ISACA.CISA-JPN.v2025-06-30.q593

試験コード:	CISA-JPN
試験名称:	Certified Information Systems Auditor (CISA日本語版)
認定資格:	ISACA
無料問題数:	593
バージョン:	v2025-06-30
アクセス数:	212
ページビュー数:	5930
https://www.jpnpdf.com/ISACA.CISA-JPN.v2025-06-30.q593-mondaishu.html	

最新問題: **1**
最近発見されたゼロデイ攻撃の影響を管理する上で、最初に実行すべきステップは次のうちどれですか?
A. 攻撃の可能性を評価する
B. 潜在的な損害の推定
C. 脆弱な資産の特定
D. 脆弱性の影響の評価
Answer: C (メーッセージを残す**)**
The first step in managing the impact of a recently discovered zero-day attack is to identify vulnerable assets.
A zero-day attack is a cyberattack that exploits a previously unknown or unpatched vulnerability in a software or system, before the vendor or developer has had time to fix it. Identifying vulnerable assets is crucial for managing the impact of a zero-day attack, because it helps to determine the scope and severity of the attack, prioritize the protection and mitigation measures, and isolate or quarantine the affected assets from further damage or compromise. The other options are not the first steps in managing the impact of a zero-day attack, because they either require more information about the vulnerable assets, or they are part of the subsequent steps of assessing, responding, or recovering from the attack. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.4

最新問題: **2**
エンタープライズ リソース プランニング (ERP) システムの監査中に、IS 監査人はアプリケーション パッチが実稼働環境に適用されていることを発見しました。IS 監査人にとって最も重要なのは、次の承認を確認することです。
A. 情報セキュリティ担当者。
B. プロジェクトマネージャー。

C. システム管理者。
D. 情報資産の所有者。
Answer: B (メーッセージを残す**)**

最新問題**: 3**
IS 品質保証 (OA) グループは、次の責任を負います。
A. プログラムの変更が確立された標準に準拠していることを確認します。
B. データが偶発的に漏洩しないように保護するための手順を設計します。
C. システム処理から受信した出力が完了していることを確認します。
D. コンピュータ処理タスクの実行を監視します。
Answer: A (メーッセージを残す**)**
The IS quality assurance (QA) group is responsible for ensuring that program changes adhere to established standards. Program changes are modifications made to software applications or systems to fix errors, improve performance, add functionality, or meet changing requirements. Program changes should follow established standards for documentation, authorization, testing, implementation, and review. The IS QA group is responsible for verifying that program changes comply with these standards and meet the expected quality criteria. Designing procedures to protect data against accidental disclosure; ensuring that the output received from system processing is complete; and monitoring the execution of computer processing tasks are not responsibilities of the IS QA group. References: [ISACA CISA Review Manual 27th Edition], page 304.

最新問題**: 4**
セキュリティ意識向上トレーニングに含めることが最も重要なのは次のどれですか?
A. さまざまな種類の疑わしい活動への対応方法
B. 複雑なパスワードの重要性
C. 組織のセキュリティインフラストラクチャの説明
D. 組織のセキュリティチームの連絡先情報
Answer: A (メーッセージを残す**)**
The most important thing to include in security awareness training is how to respond to various types of suspicious activity. Security awareness training is a program that educates employees about the importance of security and how to avoid common threats and risks. One of the main objectives of security awareness training is to enable employees to recognize and report any signs of malicious or unauthorized activity, such as phishing emails, malware infections, data breaches, or social engineering attempts. By teaching employees how to respond to various types of suspicious activity, security awareness training can help to prevent or mitigate the impact of security incidents, protect the organization's assets and reputation, and comply with legal and regulatory requirements. The other options are not as important as option A. The importance of complex passwords is a useful topic, but not the most important thing to include in security awareness training.

Complex passwords are passwords that are hard to guess or crack by using a combination of letters, numbers, symbols, and cases. Complex passwords can help to protect user accounts and data from unauthorized access, but they are not sufficient to prevent all types of security incidents. Moreover, complex passwords may be difficult to remember or manage by users, and may require additional measures such as password managers or multi-factor authentication.
Descriptions of the organization's security infrastructure is a technical topic, but not the most important thing to include in security awareness training. Security infrastructure is the set of hardware, software, policies, and procedures that provide the foundation for the organization's security posture and capabilities. Security infrastructure may include firewalls, antivirus software, encryption tools, access control systems, backup systems, etc. Descriptions of the organization's security infrastructure may be relevant for some employees who are involved in security operations or administration, but they may not be necessary or understandable for all employees who need security awareness training.
Contact information for the organization's security team is a practical detail, but not the most important thing to include in security awareness training. Security team is the group of people who are responsible for planning, implementing, monitoring, and improving the organization's security strategy and activities. Contact information for the organization's security team may be useful for employees who need to report or escalate a security issue or request a security service or support. However, contact information for the organization's security team is not enough to ensure that employees know how to respond to various types of suspicious activity. References: Security Awareness Training | SANS Security Awareness, Security Awareness Training | KnowBe4, Security Awareness Training Course (ISC)² | Coursera

最新問題**: 5**
情報システム監査人が、オンライン顧客の支払い処理に使用される公開ウェブサーバーに高リスクの脆弱性を発見しました。情報システム監査人はまず、
A. 監査レポートに例外を文書化します。
B. セキュリティ インシデント レポートを確認します。
C. 補正コントロールを識別します。
D. 監査委員会に通知します。
Answer: C (メーッセージを残す**)**
The first action that an IS auditor should take when finding a high-risk vulnerability in a public-facing web server used to process online customer payments is to identify compensating controls. Compensating controls are alternative or additional controls that provide reasonable assurance of mitigating the risk of exploiting the vulnerability. The IS auditor should assess the effectiveness of the compensating controls and determine whether they reduce the risk to an acceptable level. If not, the IS auditor should recommend remediation actions to address the vulnerability. Documenting the exception in

an audit report is an important action, but it should not be the first action, as it does not address the urgency of the situation. Reviewing security incident reports is a useful action, but it should not be the first action, as it does not provide assurance of preventing future incidents. Notifying the audit committee is a necessary action, but it should not be the first action, as it does not involve taking any corrective measures. References:
* CISA Review Manual, 27th Edition, pages 295-2961
* CISA Review Questions, Answers & Explanations Database, Question ID: 260

最新問題: **6**
サービス レベル アグリーメント (SLAP) を作成する際に考慮すべき最も重要なのは次のどれですか。
A. プロバイダーの観点から見たサービスの説明
B. 完了すべき作業の詳細な識別
C. エンドユーザーのビジネスに影響を与える規制要件の規定
D. クライアント組織の観点から見たサービスの説明
Answer: D (メーッセージを残す**)**
The most important factor to consider when developing a service level agreement (SLA) is the description of the services from the viewpoint of the client organization, because the SLA should reflect the needs and expectations of the client and specify the measurable outcomes and performance indicators that the provider must deliver34. The description of the services from the viewpoint of the provider, the detailed identification of work to be completed, and the provisions for regulatory requirements that impact the end users' businesses are also important elements of an SLA, but not as crucial as the client's perspective. References: 3: CISA Review Manual (Digital Version), Chapter 5, Section 5.3.1 4: CISA Online Review Course, Module 5, Lesson 3

最新問題: **7**
セキュリティ インシデント対応計画を再検討する際に、机上演習を実施する主な目的は次のどれですか。
A. セキュリティ監査の問い合わせに対応するための文書を収集する
B. インシデント対応テストシナリオとの整合を効率化する
C. インシデント対応計画のプロセス改善オプションを決定する
D. インシデント対応計画をサポートする技術が整っていることを確認する
Answer: C (メーッセージを残す**)**

最新問題: **8**
フォローアップ監査の優先順位付けにおける主な基準は次のどれですか?
A. 監査計画で定義された監査サイクル
B. 経営陣の行動計画の複雑さ
C. 経営幹部からの推薦

D. 前回の監査結果からの残留リスク

Answer: D (メーッセージを残す**)**

Residual risk from the findings of previous audits should be the primary basis for prioritizing follow-up audits, because it reflects the level of exposure and potential impact that remains after management has implemented corrective actions or accepted the risk. Follow-up audits should focus on verifying whether the residual risk is within acceptable levels and whether the corrective actions are effective and sustainable. Audit cycle defined in the audit plan, complexity of management's action plans, and recommendation from executive management are not valid criteria for prioritizing follow-up audits, because they do not consider the residual risk from previous audits. References: CISA Review Manual (Digital Version), Chapter 2, Section
2.4.3

最新問題**: 9**

開発者が本番環境への書き込みアクセス権を持つ必要がある小規模な IT Web 開発会社の場合、IS 監査人の最善の推奨事項は次のようになります。

A. 本番環境への移行を実行するために別の人を雇います。

B. 継続的な監視制御を実装します。

C. 開発者から本番環境へのアクセスを削除します。

D. 開発チームのユーザーアクセスレビューを実行する

Answer: C (メーッセージを残す**)**

The best recommendation for a small IT web development company where developers must have write access to production is to remove production access from the developers. Production access is the ability to modify or update the live systems or applications that are used by customers or end users. Production access should be restricted to authorized and qualified personnel only, as any changes or errors in production can affect the functionality, performance, or security of the systems or applications. Developers should not have write access to production, as they may introduce bugs, vulnerabilities, or inconsistencies in the code that can compromise the quality or reliability of the systems or applications. The other options are not as effective as removing production access from the developers, as they do not address the root cause of the problem or provide the same benefits. Hiring another person to perform migration to production is a costly solution that can help segregate the roles and responsibilities of developers and migrators, but it does not remove production access from the developers. Implementing continuous monitoring controls is a good practice that can help detect and correct any issues or anomalies in production, but it does not remove production access from the developers. Performing a user access review for the development team is a detective control that can help verify and validate the access rights and privileges of developers, but it does not remove production access from the developers. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

最新問題: **10**
監査中、IT の発見事項は関係するすべての IT チームによって合意されますが、どのチームも修復の責任を負いたがらず、発見事項を責任範囲内で考慮しません。次のどれが IS 監査人の最善の行動方針ですか?
A. 解決のために IT 管理部門にエスカレーションします。
B. 所有者を特定せずに調査結果を発行する
C. すべての IT チームに共通の責任を割り当てます。
D. 最も適切なチームを決定し、それに応じて割り当てます。
Answer: A (メーッセージを残す**)**
The best course of action for the IS auditor is A. Escalate to IT management for resolution. This is because IT management is responsible for overseeing and coordinating the IT activities and functions within the organization, and ensuring that they comply with the audit findings and recommendations1. IT management can help resolve the issue of finding ownership by:
Clarifying and communicating the roles and responsibilities of each IT team, and how they relate to the finding and its remediation2.
Evaluating and assigning the finding to the most appropriate IT team, based on their expertise, authority, and availability2.
Providing guidance and support to the assigned IT team, and monitoring their progress and performance in remediating the finding2.

最新問題: **11**
クレジットカード会社は、顧客明細書の印刷を外注することに決めました。会社にとって最も重要なのは、以下の点を確認することです。
A. プロバイダーには代替のサービス拠点があります。
B. 契約には不十分なサービスレベルに対する補償が含まれています。
C. プロバイダーの情報セキュリティ管理は、会社のものと一致しています。
D. プロバイダーは会社のデータ保持ポリシーを遵守します。
Answer: C (メーッセージを残す**)**
The most important thing for the company to verify when outsourcing the printing of customer statements is whether the provider's information security controls are aligned with the company's. This is because customer statements contain sensitive personal and financial information that need to be protected from unauthorized access, disclosure, modification or destruction. The provider's information security controls should be consistent with the company's policies, standards and regulations, and should be audited periodically to ensure compliance. The other options are also relevant, but not as critical as information security. References: CISA Review Manual (Digital Version)1, Chapter 3, Section 3.2.2

最新問題**: 12**
組織の構成およびリリース管理プロセスを評価する IS 監査人にとって、最も懸念すべき事項は次のどれですか?
A. 組織は業界で認められた方法論を使用していない
B. 変更と変更承認が文書化されていない
C. すべての変更には中間管理職と上級管理職の承認が必要
D. 集中型構成管理データベース (CMDB) が存在しない
Answer: B (メーッセージを残す**)**
The greatest concern to an IS auditor who is assessing an organization's configuration and release management process is that changes and change approvals are not documented. This is because documentation is essential for ensuring the traceability, accountability, and quality of the changes made to the configuration items (CIs) and the releases deployed to the production environment. Without documentation, it would be difficult to verify the authenticity, validity, and authorization of the changes, as well as to identify and resolve any issues or incidents that may arise from the changes. Documentation also helps to maintain compliance with internal and external standards and regulations, as well as to facilitate audits and reviews.
The other options are not as concerning as option B, although they may also indicate some weaknesses in the configuration and release management process. The organization does not use an industry-recognized methodology, but this does not necessarily mean that their process is ineffective or inefficient. The organization may have developed their own methodology that suits their specific needs and context. However, using an industry-recognized methodology could help them adopt best practices and improve their process maturity. All changes require middle and senior management approval, but this may not be a problem if the organization has a clear and streamlined approval process that does not cause delays or bottlenecks in the change implementation. However, requiring too many approvals could also introduce unnecessary complexity and bureaucracy in the process. There is no centralized configuration management database (CMDB), but this does not mean that the organization does not have a way of managing their CIs and their relationships. The organization may use other tools or methods to store and access their configuration data, such as spreadsheets, documents, or repositories. However, having a centralized CMDB could help them improve their visibility, accuracy, and consistency of their configuration data.
References:
* 1: The Essential Guide to Release Management | Smartsheet
* 2: 5 steps to a successful release management process - Lucidchart
* 3: Configuration Management process overview - Micro Focus
* 4: Release and Deployment Management process overview - Micro Focus

最新問題**: 13**
一連の取引における不正行為を識別する最も効率的な方法はどれですか?

A. 自己評価（CSA）の制御
B. コントロール所有者へのインタビュー
C. 回帰分析
D. ベンフォードの法則の分析
Answer: (解答を表示する**)**
Benford's law analysis is a powerful technique for identifying irregularities or anomalies in numerical datasets, such as financial transactions. It detects deviations from expected frequency distributions, which may indicate fraud.
* Control Self-Assessments (CSAs) (Option A): Useful for control evaluation but not for fraud detection.
* Interviews with Control Owners (Option B): Provide insights but are not efficient for identifying fraudulent patterns.
* Regression Analysis (Option C): Effective for predictive modeling but less so for detecting fraud in transactional data.
Reference: ISACA CISA Review Manual, Job Practice Area 4: Protection of Information Assets.

最新問題**: 14**
開発環境のソース コードのセキュリティ脆弱性を特定するために使用されるテストの種類は何ですか?
A. 動的分析セキュリティテスト (DAST)
B. 静的解析セキュリティテスト (SAST)
C. ランタイムアプリケーション自己保護 (RASP)
D. インタラクティブ アプリケーション セキュリティ テスト (IAST)
Answer: B (メーッセージを残す**)**

最新問題**: 15**
技術組織の成熟度モデルを確認する際に、情報システム監査人が重点を置くべき最も重要な領域は次のどれですか?
A. 標準操作手順
B. サービスレベル契約 (SLA)
C. 役割と責任のマトリックス
D. ビジネスの回復力
Answer: C (メーッセージを残す**)**
A maturity model for a technology organization is a tool that measures the progress and capability of the IT function in relation to its goals, processes, and practices. A maturity model can help identify gaps and areas for improvement, as well as benchmark the IT function against industry standards or best practices. One of the key aspects of a maturity model is the definition and clarity of roles and responsibilities for the IT function and its stakeholders. A roles and responsibility matrix, such as a RACI matrix, is a document that

clarifies who is responsible, accountable, consulted, and informed for each task or deliverable in a project or process.
A roles and responsibility matrix can help avoid confusion, duplication, or omission of work, as well as ensure accountability and communication among the IT function and its customers, partners, and suppliers.
Therefore, an IS auditor should focus on reviewing the roles and responsibility matrix when evaluating the maturity model for a technology organization.
A standard operating procedure (SOP) is a document that describes the steps and instructions for performing a routine or repetitive task or process. SOPs are important for ensuring consistency, quality, and compliance in the IT function, but they are not directly related to the maturity model. A service level agreement (SLA) is a contract that defines the expectations and obligations between an IT service provider and its customers. SLAs are important for ensuring customer satisfaction, performance measurement, and dispute resolution in the IT function, but they are not directly related to the maturity model. A business resiliency plan is a document that outlines how an IT function will continue to operate or recover from a disruption or disaster. Business resiliency is important for ensuring availability, reliability, and security in the IT function, but it is not directly related to the maturity model. References: 1: Maturity Models for IT & Technology | Splunk 2: Responsibility assignment matrix - Wikipedia 3: Roles and Responsibilities Matrix - SDLCforms

最新問題**: 16**
永続的に重要なアーカイブされた電子情報が長期間アクセス可能であることを最も確実に保証できるのは次のどれですか?
A. アーカイブされたデータを定期的にバックアップする
B. 古いハードウェアの予防保守を実行する
C. データを定期的に最新技術に移行する
D. 古いソフトウェアをエミュレートするアプリケーションの取得
Answer: (解答を表示する**)**

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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**

実稼働ソース ライブラリを保護することで最も効果的に対処できる懸念事項は次のどれですか。
A. 実稼働ソース ライブラリが更新されるまで、プログラムは承認されません。
B. 実稼働ソース ライブラリとオブジェクト ライブラリが同期されていない可能性があります。
C. 変更が間違ったバージョンの運用ソース ライブラリに適用されます。
D. 許可されていない変更が本番環境に移行される可能性があります。
Answer: D (メーッセージを残す)
Unauthorized changes can be moved into production is the best concern that is addressed by securing production source libraries. Production source libraries contain the source code of programs that are used in the production environment. Securing production source libraries means implementing access controls, change management procedures, and audit trails to prevent unauthorized or improper changes to the source code that could affect the functionality, performance, or security of the production programs. The other options are less relevant concerns that may not be directly addressed by securing production source libraries, but rather by other controls such as program approval, version control, or change testing. References:
* CISA Review Manual (Digital Version), Chapter 4, Section 4.2.3.21
* CISA Review Questions, Answers & Explanations Database, Question ID 213

最新問題**: 18**
データ通信システムを監査する最初のステップは、次の点を決定することです。
A. トラフィック量と応答時間の基準
B. ネットワーク機器の物理的セキュリティ
C. さまざまな通信パスの冗長性のレベル
D. ビジネス用途と送信されるメッセージの種類
Answer: D (メーッセージを残す)
The first step in auditing a data communication system is to determine the business use and types of messages to be transmitted. This is because the auditor needs to understand the purpose, scope, and objectives of the data communication system, as well as the nature, volume, and sensitivity of the data being transmitted. This will help the auditor to identify the risks, controls, and audit criteria for the data communication system.
Traffic volumes and response-time criteria, physical security for network equipment, and the level of redundancy in the various communication paths are important aspects of a data communication system, but they are not the first step in auditing it. They depend on the business use and types of messages to be transmitted, and they may vary according to different scenarios and requirements. References: CISA Review Manual (Digital Version), [ISACA Auditing Standards]

最新問題**: 19**

内部のインターネット プロトコル (IP) アドレスを偽装する外部の攻撃者を最もよく検出できるのは次のうちどれですか?
A. 識別に静的IPアドレスを使用する
B. 状態テーブルを使用して、各パケットがシステムに入るときにそのメッセージ状態を比較する
C. 送信元アドレスとドメインネームサーバー (DNS) エントリを比較する
D. 送信元アドレスとエントリポイントとして使用されるインターフェースを比較する
Answer: (解答を表示する**)**

最新問題**: 20**
災害対応計画において最も重要な考慮事項は次のどれですか?
A. 収益の損失
B. IT資産保護
C. 人員の安全
D. 十分なリソース容量
Answer: C (メーッセージを残す**)**

最新問題**: 21**
フォローアップ業務中に、情報システム監査人は、元の監査では問題ではなかった問題の証拠を確認します。次のうち、監査人の最善の行動方針はどれですか?
A. フォローアップの範囲内の領域のみを報告します。
B. フォローアップの範囲を拡大して証拠の調査を含めます。
C. 将来の監査の一部として証拠を含めます。
D. フォローアップレポートで経営陣にリスクを報告します。
Answer: D (メーッセージを残す**)**

最新問題**: 22**
重要なデータがすでに RAID (Redundant Array of Inexpensive Disks) 上にあるにもかかわらず、情報システム監査人がオフサイト バックアップを推奨する主な理由はどれですか。
A. アレイはディスク破損に対する保護を提供できません。
B. アレイは適切なメンテナンスに依存します。
C. アレイは自然災害から回復できません。
D. アレイのディスクは、迅速な回復のためにホットスワップできません。
Answer: C (メーッセージを残す**)**

最新問題**: 23**
送信中の電子メールの機密性を確保するための最良の方法はどれですか?
A. 企業ネットワークトラフィックの暗号化
B. 複雑なユーザーパスワード
C. エンドツーエンドの暗号化

D. デジタル署名
Answer: C (メーッセージを残す**)**
End-to-end encryption ensures that email content is encrypted during transmission and can only be decrypted by the intended recipient. This approach provides robust protection against interception and unauthorized access.
* Encryption of Corporate Network Traffic (Option A): This does not address email confidentiality once the email leaves the corporate network.
* Complex User Passwords (Option B): Enhances account security but does not ensure email confidentiality in transit.
* Digital Signatures (Option D): Ensures authenticity and integrity but does not encrypt the email content.
Reference: ISACA CISA Review Manual, Job Practice Area 4: Protection of Information Assets.

最新問題**: 24**
IS 監査人がデータ センターのレビューを実施しています。次の観察結果のうち、アクセス制御の問題を示している可能性があるものはどれですか。
A. 正面玄関の外に防犯カメラを設置
B. コンピュータ室の入口に静電気防止マットを設置
C. 非常口のすぐ内側に泥だらけの足跡
D. 施設の周囲のフェンスは高さ2メートルです
Answer: C (メーッセージを残す**)**
An IS auditor is conducting a review of a data center. An observation that could indicate an access control issue is muddy footprints directly inside the emergency exit. Access control is a process that ensures that only authorized entities or individuals can access or use an information system or resource, and prevents unauthorized access or use. Access control can be implemented using various methods or mechanisms, such as physical, logical, administrative, etc. Muddy footprints directly inside the emergency exit could indicate an access control issue, as they could suggest that someone has entered the data center through the emergency exit without proper authorization or authentication, and potentially compromised the security or integrity of the data center. Security cameras deployed outside main entrance is not an observation that could indicate an access control issue, but rather a control that could enhance access control, as security cameras are devices that capture and record video footage of the surroundings, and can help monitor and deter unauthorized access or activity. Antistatic mats deployed at the computer room entrance is not an observation that could indicate an access control issue, but rather a control that could prevent static electricity damage, as antistatic mats are devices that dissipate or reduce static charges from people or objects, and can help protect electronic equipment from electrostatic discharge (ESD). Fencing around facility is two meters high is not an observation that could indicate an access control issue, but rather a control that could

improve physical security, as fencing is a barrier that encloses or surrounds an area, and can help prevent unauthorized entry or intrusion.

最新問題: **25**
外部監査会社が、システム実装プロジェクトの検証および検証レビューを実行するために雇用されました。IS 監査人は、回帰テストがプロジェクト計画の一部ではなく、システム実装チームによって実行されていないことを確認しました。チームによると、実行されている並行テストで十分であり、回帰テストは不要です。監査人の次のステップは何でしょうか。
A. 実行されている並列テストの範囲を評価する
B. システム実装チームによる統合テストとストレステストの実施を推奨する
C. 並列テストで十分であり、回帰テストは必要ないという結論に達する
D. システム実装チームによる回帰テストの実施を推奨する
Answer: D (メーッセージを残す**)**
Regression testing is crucial to ensure that new changes do not negatively impact existing functionalities. The IS auditor should recommend that regression testing be conducted to confirm that the system operates correctly after changes are made.
References
* ISACA CISA Review Manual 27th Edition, Page 256-257 (Testing Strategies)

最新問題: **26**
有名な商業信用機関からの信用スコアを組織システムに取り込むアプリケーション プログラミング インターフェイス (API) のリスク評価を実行する IS 監査人にとって、最も役立つのは次のどれですか。
A. 信用機関からの最新の監査報告書
B. API の承認されたビジネスケース
C. 転送されたデータのデータ辞書
D. インターフェース構成の技術設計文書
Answer: (解答を表示する**)**

最新問題: **27**
統制自己評価 (CSA) における IS 監査人の役割を最もよく説明しているのはどれですか?
A. ファシリテーター
B. 実装者
C. レビュー担当者
D. 承認者
Answer: A (メーッセージを残す**)**

最新問題: **28**
プロジェクト運営委員会の主な責任は次のとおりです。

A. 最終ビルド ドキュメントを承認します。
B. 各プロジェクトの期限が守られるようにします。
C. 開発されたシステムがビジネスニーズを満たしていることを確認します。
D. 定期的なプロジェクトの更新と監視を提供します。
Answer: D (メーッセージを残す)
The primary responsibility of a project steering committee is to provide regular project updates and oversight.
A project steering committee is an advisory group that consists of senior stakeholders and experts who offer guidance and support to a project manager and their team. The steering committee is mainly concerned with the direction, scope, budget, timeline, and methods used to realize a given project1.
One of the key roles of a steering committee is to monitor the progress and performance of the project and ensure that it aligns with the business objectives and stakeholder expectations. The steering committee also provides feedback, advice, and recommendations to the project manager and helps them resolve any issues or challenges that may arise during the project lifecycle. The steering committee communicates regularly with the project manager and other stakeholders through meetings, reports, and presentations23.
Therefore, providing regular project updates and oversight is the primary responsibility of a project steering committee.
References:
Steering Committee: Definition, Roles & Meeting Tips - ProjectManager
Project Steering Committee: Roles, Best Practices, Challenges - ProjectPractical Steering Committee: Complete Guide with Examples & Templates - Status.net

最新問題**: 29**
IT ガバナンスは、次の要素によって推進される必要があります。
A. ビジネス ユニットのイニシアチブ。
B. バランストスコアカード。
C. ポリシーと標準。
D. 組織戦略。
Answer: D (メーッセージを残す)
IT governance should be driven by organizational strategies. It provides a formal structure for organizations to produce measurable results toward achieving their strategies and ensures that IT investments support business objectives12. While business unit initiatives, balanced scorecards, and policies and standards can play a role in IT governance, they are tools or methods that support the implementation of the organizational strategies.

最新問題**: 30**

予定された更新の 1 週間後にコア システムに障害が発生し、サービスに影響する停止が発生しました。この問題に対処する際にインシデント管理で重点を置くべき最も重要なのは次のどれですか。
A. 障害の根本原因を分析し、インシデントが再発しないようにする
B. システムをできるだけ早く運用状態に復元する
C. システムをサービスに戻す前に、すべての解決手順が完全に文書化されていることを確認する
D. 失敗した変更を前の状態に戻す
Answer: B (メーッセージを残す)
The most important thing for incident management to focus on when addressing an issue that causes an outage is restoring the system to operational state as quickly as possible. Incident management is the process of detecting, investigating, and resolving incidents that disrupt or degrade a service or system. An incident is an unplanned event that affects the normal functioning or quality of a service or system. An outage is a type of incident that causes a complete loss of service or system availability. The main goal of incident management is to restore the service or system to its operational state as quickly as possible, minimizing the impact on users and business operations.
*The other options are not as important as option B. Analyzing the root cause of the outage to ensure the incident will not re-occur is a valuable activity, but not the most important thing for incident management to focus on when addressing an issue that causes an outage. Root cause analysis is a process of identifying and eliminating the underlying factors that caused an incident or problem. Root cause analysis can help to prevent or reduce the likelihood of similar incidents or problems in the future. However, root cause analysis is usually performed after the incident has been resolved and the service or system has been restored. Ensuring all resolution steps are fully documented prior to returning the system to service is a good practice, but not the most important thing for incident management to focus on when addressing an issue that causes an outage. Documentation is a process of recording and maintaining information about an incident and its resolution steps. Documentation can help to improve communication, accountability, learning, and improvement within incident management. However, documentation should not delay or interfere with the restoration of the service or system. Rolling back the unsuccessful change to the previous state is a possible solution, but not the most important thing for incident management to focus on when addressing an issue that causes an outage.
Rolling back is a process of reverting a change that has been applied to a service or system that caused an incident or problem. Rolling back can help to restore the service or system to its previous state before the change was made.

最新問題**: 31**

組織のエンタープライズ リソース プランニング (ERP) アプリケーションのアップグレードを評価する際に、情報システム監査人が検証する必要がある最も重要な項目は次のどれですか。
A. セキュリティ設定が新しいバージョンに適切に適用されました
B. ユーザーに新しいバージョンのセキュリティトレーニングが提供されました
C. アップグレード後にレッスンチームによる分析が文書化されました
D. アプリケーション関連のドキュメントは、新しいバージョンの変更を反映するように更新されました
Answer: (解答を表示する**)**

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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**
組織のソフトウェア開発者は、特定のデータ形式で保存された個人情報 (PII) にアクセスする必要があります。開発者が開発環境やテスト環境でこの機密情報を使用できるようにしながら、この機密情報を保護する最善の方法は次のどれですか。
A. データマスキング
B. データのトークン化
C. データの暗号化
D. データ抽象化
Answer: A (メーッセージを残す**)**
The best way to protect sensitive information such as personally identifiable information (PII) stored in a particular data format while allowing the software developers to use it in development and test environments is data masking. Data masking is a technique that replaces or obscures sensitive data elements with fictitious or modified data elements that retain the original format and characteristics of the data. Data masking can help protect sensitive information such as PII stored in a particular data format while allowing the software developers to use it in development and test environments by preventing the exposure or disclosure of the real data values without affecting the functionality or performance of the software or application. The other options are not as effective as data masking in protecting sensitive information such as PII stored in a particular data format while allowing the software developers to use it in development and test environments, as they have different limitations or drawbacks. Data tokenization is a technique that replaces

sensitive data elements with non-sensitive tokens that have no intrinsic value or meaning. Data tokenization can protect sensitive information such as PII from unauthorized access or theft, but it may not retain the original format and characteristics of the data, which may affect the functionality or performance of the software or application. Data encryption is a technique that transforms sensitive data elements into unreadable or unintelligible ciphertext using an algorithm and a key. Data encryption can protect sensitive information such as PII from unauthorized access or modification, but it requires decryption to restore the original data values, which may introduce additional complexity or overhead to the software development process. Data abstraction is a technique that hides the details or complexity of data structures or operations from users or programmers by providing a simplified representation or interface. Data abstraction can help improve the usability or maintainability of software or applications, but it does not protect sensitive information such as PII from exposure or disclosure. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.3.2

最新問題**: 33**
顧客データプライバシー監査を計画する際、情報システム監査人が最初に検討すべきものは次のうちどれですか?
A. 法的およびコンプライアンスの要件
B. 顧客契約
C. データ分類
D. 組織のポリシーと手順
Answer: D (メーッセージを残す**)**
The organizational policies and procedures are the first source of guidance for an IS auditor when planning a customer data privacy audit. They provide the framework and objectives for ensuring compliance with legal and regulatory requirements, customer agreements and data classification. The IS auditor should review them first to understand the scope, roles and responsibilities, standards and controls related to customer data privacy in the organization. The other options are also important, but they are secondary sources of information that should be reviewed after the organizational policies and procedures. References: CISA Review Manual (Digital Version) 1, Chapter 2: Governance and Management of Information Technology, Section 2.5: Privacy Principles and Policies.

最新問題**: 34**
次の生体認証アクセス制御のうち、誤検出率が最も高いのはどれですか?
A. 虹彩認識
B. 指紋スキャン
C. 顔認識
D. 網膜スキャン
Answer: B (メーッセージを残す**)**

Among the options provided, fingerprint scanning has the highest rate of false negatives. False negatives occur when a biometric system fails to recognize an authentic individual. Factors such as skin conditions (wet, dry, greasy), finger injuries, and inadequate scanning can contribute to false negatives in fingerprint scanning1. In comparison, iris recognition23, face recognition45, and retina scanning67 generally have lower rates of false negatives.
References:
How Accurate are today's Fingerprint Scanners? - Bayometric
25 Advantages and Disadvantages of Iris Recognition - Biometric Today
Iris Recognition Technology (or, Musings While Going through Airport ...
The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist Nor Sexist | ITIF NIST Launches Studies into Masks' Effect on Face Recognition Software Retinal scan - Wikipedia How accurate are retinal security scans - Smart Eye Technology

最新問題**: 35**
IS 監査人は、ベンダーの成果物に新しく取得した製品のソース コードが含まれていないと判断しました。この問題に対処するために、監査人は次のどれを契約に含めることを推奨する必要がありますか?
A. 機密保持およびデータ保護条項
B. サービスレベル契約 (SLA)
C. ソフトウェアエスクロー契約
D. 監査権条項
Answer: C (メーッセージを残す**)**
The correct answer is C. Software escrow agreement. A software escrow agreement is a legal arrangement between three parties: the software developer (licensor), the end-user (licensee), and an escrow agent. The agreement ensures that the software's source code and other relevant assets are securely stored with the escrow agent, and can be released to the licensee under certain conditions, such as the licensor's bankruptcy, insolvency, or failure to provide support or maintenance1. A software escrow agreement can provide the licensee with assurance and continuity for the software they depend on, and protect them from losing access or functionality in case of any unforeseen events or disputes with the licensor1.

