果を提供するために、適切な知識、スキル、経験を備えている必要があります。監査チームの能力には、以下の要素が含まれる必要があります12：

* 一般的な能力：監査の計画、実施、報告、フォローアップなどの監査の原則と方法を適用する能力、および倫理的な行動、公正な表示、専門的な注意、独立性、公平性などの監査人の個人的な行動と特性。

* 専門分野および業界固有の能力: 監査基準と、情報セキュリティ管理システム (ISMS) の要件、情報セキュリティのリスクと管理、法的小および規制上の義務、組織の状況と文化、プロセスと活動、製品とサービスなど、監査対象組織の関連する技術的または業界的側面を理解し、適用する能力。

* 監査チームリーダーの能力：監査活動の調整、監査プログラムマネージャーおよび被監査者とのコミュニケーション、監査関連の問題の解決、監査作業および監査報告書の品質と一貫性の確保など、監査チームと監査プロセスを管理する能力。

監査プログラムの管理責任者は、特定の監査における監査チームの規模と構成を決定する際に、以下の要素を考慮してはならない。なぜなら、それらは監査プロセスにとって無関係または不適切だからである12。

* 顧客との関係：監査チームは、被監査企業またはその他の利害関係者との個人的または職業上の関係に影響を受けてはならない。これは、監査の客観性および公平性を損なう可能性があるためである。監査チームは、監査結果または監査決定に影響を与える可能性のある利益相反または自己利益を避けるべきである。

監査チームリーダーの選任基準：監査チームリーダーは、組織内または監査プログラムにおける役職や地位ではなく、能力と経験に基づいて選任されるべきです。監査チームリーダーは、役職や地位に関わらず、監査チームと監査プロセスを管理する権限と責任を持つべきです。

監査費用：監査費用は、監査チームの規模や構成を決定する際の主要な要素であってはなりません。なぜなら、費用が高すぎると監査の質や有効性が損なわれる可能性があるからです。監査チームは、監査の目的、範囲、基準に従って監査を実施し、正確で信頼性の高い監査結果と勧告を提供するために、十分なリソースと時間を確保する必要があります。

* 被監査者の希望する期間：監査期間は、被監査者の希望や都合ではなく、監査の目的、範囲、基準、および被監査者の都合と協力に基づいて決定されるべきです。監査チームは、徹底的かつ体系的に監査を実施し、十分かつ適切な監査証拠を収集・評価するのに十分な時間を確保する必要があります。

最新問題: **293**

あなたは、医療サービスを提供する高齢者向け介護施設のISMS監査を実施しています。監査計画の次のステップは、情報セキュリティインシデント管理プロセスを検証することです。ITセキュリティマネージャーは、情報セキュリティインシデント管理手順（文書参照ID: ISMS_L2_16、バージョン4）を提示します。

あなたは文書を確認し、「情報セキュリティ上の脆弱性、インシデント、またはインシデントは、発見後1時間以内に連絡担当者（PoC）に報告しなければならない」という記述に気づきました。従業員への聞き取り調査の結果、脆弱性、インシデント、またはインシデント」という用語の意味について、従業員間で認識のずれがあることが判明しました。

ITセキュリティマネージャーは、6か月前に「情報セキュリティの取り扱い」に関するオンライン研修ワークショップが開催されたと説明した。回答者全員が参加し、報告演習とコース評価に合格した。