最新問題**: 36**
IS 監査人が、特権アクセスがユーザーの役割に適していないユーザー アカウントを発見しました。このアクセスのリスクが悪用されたかどうかを判断するための最良の証拠は次のどれですか。
A. アカウントのアクティビティログ
B. アカウントの最終ログオン日
C. ユーザーのマネージャーとのインタビュー

D. アカウントの承認を文書化
Answer: A (メーッセージを残す**)**

最新問題**: 37**
組織は、IT ポリシーの開発において、ボトムアップ アプローチからトップダウン アプローチに移行しました。その結果、次のようになります。
A. 組織全体で一貫性が向上します。
B. 既存の運用ポリシーの統合。
C. より包括的なリスク評価計画。
D. ベストプラクティスの遵守を強化します。
Answer: (解答を表示する**)**
A top-down approach in the development of IT policies means that the policies are derived from the strategic objectives and goals of the organization, and are aligned with the business needs and expectations. This should result in greater consistency across the organization, as the policies will be coherent, integrated and applicable to all levels and functions of the organization. A bottom-up approach, on the other hand, means that the policies are developed by individual units or departments based on their operational needs and preferences, which may lead to inconsistency, duplication or conflict among different policies. References:
ISACA Frameworks: Blueprints for Success, IT Governance and Process Maturity

最新問題**: 38**
財務諸表監査中に最も懸念されるのは次のうちどれでしょうか?
A. システム容量はテストされていません。
B. 財務管理システムはクラウドベースです。
C. キー承認者のバックアップが特定されていません。
D. 主要なレポートを生成する手順が承認されていません。
Answer: D (メーッセージを残す**)**

最新問題**: 39**
次のうち、情報システム監査人が各業務で考慮する必要がある最も重要なリスクはどれですか?
A. プロセスとリソースの非効率性
B. 不正行為および違法行為
C. 組織のポリシーに違反している
D. ビジネス目標との不一致
Answer: D (メーッセージを残す**)**
The most significant risk that IS auditors are required to consider for each engagement is the misalignment with business objectives. This is because IS audit engagements are intended to provide assurance that the IT systems and processes support the achievement

of the business objectives and strategies. If there is a misalignment, it could result in wasted resources, missed opportunities, inefficiencies, errors, or failures that could adversely affect the organization's performance and reputation12. References: 1: CISA Review Manual (Digital Version), Chapter 1: The Process of Auditing Information Systems, Section 1.3: Audit Risk, page
28 2: CISA Online Review Course, Module 1: The Process of Auditing Information Systems, Lesson 1.3:
Audit Risk

最新問題**: 40**
サードパーティの IT サービス プロバイダーが組織の人事 (HR) システムを海外でホストしていることがわかった場合、情報システム監査人の最善の推奨事項は何でしょうか。
A. 背景検証チェックを実行します。
B. サードパーティの監査レポートを確認します。
C. 変更管理レビューを実装します。
D. プライバシー影響分析を実施します。
Answer: (解答を表示する**)**
The best recommendation for an IS auditor when finding that a third-party IT service provider hosts the organization's HR system in a foreign country is to conduct a privacy impact analysis. A privacy impact analysis is a systematic process that identifies and evaluates the potential risks and impacts of collecting, using, disclosing, and storing personal information. A privacy impact analysis will help the IS auditor to assess the legal, regulatory, contractual, and ethical obligations of the organization and the service provider regarding the protection of personal information. A privacy impact analysis will also help to identify and mitigate any privacy risks and gaps in the service level agreement.
References:
* CISA Certification | Certified Information Systems Auditor | ISACA
* CISA Questions, Answers & Explanations Database

最新問題**: 41**
関連するタスクを実行する個人が承認権限も持っている場合、次のどの責任領域が最も大きな職務分離の矛盾を引き起こすでしょうか?
A. 購買依頼書と発注書
B. 請求書と調整
C. ベンダーの選択と作業内容の説明
D. 良好な収入と支出
Answer: (解答を表示する**)**
The greatest segregation of duties conflict would occur if the individual who performs the related tasks also has approval authority for purchase requisitions and purchase orders. This is because these two tasks are directly related to each other and involve financial

transactions. If the same person is responsible for both tasks, it could lead to potential fraud or error12. For instance, the individual could approve a purchase order for a personal need and then also approve the payment for it, leading to misuse of company funds12.
References:
Segregation of Duties: Examples of Roles, Duties & Violations - Pathlock Functions in the Purchasing Process and how to Segregate Purchasing Duties

最新問題**: 42**
統制自己評価 (CSA) ファシリテーターの主な役割は次のとおりです。
A. 背景情報を得るためにインタビューを実施します。
B. チームを内部統制に集中させます。
C. 内部統制の弱点について報告します。
D. 制御の弱点に対する解決策を提供します。
Answer: B (メーッセージを残す**)**
The primary role of a control self-assessment (CSA) facilitator is to focus the team on internal controls. A CSA facilitator is a person who guides the CSA process and helps the participants to identify, assess, and improve their internal controls. The facilitator does not conduct interviews, report on weaknesses, or provide solutions, as these are the responsibilities of the participants themselves1.
The other options are incorrect because they are not the primary role of a CSA facilitator. Option A, conduct interviews to gain background information, is a preliminary step that may be done by the facilitator or the participants before the CSA session, but it is not the main purpose of the facilitator. Option C, report on the internal control weaknesses, is an outcome of the CSA process that should be done by the participants who own and operate the controls. Option D, provide solutions for control weaknesses, is also an outcome of the CSA process that should be done by the participants who are in charge of implementing the improvements.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019, page 2822
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription, QID
1066693
* PwC, Control Self Assessments4
* Workiva, 4 factors of an effective control self-assessment (CSA) program5

最新問題**: 43**
インシデント管理監査中に、情報システム監査人は、監査期間中に類似したインシデントがいくつか記録されていることを発見しました。監査人の最も重要な行動は次のどれですか?
A. 発見した内容を文書化し、経営陣に提示します。

B. 根本原因分析が行われたかどうかを判断します。
C. インシデントの解決時間を確認します。
D. すべてのインシデントが対処されたかどうかを検証します。
Answer: B (メーッセージを残す**)**
The IS auditor's most important course of action after finding that several similar incidents were logged during the audit period is to determine if a root cause analysis was conducted. A root cause analysis is a systematic process that identifies the underlying causes of system failures or incidents. A root cause analysis can help to prevent recurrence of similar incidents, improve system performance and reliability, and enhance incident management processes. The IS auditor should evaluate whether a root cause analysis was performed for each incident, whether it was timely and thorough, and whether it resulted in effective corrective actions.

最新問題**: 44**
顧客データを保護するための特定の情報セキュリティ慣行を義務付ける新しい規制が制定されました。情報情報監査人が規制に照らして監査する際に検討するのに最も役立つものは次のうちどれですか?
A. コンプライアンスギャップ分析
B. 顧客データ保護の役割と責任
C. 顧客データのフロー図
D. 新しい規制への適応に関するベンチマーク研究
Answer: (解答を表示する**)**
A compliance gap analysis is a detailed review of an organization's current state of compliance against a specific regulation or standard. It helps identify the areas and controls that are not meeting the requirements, assess their risk levels, and determine the corrective actions that can be taken to achieve compliance12. A compliance gap analysis is the most useful tool for an IS auditor to review when auditing against a new regulation, as it provides a clear and comprehensive picture of the compliance status, gaps, and remediation plan of the organization.
References
1: Information Security Architecture: Gap Assessment and Prioritization - ISACA
2: How to perform Compliance Gap Analysis? - Sprinto

最新問題**: 45**
組織のセキュリティ情報およびイベント管理 (SIEM) システムにおけるログの有効性と整合性の最も優れた証拠は次のどれですか?
A. コンプライアンステスト
B. ストップ ･オア ･ゴー ･サンプリング
C. 実質的なテスト
D. 可変サンプリング

Answer: (解答を表示する)

Substantive testing provides the best evidence of the validity and integrity of logs in an organization's security information and event management (SIEM) system, because it is a type of audit testing that directly examines the accuracy, completeness, and reliability of the data and transactions recorded in the logs. Substantive testing can involve various methods, such as re-performance, inspection, observation, inquiry, or computer-assisted audit techniques (CAATs), to verify the existence, occurrence, valuation, ownership, presentation, and disclosure of the log data1. Substantive testing can also detect any errors, omissions, alterations, or manipulations of the log data that may indicate fraud or misstatement2.

Compliance testing (A) is not the best evidence of the validity and integrity of logs in an organization's SIEM system, because it is a type of audit testing that evaluates the design and effectiveness of the internal controls that are implemented to ensure compliance with laws, regulations, policies, and procedures. Compliance testing can involve various methods, such as walkthroughs, questionnaires, checklists, or flowcharts, to assess the adequacy, consistency, and operation of the internal controls1. Compliance testing can provide assurance that the log data are generated and processed in accordance with the established rules and standards, but it does not directly verify the accuracy and reliability of the log data itself2.

Stop-or-go sampling (B) is not a type of audit testing, but a type of sampling technique that auditors use to select a sample from a population for testing. Stop-or-go sampling is a sequential sampling technique that allows auditors to stop testing before reaching the predetermined sample size if the results are satisfactory or conclusive. Stop-or-go sampling can reduce the audit cost and time by avoiding unnecessary testing, but it can also increase the sampling risk and uncertainty by relying on a smaller sample3. Stop-or-go sampling does not provide any evidence of the validity and integrity of logs in an organization's SIEM system by itself; it depends on the type and quality of the audit tests performed on the selected sample.

Variable sampling (D) is not a type of audit testing, but a type of sampling technique that auditors use to estimate a numerical characteristic of a population for testing. Variable sampling is a statistical sampling technique that allows auditors to measure the amount or rate of error or deviation in a population by using quantitative methods. Variable sampling can provide precise and objective results by using mathematical formulas and confidence intervals4. Variable sampling does not provide any evidence of the validity and integrity of logs in an organization's SIEM system by itself; it depends on the type and quality of the audit tests performed on the selected sample.

References:

Audit Testing Procedures - 5 Types and Their Use Cases

5 Types of Testing Methods Used During Audit Procedures | I.S. Partners Stop-or-Go Sampling Definition Variable Sampling Definition

最新問題: **46**
IT システムの復旧中にビジネス機能を稼働させ続けるための回避策プロセスのドキュメント化は、以下の中核部分です。
A. ビジネス影響分析 (BIA)。
B. 脅威とリスクの評価。
C. 事業継続計画 (BCP)。
D. 災害復旧計画 (DRP)。
Answer: C (メーッセージを残す)
A business continuity plan (BCP) is a system of prevention and recovery from potential threats to a company. The plan ensures that personnel and assets are protected and are able to function quickly in the event of a disaster1. A core part of a BCP is the documentation of workaround processes to keep a business function operational during recovery of IT systems. Workaround processes are alternative methods or procedures that can be used to perform a business function when the normal IT systems are unavailable or disrupted2. For example, if an online payment system is down, a workaround process could be to accept manual payments or use a backup system. Workaround processes help to minimize the impact of IT disruptions on the business operations and ensure continuity of service to customers and stakeholders3.
References:
* 1 explains what is a business continuity plan and why it is important.
* 2 defines what is a workaround process and how it can be used in a BCP.
* 3 provides examples of workaround processes for different business functions.

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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**
BYOD (個人所有デバイス持ち込み) プログラムの実装に関する監査の計画段階で最も重要な情報を提供するのは次のどれですか?
A. 以前の監査の結果
B. リスク評価の結果
C. 企業ネットワークに接続される個人用デバイスのインベントリ
D. BYOD許容ユーザーステートメントを含むポリシー
Answer: (解答を表示する)

The most important input during the planning phase for an audit on the implementation of a bring your own device (BYOD) program is policies including BYOD acceptable user statements. Policies are documents that define the organization's objectives, requirements, expectations, and responsibilities regarding a specific topic or area. BYOD policies should include acceptable user statements that specify what types of personal devices are allowed to connect to the corporate network, what security measures must be implemented on those devices, what data can be accessed or stored on those devices, what actions must be taken in case of device loss or theft, and what consequences will apply for non-compliance. Policies including BYOD acceptable user statements can provide an IS auditor with a clear understanding of the scope, criteria, and objectives of the BYOD program audit. Findings from prior audits, results of a risk assessment, and an inventory of personal devices to be connected to the corporate network are also useful inputs for planning a BYOD program audit, but they are not as important as policies including BYOD acceptable user statements. References: ISACA CISA Review Manual 27th Edition, page 381.

最新問題**: 48**
ビジネス影響分析 (BIA) を実行するときに使用されるデータは次のどれですか?
A. 現在のビジネスが将来のビジネスに及ぼす予測される影響
B. 現在の事業運営の費用便益分析
C. 規制遵守のコスト
D. 事業回復にかかる予想コスト
Answer: D (メーッセージを残す**)**
The expected costs for recovering the business would be used when performing a business impact analysis (BIA). A BIA is a process of identifying and evaluating the potential effects of disruptions to critical business functions or processes. A BIA helps to determine the recovery priorities, strategies, and resources needed to resume normal operations after a disruption. One of the key outputs of a BIA is an estimate of the financial losses or costs associated with different types of disruptions, such as lost revenue, increased expenses, contractual penalties, or regulatory fines.

最新問題**: 49**
ビジネス アプリケーションのデータと構成ファイルの詳細なテストに最適なのは次のどれですか?
A. バージョン管理ソフトウェア
B. 監査フック
C. ユーティリティソフトウェア
D. 監査分析ツール
Answer: D (メーッセージを残す**)**
The best tool for detailed testing of a business application's data and configuration files is an audit analytics tool. An audit analytics tool is a software that helps auditors to analyze

large sets of data and identify anomalies, trends, and patterns that are relevant to the audit objectives. An audit analytics tool can also provide audit evidence and support the auditor's professional judgment and conclusions.
Some of the benefits of using an audit analytics tool are:
It can improve the efficiency and effectiveness of the audit by reducing the time and effort required to perform manual tests and procedures.
It can enhance the quality and reliability of the audit by increasing the coverage and accuracy of the data analysis and testing.
It can enable the auditor to perform more complex and sophisticated tests and procedures that may not be possible or feasible with traditional methods.
It can help the auditor to discover new insights and risks that may not be apparent or detectable with traditional methods.
Some examples of audit analytics tools are:
IDEA: A data analysis software that allows auditors to import, analyze, and visualize data from various sources and formats. It also offers features such as sampling, stratification, gap analysis, duplicate detection, Benford's law, and regression analysis.1 ACL: A data analysis software that helps auditors to access, analyze, and report on data from various sources and formats. It also offers features such as sampling, stratification, gap analysis, duplicate detection, Benford' s law, regression analysis, and scripting.2 TeamMate Analytics: A data analysis software that integrates with Microsoft Excel and provides auditors with a range of tools and functions to perform data analysis and testing. It also offers features such as sampling, stratification, gap analysis, duplicate detection, Benford's law, regression analysis, and scripting.3

最新問題**: 50**
IS 監査人が組織のビジネス インテリジェンス インフラストラクチャをレビューしています。組織が適切なレベルのデータ品質を達成できるようにするための最善の推奨事項は次のとおりです。
A. データ分類基準に照らしてデータをレビューします。
B. データクレンジングを熟練したサービスプロバイダーにアウトソーシングします。
C. 別々のデータベースに保存されているデータをウェアハウスに統合します。
D. 事前に定義された仕様に照らしてデータを分析します。
Answer: D (メーッセージを残す**)**
This is because analyzing the data against predefined specifications is a method of data quality assessment that can help the organization achieve a reasonable level of data quality. Data quality assessment is the process of measuring and evaluating the accuracy, completeness, consistency, timeliness, validity, and usability of the data. Predefined specifications are the criteria or standards that define the expected or desired quality of the data. By comparing the actual data with the predefined specifications, the organization can

identify and quantify any gaps, errors, or deviations in the data quality, and take corrective actions accordingly12.
Reviewing data against data classification standards (A) is not the best answer, because it is not a method of data quality assessment, but rather a method of data security management. Data classification standards are the rules or guidelines that define the level of sensitivity and confidentiality of the data, and determine the appropriate security and access controls for the data. For example, data can be classified into public, internal, confidential, or restricted categories. Reviewing data against data classification standards can help the organization protect the data from unauthorized or inappropriate use or disclosure, but it does not directly improve the data quality3.
Outsourcing data cleansing to skilled service providers (B) is not the best answer, because it is not a recommendation to help the organization achieve a reasonable level of data quality, but rather a decision to delegate or transfer the responsibility of data quality management to external parties. Data cleansing is the process of detecting and correcting any errors, inconsistencies, or anomalies in the data. Skilled service providers are third-party vendors or contractors that have the expertise and resources to perform data cleansing tasks. Outsourcing data cleansing to skilled service providers may have some benefits, such as cost savings, efficiency, or scalability, but it also has some risks, such as loss of control, dependency, or liability4.
Consolidating data stored across separate databases into a warehouse is not the best answer, because it is not a method of data quality assessment, but rather a method of data integration and storage. Data integration is the process of combining and transforming data from different sources and formats into a unified and consistent view. Data warehouse is a centralized repository that stores integrated and historical data for analytical purposes. Consolidating data stored across separate databases into a warehouse can help the organization improve the availability and accessibility of the data, but it does not necessarily improve the data quality.

最新問題**: 51**
2 つの企業間の相互災害復旧契約の監査中、情報システム監査人は以下の点に最も関心を持ちます。
A. 緊急時のリソースの割り当て。
B. システムテストの頻度。
C. IS ポリシーと手順の違い。
D. ハードウェアとソフトウェアの互換性の維持。
Answer: A (メーッセージを残す**)**
During an audit of a reciprocal disaster recovery agreement between two companies, the IS auditor would be most concerned with the allocation of resources during an emergency. A reciprocal disaster recovery agreement is an arrangement by which one organization agrees to use another's resources in the event of a business continuity event or incident.

The IS auditor would need to ensure that both parties have clearly defined their roles and responsibilities, their resource requirements, their priority levels, their communication channels, and their escalation procedures in case of a disaster. The IS auditor would also need to verify that both parties have tested their agreement and have updated it regularly to reflect any changes in their business environments. The frequency of system testing is not as critical as the allocation of resources during an emergency, because system testing can be performed periodically or on demand, while resource allocation is a dynamic and complex process that requires careful planning and coordination. The differences in IS policies and procedures are not as critical as the allocation of resources during an emergency, because both parties can agree on common standards and protocols for their disaster recovery operations, or they can adapt their policies and procedures to suit each other's needs. The maintenance of hardware and software compatibility is not as critical as the allocation of resources during an emergency, because both parties can use compatible or interoperable systems, or they can use virtualization or cloud computing technologies to overcome any compatibility issues. References: ISACA CISA Review Manual 27th Edition, page 281

最新問題**: 52**
データセンターの物理的なセキュリティを評価する最も効果的な方法はどれですか?
A. データセンターのカメラ映像を確認します。
B. データセンターツアーを実行します。
C. データセンターのアクセス ログを確認します。
D. データセンターの関係者にインタビューします。
Answer: (解答を表示する**)**

最新問題**: 53**
導入前評価中に、ビジネス ケースがビジネス目標の達成につながることを示す最良の指標は何ですか。
A. ビジネス ケースは利害関係者の要件を反映します。
B. ビジネス ケースは実証済みの方法論に基づいています。
C. ビジネス ケースは、独立した第三者による品質レビューに合格しました。
D. ビジネス ケースでは、コスト配分の具体的な計画が特定されます。
Answer: (解答を表示する**)**
During a pre-deployment assessment, the best indication that a business case will lead to the achievement of business objectives is that the business case reflects stakeholder requirements. A business case is a document that explains the rationale, benefits, costs, and risks of a proposed project or initiative. A business case should align with the strategic goals and vision of the organization and address the needs and expectations of the stakeholders who are involved in or affected by the project12.

Stakeholder requirements are the conditions or capabilities that stakeholders expect from a project or its outcomes. Stakeholders can include customers, users, employees, managers, suppliers, regulators, and others who have an interest or stake in the project. Stakeholder requirements should be identified, analyzed, prioritized, validated, and documented throughout the project lifecycle34.
The business case should reflect stakeholder requirements because they provide the basis for defining the project scope, objectives, deliverables, quality standards, success criteria, and benefits realization. By reflecting stakeholder requirements, the business case can demonstrate how the project will add value to the organization and its stakeholders, justify the investment and resources required for the project, and facilitate the decision-making and approval process for the project5 .
Therefore, during a pre-deployment assessment, an IS auditor should look for evidence that the business case reflects stakeholder requirements as the best indication that the business case will lead to the achievement of business objectives.
References:
How to Write a Business Case (Template Included) - ProjectManager
How to Write a Business Case | Smartsheet
What are Stakeholder Requirements? | PM Study Circle
Stakeholder Requirements - Project Management Knowledge
Business Case vs Business Requirements - Difference Between
[Business Case Development - Project Management Docs]

最新問題**: 54**
IS 監査人が IT ガバナンス監査を実施しているときに、多くの取り組みが孤立したプロジェクト マネージャーによって非公式に管理されていることに気付きました。次の推奨事項のうち、IT チームの成熟度の向上に最も大きな影響を与えるのはどれでしょうか。
A. IT プロセスが成熟したかどうかを確認するために、翌年にフォローアップ監査をスケジュールします。
B. IT の優先順位付けと支出を監視するための学際的な IT 運営委員会を作成します。
C. プロジェクト管理ツールですべての IT 決定を文書化して追跡します。
D. 正式な承認が得られ、文書化されるまで、現在のすべての IT プロジェクトを中止します。
Answer: B (メーッセージを残す**)**
An IT steering committee is a group of senior executives and stakeholders who provide strategic direction, guidance, and oversight for the IT function of an organization. An IT steering committee can help to improve the maturity of the IT team by ensuring that the IT initiatives are aligned with the business goals and objectives, that the IT resources are allocated and utilized effectively and efficiently, and that the IT performance and value are measured and communicated. An IT steering committee can also help to resolve conflicts,

prioritize demands, and foster collaboration among the IT project managers and other business units.
References
ISACA CISA Review Manual, 27th Edition, page 254
Auditing IT Governance
The Impact of Poor IT Audit Planning and Mitigating Audit Risk
IS Audit Basics: The Components of the IT Audit Report

最新問題: **55**
プロジェクト変更管理プロセスに従わずに開発フェーズ中に新しいシステム機能を追加することに関連する主なリスクは次のどれですか?
A. プロジェクトは設定された期限に間に合わない可能性があります。
B. 新しい機能は要件を満たさない可能性があります。
C. 追加された機能は文書化されていません。
D. プロジェクトの予算が超過する可能性があります。
Answer: B (メーッセージを残す**)**

最新問題: **56**
IT 監査の後、経営陣は監査レポートで強調されたリスクを受け入れることを決定しました。経営陣がビジネスのニーズとリスク管理の必要性を適切にバランスさせていることを、情報システム監査人に最も確実に保証できるのは次のどれですか。
A. リスクの影響を受ける関係者に通知するためのコミュニケーション計画が存在します。
B. 潜在的な影響と可能性が適切に文書化されています。
C. 特定されたリスクは組織のリスク委員会に報告されます。
D. リスクを受け入れて承認するための確立された基準が存在します。
Answer: D (メーッセージを残す**)**
Clear criteria ensure a consistent, rational approach to risk acceptance decisions, demonstrating management's deliberate and informed approach to risk management.
References
ISACA CISA Review Manual (Current Edition) - Chapter on Risk Management Risk Management Frameworks (e.g., ISO 31000, NIST SP 800-39) - Emphasize the importance of defined risk assessment and decision-making processes.

最新問題: **57**
次のどれが、IT 部門と企業ミッションの整合性を最もよく示していますか?
A. IT部門の機能の分析
B. 上級管理職への隔週報告
C. 年次理事会
D. 四半期ごとの運営委員会会議
Answer: (解答を表示する**)**

Quarterly steering committee meetings best demonstrate alignment of the IT department with the corporate mission because they provide a regular forum for strategic planning, decision making, and communication between IT leaders and business stakeholders12. Steering committee meetings help to ensure that IT goals and initiatives are aligned with the business vision, mission, and objectives, and that IT performance and value are monitored and evaluated34.
References
1: IT Governance and the Balanced Scorecard - ISACA Journal
2: IT Steering Committee Best Practices: A Recipe for Success
3: What is IT Governance? - Definition from Techopedia
4: CISA Cybersecurity Strategic Plan | CISA

最新問題**: 58**
システム中断インシデントのレビュー中に、IS 監査人は、IT サポート スタッフが権限レベルを超えた決定を下す立場に置かれていることに気付きました。
将来このような状況を防ぐために最適な推奨事項は次のうちどれですか?
A. エスカレーション プロトコルを導入します。
B. コンピテンシーマトリックスを開発します。
C. フォールバック オプションを実装します。
D. 緊急アクセス ID を有効にします。
Answer: A (メーッセージを残す**)**
The best recommendation to help prevent the situation where IT support staff were put in a position to make decisions beyond their level of authority during the review of a system disruption incident is to introduce escalation protocols. Escalation protocols are policies and procedures that define who should be notified, involved, or consulted when an incident occurs, how the communication and handover should take place, and what criteria or triggers should be used to escalate the incident to a higher level of authority or expertise2. Escalation protocols help to ensure that:
Incidents are handled by the appropriate staff with the required skills, knowledge, and experience Incidents are resolved in a timely and effective manner Incidents are escalated to senior management or specialized teams when necessary Incidents are documented and reported accurately and transparently Incidents are analyzed and learned from to prevent recurrence or mitigate impact Therefore, by introducing escalation protocols, an organization can improve its incident management process and avoid putting IT support staff in a position to make decisions beyond their level of authority.
References:
Escalation policies for effective incident management, Section 1: What is incident escalation?

最新問題**: 59**

組織は、ネットワーク管理者が十分な資格を有していることを保証するために特別に設計された採用ポリシーと手順を確立しています。どのような種類の制御が実施されていますか?
A. 探偵
B. 補償
C. 修正
D. ディレクティブ
Answer: D (メーッセージを残す**)**
The type of control that is in place when an organization has established hiring policies and procedures designed specifically to ensure network administrators are well qualified is directive. Directive controls are those that guide or direct the actions of individuals or groups to achieve a desired outcome. Directive controls can also help to prevent or reduce the occurrence of undesirable events. Hiring policies and procedures are examples of directive controls that aim to ensure that only qualified and competent personnel are employed to perform IT-related tasks. References:
* CISA Review Manual (Digital Version), Chapter 4, Section 4.11
* CISA Online Review Course, Domain 1, Module 2, Lesson 12

最新問題**: 60**
世界的な銀行が顧客の財務データのバックアップにクラウド プロバイダーを使用する予定です。このプロジェクトの主な焦点は次のどれですか。
A. データ保持ポリシー
B. 転送頻度
C. バックアップテストスケジュール
D. データの機密性
Answer: D (メーッセージを残す**)**

最新問題**: 61**
IS 監査人は、経営陣にデータの提供を求めるのではなく、監査手順を実行するために必要なデータへの直接アクセスを要求します。このアプローチの主な利点は次のどれですか。
A. 監査の透明性
B. データの機密性
C. プロフェッショナリズム
D. 監査の効率
Answer: D (メーッセージを残す**)**
The primary advantage of this approach is that it improves audit efficiency. Audit efficiency is the measure of how well the audit resources are used to achieve the audit objectives. Audit efficiency can be enhanced by using methods or techniques that can save time, cost, or effort without compromising the quality or scope of the audit. By requesting direct access to data required to perform audit procedures instead of asking management to

provide the data, the auditor can reduce the dependency on management's cooperation, availability, or timeliness. The auditor can also avoid potential delays, errors, or biases that may occur when management provides the data. References:
* CISA Review Manual (Digital Version), Chapter 2, Section 2.41
* CISA Online Review Course, Domain 1, Module 1, Lesson 42

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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**
長期の停電の影響を最も軽減できるのは次のうちどれですか?
A. バッテリーバンク
B. 緊急電源オフスイッチ
C. 冗長電源
D. 電力調整ユニット
Answer: (解答を表示する**)**

最新問題: **63**
ファイアウォールが組織のセキュリティ ポリシーに準拠して構成されているかどうかを判断するための最適な監査手順は次のどれですか。
A. パラメータ設定の確認
B. システムログの確認
C. ファイアウォール管理者へのインタビュー
D. 実際の手順の確認
Answer: A (メーッセージを残す**)**
The best audit procedure to determine whether a firewall is configured in compliance with the organization's security policy is reviewing the parameter settings. Parameter settings are values or options that define how a firewall operates and functions, such as rules, filters, ports, protocols, etc. By reviewing the parameter settings of a firewall, an IS auditor can verify whether they match with the organization's security policy, which is a document that outlines the security objectives, requirements, and guidelines for an organization's information systems and resources. Reviewing the system log is a possible audit procedure to determine whether a firewall is configured in compliance with the organization's security policy, but it is not the best one, as a system log records events or activities that occur on a firewall, such as connections, requests, responses, errors, alerts,

etc., and may not indicate whether they comply with the organization's security policy. Interviewing the firewall administrator is a possible audit procedure to determine whether a firewall is configured in compliance with the organization's security policy, but it is not the best one, as a firewall administrator may not provide accurate or reliable information about the firewall configuration, and may have conflicts of interest or ulterior motives. Reviewing the actual procedures is a possible audit procedure to determine whether a firewall is configured in compliance with the organization's security policy, but it is not the best one, as actual procedures describe how a firewall is configured and maintained, such as installation, testing, updating, etc., and may not reflect whether they comply with the organization's security policy.

最新問題: **64**
新しいシステム実装における並列処理の主な利点は次のどれですか?
A. 新しいシステムが機能要件を満たしていることの保証
B. ユーザーが新しいシステムのトレーニングを完了するための時間が長くなります
C. 他のシステム実装やアプローチに比べて大幅なコスト削減
D. 新しいシステムがパフォーマンス要件を満たしていることの保証
Answer: D (メーッセージを残す**)**
Parallel processing is a system implementation approach that involves running the new system and the old system simultaneously for a period of time until the new system is verified and accepted. The primary advantage of parallel processing is that it provides assurance that the new system meets performance requirements and produces the same or better results as the old system. Parallel processing also minimizes the risk of system failure and data loss, as the old system can be used as a backup or fallback option in case of any problems with the new system.

最新問題: **65**
データベース管理の評価中に、情報システム監査人は、データベース管理者 (DBA) 権限を持つ一部のアカウントに、ログイン試行の失敗回数が無制限のデフォルト パスワードが割り当てられていることを発見しました。監査人にとって最善の対応策は次のどれですか。
A. ログイン失敗回数が多すぎるアカウントを特定し、無効化をリクエストする
B. ITマネージャーに管理者のセキュリティパラメータを変更し、検出結果を更新するよう依頼する
C. 発見事項を文書化し、管理者アカウントが不適切なセキュリティ設定になっているリスクを説明する
Answer: (解答を表示する**)**
The auditor's best course of action is to document the finding and explain the risk of having administrator accounts with inappropriate security settings. This is because the auditor's role is to identify and report the issues, not to fix them or request others to fix them. The auditor should also communicate the impact of the finding, such as the possibility of

unauthorized access, data tampering, or denial of service attacks. The auditor should not assume the responsibility of the IT manager or the DBA, who are in charge of changing the security parameters or disabling the accounts. References:
* CISA Review Manual (Digital Version), Chapter 4, Section 4.2.21
* CISA Online Review Course, Domain 1, Module 3, Lesson 32

最新問題**: 66**
内部統制を自動化することによる主な利点は次のどれですか?
A. 高額取引のレビューを可能にする
B. 大量のデータを効率的にテストする
C. 職務分離のないトランザクションの識別を支援する
D. 分析レビューの実行を支援する
Answer: B (メーッセージを残す**)**
The major advantage of automating internal controls is to efficiently test large volumes of data, because automated controls can perform repetitive tasks faster, more accurately, and more consistently than manual controls. Automated controls can also provide audit trails and exception reports that facilitate the monitoring and evaluation of the control effectiveness12. Reviewing large value transactions, identifying transactions with no segregation of duties, and performing analytical reviews are possible benefits of automating internal controls, but not the major advantage. References: 1: CISA Review Manual (Digital Version), Chapter 5, Section 5.2.2 2: CISA Online Review Course, Module 5, Lesson 2

最新問題**: 67**
ファイアウォールが組織のセキュリティ ポリシーに準拠して構成されていることを示す最良の監査証拠は次のどれですか。
A. 構成変更がどのように実行されるかを分析する
B. ログファイルの分析
C. ルールベースの確認
D. 侵入テストの実行
Answer: C (メーッセージを残す**)**
The best audit evidence that a firewall is configured in compliance with the organization's security policy is to review the rule base. The rule base is a set of rules that defines the criteria for allowing or denying network traffic through the firewall. By reviewing the rule base, the auditor can verify if the firewall configuration matches the security policy requirements and objectives. Analyzing how the configuration changes are performed, analyzing log files, and performing penetration testing are useful audit techniques, but they do not provide direct evidence of the firewall configuration compliance. References: CISA Review Manual (Digital Version)1, page 383.

最新問題**: 68**

IS 監査人は、ピギーバックやテールゲーティングによって機密性の高いデータ センターへの不正アクセスが行われる可能性があることを懸念しています。次のうち、最も適切な推奨事項はどれですか。(CISA 認定 - 情報システム監査人公式書籍から正しい回答を選択し、説明を記入してください)

A. 生体認証

B. 訪問者の案内手順

C. エアロック入口

D. 侵入者警報

Answer: (解答を表示する**)**

The best recommendation to prevent unauthorized access to a highly sensitive data center by piggybacking or tailgating is to use an airlock entrance. An airlock entrance is a type of access control system that consists of two doors that are interlocked, so that only one door can be opened at a time. This prevents an unauthorized person from following an authorized person into the data center without being detected. An airlock entrance can also be integrated with other security measures, such as biometrics, card readers, or PIN pads, to verify the identity and authorization of each person entering the data center.

Biometrics (option A) is a method of verifying the identity of a person based on their physical or behavioral characteristics, such as fingerprints, iris scans, or voice recognition. Biometrics can provide a high level of security, but they are not sufficient to prevent piggybacking or tailgating, as an unauthorized person can still follow an authorized person who has been authenticated by the biometric system.

Procedures for escorting visitors (option B) is a policy that requires all visitors to the data center to be accompanied by an authorized employee at all times. This can help prevent unauthorized access by visitors, but it does not address the risk of piggybacking or tailgating by other employees or contractors who may have legitimate access to the building but not to the data center.

Intruder alarms (option D) are devices that detect and alert when an unauthorized person enters a restricted area. Intruder alarms can provide a deterrent and a response mechanism for unauthorized access, but they are not effective in preventing piggybacking or tailgating, as they rely on the detection of the intruder after they have already entered the data center.

References: 1: CISA Certification | Certified Information Systems Auditor | ISACA 2: CISA Certified Information Systems Auditor Study Guide, 4th Edition 3: CISA - Certified Information Systems Auditor Study Guide [Book]

最新問題**: 69**

オンライン注文の整合性を確保するための最も適切な制御は次のどれですか?

A. データ暗号化規格 (DES)

B. デジタル署名

C. 公開鍵暗号化

D. 多要素認証

Answer: (解答を表示する**)**

A digital signature is the most appropriate control to ensure integrity of online orders because it provides a way to verify the authenticity and integrity of the data sent by the sender. A digital signature is created by applying a cryptographic algorithm to the data and attaching the result to the data. The receiver can then use the sender's public key to verify that the data has not been altered or tampered with during transmission. A digital signature also provides non-repudiation, which means that the sender cannot deny sending the data.

Data Encryption Standard (DES) is a symmetric encryption algorithm that can provide confidentiality of online orders, but not integrity. DES uses the same key to encrypt and decrypt the data, which means that anyone who has the key can modify the data without detection.

Public key encryption is an asymmetric encryption algorithm that can also provide confidentiality of online orders, but not integrity. Public key encryption uses a pair of keys: a public key and a private key. The sender encrypts the data with the receiver's public key, and the receiver decrypts it with their own private key.

However, public key encryption does not prevent anyone from modifying the encrypted data.

Multi-factor authentication is a control that can provide authentication and authorization of online orders, but not integrity. Multi-factor authentication requires the user to provide two or more pieces of evidence to prove their identity, such as a password, a token, or a biometric factor. Multi-factor authentication can prevent unauthorized access to online orders, but it does not protect the data from being modified after being sent.

References:

* ISACA, CISA Review Manual, 27th Edition, 2019, p. 281 1
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription 2

最新問題**: 70**

電子商取引 Web サイトを運営する組織は、顧客に継続的なサービスを提供したいと考えており、サービスの重要性からホット サイトへの投資を計画しています。この決定を行う際に最も重要な考慮事項は次のどれですか。

A. 最大許容ダウンタイム (MTD)

B. 復旧時間目標 (RTO)

C. リカバリポイント目標 (RPO)

D. 平均修復時間 (MTTR)

Answer: B (メーッセージを残す**)**

The recovery time objective (RTO) is the most important consideration when making a decision to invest in a hot site due to service criticality. The RTO is the maximum acceptable time that an IT service or process can be unavailable or disrupted before it causes significant damage to the business operations and objectives. A hot site is a fully

equipped and operational backup facility that can be activated immediately in the event of a disaster or disruption. A hot site can help an organization achieve a very low RTO, as it can resume the service with minimal or no downtime. The maximum tolerable downtime (MTD) is the maximum acceptable time that an IT service or process can be unavailable or disrupted before it causes intolerable damage to the business operations and objectives. The MTD is usually longer than the RTO, as it represents the worst-case scenario. The recovery point objective (RPO) is the maximum acceptable amount of data loss that an IT service or process can tolerate in the event of a disaster or disruption. The RPO is measured in terms of time, such as hours or minutes, and indicates how frequently the data should be backed up or replicated. The mean time to repair (MTTR) is the average time that it takes to restore an IT service or process after a failure or disruption. The MTTR is a measure of the efficiency and effectiveness of the recovery process, but it does not reflect the service criticality or the business impact. References: IS Audit and Assurance Tools and Techniques, CISA Certification | Certified Information Systems Auditor | ISACA

最新問題**: 71**
最近、システム管理者が情報システム監査人に、組織外からの侵入試行が数回失敗したことを報告しました。このような侵入を検出するのに最も効果的なのは次のうちどれですか。
A. ワンタイムパスワード付きスマートカードの使用
B. 定期的にログファイルを確認する
C. ルーターをファイアウォールとして設定する
D. 生体認証ベースの認証のインストール
Answer: (解答を表示する**)**
Periodically reviewing log files is the most effective way to detect intrusion attempts from outside the organization, as they can provide evidence of unauthorized access attempts, source IP addresses, timestamps and other relevant information. Using smart cards with one-time passwords or installing biometrics-based authentication can prevent unauthorized access, but not detect it. Configuring the router as a firewall can block unwanted traffic, but not log it. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 361

最新問題**: 72**
IS 監査人がデータ変換プロジェクトをレビューしています。稼働開始前の監査人の最善の推奨事項は次のどれですか?
A. テスト手順とシナリオを確認する
B. 模擬変換テストを実施する
C. 構成ベースラインを確立する
D. テストスクリプトを自動化する
Answer: (解答を表示する**)**

The auditor's best recommendation prior to go-live is to conduct a mock conversion test. This is because a mock conversion test can help to verify the accuracy, completeness, and validity of the data conversion process. A mock conversion test can also help to identify and resolve any issues or errors before the actual conversion takes place. A mock conversion test can also provide assurance that the converted data meets the business requirements and expectations. References:
* CISA Review Manual (Digital Version), Chapter 3, Section 3.3.21
* CISA Online Review Course, Domain 2, Module 2, Lesson 22

最新問題: **73**
運用ログ管理を実装する際に、IT 部門の責任者が主に考慮すべき事項は次のどれですか?
A. さまざまなITリソースによって生成されるログ形式の多様性
B. ログボリュームによる保持とストレージの問題
C. 運用ユーザーによる抵抗
D. ITリソースのパフォーマンスへの影響
Answer: B (メーッセージを残す**)**

最新問題: **74**
合併後、国際組織を調査した結果、IT 運営委員会の決定が、統合 IT 運用モデルで要求されているように地域オフィスにまで及んでいないことが判明しました。次のうち、情報システム監査人の最善の推奨事項はどれですか。
A. 地域の卓越センターを創設する。
B. 地域 IT 運営委員会を作成します。
C. IT ガバナンス コンサルタントを雇用します。
D. IT 運営委員会の正式な規約を更新します。
Answer: (解答を表示する**)**

最新問題: **75**
ある組織が、HR アプリケーションをプライベート クラウドの Infrastructure as a Service (IaaS) モデルに移行しています。展開されたアプリケーションのオペレーティング システムのセキュリティ構成について、主に責任を負うのは誰ですか?
A. クラウドプロバイダーの外部監査人
B. クラウドプロバイダー
C. オペレーティングシステムベンダー
D. 組織
Answer: (解答を表示する**)**
The organization is primarily responsible for the security configurations of the deployed application's operating system when migrating its HR application to an Infrastructure as a Service (IaaS) model in a private cloud. This is because in an IaaS model, the cloud provider is responsible for the security of the underlying infrastructure that they lease to

their customers, such as servers, storage, and networks, while the customer is responsible for the security of the areas of the cloud infrastructure over which they have control, such as operating systems, middleware, and applications. Therefore, the organization needs to ensure that the operating system is properly configured, patched, hardened, and monitored to protect the HR application from unauthorized access or malicious attacks.
The other options are not primarily responsible for the security configurations of the deployed application's operating system. The cloud provider's external auditor is not responsible for any security configurations, but rather for verifying and reporting on the cloud provider's compliance with relevant standards and regulations.
The cloud provider is responsible for the security of the underlying infrastructure, but not for the operating system or any software installed on it by the customer. The operating system vendor is responsible for providing updates and patches for the operating system, but not for configuring or securing it according to the customer's needs.
References:
* 11: What Is IaaS (Infrastructure As A Service)? - Forbes
* 12: What is Shared Responsibility Model? - Check Point Software
* 13: Who Is Responsible for Cloud Security? - Security Intelligence

最新問題**: 76**
企業の電子メールで送信された機密文書の不正な開示を検出するのに最も役立つ方法はどれですか?
A. すべてのユーザーに文書を送信する前に暗号化を要求する
B. 企業ネットワークへのファイアウォールのインストール
C. 機密としてマークされたすべての送信メールを報告する
D. 事前に定義された基準に基づいてすべてのメールを監視する
Answer: D (メーッセージを残す**)**
To detect unauthorized disclosure of confidential documents sent over corporate email, monitoring all emails based on pre-defined criteria is the best approach. This involves setting up automated monitoring systems that analyze email content, attachments, and metadata to identify any potential unauthorized disclosures. By defining specific criteria (such as keywords related to confidential information), organizations can proactively detect and prevent leaks. Requiring encryption before sending documents (option A) is important but does not address monitoring for unauthorized disclosures. Firewalls (option B) protect the network but do not specifically focus on email content. Reporting outgoing emails marked as confidential (option C) relies on user self-reporting and may not catch all incidents12. References: 1(https://www.isaca.org/resources/isaca- journal/past-issues/2010/data-governance-for-privacy-confidentiality-and-compliance-a-holistic-approach) 2 (https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2020/volume-6/best-practices-for- privacy-audits)

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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**
インシデント対応計画の最初のステップは次のとおりです。
A. インシデントを検証します。
B. IT 部門の責任者に通知します。
C. インシデントの影響を受けたシステムを分離します。
D. 根本原因分析を開始します。
Answer: A (メーッセージを残す**)**
The first step in an incident response plan is typically preparation12. However, among the options provided, validating the incident would be the first step. This involves confirming that a security event is actually an incident3. It's important to verify the event to avoid wasting resources on false positives.
References:
Incident Response Plan: Frameworks and Steps - CrowdStrike
What is Incident Response? Plan and Steps | Microsoft Security
What Are the Phases of an Incident Response Plan? - ISC2 Blog

最新問題: **78**
投資を実行する前に IT 開発プロジェクトを評価するには、次のどれを使用する必要がありますか?
A. 達成価値分析 (EVA)
B. 実現可能性調査
C. ファンクションポイント分析
D. 迅速なアプリケーション開発
Answer: (解答を表示する**)**

最新問題: **79**
非構造化データのリスクを最小限に抑えるために、最初に行うべきことはどれですか?
A. 非構造化データのリポジトリを識別します。
B. 非構造化データを分析するためのツールを購入します。
C. 非構造化データに対して強力な暗号化を実装します。
D. 非構造化データへのユーザー アクセス制御を実装します。
Answer: A (メーッセージを残す**)**

Unstructured data is data that does not have a predefined model or organization, making it difficult to store, process, and analyze using traditional relational databases or spreadsheets. Unstructured data can pose a risk to an organization if it contains sensitive, confidential, or regulated information that is not properly secured, managed, or governed. To minimize the risk of unstructured data, the first step is to identify the repositories of unstructured data, such as file servers, cloud storage, email systems, social media platforms, etc. This will help to understand the scope, volume, and nature of unstructured data in the organization, and to prioritize the areas that need further analysis and action. References: Unstructured data - Wikipedia

最新問題**: 80**
データ センターの監査で、IS 監査人は湿度レベルが非常に低いことを発見しました。IS 監査人は、次の項目の増加が予想されるため、最も懸念することになります。
A. バックアップ テープの障害。
B. 静電気の問題。
C. 従業員の不快感。
D. 火災の危険があります。
Answer: (解答を表示する**)**

最新問題**: 81**
法医学調査において証拠を保護するのに最適なのは次のうちどれですか?
A. 影響を受けるシステムのイメージング
B. 影響を受けるシステムの電源を切る
C. 影響を受けるシステムのハードウェアを保護する
D. 影響を受けるシステムを再起動する
Answer: A (メーッセージを残す**)**
Imaging the affected system is the best way to protect evidence in a forensic investigation, because it creates a bit-by-bit copy of the original data that can be analyzed without altering or compromising the original source. Imaging preserves the integrity and authenticity of the evidence and allows for verification and validation of the results34. Powering down or rebooting the affected system can cause data loss or corruption, while protecting the hardware does not prevent unauthorized access or tampering with the software or data.
References: 3: CISA Review Manual (Digital Version), Chapter 6, Section 6.4.1 4: CISA Online Review Course, Module 6, Lesson 4

最新問題**: 82**
実装前にプロジェクトを評価する際に、システム要件が満たされていることを最もよく証明する証拠は次のどれですか?
A. 統合テストの結果

B. 上級管理職からの承認
C. ユーザー受け入れテスト (UAT) の結果
D. 回帰テストの結果
Answer: C (メーッセージを残す**)**

最新問題**: 83**
ある組織が社内で Web アプリケーションを開発しています。アプリケーションが外部からの攻撃に対して安全であることを IS 監査人に証明する最良の証拠は次のどれですか。
A. データベースアプリケーション監視ログ
B. 第三者によるコードレビュー
C. Web アプリケーション ファイアウォール (WAF) の実装
D. 侵入テストの結果
Answer: D (メーッセージを残す**)**

最新問題**: 84**
ネットワーク サービスのサービス レベル契約 (SLA) を開発する際の課題は次のどれですか。
A. ネットワーク サービスのための適切に設計されたフレームワークを確立します。
B. 適切に測定できるパフォーマンス指標を見つける
C. ネットワークコンポーネントがクライアントによって変更されないようにする
D. ネットワークへのエントリポイントの数を減らす
Answer: B (メーッセージを残す**)**
One of the challenges in developing a SLA for network services is finding performance metrics that can be measured properly and reflect the quality of service expected by the customer. Establishing a well-designed framework for network services is not a challenge, but a good practice. Ensuring that network components are not modified by the client or reducing the number of entry points into the network are security issues, not SLA issues.
References: ISACA, CISA Review Manual, 27th Edition, 2018, page 333

最新問題**: 85**
継続的デプロイメント プログラムの一環としての安全なコード レビューは、どのタイプの制御ですか?
A. 探偵
B. 論理
C. 予防的
D. 修正
Answer: C (メーッセージを残す**)**
Secure code reviews as part of a continuous deployment program are preventive controls. Preventive controls are controls that aim to prevent or avoid undesirable events or outcomes from occurring, such as errors, defects, or incidents. Secure code reviews are

activities that examine and evaluate the source code of a software or application to identify and eliminate any vulnerabilities, flaws, or weaknesses that may compromise its security, functionality, or performance. Secure code reviews as part of a continuous deployment program can help prevent or avoid security issues or incidents from occurring by ensuring that the code is secure and compliant before it is deployed to production. The other options are not correct types of controls for secure code reviews as part of a continuous deployment program, as they have different meanings and functions. Detective controls are controls that aim to detect or discover undesirable events or outcomes that have occurred, such as errors, defects, or incidents. Logical controls are controls that use software or hardware mechanisms to regulate or restrict access to IT resources, such as data, systems, or networks.
Corrective controls are controls that aim to correct or rectify undesirable events or outcomes that have occurred, such as errors, defects, or incidents. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

最新問題**: 86**
ウォーターフォール方式よりもアジャイル ソフトウェア開発方式を使用する利点は次のどれですか?
A. 全体的に必要な資金が少なくなる
B. より迅速な納品
C. エンドユーザーの受け入れが迅速化
D. 明確に定義されたビジネス上の期待
Answer: B (メーッセージを残す**)**
The advantage of using agile software development methodology over the waterfall methodology is that it allows for quicker deliverables. Agile software development is an iterative and incremental approach that emphasizes customer feedback, collaboration, and adaptation. Agile software development delivers working software in short cycles, called sprints, that typically last from two to four weeks. This enables the development team to respond to changing requirements, deliver value faster, and improve quality. Waterfall software development is a linear and sequential approach that follows a predefined set of phases, such as planning, analysis, design, implementation, testing, and maintenance. Waterfall software development requires a clear and stable definition of the project scope, deliverables, and expectations before starting the development process. Waterfall software development can be slow, rigid, and costly, especially if changes occur during the later stages of the project. References: CISA Review Manual (Digital Version), Chapter 3: Information Systems Acquisition, Development & Implementation, Section 3.1: Project Management Practices

最新問題**: 87**
エンタープライズ リソース プランニング (ERR) システムで 3 者一致が発生したことを確認するときに、IS 監査人が使用する必要があるのは次のどれですか。

A. 銀行確認
B. 商品配送通知
C. 購入依頼
D. 注文書
Answer: (解答を表示する**)**
A three-way match is a process of verifying that a purchase order, a goods receipt and an invoice are consistent before making a payment1. A three-way match ensures that the organization only pays for the goods or services that it ordered and received, and that the prices and quantities are accurate. A three-way match can prevent errors, fraud and overpayments in the accounts payable process.
An IS auditor should use a purchase order when verifying a three-way match has occurred in an enterprise resource planning (ERP) system. A purchase order is a document that authorizes a purchase transaction and specifies the items, quantities, prices and terms of the order2. A purchase order is the first document in the three-way match process, and it serves as the basis for comparing the goods receipt and the invoice. An IS auditor can use a purchase order to check if the ERP system has correctly recorded, matched and approved the three documents before making a payment.
The other options are not as useful for verifying a three-way match. A bank confirmation is a document that verifies the balance and activity of a bank account3. A bank confirmation can be used to confirm that a payment has been made or received, but it does not provide information about the details of the purchase transaction or the three-way match process. A goods delivery notification is a document that informs the buyer that the goods have been shipped or delivered by the seller4. A goods delivery notification can be used to track the status of the delivery, but it does not provide information about the quantity or quality of the goods or the invoice amount. A purchase requisition is a document that requests authorization to purchase goods or services from a specific supplier2. A purchase requisition can be used to initiate the purchasing process, but it does not provide information about the actual purchase order, goods receipt or invoice.
References:
Bank Confirmation - Overview, How It Works, Importance3
What is Goods Delivery Note? | Definition & Example4
What Is Three-Way Matching & Why Is It Important? | NetSuite1
Enterprise Resource Planning (ERP) - Definition, Types, Uses2

最新問題**: 88**
IT 管理に関する組織の標準とガイドラインのレビューでは、IS 開発方法論に次のどれを含める必要がありますか?
A. 付加価値活動分析
B. リスク管理手法
C. アクセス制御ルール
D. インシデント管理手法

Answer: (解答を表示する**)**
Risk management techniques should be included in an IS development methodology. An IS development methodology is a set of guidelines, standards, and procedures that provide a structured and consistent approach to developing information systems. A good IS development methodology should cover all the phases of the system development life cycle (SDLC), from planning and analysis to design, implementation, testing, and maintenance1.
Risk management techniques are an essential part of an IS development methodology, as they help to identify, assess, prioritize, mitigate, monitor, and communicate the risks that may affect the success of the system development project. Risk management techniques can also help to ensure that the system meets the requirements and expectations of the stakeholders, complies with the relevant laws and regulations, and delivers value to the organization2.
The other options are not as relevant or appropriate as risk management techniques for an IS development methodology. Value-added activity analysis is a technique for evaluating the efficiency and effectiveness of business processes, but it is not specific to IS development3. Access control rules are policies and mechanisms for restricting or granting access to information systems and resources, but they are more related to security management than IS development4. Incident management techniques are methods for handling and resolving incidents that disrupt the normal operation of information systems and services, but they are more related to service management than IS development5.
References:
ISACA, CISA Review Manual, 27th Edition, 2019, p. 1911
ISACA, CISA Review Manual, 27th Edition, 2019, p. 1942
Value-Added Activity Analysis3
Access Control Rules4
Incident Management Techniques5

最新問題**: 89**
組織の情報セキュリティ ポリシーを確認する場合、IS 監査人は、ポリシーが主に次の基準に基づいて定義されていることを確認する必要があります。
A. リスク管理プロセス。
B. 情報セキュリティフレームワーク。
C. 過去の情報セキュリティインシデント。
D. 業界のベストプラクティス。
Answer: (解答を表示する**)**
Information security policies are high-level statements that define the organization's approach to protecting its information assets from threats and risks. They should be based primarily on a risk management process, which is a systematic method of identifying, analyzing, evaluating, treating, and monitoring information security risks. A risk

management process can help ensure that the policies are aligned with the organization's risk appetite, business objectives, legal and regulatory requirements, and stakeholder expectations. An information security framework is a set of standards, guidelines, and best practices that provide a structure for implementing information security policies. It can support the risk management process, but it is not the primary basis for defining the policies. Past information security incidents and industry best practices can also provide valuable inputs for defining the policies, but they are not sufficient to address the organization's specific context and needs. References: Insights and Expertise, CISA Review Manual (Digital Version)

最新問題**: 90**
フォローアップ監査をスケジュールする際に考慮すべき最も重要なのは次のどれですか?
A. 新しい監査人による独立した検証に必要な努力
B. 是正措置を講じなかった場合の影響
C. 監査対象者が監査人と過ごすことに同意した時間の長さ
D. 観察に関連する制御と検出リスク
Answer: B (メーッセージを残す**)**
The impact if corrective actions are not taken is the most important factor to consider when scheduling follow- up audits. An IS auditor should prioritize the follow-up audits based on the risk and potential consequences of not addressing the audit findings and recommendations. The other options are less important factors that may affect the timing and scope of the follow-up audits, but not their necessity or urgency. References:
* CISA Review Manual (Digital Version), Chapter 2, Section 2.5.31
* CISA Review Questions, Answers & Explanations Database, Question ID 207

最新問題**: 91**
IT インフラストラクチャに対する効果的なガバナンスを最もよく示すものはどれですか?
A. 継続的かつ信頼性の高いパフォーマンスを提供する能力
B. 年次セキュリティ意識向上プログラムの要件
C. ITインフラサーバ数の増加
D. 情報セキュリティインシデント数の減少
Answer: A (メーッセージを残す**)**
Effective governance over IT infrastructure is indicated by the ability to deliver continuous, reliable performance12. This is because good governance ensures that IT investments support business objectives and produce measurable results towards achieving their strategies2. It involves implementing management and internal controls, strengthening security, financial controls, risk mitigation, and inspection and compliance obligations3. While security awareness programs, the number of servers, and the number of security incidents can be aspects of IT governance, they are not the best indicators of its effectiveness.
References:

The Value of IT Governance - ISACA
What is IT governance? A formal way to align IT & business strategy | CIO Robust Governance - KPMG Global

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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**
ネットワーク プリンタの廃棄プロセスを確認する IS 監査人にとって、最も懸念すべき事項は次のどれですか。
A. 廃棄ポリシーと手順が一貫して実施されていない
B. プリンターのハードドライブが廃棄前に消毒されたことを確認する証拠はありません。
C. ビジネスユニットはプリンターを直接処分することができます
D. 動作不能なプリンターは安全でない領域に保管されています。
Answer: (解答を表示する**)**
The greatest concern for an IS auditor reviewing a network printer disposal process is that evidence is not available to verify printer hard drives have been sanitized prior to disposal. This can expose sensitive data to unauthorized parties and cause data breaches. Disposal policies and procedures not being consistently implemented or business units being allowed to dispose printers directly to vendors are compliance issues, but not as critical as data protection. Inoperable printers being stored in an unsecured area is a physical security issue, but not as severe as data leakage. References: ISACA, CISA Review Manual, 27th Edition, 2018, page
387

最新問題: **93**
監査機能が基準と倫理規定に準拠していることを上級管理職と取締役会に最もよく示すのは次のどれですか?
A. 監査スタッフのインタビュー
B. 品質管理レビュー
C. 自己評価（CSA）の制御
D. 是正措置計画
Answer: B (メーッセージを残す**)**

Quality control reviews are the best way to demonstrate to senior management and the board that an audit function is compliant with standards and the code of ethics. These reviews assess the efficiency and effectiveness of the audit function, ensure compliance with audit standards and ethics, and identify areas for improvement12. While audit staff interviews, control self-assessments (CSAs), and corrective action plans can provide valuable insights, they do not offer the same level of assurance as a comprehensive quality control review12.
References: The Institute of Internal Auditors1, AuditBoard2

最新問題**: 94**
次のどれが、情報システム監査人がエンドユーザー コンピューティング (EUC) 監査の財務報告スプレッドシートを優先できるようにする最適な方法でしょうか。
A. 各スプレッドシートの目的を理解する
B. ファイルサイズに基づいてスプレッドシートを確認する
C. どのスプレッドシートが最も頻繁に使用されているかを確認する
D. マクロが組み込まれたスプレッドシートの識別
Answer: A (メーッセージを残す**)**

最新問題**: 95**
データ損失防止 (DLP) に重点を置いたセキュリティ レビューにより、組織はクラウドに保存されているデータをまったく把握していないことが明らかになりました。この問題に対処するための IS 監査人の最善の推奨事項は何ですか?
A. ネットワーク境界のファイアウォールを強化します。
B. クラウドに保存されているデータを検出するためのファイル システム スキャナーを実装します。
C. クラウド アクセス セキュリティ ブローカー (CASB) を採用します。
D. デスクトップ上の DLP ツールを使用して、ユーザーのアクティビティを監視します。
Answer: (解答を表示する**)**
Here's the breakdown, considering
the need for DLP visibility in the cloud:
Verified Answer
C: Employ a cloud access security broker (CASB).
Very Short Explanation
CASBs are specifically designed to enhance visibility and control over cloud-based data. They can monitor data flows, enforce security policies, and often have DLP capabilities built-in, making them the ideal solution in this scenario.
References
ISACA Resources (Glossary): Definitions of Cloud Access Security Broker (CASB) highlight their role in cloud security and governance.

Industry Research (Gartner, etc.): Research on CASB tools emphasizes their ability to address visibility and control challenges for cloud data.

最新問題**: 96**
経営陣がサイバーセキュリティ インシデント対応プロセスの有効性を確保するための最良の方法はどれですか?
A. 主要な利害関係者へのサイバーセキュリティインシデントの定期的な報告
B. インシデント対応プロセスドキュメントの定期的な更新
C. インシデント対応に携わるスタッフに対する定期的なサイバーセキュリティトレーニング
D. 主要な関係者が参加する定期的な机上演習
Answer: (解答を表示する**)**
Tabletop exercises are a type of simulation used to test an organization's incident response plan12. They involve key stakeholders in a hypothetical scenario to see how they would respond12. This allows management to assess the effectiveness of the incident response process and identify areas for improvement12. Regularly conducting these exercises ensures that the organization is prepared for a real incident and that the incident response process remains effective over time12.
References:
Cybersecurity incident response: The 6 steps to success
Six steps for building a robust incident response strategy - IBM

最新問題**: 97**
IT ガバナンスを効果的に実装するために最も重要なのは次のどれですか?
A. 強力なリスク管理の実践
B. 内部監査員のコミットメント
C. 協力的な企業文化
D. 文書化されたポリシー
Answer: C (メッセージを残す**)**
The most critical factor for the effective implementation of IT governance is a supportive corporate culture. A supportive corporate culture is one that fosters collaboration, communication and commitment among all stakeholders involved in IT governance processes. A supportive corporate culture also promotes a shared vision, values and goals for IT governance across the organization. Strong risk management practices, internal auditor commitment or documented policies are important elements for IT governance implementation, but they are not sufficient without a supportive corporate culture.
References: ISACA, CISA Review Manual,
27th Edition, 2018, page 41

最新問題**: 98**
IS 監査人は、次の方法でシステム障害のビジネスへの影響を最もよく評価できます。

A. ユーザー満足度の評価。
B. 機器メンテナンスログを分析します。
C. セキュリティ管理者へのインタビュー。
D. システム生成ログを確認しています。
Answer: (解答を表示する**)**

最新問題**: 99**
IS 監査でファイアウォールが多数の攻撃試行を認識できなかったことが判明した場合、監査人の最善の推奨事項は、ファイアウォールと次のものの間に侵入検知システム (IDS) を配置することです。
A. 組織の Web サーバー。
B. 非武装地帯 (DMZ)。
C. 組織のネットワーク。
D. インターネット
Answer: D (メーッセージを残す**)**
The best recommendation is to place an intrusion detection system (IDS) between the firewall and the Internet. An IDS is a device or software that monitors network traffic for malicious activity and alerts the network administrator or takes preventive action. By placing an IDS between the firewall and the Internet, the IS auditor can enhance the security of the network perimeter and detect any attack attempts that the firewall was unable to recognize.
The other options are not as effective as placing an IDS between the firewall and the Internet:
* Placing an IDS between the firewall and the organization's web server would not protect the web server from external attacks that bypass the firewall. The web server should be placed in a demilitarized zone (DMZ), which is a separate network segment that isolates public-facing servers from the internal network.
* Placing an IDS between the firewall and the demilitarized zone (DMZ) would not protect the DMZ from external attacks that bypass the firewall. The DMZ should be protected by two firewalls, one facing the Internet and one facing the internal network, with an IDS monitoring both sides of each firewall.
* Placing an IDS between the firewall and the organization's network would not protect the organization' s network from external attacks that bypass the firewall. The organization's network should be protected by a firewall that blocks unauthorized traffic from entering or leaving the network, with an IDS monitoring both sides of the firewall.

最新問題**: 100**
エンタープライズ アーキテクチャ (EA) の主な目的は次のどれですか?
A. 組織全体でITポリシーを実施する
B. 詳細なシステムドキュメントの維持

C. IT投資の管理と計画
D. プロジェクトのカスタマイズされた開発と提供の実行
Answer: (解答を表示する**)**

最新問題**: 101**
セキュリティ インシデント発生後に実施されたインシデント後レビューの結果を IS 監査人が検査する最も重要な理由はどれですか。
A. 継続的な改善活動の有効性を評価する
B. インシデント対応の指標を業界ベンチマークと比較する
C. 攻撃者が仕掛けた隠れたバックドアを特定するためにインシデントを再分析する
D. 将来のセキュリティ侵害に対するネットワークファイアウォールの有効性を評価する
Answer: (解答を表示する**)**
A post-incident review (PIR) is a process to review the incident information from occurrence to closure and to identify potential findings and recommendations for improvement1. The most important reason for an IS auditor to examine the results of a PIR is to evaluate the effectiveness of continuous improvement efforts and to ensure that the lessons learned from the incident are implemented and followed up2. A PIR can help an organization to eliminate or reduce the risk of the incident to re-occur, improve the initial incident detection time, identify improvements needed to diagnose and repair the incident, and update the incident management best practices1. Therefore, a PIR is a valuable source of information for an IS auditor to assess the maturity and performance of the organization's incident management process.

最新問題**: 102**
テストのサンプルには、残高が最も大きい 80 件のクライアントと、残りのランダム サンプルを含める必要があります。IS 監査人はどのようなことを推奨すべきでしょうか。
A. データベースをクエリします。
B. 統合テスト施設 (ITF) を開発します。
C. 汎用監査ソフトウェアを使用します。
D. 乱数ジェネレータを活用します。
Answer: C (メーッセージを残す**)**
Generalized audit software is a type of computer-assisted audit technique (CAAT) that allows the IS auditor to perform various audit tasks on the data stored in different file formats and databases1. Generalized audit software can help the IS auditor to select a sample for testing that includes the 80 largest client balances and a random sample of the rest, by using functions such as sorting, filtering, stratifying, and randomizing the data23. Generalized audit software can also help the IS auditor to perform other audit procedures on the sample, such as verifying the accuracy, completeness, and validity of the data4. References

1: Generalized Audit Software (GAS) - ISACA 2: Audit Sampling - ISACA 3: How to use generalized audit software to perform audit sampling 4: Generalized Audit Software: A Review of Five Packages

最新問題**: 103**
IS 監査人は、レポート システムの読み取り専用ユーザーの定期的なレビューが実行されていないことを発見しました。
IS 監査人が次に取るべき行動は次のどれですか?
A. エンドユーザーのリストを確認し、承認を評価します。
B. この制御プロセスの弱点を上級管理職に報告します。
C. この免除に対する経営陣の承認を確認する
D. この免除については IT 部門から口頭での確認を得てください。
Answer: B (メーッセージを残す**)**
The IS auditor's next course of action should be to report this control process weakness to senior management, as it may indicate a lack of oversight and accountability for the reporting system. Read-only users may have access to sensitive or confidential information that should be restricted or monitored. Periodic reviews of read-only users are a good practice to ensure that the access rights are still valid and appropriate for the users' roles and responsibilities. Reporting this weakness to senior management will also allow them to take corrective actions or implement compensating controls if needed.
Option A is incorrect because reviewing the list of end users and evaluating for authorization is not the IS auditor's responsibility, but rather the system owner's or administrator's. The IS auditor should only verify that such reviews are performed and documented by the responsible parties.
Option C is incorrect because verifying management's approval for this exemption is not sufficient to address the control process weakness. Even if there is a valid reason for not performing periodic reviews of read-only users, the IS auditor should still report this as a potential risk and recommend mitigating controls.
Option D is incorrect because obtaining a verbal confirmation from IT for this exemption is not adequate evidence or documentation. The IS auditor should obtain written approval from management and verify that it is aligned with the organization's policies and standards.
References:
CISA Review Manual (Digital Version)1, Chapter 1: The Process of Auditing Information Systems, Section
1.4: Audit Evidence, p. 31-32.
CISA Review Manual (Print Version), Chapter 1: The Process of Auditing Information Systems, Section 1.4:
Audit Evidence, p. 31-32.

CISA Online Review Course2, Module 1: The Process of Auditing Information Systems, Lesson 4: Audit Evidence, slide 9-10.
CISA Questions, Answers & Explanations Database3, Question ID: QAE_CISA_710.

最新問題: **104**
ソフトウェア開発者が手動テストではなく自動テストを使用する最も適切な理由はどれですか?
A. CAATは簡単に開発できる
B. 受け入れテストの範囲を縮小する
C. 自動テストスクリプトのメンテナンスの容易さ
D. 回帰テストの改善
Answer: D (メーッセージを残す**)**

最新問題: **105**
社内に技術的な専門知識がない場合に、電子バンキング ソリューションの開発をアウトソーシングする最大の利点は次のどれですか。
A. 初期費用の削減
B. システムダウンタイムのリスクの軽減
C. リスクの直接監視
D. システムの適応能力の向上
Answer: A (メーッセージを残す**)**
Outsourcing the development of an e-banking solution when in-house technical expertise is not available can significantly reduce start-up costs. This is because the organization can avoid the expenses associated with hiring and training a full-time development team, purchasing necessary hardware and software, and maintaining the system1. While outsourcing can also potentially reduce the risk of system downtime, increase the ability to adapt the system, and provide direct oversight of risks, these benefits are not as immediate or guaranteed as the cost savings123.
References: Maxicus1, Forbes2, Strategy& - PwC3

最新問題: **106**
仮想化環境にとって最も重要な制御は次のどれですか?
A. 仮想化環境の運用に関するポリシーの定期的な更新
B. ハイパーバイザーとゲストマシンの強化
C. ハードウェアリソースとネットワークコンポーネントの冗長性
D. ゲストオペレーティングシステムレベルでのリソースの使用率の監視
Answer: (解答を表示する**)**
The most important control for virtualized environments is hardening for the hypervisor and guest machines.

Hardening is the process of applying security measures and configurations to reduce the vulnerabilities and risks of a system or device. Hardening for the hypervisor and guest machines is essential for protecting the virtualized environments from attacks, as they are exposed to various threats from both the physical and virtual layers. Hardening for the hypervisor and guest machines involves the following steps:

* Applying the latest patches and updates for the hypervisor and guest operating systems, as well as the applications and drivers running on them.
* Configuring the firewall and network settings for the hypervisor and guest machines, to restrict and monitor the network traffic and prevent unauthorized access or communication.
* Disabling or removing any unnecessary or unused features, services, accounts, or ports on the hypervisor and guest machines, to minimize the attack surface and reduce the potential entry points for attackers.
* Enforcing strong authentication and authorization policies for the hypervisor and guest machines, to ensure that only authorized users or administrators can access or manage them.
* Encrypting the data and communication for the hypervisor and guest machines, to protect the confidentiality and integrity of the information stored or transmitted on them.
* Implementing logging and auditing mechanisms for the hypervisor and guest machines, to record and track any activities or events that occur on them, and enable detection and investigation of any incidents or anomalies.

Hardening for the hypervisor and guest machines can help prevent or mitigate common attacks on virtualized environments, such as:

* Hypervisor escape: An attack where a malicious guest machine breaks out of its isolated environment and gains access to the hypervisor or other guest machines.
* Hypervisor compromise: An attack where an attacker exploits a vulnerability or misconfiguration in the hypervisor to gain control over it or its resources.
* Guest compromise: An attack where an attacker exploits a vulnerability or misconfiguration in a guest machine to gain access to its data or applications.
* Guest impersonation: An attack where an attacker creates a fake or cloned guest machine to trick other guests or users into interacting with it.
* Guest denial-of-service: An attack where an attacker consumes or exhausts the resources of a guest machine to disrupt its availability or performance.

Therefore, hardening for the hypervisor and guest machines is the most important control for virtualized environments, as it can enhance their security, reliability, and performance. For more information about hardening for virtualized environments, you can refer to some of these web sources:

* Hypervisor security on the Azure fleet
* Chapter 2: Hardening the Hyper-V host
* Plan for Hyper-V security in Windows Server

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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**
災害後にデータ センターが代替サイトでコンピューティング設備を復旧しようとする場合、最初に復旧する必要があるのは次のどれですか。
A. データのバックアップ
B. 意思決定支援システム
C. オペレーティング システム
D. アプリケーション
Answer: (解答を表示する**)**
When a data center is attempting to restore computing facilities at an alternative site following a disaster, the operating system should be restored FIRST. Here's why:
1. Operating System (OS):
The OS is the foundation of any computing environment. It manages hardware resources, provides essential services, and allows applications to run.
Restoring the OS ensures that the infrastructure is operational and ready for further recovery steps.
Without a functional OS, applications cannot execute, and data backups cannot be effectively restored.
2. Data Backups:
While data backups are critical for recovery, they depend on a working infrastructure.
If the OS is not operational, restoring data backups becomes challenging.
Data backups should follow the OS restoration.
3. Applications:
Applications rely on the OS to function.
Restoring applications before the OS may lead to compatibility issues or incomplete functionality.
Applications should be restored after ensuring a stable OS environment.
4. Decision Support System (DSS):
DSS is an application category.
It should follow the restoration of both the OS and critical applications.
In summary, prioritize restoring the operating system, which forms the basis for subsequent recovery steps12.
Once the OS is functional, proceed with data backups, applications, and other systems as needed.