監査証拠をさらに収集するために、他の領域についても調査を進めたいと考えています。有効な監査証拠ではないものを3つ選択してください。

A. 情報セキュリティ障害が発生した領域を隔離し、障害発生中の情報セキュリティを維持する方法を説明するために、より多くの証拠を収集する（制御A.5.29に関連）。

B. 適切な経路を通じて情報セキュリティインシデントを報告する方法に関する証拠をさらに収集する（管理策A.6.8に関連）。

C. 組織が情報セキュリティインシデント対応訓練をどのように実施しているか、またその有効性をどのように評価しているかについて、より多くの証拠を収集する。（第2項に関連）。

D. 組織が情報セキュリティインシデントから学び、改善していく方法について、より多くの証拠を収集する。（管理策A.5.27に関連）。

E. 組織が脆弱性監視のための連絡窓口（PoC）をどのように管理しているかについて、より多くの証拠を収集する。セクション8.1に関連）。

F. 組織が事業継続計画をどのようにテストしているかについて、より多くの証拠を収集する。（管理策A.5.30に関連）。

G. 情報セキュリティポリシーに用語と定義が含まれているかどうかを判断するために、さらなる証拠を収集する。（管理策A.32に関連）。

H. ISO 27035（情報セキュリティインシデント管理）が内部監査基準として使用されているかどうかを判断するために、より多くの証拠を収集します。

Answer: E,G,H (メッセージを残す)

a.（条項A.13に関連）

Explanation:

有効な監査証拠とはみなされない3つの選択肢は以下のとおりです。

* 組織が脆弱性を監視する連絡窓口（PoC）をどのように管理しているかについて、より多くの証拠を収集する。（条項A.13に関連）。

* 用語と定義が情報セキュリティポリシーに含まれているかどうかについて、より多くの証拠を収集する。（管理策A.32に関連）。

* ISO 27035（情報セキュリティインシデント管理）が内部監査基準として使用されているかどうかを判断するために、より多くの証拠を収集します。（条項A.13に関連）これらのオプションは、監査の焦点である情報セキュリティインシデント管理プロセスに直接関連していないため、有効な監査証拠ではありません。監査証拠は、監査の目的、範囲、および基準に関連している必要があり、監査結果と結論を裏付ける十分かつ信頼できる証拠を提供する必要があります1。

オプションEは無効です。PoCは情報セキュリティインシデント管理プロセスの一部ではなく、情報セキュリティインシデントを適切な当局に報告およびエスカレーションする責任を負う役割だからです2。監査証拠は、組織がPoCをどのように管理するかではなく、PoCがこの機能をどのように実行するかに焦点を当てるべきです。

オプションGは無効です。なぜなら、用語と定義は情報セキュリティインシデント管理プロセスの一部ではなく、組織の情報セキュリティの目的、原則、責任を定義する高レベルの文書である情報セキュリティポリシーの一部だからです3。監査証拠は、情報セキュリティポリシーに用語と定義が含まれているかどうかではなく、情報セキュリティポリシーがどのように伝達、実装、レビューされているかに焦点を当てるべきです。

オプションHは無効です。ISO 27035は情報セキュリティインシデント管理プロセスの一部ではなく、情報セキュリティインシデントの管理に関するベストプラクティスを提供するガイダンス文書だからです4。監査証拠は、組織がISO 27035を内部監査基準として使用しているかどうかではなく、情報セキュリティインシデント管理に関するISO/IEC 27001:2022の要件にどのように従っているかに焦点を当てるべきです。

その他の選択肢は、情報セキュリティインシデント管理プロセスに関連しているため、有効な監査証拠であり、プロセスの適合性と有効性を評価するための有用な証拠を提供できます。例えば、次のようになります。

* オプション A は、情報セキュリティ インシデントが発生した領域を隔離および検疫するための手順を確立し、さらなる損害を防ぎ、証拠を保全することを組織に求める管理策 A.5.29 に関連しているため、有効です。監査証拠では、組織がこれらの手順をどのように実装およびテストしているか、また、障害発生時に情報セキュリティの継続性をどのように確保しているかについての証拠を収集する必要があります。

* オプション B は、情報セキュリティの事象や脆弱性を報告するための仕組みを確立し、それらが組織内の適切なレベルにタイムリーに伝達されるようにすることを組織に求める管理策 A.6.8 に関連しているため有効です。監査証拠では、組織がこれらの仕組みをどのように定義し、使用しているか、また報告プロセスをどのように監視およびレビューしているかについての証拠を収集する必要があります。