最新問題: **108**
異なるセキュリティ分類のデータを含むサーバーで最小権限の原則を適用する最良の方法はどれですか?
A. 使用頻度に基づいてデータファイルへのアクセスを制限する
B. データ分類ポリシーに準拠するためのユーザーからの正式な同意の取得
C. データ所有者が決定したアクセス制御を適用する
D. スクリプト化されたアクセス制御リストを使用してサーバーへの不正アクセスを防止する
Answer: (解答を表示する**)**
The best way to enforce the principle of least privilege on a server containing data with different security classifications is to apply access controls determined by the data owner. The principle of least privilege states that users should only have the minimum level of access required to perform their tasks. The data owner is the person who has the authority and responsibility to classify, label, and protect the data according to its sensitivity and value. The data owner can define the access rights and permissions for each user or role based on the data classification policy and the business needs. This will ensure that only authorized and appropriate users can access the data and prevent unauthorized or excessive access that could compromise the confidentiality, integrity, or availability of the data. References:
* CISA Review Manual (Digital Version)
* CISA Questions, Answers & Explanations Database

最新問題: **109**
機密データを保存していたフラッシュ ドライブを廃棄するのに最適な方法はどれですか?
A. 消磁
B. 上書き
C. 暗号消去
D. 破壊
Answer: D (メーッセージを残す**)**

最新問題: **110**
効果的な IT 投資管理を最もよく示す指標は次のどれですか?
A. IT 投資はシステム開発ライフサイクル (SDLC) に従って実装および監視されます。
B. IT投資は特定のビジネス目標にマッピングされます
C. IT投資を必要とする各事業ごとに主要業績評価指標 ⅏PI)が定義される
D. IT投資予算は業界ベンチマークを大幅に下回っています
Answer: (解答を表示する**)**
This means that the IT investments are aligned with the strategic goals and priorities of the organization, and that they deliver value and benefits to the business. Mapping IT investments to specific business objectives can help ensure that the IT investments are

relevant, justified, and measurable, and that they support the organization's mission and vision.
IT investments are implemented and monitored following a system development life cycle (SDLC) is an indication of effective IT project management, but not necessarily of effective IT investment management.
The SDLC is a framework that guides the development and implementation of IT systems and applications, but it does not address the alignment, justification, or measurement of the IT investments.
Key performance indicators (KPIs) are defined for each business requiring IT investment is an indication of effective IT performance management, but not necessarily of effective IT investment management. KPIs are metrics that measure the outcomes and results of IT activities and processes, but they do not address the alignment, justification, or value of the IT investments.
The IT investment budget is significantly below industry benchmarks is not an indication of effective IT investment management, but rather of low IT spending. The IT investment budget should be based on the organization's needs and capabilities, and not on external comparisons. A low IT investment budget may indicate that the organization is underinvesting in IT, which could limit its potential for growth and innovation.

最新問題**: 111**
情報セキュリティの指標を設計する際に最も重要な考慮事項は、指標が次の点であることです。
A. は理解しやすいです。
B. すべてのビジネス ユニットに適用されます。
C. 実用的なデータを提供します。
D. 業界標準に準拠します。
Answer: C (メーッセージを残す**)**

最新問題**: 112**
情報セキュリティ プログラムの成功に最も重要なのは次のどれですか?
A. 情報セキュリティに対するユーザーの責任
B. 情報セキュリティに対する経営陣の取り組み
C. ビジネスと情報セキュリティの統合
D. 情報セキュリティとIT目標の整合
Answer: B (メーッセージを残す**)**
Management's commitment to information security is the most critical factor for the success of an information security program, as it sets the tone and direction for the organization's security culture and practices. Management's commitment is demonstrated by establishing a clear security policy, providing adequate resources, assigning roles and responsibilities, enforcing compliance, and supporting continuous improvement. The other

options are important elements of an information security program, but they depend on management's commitment to be effective. References: CISA Review Manual (Digital Version) 1, page
439.

最新問題**: 113**
組織の監査担当者の主な業務:
A. 監査を実施する監査人の権限について説明します。
B. 監査人の行動規範を定義します。
C. 年間および四半期の監査計画を正式に記録します。
D. 監査プロセスと報告基準を文書化します。
Answer: (解答を表示する**)**
An organization's audit charter primarily describes the auditors' authority to conduct audits. The audit charter is a formal document that defines the purpose, scope, responsibilities, and reporting relationships of the internal audit function. It also establishes the auditors' right of access to information, records, personnel, and physical properties relevant to their work. The audit charter provides the basis for the auditors' independence and accountability to the governing body and senior management.

最新問題**: 114**
災害復旧計画 (DRP) 内で定義することが最も重要なのは次のどれですか?
A. 事業継続計画 (BCP)
B. バックアップデータの復元のテスト結果
C. 災害復旧シナリオと優先順位の包括的なリスト
D. 復旧チームメンバーの役割と責任
Answer: D (メーッセージを残す**)**
The most important thing to define within a disaster recovery plan (DRP) is the roles and responsibilities for recovery team members, as this ensures that everyone knows what to do, who to report to, and how to communicate in the event of a disaster. A business continuity plan (BCP) is a broader document that covers the overall strategy and objectives for maintaining or resuming business operations after a disaster. Test results for backup data restoration are important to verify the integrity and availability of backup data, but they are not part of the DRP itself. A comprehensive list of disaster recovery scenarios and priorities is useful to identify the potential risks and impacts of different types of disasters, but it is not as critical as defining the roles and responsibilities for recovery team members. References: CISA Review Manual (Digital Version), Chapter 4: Information Systems Operations, Maintenance and Service Management, Section 4.3: Disaster Recovery Planning1

最新問題**: 115**

企業のスマートフォンが紛失した場合に、そのデータの機密性を保護するための最適な予防策は次のどれですか。
A. リモートデータ消去プログラム
B. デバイスに保存されたデータの暗号化
C. デバイス認証用のパスワード
D. デバイスの生体認証
Answer: (解答を表示する**)**

最新問題**: 116**
IS 監査人は、コントロール自己評価 (CSA) プログラムへのサポートを提供するよう求められています。プログラムにおける監査人の役割の範囲を最もよく表すのは次のどれですか。
A. 監査人の存在により、他のチーム メンバーの監査責任が置き換えられます。
B. 監査人は詳細な監査手順を実行する必要がある
C. 監査人はプログラムのファシリテーターとして行動する必要があります。
D. 監査人はプロセスの生産性の向上に重点を置くべきである
Answer: C (メーッセージを残す**)**

最新問題**: 117**
IS 監査人が IS 部門の品質手順を確認するよう任命されています。監査人が IS マネージャーに連絡したところ、非公式で暗黙の標準があることが分かりました。監査人が次にとるべきアクションは次のどれですか 1?
A. 適切な品質基準についてIS管理に勧告する
B. IS管理が文書化された標準を実施するまで監査を延期する
C. 非公式標準に準拠していることを文書化する
D. 監査を完了し、結果を報告する
Answer: (解答を表示する**)**
The auditor's next action after finding that there is an informal unwritten set of standards in the IS department is to document and test compliance with the informal standards. This is because the auditor's role is to evaluate the adequacy and effectiveness of the existing controls, regardless of whether they are formal or informal, written or unwritten. The auditor should also assess the risks and implications of having informal standards, such as lack of consistency, accountability, or traceability. The auditor should not make recommendations, postpone the audit, or finalize the audit without performing the audit procedures.
References:
* CISA Review Manual (Digital Version), Chapter 2, Section 2.21
* CISA Online Review Course, Domain 1, Module 1, Lesson 12

最新問題**: 118**

プロジェクト評価中に、情報システム監査人は、ビジネス オーナーがプロジェクト開始フェーズから除外されていることを発見しました。この状況で監査人が最も懸念すべきことは次のどれですか。
A. 非現実的なマイルストーン
B. 不十分な成果物
C. メリットが不明瞭
D. 要件が不完全です
Answer: (解答を表示する**)**
The answer D is correct because the greatest concern for an IS auditor with the situation of business owners being removed from the project initiation phase is that the requirements may be incomplete. The project initiation phase is the first step in starting a new project, where the project's purpose, scope, objectives, and deliverables are defined and documented. The project initiation phase also involves identifying and engaging the key stakeholders who have an interest or influence in the project, such as sponsors, customers, users, or business owners.
Business owners are the individuals or entities who have the authority and responsibility to define the business needs and expectations for the project. They are also the primary beneficiaries of the project outcomes and benefits. Business owners play a crucial role in the project initiation phase, as they provide valuable input and feedback on the requirements and specifications of the project. Requirements are the statements that describe what the project should accomplish or deliver to meet the business needs and expectations. Requirements are essential for guiding the project planning, execution, monitoring, and closure phases.
If business owners are removed from the project initiation phase, it can result in incomplete or inaccurate requirements, which can have negative impacts on the project's quality, scope, time, cost, and risk. Some of the possible consequences of incomplete requirements are:
* Misalignment: The project may not align with the business strategy, vision, or goals, which can reduce its value or relevance.
* Confusion: The project team may not have a clear understanding of what the project should achieve or deliver, which can affect their performance or productivity.
* Rework: The project may need to undergo frequent changes or revisions to accommodate new or modified requirements, which can increase the time and cost of the project.
* Dissatisfaction: The project may not meet the expectations or satisfaction of the business owners or other stakeholders, which can affect their acceptance or support of the project.
* Failure: The project may not deliver the expected outcomes or benefits, which can affect its success or viability.
Therefore, an IS auditor should be concerned about the involvement and participation of business owners in the project initiation phase, as it affects the completeness and quality of requirements. An IS auditor should review the policies and procedures for stakeholder

identification and engagement, verify that the business owners have adequate knowledge and skills to define their requirements, and test that the requirements are well-defined, documented, approved, and communicated.
References:
* Project Initiation: The First Step to Project Management [2023] * Asana
* Everything you need to know about the project initiation phase
* Project Initiation Phase - The Business Professor
* Project Initiation: A Guide to Starting a Project Right Way - Kissflow

最新問題: **119**
監査フレームワークは、次の方法で IS 監査機能を支援できます。
A. 監査を完了するために必要な具体的な手順の概要を示します。
B. 監査プログラムの実行方法の詳細を提供します。
C. IS 監査機能の権限と責任を定義します。
D. 監査の実施に関する指示と情報を提供します。
Answer: D (メーッセージを残す**)**

最新問題: **120**
情報システム監査人が入力ソースからのトランザクションを投稿するバッチ処理が成功したことを確認するために最適な方法はどれですか?
A. エラーログの確認
B. 合計金額
C. ハッシュ合計
D. アイテムの総数
Answer: C (メーッセージを残す**)**

最新問題: **121**
新しいシステムの実装中に、各マイルストーンでリスク管理を確認するために IS 監査人が任命されました。監査人は、プロジェクトの利益に対するいくつかのリスクが対処されていないことを発見しました。これらのリスクを管理する責任は誰が負うべきでしょうか?
A. エンタープライズリスクマネージャー
B. プロジェクトスポンサー
C. 情報セキュリティ担当者
D. プロジェクトマネージャー
Answer: D (メーッセージを残す**)**
The project manager should be accountable for managing the risks to project benefits. Project benefits are the expected outcomes or value that a project delivers to its stakeholders, such as improved efficiency, quality, customer satisfaction, or revenue. Project risks are uncertain events or conditions that may affect the project objectives, scope, budget, schedule, or quality. The project manager is responsible for identifying,

analyzing, prioritizing, responding to, and monitoring project risks throughout the project life cycle. The other options are not accountable for managing project risks, as they have different roles and responsibilities. The enterprise risk manager is responsible for overseeing the organization's overall risk management framework and strategy, but not for managing specific project risks. The project sponsor is responsible for initiating, approving, and supporting the project, but not for managing project risks. The information security officer is responsible for ensuring that the project complies with the organization's information security policies and standards, but not for managing project risks. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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**
財務報告におけるエンドユーザー コンピューティング (EUC) アプリケーションに関連する最大のリスクは次のどれですか。
A. ソリューションを迅速に変更して展開できない
B. ユーザーにとっての移植性の欠如
C. 手動プロセスによる時間の損失
D. スプレッドシートの計算エラー
Answer: D (メーッセージを残す**)**
Spreadsheets, often used in EUC, are prone to manual input errors and formula mistakes. These errors can significantly compromise the accuracy and integrity of financial reporting. References
ISACA CISA Review Manual (Current Edition) - Chapter on End-User Computing (EUC) risks Industry Research on Spreadsheet Errors: Multiple studies highlight the prevalence of errors in spreadsheets, especially those used for financial purposes.

最新問題: **123**
導入後のレビュー中に情報システム監査人が最も懸念すべきことは次のうちどれですか?
A. システムには保守計画がありません。
B. システムにはいくつかの軽微な欠陥が含まれています。
C. システムの導入は 3 週間遅れました。
D. システムは予算を 15% 超過していました。

Answer: A (メーッセージを残す)
A post-implementation review (PIR) is an assessment conducted at the end of a project cycle to determine if the project was indeed successful and to identify any existing flaws in the project1. One of the main objectives of a PIR is to evaluate the outcome and functional value of a project1. Therefore, an IS auditor should be most concerned with whether the system meets the intended requirements and delivers the expected benefits to the stakeholders. A system that does not have a maintenance plan is a major risk, as it may not be able to cope with changing needs, fix errors, or prevent security breaches. A maintenance plan is essential for ensuring the system's reliability, availability, and performance in the long term2.
The other options are less critical for a PIR, as they are more related to the project management aspects than the system quality aspects. The system may contain several minor defects that do not affect its functionality or usability, and these can be resolved in future updates. The system deployment may be delayed by three weeks due to unforeseen circumstances or dependencies, but this does not necessarily mean that the system is faulty or ineffective. The system may be over budget by 15% due to various factors such as scope creep, resource constraints, or market fluctuations, but this does not imply that the system is not valuable or beneficial.
References: 1: Post-Implementation Review Best Practices - MetaPM 2: What is Post-Implementation Review in Project Management?

最新問題**: 124**
コーディング標準は次のどれを提供しますか?
A. プログラムドキュメント
B. アクセス制御テーブル
C. データフロー図
D. フィールドの命名規則
Answer: D (メーッセージを残す)
Coding standards provide field naming conventions, which are rules for naming variables, constants, functions, classes, and other elements in a program. Coding standards help to ensure consistency, readability, maintainability, and portability of code. Program documentation, access control tables, and data flow diagrams are not part of coding standards. References: CISA Review Manual (Digital Version), Chapter 4, Section 4.3.1

最新問題**: 125**
組織内のエンドユーザー コンピューティング (EUC) に関連するリスクを評価する情報システム監査人にとって、次の調査結果のうちどれが最も懸念されるでしょうか。
A. 各 EUC アプリケーションの所有権を追跡するためのプロセスが不十分ですか?
B. バージョン管理に必要なプロセスが不足しています
C. EUC ユーザーに対する意識啓発トレーニングの欠如
D. EUC アプリケーションの基準が定義されていない

Answer: (解答を表示する)

The finding that should be of greatest concern to an IS auditor assessing the risk associated with end-user computing (EUC) in an organization is the lack of defined criteria for EUC applications. EUC applications are applications that are developed and maintained by end-users, rather than by IT professionals, to support their business functions and processes. Examples of EUC applications include spreadsheets, databases, reports, and scripts. The lack of defined criteria for EUC applications means that the organization does not have clear and consistent standards or guidelines to identify, classify, and manage EUC applications. This can lead to various risks, such as:

* Inaccurate or unreliable data and results from EUC applications that are not validated, verified, or tested
* Unauthorized or inappropriate access or use of EUC applications that are not secured, controlled, or monitored
* Inconsistent or incompatible data and results from EUC applications that are not integrated, documented, or updated
* Loss or corruption of data and results from EUC applications that are not backed up, recovered, or archived Therefore, the IS auditor should be most concerned about the lack of defined criteria for EUC applications, as it can affect the quality, integrity, and availability of the EUC applications and the data they produce.

Insufficient processes to track ownership of each EUC application is a finding that should be of concern to an IS auditor assessing the risk associated with EUC in an organization, but it is not the greatest concern. The ownership of an EUC application refers to the person or group who is responsible for creating, maintaining, and using the EUC application. Insufficient processes to track ownership of each EUC application means that the organization does not have adequate mechanisms or records to identify and communicate who owns each EUC application. This can lead to risks, such as:

* Lack of accountability or ownership for the quality and accuracy of the EUC application and its data
* Lack of support or maintenance for the EUC application when the owner leaves or changes roles
* Lack of awareness or training for the users of the EUC application on its purpose and functionality However, these risks are less severe than those caused by the lack of defined criteria for EUC applications.

Insufficient processes to test for version control is a finding that should be of concern to an IS auditor assessing the risk associated with EUC in an organization, but it is not the greatest concern. Version control is a process that tracks and manages the changes made to an EUC application over time. Insufficient processes to test for version control means that the organization does not have adequate procedures or tools to ensure that the changes made to an EUC application are authorized, documented, and tested. This can lead to risks, such as:

* Errors or inconsistencies in the data and results from different versions of the EUC application
* Conflicts or confusion among the users of the EUC application on which version is current or correct
* Loss or overwrite of data and results from previous versions of the EUC application However, these risks are less severe than those caused by the lack of defined criteria for EUC applications.
Lack of awareness training for EUC users is a finding that should be of concern to an IS auditor assessing the risk associated with EUC in an organization, but it is not the greatest concern. Awareness training for EUC users is a process that educates and informs the users of the EUC applications on their roles, responsibilities, and risks. Lack of awareness training for EUC users means that the organization does not have adequate programs or materials to raise the knowledge and skills of the users on how to use and manage the EUC applications effectively and securely. This can lead to risks, such as:
* Misuse or abuse of the EUC applications by users who are not aware of their impact or implications
* Non-compliance or violation of policies or regulations by users who are not aware of their requirements or expectations
* Dissatisfaction or frustration among users who are not aware of their benefits or limitations However, these risks are less severe than those caused by the lack of defined criteria for EUC applications.
References:
* End-user computing - Wikipedia 1
* How to Manage the Risks Associated with End User Computing 2
* Managing end user computing risks - KPMG UK 3

最新問題**: 126**
情報を分類する場合、分類を次の基準に合わせることが最も重要です。
A. ビジネスリスク
B. セキュリティポリシー
C. データ保持要件
D. 業界標準
Answer: A (メーッセージを残す**)**
When classifying information, it is most important to align the classification to business risk, because it ensures that the information is protected according to its value and impact to the organization34. Business risk considers factors such as legal, regulatory, contractual, operational, reputational, and financial implications of information disclosure or compromise34. Aligning information classification to business risk also helps to prioritize and allocate resources for information security measures. Security policy, data retention requirements, and industry standards are important considerations for information

classification, but not as important as business risk. References: 3: CISA Review Manual (Digital Version), Chapter 5, Section 5.4.2 4:
CISA Online Review Course, Module 5, Lesson 4

最新問題**: 127**
現在の規制では、組織は重大なセキュリティ インシデントを特定してから 24 時間以内に規制当局に報告することが義務付けられています。規制への準拠を促進するために、情報システム監査人が推奨するベスト プラクティスは次のうちどれですか。
A. セキュリティ インシデントをタイムリーに特定するための主要業績評価指標 (KPI) を確立します。
B. インシデント処理のために外部のセキュリティ インシデント対応の専門家を雇用します。
C. 侵入検知システム (IDS) の警告機能を強化します。
D. インシデント管理対応計画に要件を含めます。
Answer: (解答を表示する**)**
The best recommendation for the IS auditor to facilitate compliance with the new regulation is to include the requirement in the incident management response plan. An incident management response plan is a document that defines the roles, responsibilities, processes, and procedures for responding to security incidents. By including the new regulation in the plan, the IS auditor can ensure that the organization is aware of the reporting obligation, has a clear workflow for notifying the regulator within 24 hours, and has the necessary documentation and evidence to support the report.
The other options are not as effective as including the requirement in the incident management response plan:
* Establishing key performance indicators (KPIs) for timely identification of security incidents is a good practice, but it does not guarantee compliance with the regulation. KPIs are metrics that measure the performance of a process or activity, but they do not specify how to perform it. The IS auditor should also provide guidance on how to identify and report security incidents within 24 hours.
* Engaging an external security incident response expert for incident handling is a possible option, but it may not be feasible or cost-effective. The organization may not have the budget or time to hire an external expert, or may prefer to handle the incidents internally. The IS auditor should also evaluate the qualifications and trustworthiness of the external expert, and ensure that they comply with the regulation and other contractual or legal obligations.
* Enhancing the alert functionality of the intrusion detection system (IDS) is a useful measure, but it is not sufficient to comply with the regulation. An IDS is a tool that monitors network traffic for malicious activity and alerts the network administrator or takes preventive action. However, an IDS may not detect all types of security incidents, or may

generate false positives or negatives. The IS auditor should also consider other sources of incident detection, such as logs, reports, audits, or user feedback.

最新問題: **128**
インシデント管理プロセスが効果的であることを最もよく示すのは次のどれですか?
A. IT 管理者が確認するインシデントの数の増加
B. 報告された重大なインシデントの数の増加
C. ヘルプデスクへの電話件数が減少
D. インシデント解決時間の短縮
Answer: D (メーッセージを残す)

最新問題: **129**
エンドユーザー コンピューティング (EUC) アプリケーションにバージョン管理を実装する最も重要な理由はどれですか?
A. 古いバージョンを参照用に利用できるようにするため
B. アプリケーションの最新の承認バージョンのみが使用されるようにするため
C. アプリケーションの異なるバージョン間の互換性を確保するため
D. 許可されたユーザーのみがアプリケーションにアクセスできるようにする
Answer: (解答を表示する)
Version control is a process of managing changes to an application or a document. It ensures that only the latest approved version of the application is used by end-users, which reduces the risk of errors, inconsistencies, and unauthorized modifications. Version control also allows tracking the history of changes and restoring previous versions if needed.

最新問題: **130**
IS 監査人は、ビジネス クリティカルなアプリケーションには現在、いかなるレベルのフォールト トレランスも備わっていないことに気付きました。
この状況に関して最も懸念されるのは次のうちどれですか?
A. 単一障害点
B. サービスの低下
C. ダメージに対する許容度が制限される
D. 平均故障間隔 (MTBF) の短縮
Answer: A (メーッセージを残す)

最新問題: **131**
経営陣は、従業員が意図的または意図せずに機密情報を添付ファイルとして組織外に電子メールで送信することを懸念しています。関連する電子メール制御を実装する前に最も重要なタスクは何ですか?
A. 情報分類スキームを開発します。

B. 電子メールの監視の可能性について従業員に通知します。
C. すべての従業員に秘密保持契約 (NDA) に署名することを義務付けます。
D. エンドユーザー コンピューティング (EUC) の許容使用ポリシーを策定します。
Answer: (解答を表示する**)**

最新問題**: 132**
組織の定義済みデータ バックアップおよび復元手順を確認する際に考慮すべき最も重要なのは次のどれですか。
A. 事業継続計画 (BCP)
B. リカバリポイント目標 (RPO)
C. 平均復旧時間 (MTTR)
D. 平均故障間隔 (MTBF)
Answer: B (メーッセージを残す**)**
A recovery point objective (RPO) is the maximum acceptable amount of data loss after an unplanned data- loss incident, expressed as an amount of time. This is generally thought of as the point in time before the event at which data can be successfully recovered - that is, the time elapsed since the most recent reliable backup1. RPOs are important to consider when reviewing an organization's defined data backup and restoration procedures, because they determine how frequently the organization needs to perform backups, and how much data it can afford to lose in case of a disaster. RPOs are usually defined based on the business impact and criticality of the data, as well as the compliance and regulatory requirements. For example, a financial institution may have a very low RPO (such as a few minutes or seconds) for its transactional data, while a research institute may have a higher RPO (such as a few hours or days) for its experimental data.
The other possible options are:
* A. Business continuity plan (BCP): A BCP is a document that outlines how an organization will continue to operate or resume its critical functions and processes in the event of a disruption or disaster.
A BCP includes various elements, such as risk assessment, business impact analysis, recovery strategies, roles and responsibilities, communication plan, and testing and maintenance. A BCP is related to an organization's defined data backup and restoration procedures, but it is not the most important factor to consider when reviewing them. A BCP defines the recovery objectives and strategies for the entire organization, while the data backup and restoration procedures are more specific and technical in nature.
* C. Mean time to restore (MTTR): MTTR is a metric that measures the average time it takes to restore a system or service after a failure or outage. MTTR is an indicator of the efficiency and effectiveness of an organization's recovery process, as well as the availability and reliability of its systems or services.
MTTR is related to an organization's defined data backup and restoration procedures, but it is not the most important factor to consider when reviewing them. MTTR reflects the

actual performance of the recovery process, while the data backup and restoration procedures define the expected steps and actions for the recovery process.
* D. Mean time between failures (MTBF): MTBF is a metric that measures the average time between failures or outages of a system or service. MTBF is an indicator of the quality and durability of an organization's systems or services, as well as their susceptibility to failures or outages. MTBF is related to an organization's defined data backup and restoration procedures, but it is not the most important factor to consider when reviewing them. MTBF reflects the potential frequency of failures or outages, while the data backup and restoration procedures define the contingency plans for failures or outages.

最新問題**: 133**
公開鍵基盤 (PKI) 環境内で否認防止はどのようにサポートされますか?
A. ユーザーが受信したデータを秘密鍵を使用して復号化することで
B. エンタープライズキー管理システムの使用を通じて
C. 証明機関 (CA) が発行した証明書を使用することで
D. 送信されるメッセージに楕円曲線暗号を使用することで
Answer: C (メーッセージを残す**)**

最新問題**: 134**
IS 監査人は、メジャーリリース後に注文処理システムのトランザクション処理時間が大幅に増加したことに気づきました。IS 監査人が最初に確認する必要があるのは次のうちどれですか。
A. キャパシティ管理計画
B. トレーニングプラン
C. データベース変換結果
D. ストレステストの結果
Answer: D (メーッセージを残す**)**
The first thing that an IS auditor should review when finding that transaction processing times in an order processing system have significantly increased after a major release is stress testing results. Stress testing is a type of testing that evaluates how a system performs under extreme or abnormal conditions, such as high volume, load, or concurrency of transactions. Stress testing results can help explain why transaction processing times in an order processing system have significantly increased after a major release by revealing any bottlenecks, limitations, or errors in the system's capacity, performance, or functionality under stress. The other options are not as relevant as stress testing results in explaining why transaction processing times in an order processing system have significantly increased after a major release, as they do not directly measure how the system performs under extreme or abnormal conditions. Capacity management plan is a document that defines and implements the processes and activities for ensuring that the system has adequate resources and capabilities to meet current and future

demands. Training plans are documents that define and implement the processes and activities for ensuring that the system users have adequate skills and knowledge to use the system effectively and efficiently. Database conversion results are outcomes or outputs of transforming data from one format or structure to another to suit the system's requirements or specifications. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3

最新問題**: 135**
事業継続計画の一環として、ビジネス影響分析 (B1A) を実施する際に評価することが最も重要なのは次のどれですか。
A. リスク許容度
B. クラウド上の重要なアプリケーション
C. 重要な資産インベントリの完全性
D. 回復シナリオ
Answer: C (メーッセージを残す**)**
The most important thing to assess when conducting a business impact analysis (BIA) is the completeness of critical asset inventory. This is because the critical asset inventory is the basis for identifying and prioritizing the business processes, functions, and resources that are essential for the continuity of operations. The critical asset inventory should include both tangible and intangible assets, such as hardware, software, data, personnel, facilities, contracts, and reputation. The critical asset inventory should also be updated regularly to reflect any changes in the business environment or needs. References:
* CISA Review Manual (Digital Version), Chapter 5, Section 5.41
* CISA Online Review Course, Domain 3, Module 3, Lesson 12

最新問題**: 136**
組織が新たに導入したオンライン セキュリティ意識向上プログラムをレビューする情報システム監査人にとって、次の調査結果のうち最も懸念すべきものはどれですか。
A. プログラムへの参加は新入社員のみに義務付けられています
B. トレーニング結果を評価するための指標が確立されていない
C. 従業員は結果をすぐには通知されません
D. プログラムの更新時期は未定です
Answer: B (メーッセージを残す**)**
The greatest concern for an IS auditor reviewing an online security awareness program is that metrics have not been established to assess training results. Without metrics, it is difficult to measure the effectiveness of the program and identify areas for improvement. The other findings are also issues that need to be addressed, but they are not as significant as the lack of metrics. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.3.11

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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**
ある組織では、データ センターに入るためにキー カードの使用を義務付けています。最近、各従業員に生体認証を要求する制御が実装されました。どのような種類の制御が追加されたのでしょうか。
A. 探偵
B. 予防的
C. 修正
D. 補償
Answer: B (メーッセージを残す**)**

最新問題: **138**
組織がサードパーティ アプリケーションのパフォーマンスに関連するリスクを軽減するための最良の方法はどれですか?
A. サードパーティが要件を満たすために十分なリソースを割り当てていることを確認します。
B. 内部監査機能内で分析を使用する
C. キャパシティ プランニング演習を実施する
D. パフォーマンス監視ツールを使用してサービス レベル契約 (SLA) を検証する
Answer: (解答を表示する**)**
The best way for an organization to mitigate the risk associated with third-party application performance is to utilize performance monitoring tools to verify service level agreements (SLAs). Performance monitoring tools are software or hardware devices that measure and report the performance of an application or system, such as speed, availability, reliability, etc. Performance monitoring tools can help mitigate the risk associated with third-party application performance, by allowing the organization to verify whether the third-party provider is meeting the SLAs, which are contracts or agreements that define the expected level and quality of service for an application or system. Performance monitoring tools can also help identify and resolve any performance issues or problems that may arise from the third-party application. Ensuring the third party allocates adequate resources to meet requirements is a possible way to mitigate the risk associated with third-party application performance, but it is not the best one, as it may not be feasible or effective depending on the availability, cost, and suitability of the resources. Using analytics within the internal

audit function is a possible way to mitigate the risk associated with third-party application performance, but it is not the best one, as it may not be timely or relevant depending on the frequency, scope, and quality of the analytics. Conducting a capacity planning exercise is a possible way to mitigate the risk associated with third-party application performance, but it is not the best one, as it may not be accurate or reliable depending on the assumptions, methods, and data used for the capacity planning.

最新問題**: 139**
オブジェクト指向テクノロジの主な利点は強化されます:
A. ロジックの要素を再利用することによる効率性。
B. データアクセスのための順次プログラム実行の管理。
C. オブジェクトをデータ アクセス用のメソッドにグループ化します。
D. データ オブジェクトの制限されたさまざまなデータ型の管理。
Answer: A (メーッセージを残す**)**
The primary advantage of object-oriented technology is enhanced efficiency due to the re-use of elements of logic. Object-oriented technology is a software design model that uses objects, which contain both data and code, to create modular and reusable programs. Objects can be inherited from other objects, which reduces duplication and improves maintainability. Grouping objects into methods for data access, managing sequential program execution for data access, and managing a restricted variety of data types for a data object are not advantages of object-oriented technology. References: ISACA CISA Review Manual 27th Edition, page 304

最新問題**: 140**
ある組織では、仮想デスクトップを使用してエンド ユーザーに企業アプリケーションを提供したいと考えています。クラウド環境でのドメイン ネーム システム (DNS) ポイズニングを防ぐために、IS 監査人が推奨すべきことは次のどれですか。
A. DNS の脆弱性をスキャンするウイルス対策ツールが組み込まれた企業のラップトップをエンドユーザーに提供します。
B. ドメイン解決要求に対して適切なサイズの応答を作成するように ONS サーバーを構成します。
C. DNS の変更が組織のクラウド アカウント内のすべてのサーバーに反映されていることを確認します。
D. なりすまし者が DNS テーブルを変更するのを防ぐために、管理者の検証を有効にします。
Answer: D (メーッセージを残す**)**

最新問題**: 141**

組織のセキュリティ ポリシーでは、すべての新入社員が適切なセキュリティ意識向上トレーニングを受けることが義務付けられています。次のどの指標が、このポリシーへの準拠を最も確実に保証しますか?
A. トレーニングを完了した新入社員の割合。
B. 企業のセキュリティ ポリシーに違反した新入社員の数。
C. 新入社員による報告されたインシデントの数。
D. インシデントを報告する新入社員の割合
Answer: (解答を表示する**)**
The best metric to assure compliance with the policy of providing security awareness training to all new employees is the percentage of new hires that have completed the training, as this directly measures the extent to which the policy is implemented and enforced. The number of new hires who have violated enterprise security policies, the number of reported incidents by new hires, and the percentage of new hires who report incidents are not directly related to the policy, as they may depend on other factors such as the nature and frequency of threats, the effectiveness of security controls, and the reporting culture of the organization.
References: CISA Review Manual (Digital Version), Chapter 5, Section 5.7

最新問題**: 142**
アプリケーション開発受け入れテストに関して最も重要なのは次のどれですか?
A. プログラミング チームがテスト プロセスに関与します。
B. 変換前にすべてのデータ ファイルの有効な情報がテストされます。
C. テストが開始される前に、ユーザー管理者がテスト設計を承認します。
D. 品質保証 (QA) チームがテスト プロセスを担当します。
Answer: C (メーッセージを残す**)**
The most important aspect of an application development acceptance test is that user management approves the test design before the test is started, as this ensures that the test objectives, criteria, and procedures are aligned with the user requirements and expectations. The programming team's involvement in the testing process, the testing of data files for valid information before conversion, and the quality assurance (QA) team' s charge of the testing process are also important, but they are not as critical as user management's approval of the test design. References: CISA Review Manual (Digital Version), Chapter 4, Section 4.4.2

最新問題**: 143**
給与計算アプリケーションに関する監査結果に応じて、経営陣は新しい自動化された制御を実装しました。新しい制御の有効性を評価する際に、情報システム監査人に最も役立つのは次のどれでしょうか。
A. 実装前に承認されたテスト スクリプトと結果
B. プロセスと制御を定義する文書化された手順

C. 承認されたプロジェクト範囲文書
D. テーブルトップ演習の結果のレビュー
Answer: (解答を表示する**)**
The best way to evaluate the effectiveness of a new automated control is to review the written procedures that define the processes and controls. This will help the IS auditor to understand the objectives, scope, roles, responsibilities, and expected outcomes of the control. The written procedures will also provide a basis for testing the control and verifying its compliance with the audit finding recommendations. References:
* ISACA Frameworks: Blueprints for Success
* CISA Review Manual (Digital Version)

最新問題**: 144**
成熟した戦略計画プロセスを最もよく反映しているのはどれですか?
A. 企業戦略をサポートするIT戦略計画
B. 制御と安全対策の仕様を含むIT戦略計画
C. 戦略計画に基づくITプロジェクトは経営陣によって承認される
D. すべてのプロジェクトにIT要件が組み込まれたアクションプラン
Answer: A (メッセージを残す**)**

最新問題**: 145**
組織の品質保証 (QA) 機能の次の責任のうち、IS 監査人が懸念すべきものはどれですか?
A. 開発プロセス内で標準が遵守されていることを確認する
B. テスト作業が観察をサポートしていることを確認する
C. 開発手法の更新
D. 欠陥を修正するためのソリューションの実装
Answer: D (メッセージを残す**)**
Implementing solutions to correct defects is a responsibility of the development function, not the quality assurance (QA) function. The QA function should ensure that the development process follows the established standards and methodologies, and that the defects are identified and reported. The QA function should not be involved in fixing the defects, as this would compromise its independence and objectivity. The other options are valid responsibilities of the QA function, and they should not raise concern for an IS auditor. References: CISA Review Manual (Digital Version) 1, page 300.

最新問題**: 146**
IS 監査人が組織の IT 戦略と計画を評価しています。次のどれが最も懸念されるでしょうか?
A. 定義された IT セキュリティ ポリシーはありません。
B. 事業戦略会議の議事録は配布されません。
C. IT はビジネス戦略計画に携わっていません。

D. IT 戦略計画に関する文書が不十分です。
Answer: C (メーッセージを残す**)**
The greatest concern for an IS auditor when evaluating an organization's IT strategy and plans is that IT is not engaged in business strategic planning, as this indicates a lack of alignment between IT and business objectives, which could result in inefficient and ineffective use of IT resources and capabilities. The absence of a defined IT security policy, the nondistribution of business strategy meeting minutes, and the inadequate documentation of IT strategic planning are also issues that should be addressed by an IS auditor, but they are not as significant as IT's noninvolvement in business strategic planning. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.1

最新問題**: 147**
次のアプリケーションのうち、最も固有のリスクがあり、監査計画中に優先する必要があるものはどれですか?
A. 廃止されたレガシーアプリケーション
B. サポートされていないオンサイトアプリケーション
C. アウトソーシングされた会計アプリケーション
D. 社内で開発されたアプリケーション
Answer: C (メーッセージを残す**)**
An outsourced accounting application has the most inherent risk and should be prioritized during audit planning because it involves external parties, sensitive data, and complex transactions that are susceptible to material misstatement, error, or fraud12. An outsourced accounting application also requires more oversight and monitoring from the internal audit department to ensure compliance with the service level agreement and the organization's policies and standards3.
References
1: Inherent Risk: Definition, Examples, and 3 Types of Audit Risks 2: 3 Types of Audit Risk - Inherent, Control and Detection - Accountinguide 3: IS Audit Basics: The Core of IT Auditing

最新問題**: 148**
監査により、コンピュータ システムが注文要求に連続した注文番号を割り当てていないことが判明しました。情報システム監査人は、経営陣がこの発見を留保しているかどうかを判断するために監査フォローアップを実施しています。次の 2 つのうち、最も信頼性の高いフォローアップ手順はどれですか。
A. 撤回された変更のドキュメントを確認して、連続した順序番号付けを実装します。
B. システムが連続した注文番号を生成するように構成され、テストされているかどうかを管理者に問い合わせます。
C. システム設定とトランザクション ログを調べて、連続した注文番号が生成されているかどうかを確認します。

D. 経営陣から取得したシステム生成の発注書のサンプルを調べる
Answer: C (メーッセージを残す**)**
The most reliable follow-up procedure to determine if management has resolved the finding of non-sequential purchase order numbers is to inspect the system settings and transaction logs to determine if sequential order numbers are generated. This will provide direct evidence of the system's functionality and compliance with the audit recommendation. The other options are less reliable because they rely on indirect evidence or information obtained from management, which may not be accurate or complete. References: CISA Review Manual (Digital Version), Standards, Guidelines, Tools and Techniques

最新問題**: 149**
デジタル署名を最もよく表すのは次のどれですか?
A. 受信者の制御下にあります。
B. 認証が可能です。
C. データの変更を動的に検証します。
D. 使用する送信者に固有のものです。
Answer: (解答を表示する**)**
A digital signature is a type of electronic signature that uses cryptographic techniques to provide authentication, integrity, and non-repudiation of digital documents. A digital signature is created by applying a mathematical function (called a hash function) to the document and then encrypting the result with the sender's private key. The encrypted hash, along with the sender's public key and other information, forms the digital signature. The receiver can verify the digital signature by decrypting it with the sender's public key and comparing the hash with the one computed from the document. If they match, it means that the document has not been altered and that it was signed by the owner of the private key.
Option D is correct because a digital signature is unique to the sender using it, as it depends on the sender's private key, which only the sender knows and controls. No one else can create a valid digital signature with the same private key, and no one can forge or modify a digital signature without being detected.
Option A is incorrect because a digital signature is not under control of the receiver, but rather under control of the sender. The receiver can only verify the digital signature, but cannot create or modify it.
Option B is incorrect because a digital signature is not capable of authorization, but rather capable of authentication. Authorization is the process of granting or denying access to resources based on predefined rules or policies. Authentication is the process of verifying the identity or legitimacy of a person or entity. A digital signature can authenticate the sender of a document, but it cannot authorize what actions the receiver can perform on the document.

Option C is incorrect because a digital signature does not dynamically validate modifications of data, but rather statically validates the integrity of data. A digital signature is based on a snapshot of the document at the time of signing, and any subsequent changes to the document will invalidate the digital signature. A digital signature does not monitor or update itself based on data modifications.
References:
CISA Online Review Course1, Module 5: Protection of Information Assets, Lesson 2: Encryption Basics, slide 13-14.
CISA Review Manual (Digital Version)2, Chapter 5: Protection of Information Assets, Section 5.2:
Encryption Basics, p. 273-274.
CISA Review Manual (Print Version), Chapter 5: Protection of Information Assets, Section 5.2: Encryption Basics, p. 273-274.
CISA Questions, Answers & Explanations Database3, Question ID: QAE_CISA_712.
What Is a Digital Signature (and How Does it Work)1
What are digital signatures and certificates?2
Digital Signature Definition3
Examples and uses of electronic signatures4
What is an Electronic Signature?5

最新問題**: 150**
IS 管理者は最近、ユーザーにクエリ パフォーマンスの向上を提供するために、データベース管理システム (DBMS) ソフトウェアの特定の参照整合性コントロールを無効にしました。次のコントロールのうち、参照整合性の欠如を最も効果的に補うのはどれですか。
A. より頻繁なデータバックアップ
B. 周期表のリンクチェック
C. 同時アクセス制御
D. パフォーマンス監視ツール
Answer: (解答を表示する**)**
Referential integrity is a property of data that ensures that all references between tables are valid and consistent. Disabling referential integrity controls can result in orphaned records, data anomalies, and inaccurate queries. The most effective way to compensate for the lack of referential integrity is to perform periodic table link checks, which verify that all foreign keys match existing primary keys in the related tables.
More frequent data backups, concurrent access controls, and performance monitoring tools do not address the issue of data consistency and accuracy. References: ISACA CISA Review Manual 27th Edition, page 291

最新問題**: 151**
契約上の合意においてソースコード エスクローを要求する主な目的は次のとおりです。
A. ベンダー管理ポリシーに準拠する

B. ソース コードを新しい実行可能コードに変換します。
C. 規制要件を満たす。
D. ソースコードが利用可能であることを確認します。
Answer: D (メーッセージを残す**)**
The primary purpose of requiring source code escrow in a contractual agreement is to ensure the source code is available. Source code escrow is a service that involves depositing the source code of a software or system with a third-party agent or escrow provider, who can release it to a designated beneficiary under specific conditions, such as bankruptcy, termination, or breach of contract by the software vendor or developer. Source code escrow can help to protect the interests and rights of the software user or licensee, who may need access to the source code for maintenance, modification, enhancement, or troubleshooting purposes. The IS auditor should verify that the contractual agreement specifies the terms and conditions for source code escrow, such as the escrow agent, the escrow fees, the deposit frequency and format, the release events and procedures, and the verification and audit requirements. References: CISA Review Manual (Digital Version)
1, Chapter 3, Section 3.2.2

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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**
データ漏洩のリスクを軽減するための最も効果的な予防管理として、情報システム監査人が推奨するのは何でしょうか?
A. 紙の文書が安全に廃棄されていることを確認します。
B. 侵入検知システム (IDS) を実装します。
C. アプリケーション ログに、行われた変更がすべて記録されていることを確認します。
D. すべてのデータファイルにデジタル透かしが含まれていることを検証します
Answer: D (メーッセージを残す**)**
Digital watermarks are hidden marks or codes that can be embedded into digital files, such as images, videos, audio, or documents. They can be used to identify the source, owner, or authorized user of the data, as well as to track any unauthorized copying or distribution of the data. Digital watermarks can help prevent data leakage by deterring potential leakers from sharing sensitive data or by providing evidence of data leakage if it occurs.

The other options are not as effective as digital watermarks in preventing data leakage. Ensuring that paper documents are disposed securely can reduce the risk of physical data leakage, but it does not address the digital data leakage that is more prevalent in today's environment. Implementing an intrusion detection system (IDS) can help detect and respond to cyberattacks that may cause data leakage, but it does not prevent data leakage from insiders or authorized users who have legitimate access to the data. Verifying that application logs capture any changes made can help audit and investigate data leakage incidents, but it does not prevent them from happening in the first place.
References:
* What is Data Leakage?
* What is Digital Watermarking?

最新問題**: 153**
IS 監査人は、適切にチェックアウトされておらず、使用後に再度チェックインされていないサーバーの管理者アカウントを昇格させます。問題の範囲を判断するための最も適切なサンプリング手法は次のどれですか。
A. ランダムサンプリング
B. 層別抽出法
C. 無作為抽出
D. 統計的サンプリング
Answer: D (メーッセージを残す**)**

最新問題**: 154**
効果的な災害復旧計画 (DRP) が実施されていることを最もよく示すのは次のどれですか?
A. バックアップの頻繁なテスト
B. 年次ウォークスルーテスト
C. 定期的なリスク評価
D. 完全な動作テスト
Answer: (解答を表示する**)**
A disaster recovery plan (DRP) is a set of procedures and resources that enable an organization to restore its critical operations, data, and applications in the event of a disaster1. A DRP should be aligned with the organization's business continuity plan (BCP), which defines the strategies and objectives for maintaining business functions during and after a disaster1.
To ensure that a DRP is effective, it should be tested regularly and thoroughly to identify and resolve any issues or gaps that might hinder its execution2345. Testing a DRP can help evaluate its feasibility, validity, reliability, and compatibility with the organization's environment and needs4. Testing can also help prepare the staff, stakeholders, and vendors involved in the DRP for their roles and responsibilities during a disaster3.

There are different methods and levels of testing a DRP, depending on the scope, complexity, and objectives of the test4. Some of the common testing methods are:
* Walkthrough testing: This is a step-by-step review of the DRP by the disaster recovery team and relevant stakeholders. It aims to verify the completeness and accuracy of the plan, as well as to clarify any doubts or questions among the participants45.
* Simulation testing: This is a mock exercise of the DRP in a simulated disaster scenario. It aims to assess the readiness and effectiveness of the plan, as well as to identify any challenges or weaknesses that might arise during a real disaster45.
* Checklist testing: This is a verification of the availability and functionality of the resources and equipment required for the DRP. It aims to ensure that the backup systems, data, and documentation are accessible and up-to-date45.
* Full interruption testing: This is the most realistic and rigorous method of testing a DRP. It involves shutting down the primary site and activating the backup site for a certain period of time. It aims to measure the actual impact and performance of the DRP under real conditions45.
* Parallel testing: This is a less disruptive method of testing a DRP. It involves running the backup site in parallel with the primary site without affecting the normal operations. It aims to compare and validate the results and outputs of both sites45.
Among these methods, full interruption testing would best demonstrate that an effective DRP is in place, as it provides the most accurate and comprehensive evaluation of the plan's capabilities and limitations4. Full interruption testing can reveal any hidden or unforeseen issues or risks that might affect the recovery process, such as data loss, system failure, compatibility problems, or human errors4. Full interruption testing can also verify that the backup site can support the critical operations and services of the organization without compromising its quality or security4.
However, full interruption testing also has some drawbacks, such as being costly, time-consuming, risky, and disruptive to the normal operations4. Therefore, it should be planned carefully and conducted periodically with proper coordination and communication among all parties involved4.
The other options are not as effective as full interruption testing in demonstrating that an effective DRP is in place. Frequent testing of backups is only one aspect of checklist testing, which does not cover other components or scenarios of the DRP4. Annual walk-through testing is only a theoretical review of the DRP, which does not test its practical implementation or outcomes4. Periodic risk assessment is only a preparatory step for developing or updating the DRP, which does not test its functionality or performance4.
References: 2: Best Practices For Disaster Recovery Testing | Snyk 3: Disaster Recovery Plan (DR) Testing
- Methods and Must-haves - US Signal 4: Disaster Recovery Testing: What You Need to Know - Enterprise Storage Forum 5: Disaster Recovery Testing Best Practices - MSP360 1: How to Test a Disaster Recovery Plan - Abacus

最新問題: **155**
新しいアプリケーション システムの実現可能性調査をレビューする IS 監査人にとって、最も懸念されるのは次のどれでしょうか。
A. ビジネスケースには、明確に定義された戦略的メリットが含まれていません。
B. セキュリティ要件が定義されていません。
C. システムが動作する条件は不明です。
D. システム要件と期待が明確にされていません。
Answer: (解答を表示する)

最新問題: **156**
IS 監査人は、患者の体に装着され、自動的に測定値を取得してクラウド サーバーにアップロードする医療機器をレビューしています。測定値に基づいて治療が更新されることがあります。監査人が主に重点を置くべきは次のどれですか。
A. デバイスが定期的に更新されていることの確認
B. デバイスの識別と認証
C. デバイスのセキュリティと品質の認証
D. デバイス上の物理的なアクセス制御
Answer: C (メーッセージを残す)

最新問題: **157**
新しいソフトウェア アプリケーションを迅速に開発するためのアジャイル プロジェクトの有効性を実現するベストな方法は、次のうちどれですか。
A. プロジェクトセグメントが確立されます。
B. 作業はフェーズに分かれています。
C. 作業はスプリントに分割されます。
D. プロジェクトのマイルストーンが作成されます。
Answer: C (メーッセージを残す)
The best way to enable the effectiveness of an agile project for the rapid development of a new software application is to separate the work into sprints. Sprints are short, time-boxed iterations that deliver a potentially releasable product increment at the end of each sprint. Sprints allow agile teams to work in a flexible and adaptive manner, respond quickly to changing customer needs and feedback, and deliver value faster and more frequently. Sprints also help teams to plan, execute, review, and improve their work in a collaborative and transparent way. Project segments, phases, and milestones are not specific to agile projects and do not necessarily enable the effectiveness of an agile project. References: Agile Project Management
[What is it & How to Start] - Atlassian, CISA Review Manual (Digital Version).

最新問題: **158**
IT 災害復旧時間目標 (RTO) は、次の基準に基づく必要があります。

A. 許容可能な最大データ損失。
B. 停止の性質
C. 最大許容ダウンタイム (MTD)。
D. ビジネスで定義されたシステムの重要度。
Answer: (解答を表示する**)**
IT disaster recovery time objectives (RTOs) are the maximum acceptable time that an IT system can be unavailable after a disaster before it causes unacceptable consequences for the business. IT RTOs should be based on the business-defined criticality of the systems, which reflects how important they are for supporting the business processes and functions. The maximum tolerable loss of data, the nature of the outage, and the maximum tolerable downtime (MTD) are also factors that affect the IT RTOs, but they are not the primary basis for determining them.

最新問題**: 159**
オンコール プログラマーから真夜中にセキュリティ管理者に電話がかかってきました。いくつかのプログラムが失敗し、プログラマーはライブ システムへのアクセスを要求しました。最善の対応策は何でしょうか?
A. 変更要求が完了して承認されることを要求する
B. プログラマーに一時的なアクセスのための緊急IDを与え、アクティビティを確認する
C. 問題を調査するためにプログラマーに読み取り専用アクセス権を与える
D. 翌日のアクティビティログを確認し、疑わしいアクティビティがあれば調査する
Answer: (解答を表示する**)**
The best course of action for a security administrator who is called in the middle of the night by the on-call programmer who needs access to the live system is to give the programmer an emergency ID for temporary access and review the activity. This is because:
Requiring that a change request be completed and approved may delay the resolution of the problem and cause further damage or disruption to the system or business operations. A change request is a formal document that describes the proposed change, its rationale, impact, benefits, risks, costs, and approval process. A change request is usually required for planned or scheduled changes, not for emergency or urgent changes.
Giving the programmer read-only access to investigate the problem may not be sufficient or effective, as the programmer may need to perform actions or tests that require write or execute permissions. Read-only access means that the user can only view or copy data or files, but cannot modify or delete them.
Reviewing activity logs the following day and investigating any suspicious activity may not prevent or detect any unauthorized or malicious actions by the programmer in real time. Activity logs are records of events and actions that occur within a system or network. Activity logs can provide evidence and accountability for system activities, but they are not proactive or preventive controls.

Therefore, giving the programmer an emergency ID for temporary access and reviewing the activity is the best course of action, as it allows the programmer to access the live system and resolve the problem quickly, while also ensuring that the security administrator can monitor and verify the programmer's activity and revoke the access when it is no longer needed. An emergency ID is a temporary account that grants a user elevated privileges or access to a system or resource for a specific purpose and duration. An emergency ID should be:
Created and authorized by a security administrator or manager
Assigned to a specific user and purpose
Limited in scope and time
Logged and audited
Revoked and deleted after use
Some of the best practices for emergency access to live systems are12:
Establish clear policies and procedures for requesting, approving, granting, monitoring, reviewing, and revoking emergency access Define criteria and scenarios for emergency access, such as severity, impact, urgency, and risk Implement controls to prevent unauthorized or unnecessary use of emergency access, such as multifactor authentication, approval workflows, alerts, notifications, and time restrictions Implement controls to track and audit emergency access activities, such as logging, reporting, analysis, and investigation Implement controls to ensure accountability and responsibility for emergency access users, such as attestation, justification, documentation, and feedback

最新問題**: 160**
最近の実装後のレビューで、IS 監査人は、導入されたアプリケーションのいくつかがビジネスで使用されていないことに気づきました。最も可能性の高い原因は、次の不足です。
A. IT ポートフォリオ管理。
B. システム サポート ドキュメント。
C. IT リソース管理。
D. 変更管理。
Answer: C (メーッセージを残す**)**

最新問題**: 161**
ファイル サーバーを外部ユーザーがアクセスできるようにする必要がある場合に、組織を攻撃から保護するための IS 監査人の最善の推奨事項は次のどれですか。
A. 安全なトンネル接続を強制します。
B. 内部ファイアウォールを強化します。
C. 非武装地帯 (DMZ) を設定します。
D. 安全なプロトコルを実装します。
Answer: (解答を表示する**)**

A demilitarized zone (DMZ) is a network segment that is separated from the internal network and the external network, such as the internet, by firewalls or other security devices. A DMZ provides an extra layer of security for the organization's internal network by isolating the servers and services that need to be accessible to external users, such as a file server, from the rest of the network. A DMZ also prevents external users from accessing the internal network directly, as they have to go through two firewalls to reach it. Therefore, setting up a DMZ is an IS auditor's best recommendation to protect an organization from attacks when its file server needs to be accessible to external users12.
The other possible options are:
* Enforce a secure tunnel connection: This means that the organization requires external users to establish a secure and encrypted connection, such as a virtual private network (VPN), to access its file server.
This can provide some level of security and privacy for the data transmission, but it does not protect the file server or the internal network from attacks if the connection is compromised or if the external users are malicious. Therefore, enforcing a secure tunnel connection is not an IS auditor's best recommendation to protect an organization from attacks when its file server needs to be accessible to external users3.
* Enhance internal firewalls: This means that the organization improves the security and performance of its internal firewalls, which are devices that filter and control the network traffic between different segments of the network. This can provide some level of protection for the internal network from unauthorized or malicious access, but it does not protect the file server or the external network from attacks if the file server is exposed to the internet or if the external network is compromised. Therefore, enhancing internal firewalls is not an IS auditor's best recommendation to protect an organization from attacks when its file server needs to be accessible to external users4.
* Implement a secure protocol: This means that the organization uses a secure and standardized protocol, such as Secure File Transfer Protocol (SFTP) or Secure Shell (SSH), to transfer files between its file server and external users. This can provide some level of security and integrity for the data transmission, but it does not protect the file server or the internal network from attacks if the protocol is exploited or if the external users are malicious. Therefore, implementing a secure protocol is not an IS auditor's best recommendation to protect an organization from attacks when its file server needs to be accessible to external users5. References: 1: What Is a DMZ Network and Why Would You Use It? | Fortinet 2: Demilitarised zone (DMZ) | Cyber.gov.au 3: What Is VPN Tunneling? | Fortinet 4: Firewall
- Wikipedia 5: Secure Shell - Wikipedia

最新問題**: 162**
IS 監査人が最近のセキュリティ インシデントを調査しており、データベース システムのセキュリティ設定に対する最近の変更の承認に関する情報を求めています。監査人がこの情報を見つける可能性が最も高いのはどこでしょうか。

A. システムイベント相関レポート
B. データベースログ
C. 変更ログ
D. セキュリティインシデントおよびイベント管理 (SIEM) レポート
Answer: (解答を表示する**)**
A change log is a record of all changes made to a system or application, including the date, time, description, and approval of each change. A change log can help an IS auditor to trace the source and authorization of a modification to a system's security settings. A system event correlation report is a tool that analyzes data from multiple sources to identify patterns and anomalies that indicate potential security incidents. A database log is a record of all transactions and activities performed on a database, such as queries, updates, and backups. A security incident and event management (SIEM) report is a tool that collects, analyzes, and reports on data from various sources to detect and respond to security incidents.

最新問題**: 163**
IT の目標が組織の目標と一致しているかどうかを判断するのに最も役立つのは次のどれですか?
A. バランストスコアカード
B. エンタープライズダッシュボード
C. エンタープライズ アーキテクチャ (EA)
D. 主要業績評価指標 (KPI)
Answer: A (メーッセージを残す**)**
The most useful tool for determining whether the goals of IT are aligned with the organization's goals is a balanced scorecard. A balanced scorecard is a strategic management system that translates an organization's vision and mission into a set of objectives and measures across four perspectives: financial, customer, internal process, and learning and growth. A balanced scorecard helps align IT goals with organizational goals by linking them to a common strategy map that shows how IT contributes to value creation and performance improvement in each perspective. A balanced scorecard also helps monitor and evaluate IT performance against predefined targets and indicators. Enterprise dashboard, enterprise architecture (EA), and key performance indicators (KPIs) are not the most useful tools for determining whether the goals of IT are aligned with the organization's goals. These tools may help communicate, design, or measure IT goals or activities, but they do not provide a comprehensive framework for aligning IT goals with organizational goals across multiple dimensions.

最新問題**: 164**
従業員所有のモバイル デバイスにプッシュされる企業アプリケーションのセキュリティを維持するための BE ST 方式を提供するのは次のどれですか。
A. リモートデータ破壊機能の有効化

B. モバイルデバイス管理 (MDM) の実装
C. 不要なネットワーク接続オプションを無効にする
D. モバイルユーザーに対するセキュリティ意識向上トレーニングの義務付け
Answer: B (メーッセージを残す)
The best method for maintaining the security of corporate applications pushed to employee-owned mobile devices is implementing mobile device management (MDM). MDM is a software solution that allows an organization to remotely manage, configure, and secure the mobile devices that access its network and data.
MDM can help protect corporate applications on employee-owned devices by:
Enforcing security policies and settings, such as encryption, password, firewall, antivirus, and VPN.
Controlling the installation, update, and removal of corporate applications and data.
Separating corporate and personal data and applications on the device using containers or profiles.
Monitoring and auditing the device's compliance status, activity, and location.
Performing remote actions, such as lock, wipe, backup, or restore, in case of loss, theft, or compromise.
MDM can provide a comprehensive and centralized approach to maintain the security of corporate applications on employee-owned devices, regardless of the device type, platform, or ownership. MDM can also help the organization comply with regulatory and industry standards for data protection and privacy.
Enabling remote data destruction capabilities is a useful feature for maintaining the security of corporate applications on employee-owned devices, but it is not the best method by itself. Remote data destruction allows the organization to erase the corporate data and applications from the device in case of loss, theft, or compromise. However, this feature does not prevent unauthorized access or misuse of the corporate data and applications before they are destroyed. Remote data destruction is usually part of an MDM solution.
Disabling unnecessary network connectivity options is a good practice for maintaining the security of corporate applications on employee-owned devices, but it is not the best method by itself. Network connectivity options, such as Wi-Fi, Bluetooth, NFC, or USB, can expose the device to potential attacks or data leakage. Disabling these options when they are not needed can reduce the attack surface and improve battery life. However, this practice does not address other security risks or requirements for the corporate applications on the device. Disabling network connectivity options can also be part of an MDM solution.
Requiring security awareness training for mobile users is an important measure for maintaining the security of corporate applications on employee-owned devices, but it is not the best method by itself. Security awareness training can educate the users about the potential threats and best practices for using their devices securely. It can also help foster a culture of security and responsibility among the users. However, security awareness

training cannot guarantee that the users will follow the security policies and guidelines consistently and correctly. Security awareness training should be complemented by technical controls, such as MDM.
References:
Protecting Corporate Data on Mobile Devices for All Companies1
Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)23

最新問題**: 165**
経営陣は、ビジネス要件が満たされている範囲を判断するために、新しく実装された購買パッケージの実装後レビューを要求しました。次のうち、最も評価される可能性が高いのはどれですか?
A. 購入ガイドラインとポリシー
B. ライブ処理の結果
C. 実装方法
D. 受け入れテストの結果
Answer: (解答を表示する**)**

最新問題**: 166**
ある組織は、サードパーティのサービス プロバイダーからエンタープライズ データ ウェアハウスに自動データ フィードを受信することを計画しています。不良データの受け入れを防ぐ最善の方法は次のどれでしょうか。
A. データ フィードが失敗したことを示すエラー コードを取得します。
B. 組織全体でデータ品質の推進者を任命します。
C. 信頼できるベンダーからデータクレンジングツールを購入します。
D. 無効なデータを拒否するビジネス ルールを実装します。
Answer: D (メーッセージを残す**)**
The best way to prevent accepting bad data from a third-party service provider is to implement business rules to reject invalid data. Business rules are logical expressions that define the business requirements and constraints for specific data elements. They can be used to validate, transform, or filter incoming data from external sources, ensuring that only high-quality data is accepted into the enterprise data warehouse. Business rules can also help to identify and resolve data quality issues, such as missing values, duplicates, outliers, or inconsistencies.

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

https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (1394**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: **167**
チェックサムはどのタイプの制御に分類されますか?
A. 予防管理
B. 検出制御
C. 管理制御
D. 是正制御
Answer: (解答を表示する**)**

最新問題: **168**
ウェットパイプシステムではなくドライパイプ消火システムを使用する主な利点は、ドライパイプシステムには次のような利点があることです。
A. 炎を抑える効果が高い。
B. 抑制剤の放出を中止するための時間を延長します。
C. 漏洩のリスクが減少します。
D. 乾燥化学抑制剤のみを散布します。
Answer: C (メーッセージを残す**)**
The primary benefit of using a dry-pipe fire-suppression system rather than a wet-pipe system is that a dry- pipe system has a decreased risk of leakage, as the pipes are filled with pressurized air or nitrogen instead of water until the system is activated. A wet-pipe system has a higher risk of leakage, corrosion, and freezing. A dry-pipe system is not more effective at suppressing flames, as it uses the same water-based suppressant as a wet-pipe system. A dry-pipe system does not allow more time to abort release of the suppressant, as it has a delay of only a few seconds before the water is released. A dry-pipe system does not disperse dry chemical suppressants exclusively, as it uses water as the primary suppressant. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.2.3

最新問題: **169**
次のどれが、IS 監査人がさまざまなアプリケーションやデバイスのアクセス制御リストを組み合わせて比較するのに最適な方法でしょうか?
A. 統合テスト施設 (ITF)
B. スナップショット
C. データ分析
D. 監査フック
Answer: C (メーッセージを残す**)**
Data analytics is the process of analyzing large and complex data sets to discover patterns, trends, and insights that can support decision making and problem solving. Data

analytics can enable an IS auditor to combine and compare access control lists from various applications and devices by using techniques such as data extraction, transformation, loading, cleansing, integration, aggregation, visualization, and reporting. Data analytics can help an IS auditor to identify and assess the risks and controls related to access management, such as unauthorized or excessive access, segregation of duties violations, access policy compliance, access activity monitoring, and access review and remediation.
The other options are not as effective or relevant as data analytics for combining and comparing access control lists from various applications and devices. Integrated test facility (ITF) is a technique for testing the validity and accuracy of application processing by inserting fictitious transactions into the system and verifying the results. ITF does not directly involve the analysis of access control lists. Snapshots are records of selected information at a specific point in time that can be used to monitor system activity or performance.
Snapshots can provide some information about access control lists, but they are not sufficient to combine and compare them across different sources. Audit hooks are software routines embedded in an application that can trigger an alert or a report when certain conditions are met. Audit hooks can help to detect anomalies or exceptions in access control lists, but they do not provide a comprehensive or integrated view of them.
References:
ISACA, CISA Review Manual, 27th Edition, 2019, p. 2361
ISACA, ITAF: A Professional Practices Framework for IS Audit/Assurance, 3rd Edition, 2014, p. 882 Data Analytics for Auditing Access Control3

最新問題**: 170**
組織の IT パフォーマンス指標が同じ業界の他の組織と比較可能かどうかを評価する場合、次のどれを確認するのが最も役立ちますか?
A. ITガバナンスフレームワーク
B. ベンチマーク調査
C. 使用状況レポート
D. バランストスコアカード
Answer: B (メーッセージを残す**)**
IT performance measures are indicators of how well an organization is achieving its IT goals and objectives.
Benchmarking surveys are useful tools for comparing an organization's IT performance measures with those of other organizations in the same industry or sector. Benchmarking surveys can provide insights into best practices, gaps, trends, and opportunities for improvement. IT governance frameworks, utilization reports, and balanced scorecards are not as helpful for comparing IT performance measures across organizations, as they may vary in scope, methodology, and terminology. References: IT Resources | Knowledge & Insights | ISACA, CISA Review Manual (Digital Version)

最新問題**: 171**
24 時間 365 日の処理環境では、データベースに、パスワードが期限切れにならないように設定された特権アプリケーション アカウントがいくつか含まれています。次の推奨事項のうち、ビジネスへの影響を最小限に抑えながらリスクに対処するにはどれが最適ですか。
A. アプリケーションを変更して、データベースへの直接アクセスが不要になるようにします。
B. 環境にデータベースアクセス監視を導入する
C. アプリケーション アカウントを許可するようにアクセス管理ポリシーを変更します。
D. パスワードの変更を実施するためにダウンタイムをスケジュールします。
Answer: B (メーッセージを残す**)**
The best recommendation to address the risk of privileged application accounts with passwords set to never expire in a 24/7 processing environment is to introduce database access monitoring into the environment.
Database access monitoring is a security control that tracks and records all activities and transactions performed on a database, especially by privileged users or accounts. Database access monitoring can help address the risk of privileged application accounts with passwords set to never expire by detecting and alerting any unauthorized or abnormal access or actions on the database. The other options are not as effective as database access monitoring in addressing the risk, as they may cause disruption to the business or violate the access management policy. Modifying applications to no longer require direct access to the database is a complex and costly solution that may affect the functionality or performance of the applications, and it may not be feasible or practical in a 24/7 processing environment. Modifying the access management policy to make allowances for application accounts is a risky solution that may create exceptions or loopholes in the policy, and it may not comply with the best practices or standards for password management. Scheduling downtime to implement password changes is a disruptive solution that may affect the availability or continuity of the systems or applications, and it may not be acceptable or possible in a 24/7 processing environment. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.2.4

最新問題**: 172**
情報システム監査人は、何人かの従業員が個人的な理由でソーシャル メディア サイトの使用に過度の時間を費やしていることに気付きました。監査人が最初に実行することを推奨すべきなのは次のうちどれですか。
A. ソーシャル ネットワーキング サイトへの投稿を積極的に監視するプロセスを実装します。
B. ソーシャル メディアの使用を含めるようにネットワーク使用の予算を調整します。
C. エンドポイントでデータ損失防止 (DLP) ツールを使用します。
D. 勤務時間中のソーシャル メディアの許容される使用に関するポリシーを実装します。

Answer: D (メーッセージを残す)
The first course of action that the auditor should recommend after finding that several employees are spending an excessive amount of time using social media sites for personal reasons is to implement policies addressing acceptable usage of social media during working hours. Policies can help define the scope, purpose, rules, and expectations of using social media in the workplace, both for personal and professional reasons. Policies can also specify the consequences of violating the policies, such as disciplinary actions or termination. Policies can help deter employees from misusing social media at work, which could affect their productivity, performance, or security. Policies can also help protect the organization from legal liabilities or reputational damages that could arise from inappropriate or unlawful employee behavior on social media.

最新問題**: 173**
監査報告書に含める問題を決定する際に、情報システム監査人が主に考慮すべき事項は次のどれですか?
A. 専門家としての懐疑心
B. 経営陣の同意
C. 物質性
D. 固有のリスク
Answer: C (メーッセージを残す)
Materiality is the primary consideration when determining which issues to include in an audit report, as it reflects the significance or importance of the issues to the users of the report. Materiality is a relative concept that depends on the nature, context, and amount of the issues, as well as the expectations and needs of the users. Materiality helps the auditor to prioritize the issues and communicate them clearly and concisely.
References
ISACA CISA Review Manual, 27th Edition, page 256
Materiality in Auditing - AICPA
Materiality in Planning and Performing an Audit - IAASB

最新問題**: 174**
IS 監査人は、組織が分散環境で複数のサーバー障害を経験したことを知ります。
将来のサーバー障害の潜在的な影響を制限するための最良の推奨事項は次のどれですか?
A. 冗長経路
B. クラスタリング
C. フェイルオーバー電源
D. 並列テスト
Answer: B (メーッセージを残す)
Clustering is a technique that allows multiple servers to work together as a single system, providing high availability, load balancing, and fault tolerance. Clustering can limit the potential impact of server failures in a distributed environment, as it can automatically

switch the workload to another server in the cluster if one server fails, without interrupting the service. Redundant pathways, failover power, and parallel testing are also useful for improving the reliability and availability of servers, but they do not directly address the issue of server failures.

最新問題**: 175**
調達部門の業務監査中に、監査チームは人工知能 (AI) アルゴリズムを使用する主要システムに遭遇しました。監査チームには、監査を進めるために必要な知識がありません。この状況に対処する最善の方法は次のどれですか?
A. スキル評価を実行して、AI の知識を持つ他のビジネス ユニットのメンバーを特定します。
B. 監査範囲から AI 部分を削除し、監査を続行します。
C. チームが AI に関するトレーニングを受けるまで監査を延期します。
D. 監査経験と AI の知識を持つ外部コンサルタントを雇用します。
Answer: (解答を表示する**)**
If the audit team lacks the necessary knowledge to audit a system that uses an AI algorithm, engaging external consultants who have audit experience and knowledge of AI would be the best approach12. These consultants can provide the expertise needed to effectively audit the AI system12. This approach ensures that the audit is conducted thoroughly and accurately, without requiring the audit team to acquire new skills or knowledge12.
References:
Auditing Guidelines for Artificial Intelligence - ISACA
An In-Depth Guide To Audit AI Models - Censius

最新問題**: 176**
効果的なセキュリティ意識向上プログラムを開発する際に、最も重要なのは次のどれですか?
A. トレーニング担当者は情報セキュリティの専門家です。
B. プログラムの成果指標が確立されます。
C. プログラム コンテンツにはセキュリティ脅威のシナリオが含まれています。
D. トレーニング後にフィッシング演習を実施します
Answer: B (メーッセージを残す**)**
The most important factor to ensure when developing an effective security awareness program is B. Outcome metrics for the program are established. This is because outcome metrics are measures that evaluate the impact and results of the security awareness program on the behavior and performance of the users, and the security posture and objectives of the organization1. Outcome metrics can help ensure the effectiveness of the security awareness program by:

Providing feedback and evidence on whether the security awareness program is achieving its goals and expectations, such as reducing the number of incidents, improving the compliance rate, or increasing the reporting rate1.
Identifying and quantifying the strengths and weaknesses of the security awareness program, and enabling continuous improvement and optimization of the program content, delivery, and frequency1.
Demonstrating and communicating the value and return on investment of the security awareness program to the stakeholders and management, and securing their support and commitment for the program1.