- * オプション C は、組織が管理下にあるすべての人に情報セキュリティに関する意識向上、教育、トレーニングを提供し、これらの活動の有効性を評価することを義務付ける条項 7.2 に関連しているため有効です。監査証跡には、組織が情報セキュリティのトレーニングニーズをどのように特定するか、トレーニングをどのように実施および記録するか、学習成果とフィードバックをどのように測定するかについての証拠を収集する必要があります。
- * オプション D は、情報セキュリティ インシデントから学び、再発防止または影響軽減のための是正措置を実施することを組織に求める管理策 A.5.27 に関連しているため、有効です。監査証跡には、組織が情報セキュリティ インシデントの根本原因と結果をどのように分析および文書化しているか、是正措置をどのように特定および実施しているか、そしてこれらの措置の有効性をどのように検証しているかについての証拠を収集する必要があります。
- * オプション F は、組織が重大な情報セキュリティ インシデント 9 が発生した場合に情報および情報処理施設の可用性を確保するために事業継続計画を策定および維持することを義務付ける管理策 A.5.30 に関連しているため、有効です。監査証跡には、組織が事業継続計画をどのように策定および更新しているか、計画をどのようにテストおよびレビューしているか、計画について関係者にどのように伝達およびトレーニングしているかに関する証拠を収集する必要があります。

最新問題: 294

監査計画を作成する際に、認証監査員が要求しない作業文書は次のうちどれか（2）はどれか？

- A. 監査計画
- B. ITマネージャーの職務経歴
- C. リスト
- D. 外部プロバイダー一覧
- E. 模範的なプロジェクト
- F. 組織の財務諸表

Answer: B,F (メッセージを残す)

認証監査の監査計画は、ISO 19011:2018の6.3項（監査活動の準備）およびISO/IEC 27006で定義されています。

主要な監査計画文書には以下が含まれます。

- * 監査計画書（必須 チームリーダー作成）
- * チェックリスト（要件の一貫性と網羅性を確保するための補助ツール）
- * 外部供給業者リスト ISO/IEC 27001附属書A.5.19 - 供給業者との関係およびA.5.20 - 供給業者契約への準拠を確認するために必要）
- * サンプル計画（特にステージ2監査において、サイト、プロセス、または記録全体にわたる証拠のサンプリングが必要な場合に使用）ただし、以下は必須ではありません。
- * B. ITマネージャーの職務経歴 - 担当者の能力は面接や証拠の確認によって検証できますが、監査計画の一環として職務経歴は監査員には必要ありません。ISO 19011では、必要に応じて能力記録へのアクセスのみを要求しており、履歴書へのアクセスは要求していません。
- * F. 組織の財務諸表 - 財務実績は、特定されたリスクまたは契約上の義務に関連する場合を除き、ISMS監査計画の一部ではありません。ISO/IEC 27001は情報セキュリティリスクに焦点を当てており、財務監査への準拠には焦点を当てていません。

ISO 19011:2018 6.3.2項）では、必要な計画入力項目が明確に以下のように定義されています。

監査の目的、範囲、および基準

* 監査チームの役割と責任

* 資源の配分

* 被監査者のISMSに関する情報（例：文書化された範囲、プロセス、外部プロバイダーとの関係、関連する法的/規制上の要件）。人事履歴書や財務諸表の提出が求められるという記述はありません。

最終正解 :BとF

参考文献：

ISO 19011:2018、6.3項（監査活動の準備）

ISO/IEC 27006:2015、第9.2項 ISMS認証機関に対する監査計画要件）

Valid ISO-IEC-27001-Lead-Auditor-CN Dumps shared by GoShiken.com for Helping Passing ISO-IEC-27001-Lead-Auditor-CN Exam! GoShiken.com now offer the **newest ISO-IEC-27001-Lead-Auditor-CN exam dumps**, the GoShiken.com ISO-IEC-27001-Lead-Auditor-CN exam **questions have been updated** and **answers have been corrected** get the **newest** GoShiken.com ISO-IEC-27001-Lead-Auditor-CN dumps with Test Engine here:
<https://www.goshiken.com/PECB/ISO-IEC-27001-Lead-Auditor-CN-mondaishu.html> (418 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)