最新問題**: 177**
フルディスク暗号化に関連するポリシーと手順を実装することで最も効果的に対処できるリスクシナリオはどれですか?
A. 従業員が競合他社に転職したことによるデータ漏洩
B. 規制対象情報の保管に関連する違反罰金
C. アプリケーションインターフェースを介した情報への不正な論理アクセス
D. 情報が保存されているメディアの物理的な盗難
Answer: D (メーッセージを残す**)**
Full disk encryption (FDE) is a means of protecting information by encrypting all of the data on a disk, including temporary files, programs, and system files1. FDE is best suited for addressing the risk scenario of physical theft of media on which information is stored, as it prevents unauthorized access to the data even if the device is lost or stolen2. FDE does not prevent data leakage as a result of employees leaving to work for competitors, as they may still have access to the data while using the device or copy the data to another device before leaving. FDE does not prevent noncompliance fines related to storage of regulated information, as it does not ensure that the data is stored in accordance with the applicable laws and regulations. FDE does not prevent unauthorized logical access to information through an application interface, as it does not control the access rights and permissions of users and applications. *References: According to the ISACA IT Audit and Assurance Standards, Guidelines and Tools and Techniques for IS Audit and Assurance Professionals, section 2402 Planning, "The IS audit and assurance professional should identify and assess risk relevant to the area under review." 3 One of the risk factors to consider is "the sensitivity of information processed, stored or transmitted by the system" 3. FDE is one of the possible controls to mitigate the risk of unauthorized disclosure of sensitive information due to physical theft of media.

最新問題**: 178**
次のどれが非対称暗号化によってのみ提供できますか?
A. 情報プライバシー
B. 256-brt キーの長さ
C. データの可用性

D. 否認防止
Answer: (解答を表示する**)**
The only thing that can be provided by asymmetric encryption is nonrepudiation. Nonrepudiation is the ability to prove that a message or transaction was originated or authorized by a specific party. Asymmetric encryption uses a pair of keys: a public key and a private key. The public key can be shared with anyone, while the private key is kept secret by the owner. If a message is encrypted with the sender's private key, only the sender's public key can decrypt it. This proves that the message was sent by the sender and not by anyone else. This is called digital signature and it provides nonrepudiation. Asymmetric encryption can also provide information privacy by encrypting a message with the receiver's public key, so that only the receiver's private key can decrypt it. However, information privacy can also be provided by symmetric encryption, which uses a single key to encrypt and decrypt messages. References:
* CISA Review Manual (Digital Version), Chapter 5, Section 5.21
* CISA Online Review Course, Domain 3, Module 2, Lesson 12

最新問題**: 179**
制御合計の使用は、次の制御目的のどれを満たしますか?
A. トランザクションの整合性
B. 処理の整合性
C. 配布制御
D. システムの回復可能性
Answer: (解答を表示する**)**
The use of control totals satisfies the control objective of processing integrity. Processing integrity refers to the accuracy, completeness, timeliness, and validity of data processing. Control totals are a method of verifying the correctness of data processing by comparing the total value or count of a batch of transactions before and after processing. For example, if a batch of 100 invoices is entered into an accounting system, the total amount and number of invoices should match before and after processing. If there is a discrepancy, it indicates an error in data entry, transmission, or processing. Control totals help to ensure that no transactions are lost, duplicated, or altered during processing. References:
* Control Objectives & Activities: Examples, Appropriateness
* Levels and Types of Control | Principles of Management
* CISA Review Manual 27th Edition, page 337

最新問題**: 180**
IS 監査人は、組織内の IT ガバナンスを改善するための対策についてアドバイスを求められています。次のうち、最も適切な推奨事項はどれですか。
A. 主要業績評価指標 (KPI) を実装する

B. 毎年第三者による監査を実施します。
C. 組織のパフォーマンスを業界の同業他社と比較します。
D. 経営幹部にIT戦略の立案を要求する
Answer: A (メーッセージを残す**)**
The best recommendation for improving IT governance within the organization is to implement key performance indicators (KPIs). KPIs are measurable values that show how effectively the organization is achieving its key business objectives. KPIs can help the organization to monitor and evaluate the performance, efficiency, and alignment of its IT processes and resources with its business goals and strategies1.
The other options are not as effective as implementing KPIs for improving IT governance. Option B, implementing annual third-party audits, is a good practice but may not be sufficient or timely to identify and address the issues or gaps in IT governance. Option C, benchmarking organizational performance against industry peers, is a useful technique but may not reflect the specific needs and expectations of the organization's stakeholders. Option D, requiring executive management to draft IT strategy, is a necessary step but not enough to ensure that IT governance is implemented and monitored throughout the organization.

最新問題**: 181**
効果的な IT ポートフォリオ管理の最も優れた証拠となるのは次のどれですか?
A. IT ポートフォリオは、現在の業界ベンチマークに基づいて更新されます。
B. IT ポートフォリオの更新は、承認されると伝達されます。
C. IT ポートフォリオ内のプログラムは、各ビジネス機能によって優先順位が付けられます。
D. ビジネス戦略の変更に応じて IT ポートフォリオが更新されます。
Answer: D (メーッセージを残す**)**

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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**
非対称暗号化を使用して機密性を確保するために、メッセージは次のどれで暗号化されますか?
A. 受信者の公開鍵

B. 送信者の秘密鍵
C. 送信者の公開鍵
D. 受信者の秘密鍵
Answer: A (メーッセージを残す**)**
The best option for ensuring confidentiality through the use of asymmetric encryption is to encrypt a message with the recipient's public key (option A). This is because:
Asymmetric encryption, also known as public-key cryptography, is a type of encryption that uses a pair of keys to encrypt and decrypt data. The pair of keys includes a public key, which can be shared with anyone, and a private key, which is kept secret by the owner12.
In asymmetric encryption, the sender uses the recipient's public key to encrypt the data. The recipient then uses their private key to decrypt the data. This approach allows for secure communication between two parties without the need for both parties to have the same secret key12.
Encrypting a message with the recipient's public key ensures that only the recipient can decrypt it with their private key. This provides confidentiality, which means that the message is protected from unauthorized access or disclosure12.
Encrypting a message with the sender's private key (option B) does not ensure confidentiality, but rather authentication, which means that the message can be verified as coming from the sender. This is because anyone can decrypt the message with the sender's public key, but only the sender can encrypt it with their private key12.
Encrypting a message with the sender's public key (option C) or the recipient's private key (option D) does not make sense, as it would render the message unreadable by both parties. This is because neither party has the corresponding key to decrypt it12.
Therefore, the best option for ensuring confidentiality through the use of asymmetric encryption is to encrypt a message with the recipient's public key (option A), as this ensures that only the recipient can decrypt it with their private key.
References: 1: What is asymmetric encryption? | Asymmetric vs. symmetric ... - Cloudflare 2: What is Asymmetric Encryption? - GeeksforGeeks

最新問題**: 183**
情報システム監査人が、会社の幹部が従業員に業務目的でソーシャル ネットワーキング サイトの使用を奨励していることを発見しました。次の推奨事項のうち、データ漏洩のリスクを軽減するのに最も役立つものはどれですか。
A. 従業員によるポリシー承認と秘密保持契約の署名の義務付け
B. 従業員にソーシャルネットワーキングサイトの使用に関する教育とガイドラインを提供する
C. 機密データに対する強力なアクセス制御を確立する
D. 従業員のソーシャル ネットワーキングの使用状況を監視する
Answer: B (メーッセージを残す**)**
While all the options can help reduce the risk of data leakage, providing education and guidelines to employees on the use of social networking sites would be the most effective.

This is because it directly addresses the issue at hand - the use of social networking sites for business purposes1. Education and guidelines can help employees understand the risks associated with social media use and teach them how to safely and responsibly use these platforms for business purposes1. This includes understanding privacy settings, recognizing phishing attempts, and knowing what information should not be shared on these platforms1.
References:
10 Social Media Guidelines for Employees in 2023 - Hootsuite

最新問題**: 184**
IT 戦略が組織のビジョンとミッションをサポートしているかどうかを評価するために、情報システム監査人が行う最善のアプローチは次のどれですか。
A. 投資収益率 (ROIs) に関する戦略的プロジェクトのレビュー
B. 組織の成熟度を測るために他の部門からのフィードバックを求める
C. 経営幹部と会ってビジネス目標を理解する
D. 組織の主要業績評価指標 (KPI) を確認する
Answer: C (メーッセージを残す**)**
The best approach for an IS auditor to evaluate whether the IT strategy supports the organization's vision and mission is to meet with senior management to understand the business goals and how IT can enable them.
This will help the IS auditor to assess the alignment and integration of IT with the business strategy and to identify any gaps or opportunities for improvement. Reviewing ROIs, KPIs, or feedback from other departments may provide some insights, but they are not sufficient to evaluate the IT strategy. References: IS Audit and Assurance Standards, section "Standard 1201: Engagement Planning"

最新問題**: 185**
組織のセキュリティ プログラムの有効性を測る最も重要な指標は次のとおりです。
A. 競合他社が経験した重大なインシデントとの比較。
B. 上級管理職にエスカレーションされた脆弱性アラートの数。
C. 重要なビジネス活動に対するインシデントの悪影響。
D. 報告された新しい脆弱性の数。
Answer: C (メーッセージを残す**)**

最新問題**: 186**
スプレッドシートは、プロジェクトのコスト見積りを計算するために使用されます。各コスト カテゴリの合計は、ジョブ コスト計算システムに入力されます。データがシステムに正確に入力されるようにするための最適な制御方法は何ですか。
A. プロジェクト別の合計金額の調整
B. 有効性チェック、文字データの入力を防止

C. 各コストタイプの妥当性チェック
D. エントリの後にプロジェクト詳細の裏面を表示します
Answer: A (メーッセージを残す**)**
Reconciliation of total amounts by project is the best control to ensure that data is accurately entered into the job-costing system from spreadsheets. Reconciliation is a process of comparing two sets of data to identify any differences or discrepancies between them. By reconciling the total amounts by project from spreadsheets with those from the job-costing system, any errors or omissions in data entry can be detected and corrected.
Validity checks are controls that verify that data conforms to predefined formats or ranges. They can prevent entry of character data into numeric fields, but they cannot ensure that the numeric data is correct or complete.
Reasonableness checks are controls that verify that data is within expected or acceptable limits. They can detect outliers or anomalies in data, but they cannot ensure that the data matches the source. Display back of project detail after entry is a control that allows the user to review and confirm the data entered into the system. It can help reduce human errors, but it cannot guarantee that the data is accurate or consistent with the source.
References: Information Systems Operations and Business Resilience, CISA Review Manual (Digital Version)

最新問題**: 187**
組織のコンピューティング リソースの効率を向上させるために、情報システム監査人が推奨する最良の方法はどれですか。
A. 中央処理装置 (CPU) のオーバークロック
B. ハードウェアのアップグレード
C. 仮想化
D. リアルタイムバックアップ
Answer: (解答を表示する**)**

最新問題**: 188**
企業の外部リソースへの接続用の Web プロキシ サーバーは、次の方法で組織のリスクを軽減します。
A. IP アドレスを変更してユーザーを匿名化します。
B. 追加のセキュリティのために多要素認証を提供します。
C. 直接アクセスよりも高速な応答を提供します。
D. トラフィックを負荷分散してデータ経路を最適化します。
Answer: (解答を表示する**)**
A web proxy server for corporate connections to external resources reduces organizational risk by anonymizing users through changed IP addresses. A web proxy server is an intermediary between the web and client devices, that can provide proxy services to a client or a group of clients1. One of the main benefits of using a web proxy server is that it

allows users to change their IP address and location, circumventing geoblocking and hiding their identity from the target website2.
Anonymizing internal IP addresses is important for online security, as it helps protect the organization from several threats. If an attacker controls a server that employees connect to, the outgoing IP address of the organization's router is logged on the server. This IP address can be used by the attacker to launch a denial-of- service (DoS) attack or to create more targeted attacks such as phishing2. With a web proxy server, the IP shown in web logs is the web proxy's, which means an attacker would not have access to the organization's router outgoing IP address2.
Anonymizing outgoing IP addresses is also important when carrying out sensitive actions online, such as law enforcement investigations or competitive intelligence. A web proxy server can help users avoid exposing their internal IP address that leads back to their organization, and instead use a third-party web proxy that provides more anonymity2.
The other options are not directly related to reducing organizational risk by using a web proxy server. Providing multi-factor authentication for additional security (option B) is a benefit of some web proxy servers, but it is not the main purpose of using a web proxy server3. Providing faster response than direct access (option C) is a benefit of some web proxy servers that cache content for better data transfer speeds and less bandwidth usage, but it is not directly related to reducing organizational risk1. Load balancing traffic to optimize data pathways (option D) is a benefit of some web proxy servers that distribute traffic across multiple servers, but it is not directly related to reducing organizational risk4.
References: 1: Proxy servers and tunneling 2: Multi-factor authentication: How to enable 2FA and boost your security 3: What Is Multi-factor Authentication (MFA) Security? 4: How it works: Microsoft Entra multifactor authentication

最新問題**: 189**
実装後のレビューは、ユーザーへのアンケート調査によって実施されました。情報システム監査人が最も懸念すべき事項は次のどれですか?
A. 調査結果は経営陣に詳細に提示されませんでした。
B. 調査の質問では、ビジネスケースの範囲が扱われていませんでした。
C. アンケートフォーム テンプレートでは追加のフィードバックを提供できませんでした。
D. アンケートは実施から1か月後に従業員に配布されました。
Answer: B (メーッセージを残す**)**
The greatest concern for an IS auditor when a post-implementation review was conducted by issuing a survey to users is that the survey questions did not address the scope of the business case. A post-implementation review is a process of evaluating the outcomes and benefits of a project after it has been completed and implemented. A post-implementation review can help to assess whether the project met its objectives, delivered its expected value, and satisfied its stakeholders1. A survey is a method of collecting feedback and opinions from users or other stakeholders about their experience and satisfaction with the

project. A survey can help to measure the user acceptance, usability, and functionality of the project deliverables2. A business case is a document that justifies the need for a project based on its expected benefits, costs, risks, and alternatives. A business case defines the scope, objectives, and requirements of the project and provides a basis for its approval and initiation3. Therefore, an IS auditor should be concerned if the survey questions did not address the scope of the business case, as it may indicate that the post-implementation review was not comprehensive, relevant, or aligned with the project goals. The other options are less concerning or incorrect because:
* A. The survey results were not presented in detail to management is not a great concern for an IS auditor when a post-implementation review was conducted by issuing a survey to users, as it is more of a communication or reporting issue than an audit issue. While presenting the survey results in detail to management may help to inform them about the project performance and outcomes, it does not affect the validity or quality of the post-implementation review itself.
* C. The survey form template did not allow additional feedback to be provided is not a great concern for an IS auditor when a post-implementation review was conducted by issuing a survey to users, as it is more of a design or format issue than an audit issue. While allowing additional feedback to be provided may help to capture more insights or suggestions from users, it does not affect the validity or quality of the post-implementation review itself.
* D. The survey was issued to employees a month after implementation is not a great concern for an IS auditor when a post-implementation review was conducted by issuing a survey to users, as it is more of a timing or scheduling issue than an audit issue. While issuing the survey to employees sooner after implementation may help to collect more accurate and timely feedback from users, it does not affect the validity or quality of the post-implementation review itself. References: Post Implementation Review - ISACA, Survey - ISACA, Business Case - ISACA

最新問題**: 190**
最近導入された BYOD (個人所有デバイスの持ち込み) 戦略に関連するセキュリティ リスクに組織が対処するには、次のどれが最適ですか?
A. モバイルデバイス追跡プログラム
B. モバイルデバイスアップグレードプログラム
C. モバイルデバイステストプログラム
D. モバイルデバイス認識プログラム
Answer: D (メーッセージを残す**)**
A mobile device awareness program would best enable an organization to address the security risks associated with a recently implemented bring your own device (BYOD) strategy. A mobile device awareness program is a set of activities that aim to educate and inform the employees about the benefits, challenges, and best practices of using their

personal mobile devices for work purposes. A mobile device awareness program can help the organization to:
* Communicate the organization's policies and expectations regarding BYOD, such as which devices are allowed, what data can be accessed or stored, and what security measures are required.
* Raise the employees' awareness of the potential threats and vulnerabilities that affect their mobile devices, such as malware, phishing, data leakage, or device loss.
* Provide the employees with guidance and tips on how to protect their mobile devices and the organization's data, such as using strong passwords, encryption, antivirus software, remote wipe, or VPN.
* Encourage the employees to report any incidents or issues related to their mobile devices, such as suspicious messages, unauthorized access, or device damage.
A mobile device awareness program can help the organization to reduce the security risks associated with BYOD by enhancing the employees' knowledge, skills, and behavior in using their mobile devices securely and responsibly. A mobile device awareness program can also help the organization to comply with relevant regulations and standards that govern data privacy and security in the cloud1.
The other options are not as effective as a mobile device awareness program in enabling an organization to address the security risks associated with BYOD. Option A, mobile device tracking program, is a tool that allows the organization to monitor and locate the employees' mobile devices in case of loss or theft. However, this tool may not prevent or detect other types of security risks, such as malware infection or data breach.
Option B, mobile device upgrade program, is a process that ensures that the employees' mobile devices are running the latest versions of operating systems and applications. However, this process may not address other aspects of security, such as user behavior or data protection. Option C, mobile device testing program, is a method that verifies the functionality and compatibility of the employees' mobile devices with the organization's systems and networks. However, this method may not cover all the scenarios or factors that may affect the security of the mobile devices or the organization's data2.
References:
* Mobile Device Security Awareness Topics3
* Security Awareness Top Ten Topics - #8 Mobile Devices

最新問題**: 191**
ある組織では、アジャイル プロジェクト管理方法論を使用する新しいエンタープライズ リソース プランニング (ERP) システムの実装のために運営委員会を設立しています。この委員会の構成において最も重要な基準は何ですか?
A. ERP導入経験
B. 要求される時間的コミットメントを満たす能力
C. 上級管理職の代表
D. アジャイルプロジェクト管理の経験

Answer: (解答を表示する**)**

最新問題**: 192**
構成管理システムの主な目的は次のとおりです。
A. ソフトウェアの更新を追跡します。
B. ソフトウェアのベースラインを定義します。
C. リリース手順をサポートします。
D. 変更承認を標準化します。
Answer: B (メーッセージを残す**)**
A configuration management system is a process that establishes and maintains the consistency of a product's attributes throughout its life cycle. It helps to identify and control the functional and physical characteristics of a product, and to record and report any changes to those characteristics. A configuration management system also supports the audit of the product to verify its conformance to requirements.
One of the key activities of a configuration management system is to define baselines for software. A baseline is a fixed reference point that serves as a basis for comparison and measurement. A baseline can be established for any configuration item, such as a requirement, a design document, a test plan, or a software component. A baseline helps to ensure that the software product meets its intended purpose and quality standards, and that any changes to the software are controlled and documented.
A configuration management system also supports other activities, such as tracking software updates, supporting the release procedure, and standardizing change approval, but these are not its primary purpose.
Therefore, the other options are incorrect.
References: : What is configuration management - Red Hat : Configuration Management | Definition, Importance & Benefits - ServerWatch

最新問題**: 193**
ライブラリ制御ソフトウェア パッケージの次の機能のうち、ソース コードの不正な更新から保護するものはどれですか。
A. ライフサイクルの各ステップで必要な承認
B. ソースコードとオブジェクトコードの日付と時刻のスタンプ
C. ソースライブラリのアクセス制御
D. ソースコードのリリース間の比較
Answer: (解答を表示する**)**
Access controls for source libraries are the features of a library control software package that would protect against unauthorized updating of source code. Access controls are the mechanisms that regulate who can access, modify, or delete the source code stored in the source libraries. Source libraries are the repositories that contain the source code files and their versions. By implementing access controls for source libraries, the library control

software package can prevent unauthorized or malicious users from tampering with the source code and compromising its integrity, security, or functionality1.
The other options are not as effective as access controls for source libraries in protecting against unauthorized updating of source code. Option A, required approvals at each life cycle step, is a good practice but may not be sufficient to prevent unauthorized updates if the approval process is bypassed or compromised. Option B, date and time stamping of source and object code, is a useful feature but may not prevent unauthorized updates if the date and time stamps are altered or ignored. Option D, release-to-release comparison of source code, is a helpful feature but may not prevent unauthorized updates if the comparison results are not reviewed or acted upon.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription
* How to protect your source code from attackers2
* How to Stop Unauthorized Use of Open Source Code

最新問題**: 194**
IS 監査人は、ビジネス オーナーが運用データにアクセスできる Web ページを作成して組織のセキュリティ ポリシーに違反したことを知りました。監査人の次のステップは次のようになります。
A. 十分なアクセス制御が存在するかどうかを判断します。
B. 上級管理職にエスカレートします。
C. Web ページをシャットダウンします。
D. 生産データの機密性を評価します。
Answer: B (メーッセージを残す**)**

最新問題**: 195**
ある銀行が、他国にあるクラウド プロバイダーにシステムをアウトソーシングしたいと考えています。次のどれが最も適切な情報システム監査の推奨事項でしょうか。
A. 銀行の本国で代替プロバイダーを探します。
B. プロバイダーの内部統制システムが銀行の要件を満たしていることを確認します。
C. プロバイダーはクライアントの国のすべての法律を遵守する必要があるため、意図したとおりに続行します。
D. プロバイダーに災害復旧機能があることを確認します。
Answer: C (メーッセージを残す**)**
A post-implementation review (PIR) is a process to evaluate whether the objectives of the project were met, determine how effectively this was achieved, learn lessons for the future, and ensure that the organisation gets the most benefit from the implementation of

projects1. A PIR is an important tool for assessing the success and value of a project, as well as identifying the areas for improvement and best practices for future projects.
One of the key elements of a PIR is to measure the benefits of the project against the expected outcomes and benefits that were defined at the beginning of the project. Measurable benefits are the quantifiable and verifiable results or outcomes that the project delivers to the organisation or its stakeholders, such as increased revenue, reduced costs, improved quality, enhanced customer satisfaction, or compliance with regulations2. Measurable benefits should be aligned with the organisation's strategy, vision, and goals, and should be SMART (specific, measurable, achievable, relevant, and time-bound).
The finding that measurable benefits were not defined is of greatest significance among the four findings, because it implies that:
* The project did not have a clear and agreed-upon purpose, scope, objectives, and deliverables
* The project did not have a valid and realistic business case or justification for its initiation and implementation
* The project did not have a robust and effective monitoring and evaluation mechanism to track its progress, performance, and impact
* The project did not have a reliable and transparent way to demonstrate its value proposition and return on investment to the organisation or its stakeholders
* The project did not have a meaningful and actionable way to learn from its achievements and challenges, and to improve its processes and practices Therefore, an IS auditor should recommend that measurable benefits are defined for any project before its implementation, and that they are reviewed and reported regularly during and after the project's completion.
The other possible findings are:
* A lessons-learned session was never conducted: This is a significant finding, but not as significant as the lack of measurable benefits. A lessons-learned session is a process of capturing and documenting the knowledge, experience, and feedback gained from a project, both positive and negative. A lessons- learned session helps to identify the strengths and weaknesses of the project management process, as well as the best practices and lessons for future projects. A lessons-learned session should be conducted at the end of each project phase or milestone, as well as at the end of the project. However, even without a formal lessons-learned session, some learning may still occur informally or implicitly among the project team members or stakeholders.
* The projects 10% budget overrun was not reported to senior management: This is a significant finding, but not as significant as the lack of measurable benefits. A budget overrun is a situation where the actual cost of a project exceeds its planned or estimated cost. A budget overrun may indicate poor planning, estimation, or control of the project resources, or unexpected changes or risks that occurred during the project implementation. A budget overrun should be reported to senior management as soon as possible, along with the reasons for it and the corrective actions taken or proposed.

However, a budget overrun may not necessarily affect the quality or value of the project deliverables or outcomes if they are still within acceptable standards or expectations.
* Monthly dashboards did not always contain deliverables: This is a significant finding, but not as significant as the lack of measurable benefits. A dashboard is a visual tool that displays key performance indicators (KPIs) or metrics related to a project's progress, status, or results. A dashboard helps to monitor and communicate the performance of a project to various stakeholders in a concise and clear manner. A dashboard should include deliverables as one of its components, along with other elements such as schedule, budget, quality, risks, issues, or benefits. However, even without deliverables in monthly dashboards, some information about them may still be available from other sources such as reports or documents.
References: 1: The role & importance of the Post Implementation Review 2: What is Post-Implementation Review in Project Management?

最新問題**: 196**
事件が発生した場合に法的手続きを最も容易にするのはどれですか?
A. 電子証拠開示を行う権利
B. 法律顧問からのアドバイス
C. 保管チェーンの維持
D. 根本原因分析の結果
Answer: C (メーッセージを残す**)**
The best way to facilitate the legal process in the event of an incident is to preserve the chain of custody of the evidence. The chain of custody is a record of who handled, accessed, or modified the evidence, when, where, how, and why. The chain of custody helps to ensure the integrity, authenticity, and admissibility of the evidence in a court of law. The chain of custody also helps to prevent tampering, alteration, or loss of evidence that could compromise the investigation or the prosecution. References:
* CISA Review Manual (Digital Version)
* CISA Questions, Answers & Explanations Database

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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**

情報システム監査人が、トランザクションが頻繁に変更される大量のデータを持つ組織のバックアップ手順を確認しています。中断が発生した場合に復旧時間を短縮する必要があることを考慮すると、推奨する最適なバックアップ スキームは次のうちどれですか。
A. 差分バックアップ
B. フルバックアップ
C. 増分バックアップ
D. ミラーバックアップ
Answer: D (メーッセージを残す**)**
A mirror backup is a type of backup that creates an exact copy of the source data to the destination, without using any compression or encryption. A mirror backup is the best backup scheme to recommend given the need for a shorter restoration time in the event of a disruption, because it allows for the fastest and easiest recovery of data. A mirror backup does not store any previous versions of the files, so it only reflects the current state of the source data. Therefore, a mirror backup requires less storage space than a full backup, but more than an incremental or differential backup.
A differential backup is a type of backup that stores the changes made to the source data since the last full backup. A differential backup requires less storage space and time than a full backup, but more than an incremental backup. However, a differential backup also requires more time and resources to restore than a mirror or full backup, because it needs to combine the last full backup and the latest differential backup to recover the data.
A full backup is a type of backup that copies all the files and folders from the source data to the destination, regardless of whether they have changed or not. A full backup provides the most complete protection of data and the simplest recovery process, but it also requires the most storage space and time to perform. A full backup is usually done periodically, such as weekly or monthly, and followed by incremental or differential backups.
An incremental backup is a type of backup that stores the changes made to the source data since the last backup, whether it was a full or an incremental backup. An incremental backup requires the least storage space and time to perform, but it also requires the most time and resources to restore, because it needs to combine all the previous backups in chronological order to recover the data.

最新問題**: 198**
プロパティ設定されたネットワーク ファイアウォールによって軽減できるセキュリティ リスクは次のどれですか。
A. SQLインジェクション攻撃
B. サービス拒否 (DoS) 攻撃
C. フィッシング攻撃
D. 内部者による攻撃
Answer: B (メーッセージを残す**)**

A network firewall is a device or software that monitors and controls the incoming and outgoing network traffic based on predefined rules. A network firewall can help reduce the risk of denial of service (DoS) attacks, which are attempts to overwhelm a system or network with excessive requests or traffic, by filtering or blocking unwanted or malicious packets. A SQL injection attack is a type of code injection attack that exploits a vulnerability in a web application's database query, by inserting malicious SQL statements into the input fields. A phishing attack is a type of social engineering attack that attempts to trick users into revealing sensitive information or installing malware, by sending fraudulent emails or messages that impersonate legitimate entities. An insider attack is a type of malicious activity that originates from within an organization, such as employees, contractors, or partners, who abuse their access privileges or credentials to compromise the confidentiality, integrity, or availability of information systems or data. A network firewall cannot prevent these types of attacks, as they rely on exploiting human or application weaknesses rather than network vulnerabilities.

最新問題**: 199**
現在のシステムを並列実行することの主な目的は何ですか?
A. エンドユーザーとサポートスタッフに新しいシステムをトレーニングする
B. 新しいシステムが必要なビジネス機能を備えていることを確認する
C. 追加テストの必要性を減らすため
D. 新しいシステムを以前のシステムと比較して検証する
Answer: D (メーッセージを残す**)**
The primary purpose of performing a parallel run of a new system is to validate the new system against its predecessor. A parallel run is a strategy for system changeover where a new system slowly assumes the roles of the older system while both systems operate simultaneously. This allows for comparison of the results and outputs of both systems to ensure that the new system is working correctly and reliably. A parallel run can also help identify and resolve any errors, discrepancies, or inconsistencies in the new system before the old system is discontinued.
The other options are not the primary purpose of performing a parallel run of a new system. A. To train the end users and supporting staff on the new system. Training is an important part of system implementation, but it is not the main reason for doing a parallel run. Training can be done before, during, or after the parallel run, depending on the needs and preferences of the organization. B. To verify the new system provides required business functionality. Verifying the business functionality of the new system is part of user acceptance testing (UAT), which is a formal and structured process of testing whether the new system meets the specifications and expectations of the users and stakeholders. UAT is usually done before the parallel run, as a prerequisite for system changeover. C. To reduce the need for additional testing. Reducing the need for additional testing is not the primary purpose of performing a parallel run, but rather a possible benefit or outcome of doing so. A parallel run can help ensure that the new system is thoroughly tested and

validated in a real-world environment, which may reduce the likelihood of encountering major issues or defects later on.
However, additional testing may still be needed after the parallel run, depending on the feedback and evaluation of the users and stakeholders.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019, p. 2471
* IS

最新問題**: 200**
IT リスク評価を実施する際の最初のステップは次のどれですか?
A. 潜在的な脅威を特定します。
B. 脆弱性を評価します。
C. 保護する資産を特定します。
D. 配置されたコントロールを評価します。
Answer: (解答を表示する**)**
The first step when conducting an IT risk assessment is to identify assets to be protected, which include hardware, software, data, processes, people, and facilities that support the business objectives and operations of an organization. Identifying assets to be protected helps to establish the scope and boundaries of the risk assessment, as well as the value and criticality of each asset. Identifying potential threats, assessing vulnerabilities, and evaluating controls in place are subsequent steps in the risk assessment process that depend on the identification of assets to be protected. References: CISA Review Manual (Digital Version), Chapter 2: Governance & Management of IT, Section 2.3: IT Risk Management

最新問題**: 201**
緊急時対応施設にとって最も重要な考慮事項は次のどれですか?
A. 緊急時対応施設には、プライマリ サイトと同じバッジ アクセス制御が適用されます。
B. 予備施設とプライマリ サイトの両方の在庫には、同じ数のビジネス資産があります。
C. 緊急時対応施設は主要サイトから十分な距離を置いて配置されています。
D. 緊急時対応施設と主要サイトの両方が簡単に識別できます。
Answer: C (メーッセージを残す**)**
A contingency facility is a backup site that can be used to resume business operations in the event of a disaster or disruption at the primary site. The most important consideration for a contingency facility is that it is located a sufficient distance away from the primary site, so that it is not affected by the same event that caused the disruption. For example, if the primary site is damaged by a fire, flood, earthquake, or terrorist attack, the contingency facility should be in a different geographic area that is unlikely to experience the same hazard. This way, the organization can continue to provide its services and products to its customers and stakeholders without interruption.

The other options are not as important as the location of the contingency facility. The badge access controls, the number of business assets, and the identifiability of the sites are secondary factors that may affect the security and efficiency of the contingency facility, but they are not essential for its functionality. Therefore, option C is the correct answer.
References:
The Importance of Contingency Planning
WHO guidance for contingency planning

最新問題: **202**
効果的なコントロール自己評価 (CSA) プログラムにとって最も重要なのは次のどれですか?
A. 評価の範囲の決定
B. 詳細なテスト手順を実行する
C. リスク環境の変化の評価
D. ビジネスプロセスの理解
Answer: D (メーッセージを残す**)**
Understanding the business process is the most important factor for an effective control self-assessment (CSA) program. A CSA program is a technique that allows managers and work teams directly involved in business units, functions or processes to participate in assessing the organization's risk management and control processes1. A CSA program can help identify risks and potential exposures to achieving strategic bus iness objectives, evaluate the adequacy and effectiveness of controls, and implement remediation plans to address any gaps or weaknesses2. To conduct a successful CSA, it is essential to have a clear and comprehensive understanding of the business process under review, including its objectives, inputs, outputs, activities, resources, dependencies, stakeholders, performance indicators, etc. This will help to identify the relevant risks and controls associated with the process, as well as to evaluate their impact and likelihood. Determining the scope of the assessment, performing detailed test procedures, and evaluating changes to the risk environment are also important factors for an effective CSA program, but not as important as und erstanding the business process. These factors are more related to the execution and monitoring phases of the CSA program, while understanding the business process is related to the planning and preparation phase. Without a solid understanding of the business process, the scope, testing, and evaluation of the CSA may not be accurate or complete. References: ISACA CISA Review Manual 27th Edition, page 310

最新問題: **203**
IS 監査人は、複数のビジネス ユニットにサービスを提供する IT 組織がすべての取り組みに同等の優先順位を割り当てているため、プロジェクト資金の確保が遅れるリスクが生じ

ていることを発見しました。次のどれが、ビジネス目標をサポートする方法でプロジェクトとサービスの需要と利用可能なリソースを一致させるのに最も役立ちますか。
A. プロジェクト管理
B. リスク評価結果
C. ITガバナンスフレームワーク
D. ポートフォリオ管理
Answer: D (メーッセージを残す)
The most helpful tool in matching demand for projects and services with available resources in a way that supports business objectives is portfolio management. Portfolio management is the process of selecting, prioritizing, balancing and aligning IT projects and services with the strategic goals and value proposition of the organization3. Portfolio management helps the IT organization to allocate resources efficiently and effectively, to deliver value to the business units, and to align IT initiatives with business strategies. Project management, risk assessment results and IT governance framework are also important tools, but they are not as helpful as portfolio management in matching demand and supply of IT projects and services. References:
* CISA Review Manual, 27th Edition, page 721
* CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

最新問題**: 204**
ストレージ容量が限られているため、組織は完了した低価値トランザクションを含むメディアの実際の保存期間を短縮することを決定しました。次のどれが組織にとって最も重要なことでしょうか。
A. ポリシーには強力なリスクベースのアプローチが含まれています。
B. 保存期間により、年度末の監査時に確認することができます。
C. 保持期間はデータ所有者の責任に準拠しています。
D. 取引総額は財務報告に影響を及ぼさない
Answer: C (メーッセージを残す)
The most important factor for the organization to ensure when reducing the retention period for media containing completed low-value transactions is that the retention period complies with data owner responsibilities. Data owners are accountable for defining the retention and disposal requirements for the data under their custody, based on business, legal, regulatory, and contractual obligations. The policy should reflect the data owner's decisions and obtain their approval. The policy should also include a risk-based approach, but this is not as important as complying with data owner responsibilities. The retention period should allow for review during the year-end audit, but this may not be necessary for low-value transactions that have minimal impact on financial reporting. The total transaction amount may have some impact on financial reporting, but this is not a direct consequence of reducing the retention period. References:
* CISA Review Manual, 27th Edition, pages 414-4151

* CISA Review Questions, Answers & Explanations Database, Question ID: 255

最新問題: **205**
プロジェクト監査中に、IS 監査人は、プロジェクト レポートが現在の進捗状況を正確に反映していないことに気付きました。
次のどれが最も大きな結果をもたらすでしょうか?
A. プロジェクト マネージャーを交代する必要があります。
B. 取締役会へのプロジェクト報告は不完全になります。
C. プロジェクト運営委員会は効果的なガバナンスを提供できません。
D. プロジェクトは品質保証 (QA) レビューに耐えられません。
Answer: C (メーッセージを残す)
The greatest resulting impact of project reporting not accurately reflecting current progress is that the project steering committee cannot provide effective governance. The project steering committee is a group of senior executives or stakeholders who oversee the project and provide strategic direction, guidance, and support.
The project steering committee relies on accurate and timely project reporting to monitor the project's status, performance, risks, issues, and changes. If the project reporting is inaccurate, the project steering committee cannot make informed decisions, resolve problems, allocate resources, or ensure alignment with the organizational goals and objectives.
The other options are not as impactful as option C. The project manager will have to be replaced is a possible consequence, but not the greatest impact, of inaccurate project reporting. The project manager is responsible for planning, executing, monitoring, controlling, and closing the project. The project manager may face disciplinary actions or termination if they fail to provide accurate and honest project reporting. However, this does not necessarily affect the overall governance of the project. The project reporting to the board of directors will be incomplete is a potential risk, but not the greatest impact, of inaccurate project reporting.
The board of directors is the highest governing body of an organization that sets the vision, mission, values, and policies. The board of directors may receive periodic or ad hoc project reporting to ensure that the project is aligned with the organizational strategy and delivers value. If the project reporting is inaccurate, the board of directors may lose confidence in the project or intervene in its management. However, this does not directly affect the day-to-day governance of the project. The project will not withstand a quality assurance (QA) review is a possible outcome, but not the greatest impact, of inaccurate project reporting. A quality assurance review is a process to evaluate the quality of the project's processes and deliverables against pred efined standards and criteria. A quality assurance review may reveal discrepancies or errors in the project reporting that may affect the credibility and reliability of the project. However, this does not necessarily affect the governance of the

project. References: Project Steering Committee - Roles & Responsibilities, Project Reporting Best Practices, Quality Assurance in Project Management

最新問題**: 206**
IT戦略計画を検討する際、最も懸念されるのは
A. IT戦略委員会は設立されていない
B. 計画は関連する組織の目標をサポートしていません。
C. 主要業績評価指標 (KPI) がありません。
D. この計画は取締役会によって正式に承認されなかった
Answer: (解答を表示する**)**
The greatest concern when reviewing an IT strategic plan is B. The plan does not support relevant organizational goals. This is because an IT strategic plan should align and integrate the IT goals and objectives with the organization's overall strategy and vision, and ensure that IT supports and enables the business processes and functions1. If the IT strategic plan does not support relevant organizational goals, it may lead to:
Suboptimal or negative outcomes and value for the organization, as IT investments and initiatives may not align with the organization's priorities, needs, or expectations1.
Conflicts or inconsistencies between IT and business functions, as IT may not deliver the expected level of service, quality, or performance2.
Wasted or inefficient use of resources, as IT may spend time, money, or effort on projects or activities that are not relevant or beneficial for the organization2.

最新問題**: 207**
IS 監査人が、組織の買掛金プロセスの監査を計画しています。監査で評価する上で最も重要なコントロールは次のどれですか。
A. 発注書の発行と支払いの実行の間の職務の分離。
B. 請求書の受け取りと承認限度額の設定の職務分掌
C. 管理レビューと承認階層の承認
D. 購買発注の管理レビューと承認
Answer: (解答を表示する**)**
The most important control to assess in an audit of an organization's accounts payable processes is segregation of duties between issuing purchase orders and making payments. Segregation of duties is a principle that requires different individuals or departments to perform different tasks or functions within a process, in order to prevent fraud, errors, or conflicts of interest. In the accounts payable process, segregation of duties between issuing purchase orders and making payments ensures that no one person can initiate and complete a transaction without proper authorization and verification. This reduces the risk of duplicate payments, overpayments, unauthorized payments, or payments to fictitious vendors.
References:

* Accounts payable controls
* Accounts Payable Internal Controls: A Simple Checklist

最新問題**: 208**
組織が災害復旧の責任を果たすために IS 機能をアウトソーシングする場合、組織は次のことを行う必要があります。
A. 災害復旧計画 (DRP) のメンテナンスを中止する
B. アウトソーシングベンダーと災害復旧管理を調整する
C. 災害復旧の評価を第三者に委託する
D. 災害復旧の評価を内部監査に委任する
Answer: B (メーッセージを残す**)**
An organization outsourced its IS functions. To meet its responsibility for disaster recovery, the organization should coordinate disaster recovery administration with the outsourcing vendor. This is because the organization remains accountable for ensuring the continuity and availability of its IS functions, even if they are outsourced to a third party. The organization should establish clear roles and responsibilities, communication channels, testing procedures, and escalation processes with the outsourcing vendor for disaster recovery purposes. The organization should not discontinue maintenance of the disaster recovery plan (DRP), as it still needs to have a documented and updated plan for restoring its IS functions in case of a disaster. The organization should not delegate evaluation of disaster recovery to a third party or internal audit, as it still needs to monitor and review the performance and compliance of the outsourcing vendor with respect to disaster recovery objectives and standards. References: CISA Review Manual (Digital Version), [ISACA Auditing Standards]

最新問題**: 209**
IS 監査人は、Software as a Service (SaaS) ベンダーを選択する前に、経営陣に対して最も重要なアクションとして何を推奨すべきでしょうか?
A. サービス レベル要件を決定します。
B. リスク評価を完了します。
C. ビジネス影響分析 (BIA) を実行する
D. ベンダー監査を実施します。
Answer: (解答を表示する**)**
Before selecting a SaaS vendor, the most important action is to complete a risk assessment. A risk assessment is a process of identifying, analyzing, and evaluating the potential risks associated with outsourcing software and IT infrastructure to a third-party provider. A risk assessment helps to determine the impact and likelihood of various threats, such as data breaches, service disruptions, vendor lock-in, compliance issues, and legal disputes. A risk assessment also helps to identify the mitigation strategies and controls that can reduce or eliminate the risks.

A risk assessment is more important than determining service level requirements, performing a business impact analysis (BIA), or conducting a vendor audit because it provides the basis for these other actions.
Service level requirements are the expectations and obligations that define the quality and quantity of service that the vendor must provide to the customer. A BIA is a process of assessing the potential effects of an interruption or disruption of critical business functions or processes due to an incident or disaster. A vendor audit is a process of verifying the vendor's compliance with the contract terms, service levels, security policies, and best practices.
Service level requirements, BIA, and vendor audit are all important actions for selecting a SaaS vendor, but they depend on the results of the risk assessment. For example, service level requirements should reflect the risk appetite and tolerance of the customer, which are determined by the risk assessment. A BIA should prioritize the recovery of the most critical and vulnerable business functions or processes, which are identified by the risk assessment. A vendor audit should focus on the areas of highest risk and concern, which are highlighted by the risk assessment.
Therefore, an IS auditor should recommend to management that completing a risk assessment is the most important action before selecting a SaaS vendor.
References:
SaaS checklist: Nine factors to consider when selecting a vendor
SaaS vendor management: 10 best practices to achieve success
Best Practices for Software SaaS Vendor Selection and Negotiation
How to Evaluate SaaS Providers and Solutions by Developing ... - Gartner

最新問題**: 210**
IS 監査人が人工知能 (AI) とエキスパート システム アプリケーションをレビューしています。システムで重大なエラーがいくつか発生し、深刻な影響が出ています。エラーの原因を解明するために、IS 監査人が次に行うべきことは何ですか。
A. システム所有者にインタビューします。
B. システムが企業ポリシーに準拠していることを確認します。
C. システムの目的と機能を理解する。
D. システムに組み込まれた意思決定ロジックを確認します。
Answer: D (メーッセージを残す**)**

最新問題**: 211**
組織のリスク管理慣行の監査中に、情報システム監査人は、文書化された IT リスク受け入れが、割り当てられた有効期限後にタイムリーに更新されていないことを発見しました。この発見事項を評価する際、どの緩和要因が関連する影響を最も大幅に最小限に抑えるでしょうか。
A. ビジネス プロセスに対する補償制御が文書化されています。

B. リスク受容は、適切な上級管理職によって以前に検討され、承認されている
C. リスク受容が承認されて以来、ビジネス環境は大きく変化していません。
D. 問題のあるリスク受容は、全体の人口のわずかな割合を反映しています
Answer: (解答を表示する**)**
The mitigating factor that would most significantly minimize the impact of not renewing IT risk acceptances in a timely manner is having documented compensating controls over the business processes. Compensating controls are alternative controls that reduce or eliminate the risk when the primary control is not feasible or cost-effective. The other factors, such as previous approval by senior management, unchanged business environment, and small percentage of issues, do not mitigate the risk as effectively as compensating controls.
References: ISACA CISA Review Manual 27th Edition Chapter 1

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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**
上級情報システム監査人は、財務部門で PC が不正行為に使用された可能性があると疑っています。監査人はまずこの疑惑を次の担当者に報告する必要があります。
A. 監査管理。
B. 監査委員会。
C. 監査対象ラインの管理。
D. 警察です。
Answer: (解答を表示する**)**

最新問題**: 213**
オペレーティング システムの監査中にベースライン イメージを取得する主な目的はどれですか。
A. 異常な実行中のプロセスを識別する
B. ウイルス対策定義を確認する
C. ローカル管理者アカウントのアクセスを識別する
D. オペレーティングシステムのバックアップの整合性を検証する
Answer: (解答を表示する**)**

The primary purpose of obtaining a baseline image during an operating system audit is to identify atypical running processes. A baseline image is a snapshot of the normal state and configuration of an operating system, including the processes that are expected to run on it. By comparing the current state of the operating system with the baseline image, an IS auditor can detect any deviations or anomalies that may indicate unauthorized or malicious activity, such as malware infection, privilege escalation, or data exfiltration. A baseline image can also help an IS auditor to assess the performance and efficiency of the operating system, as well as its compliance with security standards and policies.
Verifying antivirus definitions (option B) is not the primary purpose of obtaining a baseline image, although it may be a part of the baseline configuration. Antivirus definitions are the files that contain the signatures and rules for detecting and removing malware. An IS auditor may verify that the antivirus definitions are up to date and consistent across the operating system, but this does not require obtaining a baseline image.
Identifying local administrator account access (option C) is not the primary purpose of obtaining a baseline image, although it may be a part of the baseline configuration. Local administrator accounts are user accounts that have full control over the operating system and its resources. An IS auditor may identify and review the local administrator accounts to ensure that they are properly secured and authorized, but this does not require obtaining a baseline image.
Verifying the integrity of operating system backups (option D) is not the primary purpose of obtaining a baseline image, although it may be a part of the backup process. Operating system backups are copies of the operating system data and settings that can be used to restore the system in case of failure or disaster. An IS auditor may verify that the operating system backups are complete, accurate, and accessible, but this does not require obtaining a baseline image.
References: : Linux security and system hardening checklist : CISA Certification | Certified Information Systems Auditor | ISACA : CISA Certified Information Systems Auditor Study Guide, 4th Edition : CISA - Certified Information Systems Auditor Study Guide [Book]

最新問題**: 214**
企業の電子メールの公開鍵インフラストラクチャ (PKI) を確認する情報システム監査人にとって、最も懸念すべきことは次のうちどれですか?
A. PKI ポリシーは過去 1 年以内に更新されていません。
B. 秘密鍵証明書は更新されていません。
C. 証明書失効リストは更新されていません。
D. 証明書の運用規定は公開されていません
Answer: (解答を表示する**)**

最新問題**: 215**

プログラマーが本番環境でデータを変更する権限を持っているかどうかを判断する最良の方法は、次の点を確認することです。
A. アクセス制御システムのログ設定。
B. 最新のシステム変更がどのように実装されたか。
C. アクセス制御システムの構成。
D. 付与されたアクセス権。
Answer: D (メーッセージを残す)
The best way to determine whether programmers have permission to alter data in the production environment is by reviewing the access rights that have been granted. Access rights are permissions or privileges that define what actions or operations a user can perform on an information system or resource. By reviewing the access rights that have been granted to programmers, an IS auditor can verify whether they have been authorized to modify data in the production environment, which is where live data and applications are stored and executed. The access control system's log settings are parameters that define what events or activities are recorded by the access control system, which is a system that enforces the access rights and policies of an information system or resource. The access control system's log settings are not the best way to determine whether programmers have permission to alter data in the production environment, as they do not indicate what permissions or privileges have been granted to programmers. How the latest system changes were implemented is a process that describes how software updates or modifications are deployed to the production environment. How the latest system changes were implemented is not the best way to determine whether programmers have permission to alter data in the production environment, as it does not indicate what permissions or privileges have been granted to programmers. The access control system's configuration is a set of rules or parameters that define how the access control system operates and functions. The access control system's configuration is not the best way to determine whether programmers have permission to alter data in the production environment, as it does not indicate what permissions or privileges have been granted to programmers.

最新問題**: 216**
IT 戦略とビジネス戦略を整合させることは、主に組織にとって次のことに役立ちます。
A. IT への投資を最適化します。
B. ビジネスユニット全体にリスク認識を構築します。
C. IT における上級管理職の関与を高める。
D. IT の有効性を監視します。
Answer: (解答を表示する)
Aligning IT strategy with business strategy primarily helps an organization to optimize investments in IT. This is because alignment ensures that IT resources and capabilities are aligned with the business goals and priorities, and that IT delivers value to the business in terms of efficiency, effectiveness, innovation, and competitive advantage12. By aligning IT

strategy with business strategy, an organization can avoid wasting money and time on IT projects or services that do not support or contribute to the business outcomes3. Alignment also helps to identify and prioritize the most critical and valuable IT initiatives that can create or optimize business value4.
Therefore, the correct answer to your question is A. optimize investments in IT.

最新問題**: 217**
組織内の情報セキュリティガバナンスを評価する際、情報システム監査人が最も懸念すべき結果は次のどれですか?
A. 情報セキュリティ部門は欠員補充に苦労している
B. 過去1年以内に情報セキュリティガバナンス監査が実施されなかった
C. データセンター管理者がセキュリティプロジェクトの最終承認を行う
D. 情報セキュリティポリシーは毎年更新されます
Answer: C (メーッセージを残す**)**
The finding that should be of most concern to an IS auditor when evaluating information security governance within an organization is that the data center manager has final sign-off on security projects. This indicates a lack of segregation of duties and a potential conflict of interest between the operational and security roles. The data center manager may have access to sensitive information or systems that should be protected by security controls, or may influence or override security decisions that are not in the best interest of the organization.
This finding also suggests that there is no clear accountability or authority for information security governance at a higher level, such as senior management or board of directors. The other findings are not as concerning as this one, although they may indicate some areas for improvement or monitoring. References:
* ISACA, CISA Review Manual, 27th Edition, chapter 5, section 5.11
* ISACA, IT Governance Using COBIT and Val IT: Student Booklet - 2nd Edition4

最新問題**: 218**
ストレージ メディアが限られている場合、次のバックアップ スキームのうちどれが最適なオプションですか?
A. リアルタイムバックアップ
B. 仮想バックアップ
C. 差分バックアップ
D. フルバックアップ
Answer: C (メーッセージを残す**)**
A differential backup scheme is the best option when storage media is limited, as it only backs up the data that has changed since the last full backup. This reduces the amount of storage space required and also simplifies the restoration process, as only the last full backup and the last differential backup are needed. A real-time backup scheme would require continuous replication of data, which would consume a lot of storage space and

network bandwidth. A virtual backup scheme would create a snapshot of the data at a point in time, but it would not reduce the storage space required, as it would still need to store the changes made to the data.
A full backup scheme would back up all the data every time, which would require the most storage space and also take longer to complete. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 405

最新問題**: 219**
最近、システム管理者が情報システム監査人に、組織外からの侵入試行が数回失敗したことを報告しました。このような侵入を検出するのに最も効果的なのは次のうちどれですか。
A. 定期的にログファイルを確認する
B. ルーターをファイアウォールとして設定する
C. ワンタイムパスワード付きスマートカードの使用
D. 生体認証ベースの認証のインストール
Answer: (解答を表示する**)**
The most effective way to detect an intrusion attempt is to periodically review log files, which record the activities and events on a system or network. Log files can provide evidence of unauthorized access attempts, malicious activities, or system errors. Configuring the router as a firewall, using smart cards with one-time passwords, and installing biometrics-based authentication are preventive controls that can reduce the likelihood of an intrusion, but they do not detect it. References: ISACA CISA Review Manual 27th Edition, page 301

最新問題**: 220**
IS 監査人が最近のセキュリティ インシデントを調査し、インシデント対応が適切ではなかったことを発見しました。
次の調査結果のうち、最も重要であると考えられるものはどれですか?
A. 攻撃を容易にするセキュリティ上の弱点は特定されませんでした。
B. 侵入検知システム (IDS) によって攻撃が自動的にブロックされませんでした。
C. 攻撃の発信者を特定できませんでした。
D. 適切な応答ドキュメントが維持されていませんでした。
Answer: A (メーッセージを残す**)**
The most critical finding for an IS auditor following up on a recent security incident is that the security weakness facilitating the attack was not identified. This finding indicates that the root cause of the incident was not analyzed, and the vulnerability that allowed the attack to succeed was not remediated. This means that the organization is still exposed to the same or similar attacks in the future, and its security posture has not improved. Identifying and addressing the security weakness is a key step in the incident response process, as it helps to prevent recurrence, mitigate impact, and improve resilience.

The other findings are not as critical as the failure to identify the security weakness, but they are still important issues that should be addressed by the organization. The attack was not automatically blocked by the intrusion detection system (IDS) is a finding that suggests that the IDS was not configured properly, or that it did not have the latest signatures or rules to detect and prevent the attack. The attack could not be traced back to the originating person is a finding that implies that the organization did not have sufficient logging, monitoring, or forensic capabilities to identify and attribute the attacker. Appropriate response documentation was not maintained is a finding that indicates that the organization did not follow a consistent and formal incident response procedure, or that it did not document its actions, decisions, and lessons learned from the incident.
References:
* ISACA CISA Review Manual 27th Edition (2019), page 254
* Incident Response Process - ISACA1
* Incident Response: How to Identify and Fix Security Weaknesses

最新問題**: 221**
次のどのタイプのファイアウォールがハッカーの侵入に対して最も高いレベルの制御を提供しますか?
A. 回線ゲートウェイ
B. アプリケーションレベルゲートウェイ
C. パケットフィルタリングルーター
D. スクリーニングルーター
Answer: B (メーッセージを残す**)**
The type of firewall that provides the greatest degree of control against hacker intrusion is an application level gateway. A firewall is a device or software that filters or blocks network traffic based on predefined rules or policies. A firewall can help protect an information system or network from unauthorized access or attack by hackers or other malicious entities. An application level gateway is a type of firewall that operates at the application layer of the network model (layer 7), which is where user applications communicate with each other over the network. An application level gateway provides the greatest degree of control against hacker intrusion, by inspecting and analyzing the content and context of each network packet at the application level, such as protocols, commands, requests, responses, etc., and allowing or denying access based on specific criteria or conditions. An application level gateway can also perform additional functions such as authentication, encryption, caching, logging, etc., to enhance the security and performance of network traffic.
A circuit gateway is a type of firewall that operates at the transport layer of the network model (layer 4), which is where data are transferred between end points over the network. A circuit gateway provides a moderate degree of control against hacker intrusion by establishing a secure connection between two end points (such as client and server) and relaying network packets between them without inspecting or analyzing their content. A

circuit gateway can also perform functions such as encryption, authentication, or address translation to improve the security and privacy of network traffic. A packet filtering router is a type of firewall that operates at the network layer of the network model (layer 3), which is where data are routed between different networks or subnets. A packet filtering router provides a low degree of control against hacker intrusion by examining the header of each network packet and allowing or denying access based on basic criteria such as source address, destination address, port number, protocol, etc. A packet filtering router can also perform functions such as routing, forwarding, or address translation to optimize the delivery and efficiency of network traffic. A screening router is a type of firewall that operates at the network layer of the network model (layer 3), which is where data are routed between different networks or subnets. A screening router provides a low degree of control against hacker intrusion by examining the header of each network packet and allowing or denying access based on basic criteria such as source address, destination address, port number, protocol, etc. A screening router can also perform functions such as routing, forwarding, or address translation to optimize the delivery and efficiency of network traffic.

最新問題**: 222**
侵害の疑いがある場合のインシデント対応プロセスの最初のステップは次のどれですか?
A. 影響を受ける可能性のある顧客にセキュリティ侵害について通知する
B. セキュリティ侵害について経営幹部に通知します。
C. 警告された侵害の妥当性を調査する
D. 警告された侵害を独立して評価するために第三者を関与させます。
Answer: C (メーッセージを残す**)**
The first step in the incident response process for a suspected breach is to research the validity of the alerted breach. An incident response process is a set of procedures that defines how to handle security incidents in a timely and effective manner. The first step in this process is to research the validity of the alerted breach, which means to verify whether the alert is genuine or false positive, to determine the scope and impact of the incident, and to gather relevant information for further analysis and action. Informing potentially affected customers of the security breach, notifying business management of the security breach, and engaging a third party to independently evaluate the alerted breach are also steps in the incident response process, but they are not the first step. References:
* CISA Review Manual, 27th Edition, page 4251
* CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

最新問題**: 223**
サイバー攻撃中のデータ流出のリスクを最も効果的に軽減する対策は次のどれですか?
A. ネットワーク アクセス制御 (NAC)
B. 機密データのハッシュ化
C. 境界ファイアウォール

D. データ損失防止 (DLP) システム
Answer: D (メーッセージを残す**)**

最新問題**: 224**
ある金融グループが最近、新しいテクノロジーとプロセスを導入しました。どのタイプの IS 監査が、部門の目的が達成されたことを最も確実に保証できるでしょうか?
A. パフォーマンス監査
B. 統合監査
C. サイバー監査
D. 財務監査
Answer: B (メーッセージを残す**)**
The type of IS audit that would provide the greatest level of assurance that the department's objectives have been met after implementing new technologies and processes is an integrated audit. An integrated audit is an audit that combines financial, operational, compliance, and IT auditing aspects to provide a holistic view of the organization's performance and risks. An integrated audit can evaluate whether the new technologies and processes are aligned with the organization's goals, strategies, policies, and controls, and whether they are delivering value, efficiency, effectiveness, and reliability. The other types of IS audits (A, C and D) would not provide the same level of assurance, as they would only focus on specific aspects of the organization's activities, such as performance, cyber security, or financial reporting, which may not capture the full impact of the new technologies and processes. References: CISA Certification | Certified Information Systems Auditor | ISACA, CISA Review Manual (Digital Version), Chapter 1: The Process of Auditing Information Systems, Section 1.2: Types of IS Audit Engagements

最新問題**: 225**
ある組織は、電子メールの本文に埋め込まれたリンクをクリックしたユーザーに現金報酬を提供するという電子メールを送信して、ユーザーのセキュリティ意識レベルをテストする演習を実施しました。次の指標のうち、意識向上トレーニングの有効性を最もよく示すものはどれですか。
A. フィッシングメールであるため報告せずにメールを削除したユーザーの数
B. メールの送信者についてさらに詳しく知るためにリンクをクリックしたユーザーの数
C. メールをビジネスユニットマネージャーに転送するユーザーの数
D. 情報セキュリティチームにメールの受信を報告したユーザーの数
Answer: D (メーッセージを残す**)**
The metric that best indicates the effectiveness of awareness training is the number of users reporting receipt of the email to the information security team. This shows that the users are able to recognize and report a phishing email, which is a common social engineering technique used by attackers to trick users into revealing sensitive information or installing malicious software. The other metrics do not demonstrate a high level of

security awareness, as they either ignore, follow, or forward the phishing email, which could expose the organization to potential risks. References: CISA Review Manual, 27th Edition, page 326

最新問題: **226**
IS 監査人は、組織のより広範なセキュリティ脅威および脆弱性管理プログラムと明確に整合していないアドホック脆弱性スキャンが実施されていることを発見しました。
組織がこの分野の改善に取り組むために最も効果的なのは次のどれですか?
A. 脅威と脆弱性の管理を強化するためのセキュリティログの実装
B. ミッションクリティカルなシステムに影響を与える可能性のある脆弱性のカタログを維持する
C. 能力成熟度モデルを使用して最適化されたプログラムへの道筋を特定する
D. 脅威と脆弱性の管理機能を第三者にアウトソーシングする
Answer: C (メーッセージを残す)
The best way to enable the organization to work toward improvement in its security threat and vulnerability management program is to use a capability maturity model to identify a path to an optimized program. A capability maturity model is a framework that helps organizations assess their current level of performance and maturity in a specific domain, and provides guidance and best practices to achieve higher levels of excellence12. A capability maturity model for vulnerability management can help the organization to evaluate its current practices, identify gaps and weaknesses, and implement improvement actions based on the defined criteria and objectives34.
References
1: What is a Capability Maturity Model?1 2: Capability Maturity Model - Wikipedia2 3: Vulnerability Management Maturity Model - SANS Institute4 4: 5 Stages Of Vulnerability Management Maturity Model - SecPod Blog3

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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**
監査計画中に、情報システム監査マネージャーは、ビジネス側からリスクが低いとみなされるエンティティの監査に予算を割くかどうかを検討しています。この状況で最善の行動方針は次のどれですか。

A. 低リスクの監査を外部監査サービスプロバイダーに委託します。
B. 低リスクの事業体に対して限定範囲の監査を実施します。
C. 低リスクのエンティティ評価を検証し、専門的な判断を適用します。
D. リスク評価に異議を唱え、低リスクのエンティティを計画に含めます。
Answer: C (メーッセージを残す)
Audit planning is the process of developing an overall strategy and approach for conducting an audit. Audit planning involves identifying the objectives, scope, criteria, and methodology of the audit, as well as the resources, schedule, and reporting requirements. Audit planning also involves performing a risk assessment to identify and prioritize the areas of highest risk and significance for the audit1.
Risk assessment is a systematic process of evaluating the potential risks that may be involved in a projected activity or undertaking. Risk assessment involves identifying the sources and causes of risk, analyzing the likelihood and impact of risk, and determining the level of risk and the appropriate response2.
During audit planning, the IS audit manager is considering whether to budget for audits of entities regarded by the business as having low risk. The best course of action in this situation is C. Validate the low-risk entity ratings and apply professional judgment.
This is because validating the low-risk entity ratings can help to ensure that the risk assessment is accurate, reliable, and consistent with the business objectives and expectations. Validating the low-risk entity ratings can also help to identify any changes or developments that may affect the risk profile of the entities since the last assessment.
Applying professional judgment can help to determine whether the low-risk entities should be included or excluded from the audit plan, based on factors such as materiality, relevance, significance, and assurance needs3.

最新問題**: 228**
悪意のある内部者による機密データの流出を識別する最も効果的な方法はどれですか?
A. データ損失防止 (DLP) ソフトウェアを実装する
B. 境界ファイアウォールのログを確認する
C. 継続的な情報セキュリティ意識向上トレーニングを提供する
D. 行動分析モニタリングを確立する
Answer: D (メーッセージを残す)
The most effective way to identify exfiltration of sensitive data by a malicious insider is to establish behavioral analytics monitoring. Behavioral analytics is the process of analyzing the patterns and anomalies in user behavior to detect and prevent insider threats. Behavioral analytics can help identify unusual or suspicious activities, such as accessing sensitive data at odd hours, transferring large amounts of data to external devices or locations, or using unauthorized applications or protocols. Behavioral analytics can also help correlate data from multiple sources, such as network logs, user profiles, and access rights, to provide a holistic view of user activity and risk.

Data loss prevention (DLP) software is a tool that can help prevent exfiltration of sensitive data by a malicious insider, but it is not the most effective way to identify it. DLP software can block or alert on unauthorized data transfers based on predefined rules and policies, but it may not be able to detect sophisticated or stealthy exfiltration techniques, such as encryption, steganography, or data obfuscation.
Reviewing perimeter firewall logs is a way to identify exfiltration of sensitive data by a malicious insider, but it is not the most effective way. Perimeter firewall logs can show the traffic volume and destination of data transfers, but they may not be able to show the content or context of the data. Perimeter firewall logs may also be overwhelmed by the amount of normal traffic and miss the signals of malicious exfiltration.
Providing ongoing information security awareness training is a way to reduce the risk of exfiltration of sensitive data by a malicious insider, but it is not a way to identify it. Information security awareness training can help educate users on the importance of protecting sensitive data and the consequences of violating policies and regulations, but it may not deter or detect those who are intentionally or maliciously exfiltrating data.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019, p. 300
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription 1
* Cybersecurity Engineering for Legacy Systems: 6 Recommendations - SEI Blog 2
* How to Secure Your Company's Legacy Applications - iCorps

最新問題**: 229**
組織の情報セキュリティ管理を確認する際に最も重要な発見は何ですか?
A. 専任のセキュリティ担当者がいない
B. 情報セキュリティ管理システムの公式名称はない
C. 脅威と脆弱性を特定するための定期的な評価が行われていない
D. 従業員の意識啓発トレーニングおよび教育プログラムがない
Answer: (解答を表示する**)**
The most critical finding when reviewing an organization's information security management is no periodic assessments to identify threats and vulnerabilities. Periodic assessments are essential for ensuring that the organization's information security policies, procedures, standards, and controls are aligned with the current and emerging risks and threats that may affect its information assets. Without periodic assessments, the organization may not be aware of its actual security posture, gaps, or weaknesses, and may not be able to take appropriate measures to mitigate or prevent potential security incidents. No dedicated security officer, no official charter for the information security management system, and no employee awareness training and education program are also findings that may indicate some deficiencies in the organization's information security management, but they are not as critical as no periodic assessments to identify threats and vulnerabilities. References: ISACA CISA Review Manual 27th Edition, page 343.

最新問題: **230**
IS 監査人が監査フォローアップ活動を開始する前に、次のどれを実施する必要がありますか?
A. 行動計画に含まれる活動に利用可能なリソース
B. 最終報告書における経営陣の回答と実施日
C. リスクの観点からギャップと推奨事項が表示された修復マップ
D. 監査報告書に記載されているギャップと推奨事項を裏付ける証拠
Answer: B (メーッセージを残す)
This must be in place before an IS auditor initiates audit follow-up activities, because it indicates that management has acknowledged and accepted the audit findings and recommendations, and has agreed to take corrective actions within a specified timeframe. Audit follow-up activities are the processes and procedures that the IS auditor performs to verify that management has implemented the agreed-upon actions effectively and in a timely manner, and that the audit findings have been resolved or mitigated.
The other options are not required to be in place before an IS auditor initiates audit follow-up activities:
* Available resources for the activities included in the action plan. This is a factor that may affect the feasibility and success of the action plan, but it is not a prerequisite for the audit follow-up activities.
The IS auditor should assess the availability and adequacy of the resources for the action plan during the audit planning and execution phases, and provide recommendations accordingly. However, the IS auditor does not need to wait for the resources to be available before initiating the audit follow-up activities.
* A heat map with the gaps and recommendations displayed in terms of risk. This is a tool that may help the IS auditor prioritize and communicate the gaps and recommendations, but it is not a requirement for the audit follow-up activities. A heat map is a graphical representation of data that uses colors to indicate the level of risk or impact of each gap or recommendation. The IS auditor may use a heat map to support the audit report or presentation, but it does not replace the need for a management response with a committed implementation date.
* Supporting evidence for the gaps and recommendations mentioned in the audit report. This is a component that should be included in the audit report, but it is not a condition for the audit follow-up activities. Supporting evidence is the information or data that supports or substantiates the audit findings and recommendations. The IS auditor should collect and document sufficient, reliable, relevant, and useful evidence during the audit execution phase, and present it in the audit report.
However, the IS auditor does not need to have supporting evidence in place before initiating the audit follow-up activities.

最新問題: **231**

災害が発生してデータ センターが利用できなくなった場合、最初に実行する必要があるタスクは次のうちどれですか。
A. データの復旧を実行します。
B. セカンダリサイトを手配します。
C. リスクを分析します。
D. 呼び出しツリーをアクティブにします。
Answer: D (メーッセージを残す)
In the event of a disaster where the data center is no longer available, the first step should be to activate the call tree1. A call tree is a layered hierarchical communication model used to notify specific individuals of an event and coordinate recovery efforts1. This ensures that all relevant parties are informed about the situation and can begin executing their parts of the disaster recovery plan1.
References:
IT Disaster Recovery Plan | Ready.gov

最新問題**: 232**
監査計画に含める領域を決定するためにリスク評価を使用する主な利点は次のうちどれですか?
A. タイムリーな監査の実行
B. 監査リソースの効果的な割り当て
C. 出張費と経費の削減
D. 効果的なリスク軽減
Answer: B (メーッセージを残す)
Using risk assessments to determine areas to be included in an audit plan is a primary benefit because it helps to prioritize the audit activities based on the level of risk and the potential impact of the audit findings. This way, the audit resources, such as time, staff, and budget, can be allocated more efficiently and effectively to the areas that need the most attention and provide the most value.
References
ISACA CISA Review Manual, 27th Edition, page 256
What is the Purpose of a Risk Assessment?
Mastering the Process of Risk Assessment

最新問題**: 233**
リスク評価の次の要素のうち、適用するリスク軽減のレベルを決定する際に管理者にとって最も役立つものはどれですか?
A. 影響評価
B. 制御自己評価 (CSA)
C. リスク分類
D. リスクの特定

Answer: (解答を表示する**)**

最新問題**: 234**
パッチの恣意的な適用を最も効果的に防止できるのは次のどれですか?
A. 変更管理
B. データベースアクセス制御
C. ネットワークベースのアクセス制御
D. メンテナンス期間の確立
Answer: A (メーッセージを残す**)**

最新問題**: 235**
情報システム監査人が、従来のシステムに代わる新しい健康記録システムに関連する最も重要なリスクとして考慮すべきものは何ですか?
A. スタッフが調達プロセスに関与していなかったため、新しいシステムに対するユーザーの抵抗が生じました。
B. データが正しく変換されないため、患者記録が不正確になります。
C. 展開プロジェクトでは大幅な超過が発生し、予算予測を超過しました。
D. 新しいシステムには容量の問題があり、ユーザーへの応答時間が遅くなります。
Answer: B (メーッセージを残す**)**
The most significant risk associated with a new health records system that replaces a legacy system is data not being converted correctly, resulting in inaccurate patient records. Data conversion is the process of transferring data from one format or system to another. Data conversion is a critical step in implementing a new health records system, as it ensures that the patient data are consistent, complete, accurate, and accessible in the new system. Data not being converted correctly may cause errors, discrepancies, or losses in patient records, which may have serious implications for patient safety, quality of care, legal compliance, and privacy protection. Staff not being involved in the procurement process, creating user resistance to the new system; the deployment project experiencing significant overruns, exceeding budget projections; and the new system having capacity issues, leading to slow response times for users are also risks associated with a new health records system implementation, but they are not as significant as data not being converted correctly. References: [ISACA CISA Review Manual 27th Edition], page 281.

最新問題**: 236**
トランザクション処理システムは、総勘定元帳とインターフェースします。データ分析により、一部のトランザクションが総勘定元帳に二重に記録されていることが判明しました。経営陣はシステム修正が実装されたと述べていますが、インターフェースが将来的に機能することを検証するために、情報システム監査人は何を推奨すべきでしょうか?
A. 定期的な調整を実行します。
B. システム修正に対するシステム所有者の承認を確認します。

C. 機能テストを実施します。
D. ユーザー受け入れテスト (UAT) を改善します。
Answer: A (メーッセージを残す**)**
A transaction processing system (TPS) is a system that captures, processes, and stores data related to business transactions1. A general ledger is a system that records the financial transactions of an organization in different accounts2. An interface is a connection point between two systems that allows data exchange3. A system fix is a change or update to a system that resolves a problem or improves its functionality4.
The IS auditor should recommend to perform periodic reconciliations to validate the interface between the TPS and the general ledger is working in the future. A reconciliation is a process of comparing and verifying the data in two systems to ensure accuracy and consistency1. By performing periodic reconciliations, the IS auditor can detect and correct any errors or discrepancies in the data, such as duplicate transactions, missing transactions, or incorrect amounts. This way, the IS auditor can ensure the reliability and integrity of the financial data in both systems.
The other options are not as effective as periodic reconciliations to validate the interface. System owner sign- off for the system fix is a form of approval that indicates the system owner agrees with the change and its expected outcome4. However, this does not guarantee that the system fix will work as intended or prevent future errors. Conducting functional testing is a process of verifying that the system performs its intended functions correctly and meets its requirements4. However, this is usually done before or after the system fix is implemented, not on an ongoing basis. Improving user acceptance testing (UAT) is a process of evaluating whether the system meets the needs and expectations of the end users4. However, this is also done before or after the system fix is implemented, not on an ongoing basis. Therefore, option A is the correct answer.
References:
Transaction Interface: Organization, Process, and System
Validation of Interfaces - Ensuring Data Integrity and Quality across Systems Oracle Payments Implementation Guide Receiving Transactions Inserted Into Interface Table as BATCH And PENDING Are Not Processed By Receiving Transaction Processor What Is a Transaction Processing System (TPS)? (Plus Types)

最新問題**: 237**
退職面接中に、上級管理職は監査報告書の草案で提示された事実の一部に同意できず、それらを報告書から削除することを希望しました。監査人が取るべき最善の行動は次のどれでしょうか。
A. 上級管理職の反対意見に基づいて評価を修正します。
B. 問題を監査管理者にエスカレートします。
C. 監査レポートのドラフトを変更せずに最終決定します。
D. 上級管理職の反対意見を分析するための証拠を集める

Answer: (解答を表示する**)**
The auditor's best course of action when senior management disagrees with some of the facts presented in the draft audit report is to gather evidence to analyze senior management's objections. The auditor should not revise the assessment, escalate the issue, or finalize the report without changes until they have evaluated the validity and relevance of senior management's objections and resolved any discrepancies or misunderstandings. The auditor should maintain a professional and objective attitude and seek to present a fair and accurate audit report based on sufficient and appropriate evidence. References:
* CISA Review Manual (Digital Version), page 372
* CISA Questions, Answers & Explanations Database, question ID 3338

最新問題**: 238**
組織の品質管理システム (QMS) の管理を確認する際に、情報システム監査人が検証する必要がある最も重要な項目は次のどれですか。
A. 失敗した変更や拒否された変更すべてに対して根本原因分析を実行するかどうか
B. 継続的な改善領域と必要な目標を監視するプロセスがあるかどうか
C. 組織が業界で認められたサービス管理フレームワークに従っているかどうか
D. 重要なサービスがタイムリーかつ持続可能な方法で提供されているかどうか
Answer: B (メーッセージを残す**)**

最新問題**: 239**
消費者サービス組織向けに、ベンダーが新しいシステムを開発しています。システム開発が完了すると、ベンダーは独自のソフトウェアを提供します。継続性を確保するためにベンダー契約に含める最も重要な要件は次のどれですか。
A. 24 時間 365 日の継続的なサポートが利用可能である必要があります。
B. ベンダーは、文書化された災害復旧計画 (DRP) を用意する必要があります。
C. ソフトウェアのソースコードはエスクローに置く必要があります。
D. ベンダーは、新しいソフトウェアを管理するためのトレーニングを組織のスタッフに実施する必要がある。
Answer: (解答を表示する**)**
Source code for the software must be placed in escrow is the most important requirement to include in the vendor contract to ensure continuity. Source code is the original code of a software program that can be modified or enhanced by programmers. Placing source code in escrow means depositing it with a trusted third party who can release it to the customer under certain conditions, such as vendor bankruptcy, breach of contract, or failure to provide support. This can help to ensure continuity of the software product and its maintenance in case of vendor unavailability or dispute. The other options are less important requirements to include in the vendor contract, as they may involve support availability, disaster recovery plan, or staff training. References:

* CISA Review Manual (Digital Version), Chapter 5, Section 5.51
* CISA Review Questions, Answers & Explanations Database, Question ID 228

最新問題: **240**
IS 監査人は、最近のリリースの欠陥により、出納係取引システムが顧客に誤って料金を請求するという最近の製造インシデントに気付きました。監査人が次に取るべきステップは次のどれですか。
A. 開発者のトレーニングを評価します。
B. インシデント管理プロセスを評価します。
C. 変更管理プロセスを評価します。
D. 安全なコードプラクティスを評価します。
Answer: C (メーッセージを残す**)**
The change management process is the set of procedures and activities that ensure that changes to the information system are authorized, tested, documented, and implemented in a controlled manner12. A defect in a recent release indicates that there may be issues with the quality assurance, testing, or approval of the changes, which could affect the reliability, security, and performance of the system3 . Therefore, the auditor's next step should be to evaluate the change management process and identify the root cause of the defect, as well as the impact and remediation of the incident.
References
1: Change Management - CISA
2: What is Change Management? - Definition from Techopedia
3: How to Audit Change Management - ISACA Journal
The Business Case for Security | CISA

最新問題: **241**
アプリケーション制御に関する議論を開始するのに最適なのは、ソフトウェア開発ライフサイクルのどのフェーズですか?
A. 利害関係者が特定されるビジネスケース開発フェーズ
B. アプリケーション設計フェーズのプロセス機能が完成しました
C. テストシナリオを設計するユーザー受け入れテスト (UAT) フェーズ
D. ビジネス上の問題を解決するためのアルゴリズムを開発するアプリケーションコーディングフェーズ
Answer: B (メーッセージを残す**)**
The best phase of the software development life cycle to initiate the discussion of application controls is the application design phase when process functionalities are finalized. Application controls are the policies, procedures, and techniques that ensure the completeness, accuracy, validity, and authorization of data input, processing, output, and storage in an application. Application controls help prevent, detect, or correct errors and

fraud in software applications. Examples of application controls include input validation, edit checks, reconciliation, encryption, access control, audit trails, etc.
The application design phase is when the software requirements are translated into a logical and physical design that specifies how the application will look and work. This phase is the best time to discuss application controls because it allows the developers to incorporate them into the design specifications and ensure that they are aligned with the business objectives and user needs. By discussing application controls early in the design phase, the developers can also avoid costly rework or changes later in the development process.
The other phases are not as optimal as the application design phase to initiate the discussion of application controls. A. Business case development phase when stakeholders are identified. The business case development phase is when the feasibility, scope, objectives, benefits, risks, and costs of a software project are defined and evaluated. This phase is important for obtaining stakeholder approval and support for the project, but it is too early to discuss application controls in detail because the software requirements and functionalities are not yet clear or finalized. B. User acceptance testing (UAT) phase when test scenarios are designed. The user acceptance testing phase is when the software is tested by the end-users or stakeholders to verify that it meets their expectations and requirements. This phase is too late to discuss application controls because it is near the end of the development process and any changes or additions to the application controls would require retesting and revalidation of the software. C. Application coding phase when algorithms are developed to solve business problems. The application coding phase is when the software design is translated into executable code using programming languages and tools. This phase is not ideal to discuss application controls because it is after the design phase and any changes or additions to the application controls would require redesigning and recoding of the software.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019, p. 2471
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription2
* What Is Application Control? | McAfee3
* What Is Application Lifecycle Management? | Red Hat4

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

https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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**
災害復旧計画 (DRP) をテストするための次の手順のうち、最も効果的なものはどれですか?
A. オフサイトデータバックアップを使用したセカンダリサイトでのテスト
B. 文書化されたバックアップおよびリカバリ手順の確認
C. リカバリ時間とリカバリポイント目標の確認
D. 四半期ごとのテーブルトップ演習の実施
Answer: A (メーッセージを残す**)**

最新問題: **243**
組織が IS 監査で合意されたアクション プランを確実に実行できるようにするために、最も効果的な方法はどれですか。
A. 十分な監査リソースが割り当てられていることを確認する。
B. 監査結果を組織全体に伝達します。
C. 所有権が割り当てられていることを確認します。
D. 完了したら修正アクションをテストします。
Answer: C (メーッセージを残す**)**
The most effective way for an organization to help ensure agreed-upon action plans from an IS audit will be implemented is to ensure ownership is assigned. This means that the management of the audited area should accept responsibility for implementing the action plans and report on their progress and completion to the audit committee or senior management. This will ensure accountability, commitment, and follow-up for the audit recommendations34. References: 3: CISA Review Manual (Digital Version), Chapter 1: The Process of Auditing Information Systems, Section 1.6: Reporting, page 41 4: CISA Online Review Course, Module 1:
The Process of Auditing Information Systems, Lesson 1.6: Reporting

最新問題: **244**
組織のビジネスクリティカルなサーバー ハードウェアのオンサイト予防保守を確認する IS 監査人にとって、次のどれが最も懸念されるでしょうか。
A. 予防保守コストがビジネスに割り当てられた予算を超えています。
B. 予防保守は情報システムによって承認されていません
C. 予防保守は、秘密保持契約 (NDA) を必要とせずに複数のベンダーにアウトソーシングされます。
D. 予防保守スケジュールは、平均故障間隔 (MTBF) パラメータに基づいています。
Answer: (解答を表示する**)**

The answer C is correct because preventive maintenance is outsourced to multiple vendors without requiring nondisclosure agreements (NDAs) would be of greatest concern to an IS auditor reviewing on-site preventive maintenance for an organization's business-critical server hardware. This is because outsourcing preventive maintenance to multiple vendors without NDAs exposes the organization to the risk of unauthorized access, disclosure, or modification of sensitive data and information stored on the servers. NDAs are legal contracts that bind the vendors to protect the confidentiality and security of the data and information they access or handle during the preventive maintenance. Without NDAs, the vendors may not have any obligation or incentive to safeguard the data and information, and they may misuse, leak, or compromise them for malicious or commercial purposes. This could result in financial losses, reputational damage, legal liabilities, or regulatory penalties for the organization.
The other options are not as concerning as option C. Preventive maintenance costs exceed the business allocated budget (option A) is a financial issue that may affect the profitability or efficiency of the organization, but it does not directly impact the security or availability of the server hardware. Preventive maintenance has not been approved by the information system (option B) is a procedural issue that may indicate a lack of coordination or communication between the IT department and the business units, but it does not necessarily affect the quality or effectiveness of the preventive maintenance. The preventive maintenance schedule is based on mean time between failures (MTBF) parameters (option D) is a technical issue that may influence the frequency or timing of the preventive maintenance, but it does not imply any risk or deficiency in the preventive maintenance itself.
References:
* What is a Maintenance Audit?
* How to audit your preventative maintenance schedule
* 5 Step Maintenance Management Program Audit
* How do you get effective Preventive Maintenance really?
* What is a Planned Preventative Maintenance Audit?

最新問題: **245**
進行中の監査中に、経営陣はこれまでの調査結果についての説明を要求します。次のどれが情報システム監査人の最善の行動方針でしょうか?
A. 監査対象者と作業書類を確認します。
B. 監査対象者に管理上の回答を求めます。
C. 最終レポートが議論できる状態になるまで管理者に待機するよう要求します。
D. 議論のためだけに観察結果を提示します。
Answer: (解答を表示する**)**
The IS auditor's best course of action in this situation is to present observations for discussion only.

Observations are factual statements or findings that are based on the audit evidence collected and analyzed during the audit. Observations can be presented to management for discussion and feedback, but they should not be considered as final conclusions or recommendations until the audit is completed and the audit report is issued. The other options are not appropriate for presenting the findings to date, as they may compromise the audit quality or integrity. Reviewing working papers with the auditee is not advisable, as working papers are confidential documents that contain the auditor's notes, calculations, and opinions that may not be relevant or accurate for management's review. Requesting the auditee provide management responses is premature, as management responses should be obtained after the audit report is issued and the audit findings and recommendations are finalized. Requesting management wait until a final report is ready for discussion is impractical, as management may have a legitimate interest or need to know the audit progress and results as soon as possible. References: CISA Review Manual (Digital Version), Chapter 2, Section 2.3

最新問題**: 246**
経営行動計画の監査フォローアップを実施する際の主な目的は次のどれですか?
A. 経営行動計画をビジネス要件と整合させる
B. 組織の新たなリスクと管理を特定する
C. 上級管理職が監査結果を把握していることを確認する
D. 監査報告書に記載されたリスクが適切に軽減されていることを確認する
Answer: (解答を表示する**)**

最新問題**: 247**
大規模なビジネス アプリケーションの開発の複雑さを見積もるのに最適な方法はどれですか?
A. 機能ポイント分析
B. 作業分解構造
C. クリティカルパスアナリスト
D. ソフトウェアコストの見積もり
Answer: (解答を表示する**)**
Function point analysis (FPA) is the best methodology to use for estimating the complexity of developing a large business application. FPA is a technique that measures the functionality of a software system based on the user requirements and the business processes that the system supports. FPA assigns a numerical value to each function or feature of the system, based on its type, complexity, and relative size. The total number of function points represents the size and complexity of the system, which can be used to estimate the development effort, cost, and time.
FPA has several advantages over other estimation methods, such as:

* It is independent of the technology, programming language, or development methodology used for the system. Therefore, it can be applied consistently across different platforms and environments.
* It is based on the user perspective and the business value of the system, rather than the technical details or implementation aspects. Therefore, it can be performed early in the project life cycle, before the design or coding phases.
* It is objective and standardized, as it follows a set of rules and guidelines defined by the International Function Point Users Group (IFPUG). Therefore, it can reduce ambiguity and improve accuracy and reliability of the estimates.
* It is adaptable and scalable, as it can handle changes in the user requirements or the system scope.
Therefore, it can support agile and iterative development approaches.
References:
* 1: Function Point Analysis - Introduction and Fundamentals
* 2: Software Engineering | Functional Point (FP) Analysis

最新問題**: 248**
ビジネス アプリケーションで最近内部的にバグが悪用されたことが発見されたことを IS 監査人が知らされた場合、実施することが最も重要なレビューの種類はどれですか。
A. 侵入テスト
B. アプリケーションセキュリティテスト
C. フォレンジック監査
D. サーバーセキュリティ監査
Answer: C (メーッセージを残す**)**
The type of review that is most important to conduct when an IS auditor is informed that a recent internal exploitation of a bug has been discovered in a business application is C. Forensic audit. A forensic audit is a type of audit that involves collecting, analyzing, and preserving evidence of fraud, corruption, or other illegal or unethical activities1. A forensic audit can help the IS auditor to identify and document the source, scope, and impact of the exploitation, as well as the perpetrators, motives, and methods involved. A forensic audit can also help the IS auditor to provide recommendations for preventing or mitigating future exploitations, and to support any legal actions or investigations that may arise from the incident2.

最新問題**: 249**
データ所有者がデータに誤った分類レベルを割り当てた場合、情報システム監査人が最も懸念すべき事項は次のどれですか?
A. データを適切に保護するための制御が適用されない可能性があります。
B. データはシステム管理者によって暗号化されていない可能性があります。
C. 競合他社がデータを閲覧できる場合があります。

D. 制御コストが IT 資産の本質的価値を超える可能性があります。
Answer: A (メーッセージを残す**)**
The answer A is correct because the greatest concern for an IS auditor when a data owner assigns an incorrect classification level to data is that controls to adequately safeguard the data may not be applied. Data classification is the process of categorizing data assets based on their information sensitivity and business impact. Data classification helps organizations to identify, protect, and manage their data according to their value and risk. Data owners are the individuals or entities who have the authority and responsibility to define, classify, and control the access and use of their data.
Data classification typically involves assigning labels or tags to data assets, such as public, internal, confidential, or restricted. These labels indicate the level of protection and handling required for the data.
Based on the data classification, organizations can implement appropriate controls to safeguard the data, such as encryption, access control lists, audit logs, backup policies, etc. These controls help to prevent unauthorized access, disclosure, modification, or loss of data, and to ensure compliance with relevant laws and regulations.
If a data owner assigns an incorrect classification level to data, it can result in either underprotection or overprotection of the data. Underprotection means that the data is classified at a lower level than it should be, which exposes it to higher risks of compromise or breach. For example, if a data owner classifies personal health information (PHI) as public instead of confidential, it may allow anyone to access or share the data without proper authorization or consent. This can violate the privacy rights of the data subjects and the compliance requirements of regulations such as HIPAA (Health Insurance Portability and Accountability Act). Overprotection means that the data is classified at a higher level than it should be, which limits its availability or usability. For example, if a data owner classifies marketing materials as restricted instead of public, it may prevent potential customers or partners from accessing or viewing the data. This can reduce the business value and opportunities of the data.
Therefore, an IS auditor should be concerned about the accuracy and consistency of data classification by data owners, as it affects the security and efficiency of data management. An IS auditor should review the policies and procedures for data classification, verify that the data owners have adequate knowledge and skills to classify their data, and test that the data classification labels match with the actual sensitivity and impact of the data.
References:
* Data Classification: What It Is and How to Implement It
* What Is Data Classification? - Definition, Levels & Examples ...
* Data Classification: A Guide for Data Security Leaders

最新問題**: 250**
以前の監査人の作業に依拠する場合、次のうち最も重要な考慮事項はどれですか?
A. 前回の監査の期間

B. 推奨事項を含む管理合意
C. 前監査人の資格
D. 前回の監査人が特定した指摘事項の数
Answer: C (メーッセージを残す**)**

最新問題**: 251**
最近、ある組織は規制当局から報告データに重大な矛盾があるという通知を受けました。予備調査により、この不一致は組織のデータ品質の問題によって生じたことが判明しました。経営陣はデータ品質チームにプログラムを強化するよう指示しました。監査委員会は内部監査にプロセスのアドバイザーを務めるよう依頼しました。経営陣の懸念に確実に対処するために、内部監査はどのデータ セットを最初にレビューすることを推奨すべきでしょうか。
A. 顧客の個人情報を含むデータ
B. 規制当局に報告されたデータ
C. 財務諸表を裏付けるデータ
D. ビジネス目標に影響を与えるデータ
Answer: (解答を表示する**)**
To ensure that management concerns are addressed, internal audit should recommend that the data quality team review the data reported to the regulatory body first. This is because this data set is the most relevant and critical to the issue that triggered the enhancement of the data quality program. The data reported to the regulatory body should be accurate, complete, consistent, and timely, as any discrepancies could result in fines, penalties, or reputational damage for the organization. Data with customer personal information is important for data quality, but it is not directly related to the regulatory reporting issue. Data supporting financial statements is important for data quality, but it may not be the same as the data reported to the regulatory body. Data impacting business objectives is important for data quality, but it may not be as urgent or sensitive as the data reported to the regulatory body. References:
* CISA Review Manual, 27th Edition, pages 404-4051
* CISA Review Questions, Answers & Explanations Database, Question ID: 262

最新問題**: 252**
多国籍銀行の処分プロセスの監査中に、情報システム監査人はいくつかの発見事項に注目しました。監査人が最も懸念すべきことは次のうちどれですか?
A. バックアップ メディアは廃棄前に確認されません。
B. 物理的な細断の代わりに消磁が使用されます。
C. バックアップ メディアは保存期間が終了する前に破棄されます
D. ハードウェアは認定ベンダーによって破壊されません。
Answer: C (メーッセージを残す**)**

During an audit of a multinational bank's disposal process, an IS auditor should be most concerned about backup media being disposed before the end of the retention period. This is because backup media contain sensitive and critical data that may be required for business continuity, legal compliance, or forensic purposes.
Disposing backup media prematurely may result in data loss, unavailability, or corruption, which may have severe consequences for the bank's reputation, operations, and security. Backup media not being reviewed before disposal, degaussing being used instead of physical shredding, and hardware not being destroyed by a certified vendor are also findings that may pose some risks to the bank's disposal process, but they are not as critical as backup media being disposed before the end of the retention period.
References: ISACA CISA Review Manual 27th Edition, page 302.

最新問題**: 253**
大規模組織向けのデータ侵害防止 (DIP) ソリューションを開発する場合、最初に行うべきステップは次のどれですか。
A. 企業全体で承認されたデータ ワークフローを特定します。
B. 機密データの使用に対する脅威分析を実施します。
C. DLP pcJc.es とテンプレートを作成する
D. データのインベントリと分類の演習を実施する
Answer: D (メーッセージを残す**)**
The first step when developing a data loss prevention (DLP) solution for a large organization is to conduct a data inventory and classification exercise. This step is essential to identify the types, locations, owners, and sensitivity levels of the data that need to be protected by the DLP solution. A data inventory and classification exercise helps to define the scope, objectives, and requirements of the DLP solution, as well as to prioritize the data protection efforts based on the business value and risk of the data. A data inventory and classification exercise also enables the organization to comply with relevant laws and regulations regarding data privacy and security.
The other options are not the first step when developing a DLP solution, but rather subsequent steps that depend on the outcome of the data inventory and classification exercise. Identifying approved data workflows across the enterprise is a step that helps to design and implement the DLP policies and controls that match the business processes and data flows. Conducting a threat analysis against sensitive data usage is a step that helps to assess and mitigate the risks associated with data leakage, theft, or misuse. Creating the DLP policies and templates is a step that helps to enforce the data protection rules and standards across the organization.
References:
* ISACA CISA Review Manual 27th Edition (2019), page 247
* Data Loss Prevention-Next Steps - ISACA1
* What is data loss prevention (DLP)? | Microsoft Security

最新問題: **254**
IS 監査の問題を経営陣に伝える際に、主に重点を置くべきは次のどれですか?
A. 問題がどのように発見され、誰が責任を負うのか
B. その後の監査フォローアップの性質、範囲、タイミング
C. 問題により組織がさらされるリスク
D. 問題を解決するための詳細な解決策
Answer: C (メーッセージを残す**)**

最新問題: **255**
悪意のあるプログラム コードがアプリケーション内で見つかり、運用環境にリリースされる前に修正されました。リリース後も同様の問題が報告されました。情報システム監査人の最良の推奨事項は次のうちどれですか?
A. 修正されたプログラム コードが専用サーバーでコンパイルされていることを確認します。
B. 変更管理レポートが独立してレビューされていることを確認します。
C. プログラム編集の完了後にプログラマーがコードにアクセスできないようにします。
D. 企業がエンドツーエンドのユーザー受け入れテスト (UAT) の結果に同意していることを確認します。
Answer: C (メーッセージを残す**)**
The IS auditor's best recommendation is to ensure that programmers cannot access code after the completion of program edits. This is because programmers who have access to code after editing may introduce unauthorized or malicious changes that could compromise the security, functionality, or performance of the application. By restricting access to code after editing, the organization can ensure that only authorized and tested code is released into production, and prevent any tampering or reoccurrence of the same issue.
References:
* 1 discusses the importance of controlling access to code after editing and testing, and provides some best practices for doing so.
* 2 explains how programmers can introduce malicious code into applications, and how to prevent and detect such attacks.
* 3 describes the role of IS auditors in reviewing and assessing the security and quality of application code.

最新問題: **256**
IS 監査人は、ある従業員が機密データに不正アクセスしていることを発見しました。IS 監査人の最善の推奨事項は次のようになります。
A. データをより低い機密レベルに再分類する
B. ビジネスオーナーに定期的なアクセスレビューの実施を義務付けます。
C. ユーザーに対して強力なパスワード スキーマを実装します。

D. セキュリティ管理者が実行すべき是正措置を推奨します。
Answer: B (メーッセージを残す**)**
The best recommendation for an IS auditor who finds that one employee has unauthorized access to confidential data is to require the business owner to conduct regular access reviews. Access reviews are periodic assessments of user access rights and permissions to ensure that they are appropriate, necessary, and aligned with the business needs and objectives. Access reviews help to identify and remediate any unauthorized, excessive, or obsolete access that could pose a security risk or violate compliance requirements.
The business owner is responsible for defining and approving the access requirements for their data and ensuring that they are enforced and monitored. References:
* CISA Review Manual (Digital Version)
* CISA Questions, Answers & Explanations Database

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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**
職務の分離に関連する次の調査結果のうち、情報システム監査人にとって最も懸念すべきものはどれですか?
A. ソース コードを編集するユーザーは、プロダクションへの書き込みアクセス権も持ちます。
B. 新しいユーザー アカウントを作成したユーザーは、ユーザー アクセス レベルも変更します。
C. サーバーを管理する人もインフラストラクチャ管理チームの一員です。
D. ソースコードをテストする人が変更も承認します。
Answer: (解答を表示する**)**

最新問題: **258**
災害の影響を予測するために組織が行うべきことは何ですか?
A. 復旧ポイント目標 (RPO) を定義する
B. 災害復旧をシミュレートする
C. ビジネス影響分析 (BIA) を開発する
D. 能力成熟度モデルのギャップを分析する
Answer: C (メーッセージを残す**)**

A business impact analysis (BIA) is the process of identifying and assessing the potential impacts a disruption or incident could have on an organization. A BIA helps organizations understand and prepare for these potential obstacles, so they can act quickly and face challenges head-on when they arise. A BIA tells the organization what to expect when unforeseen roadblocks occur, so they can make a plan to get their business back on track as quickly as possible. Therefore, a BIA is the best option to anticipate the effects of a disaster.
References:
* 10: Business Impact Analysis (BIA): Prepare for Anything [2023] * Asana
* 11: Definition of Business Impact Analysis (BIA) - IT Glossary | Gartner Information Technology
* 12: Business impact analysis (BIA) is a method to predict the consequences of disruptions to a business, its processes and systems by collecting relevant data.

最新問題**: 259**
制御目標を満たす IT 制御の設計に主に責任を負うのは誰ですか?
A. ビジネス管理
B. ITC マネージャー
C. 内部監査員
D. リスク管理
Answer: B (メーッセージを残す**)**

最新問題**: 260**
データ処理施設に設置された煙探知器の有効性にとって最も重要なのは次のどれですか?
A. 検出器は適切な業界認定を受けています。
B. 検出器は作動すると可聴アラームを発します。
C. 検知器は乾式パイプ消火システムにリンクされています。
D. 検知器は湿式パイプ消火システムにリンクされています。
Answer: B (メーッセージを残す**)**

最新問題**: 261**
仮想サーバー ファームの潜在的なソフトウェアの脆弱性の監査を実施する場合、情報システム監査人が最大のリスクと見なすのは次のどれですか。
A. ゲストオペレーティングシステムは毎月更新されます
B. ハイパーバイザーは四半期ごとに更新されます。
C. 1つの仮想サーバー上でさまざまなゲストオペレーティングシステムが動作する
D. ウイルス対策ソフトウェアはゲスト オペレーティング システムにのみ実装されています。
Answer: D (メーッセージを残す**)**

Antivirus software has been implemented on the guest operating system only is the observation that an IS auditor would consider the greatest risk when conducting an audit of a virtual server farm for potential software vulnerabilities. A virtual server farm is a collection of servers that run multiple virtual machines (VMs) on a single physical host using a software layer called a hypervisor. A guest operating system is the operating system installed on each VM. Antivirus software is a software program that detects and removes malicious software from a computer system. If antivirus software has been implemented on the guest operating system only, it means that the hypervisor and the host operating system are not protected from malware attacks, which could compromise the security and availability of all VMs running on the same host.
Therefore, antivirus software should be implemented on both the guest and host operating systems as well as on the hypervisor. References: CISA Review Manual, 27th Edition, page 378

最新問題**: 262**
組織の運用ログ管理を確認する IS 監査人にとって、最も懸念すべき事項は次のどれですか?
A. 重要なイベントが不変のログ ファイルに記録されています。
B. ログ ファイルのサイズは年々増加しています。
C. データ形式はすべてのログ間で標準化されていません。
D. アプリケーションは複数のログ ファイルにイベントを記録しています。
Answer: C (メーッセージを残す**)**

最新問題**: 263**
フォローアップ監査中に、IS 監査人は、いくつかの重要な推奨事項が IS 監査人の最善の行動方針であることを発見しましたか?
A. 監査対象者に推奨事項に完全に対処することを要求します。
B. それに応じて年間リスク評価を調整します。
C. 上級管理職のリスク受容度を評価する。
D. 経営陣のリスク受容に基づいて監査プログラムを更新します。
Answer: (解答を表示する**)**
The best course of action for an IS auditor who finds that some critical recommendations have not been implemented is to evaluate senior management's acceptance of the risk. The IS auditor should understand the reasons why the recommendations have not been implemented and the implications for the organization's risk exposure. The IS auditor should also verify that senior management has formally acknowledged and accepted the residual risk and has documented the rationale and justification for their decision. The IS auditor should communicate the findings and the risk acceptance to the audit committee and other relevant stakeholders.
References:

* CISA Review Manual (Digital Version)
* CISA Questions, Answers & Explanations Database

最新問題**: 264**
古いシステムと互換性のないテクノロジーを使用して新しいシステムに移行する場合のリスクを最も軽減できる方法はどれですか?
A. 並列切り替え
B. モジュール切り替え
C. 段階的な操作
D. パイロット操作
Answer: A (メーッセージを残す**)**
The best method to reduce the risk associated with the transition to a new system using technologies that are not compatible with the old system is parallel changeover. Parallel changeover is a method of system conversion that involves running both the old and the new systems simultaneously for a period of time, until the new system is verified to be working correctly and completely. Parallel changeover can help reduce the risk of data loss, errors, or disruptions that may occur due to the incompatibility of the technologies, as well as provide a backup option in case of failure or malfunction of the new system. Parallel changeover can also help users compare and validate the results of both systems, and facilitate their training and adaptation to the new system.
Modular changeover is a method of system conversion that involves replacing one module or component of the old system with a corresponding module or component of the new system at a time, until the entire system is replaced. Modular changeover can help reduce the complexity and scope of the conversion, as well as minimize the impact on the users and operations. However, modular changeover may not be feasible or effective when the technologies of the old and new systems are not compatible, as it may create integration or interoperability issues among the modules.
Phased operation is a method of system conversion that involves implementing the new system in stages or increments, each with a subset of functions or features, until the entire system is operational. Phased operation can help reduce the risk and cost of implementing a large and complex system, as well as allow for testing and feedback at each stage. However, phased operation may not be suitable or efficient when the technologies of the old and new systems are not compatible, as it may require extensive modifications or adaptations to enable partial functionality.
Pilot operation is a method of system conversion that involves implementing the new system in a limited or controlled environment, such as a department or a location, before rolling it out to the entire organization.
Pilot operation can help test and evaluate the performance and usability of the new system, as well as identify and resolve any issues or problems before full-scale implementation. However, pilot operation may not be relevant or reliable when the

technologies of the old and new systems are not compatible, as it may not reflect the actual conditions or challenges of operating both systems concurrently.
References:
* TRANSITION TO THE NEW SYSTEM - O'Reilly Media 1
* 10 Challenges To Think About When Upgrading From Legacy Systems - Forbes

最新問題**: 265**
報告された調査結果を関連する行動計画、所有者、目標日とともに発行することを要求する監査アプローチの主な利点は何ですか?
A. 監査のフォローアップが容易になります
B. 監査人と被監査人の間で行動計画の合意を強制する
C. 行動計画に対する説明責任を確立する
D. 調査結果の事実上の正確性を確保するのに役立ちます
Answer: (解答を表示する**)**
The primary benefit of an audit approach that requires reported findings to be issued together with related action plans, owners, and target dates is that it establishes accountability for the action plans. Accountability means that the individuals or groups who are responsible for implementing the action plans are clearly identified and held liable for their completion within the specified time frame. Accountability also implies that the action plans are monitored and evaluated to ensure that they are effective and efficient in addressing the audit findings and mitigating the associated risks1. Accountability helps to ensure that the audit recommendations are taken seriously and implemented properly, and that the audit value is realized by the organization2. The other options are less relevant or incorrect because:
* A. It facilitates easier audit follow-up is not the primary benefit of an audit approach that requires reported findings to be issued together with related action plans, owners, and target dates, as it is more of a secondary or indirect benefit. Audit follow-up is the process of verifying whether the action plans have been implemented and whether they have resolved the audit findings3. While having clear action plans, owners, and target dates may facilitate easier audit follow-up by providing a basis for tracking and reporting the progress and status of the action plans, it does not necessarily guarantee that the action plans will be implemented or effective.
* B. It enforces action plan consensus between auditors and auditees is not the primary benefit of an audit approach that requires reported findings to be issued together with related action plans, owners, and target dates, as it is more of a prerequisite or condition for such an approach. Action plan consensus means that the auditors and auditees agree on the audit findings and recommendations, and on the action plans to address them4. While having action plan consensus may enhance the credibility and acceptance of the audit approach, it does not necessarily ensure that the action plans will be implemented or effective.

* D. It helps to ensure factual accuracy of findings is not the primary benefit of an audit approach that requires reported findings to be issued together with related action plans, owners, and target dates, as it is more of an outcome or result of such an approach. Factual accuracy of findings means that the audit findings are based on sufficient, reliable, relevant, and useful evidence5. While having factual accuracy of findings may increase the confidence and trust in the audit approach, it does not necessarily ensure that the action plans will be implemented or effective. References: Accountability - ISACA, Audit Value - ISACA, Audit Follow-up - ISACA, Action Plan Consensus - ISACA, Factual Accuracy of Findings - ISACA

最新問題**: 266**
IT インフラストラクチャのパフォーマンス、リスク、機能は、次の方法を使用して最もよく測定できます。
A. リスク管理レビュー
B. コントロール自己評価 (CSA)。
C. サービス レベル アグリーメント (SLA)。
D. バランス スコアカード。
Answer: (解答を表示する**)**
A service level agreement (SLA) is a contract between a service provider and a customer that defines the expected level of performance, risks, and capabilities of an IT infrastructure. An IS auditor can use an SLA to measure how well the IT infrastructure meets the business needs and objectives, as well as to identify any gaps or issues that need to be addressed. The other options are not directly related to measuring the performance, risks, and capabilities of an IT infrastructure. References:
* CISA Review Manual (Digital Version), Chapter 5, Section 5.2.11
* CISA Review Questions, Answers & Explanations Database, Question ID 203

最新問題**: 267**
従業員がモバイル デバイスを紛失し、企業の機密データが失われました。次のどれがデータ漏洩を最も効果的に防ぐことができますか?
A. モバイルデバイス上のデータ暗号化
B. モバイルデバイス向けの複雑なパスワードポリシー
C. リモートデータ消去機能の起動
D. モバイルデバイスユーザー向けの意識啓発トレーニング
Answer: A (メーッセージを残す**)**
The best way to prevent data leakage from a lost mobile device is data encryption on the mobile device. Data encryption is a technique that transforms data into an unreadable format using a secret key or algorithm. Data encryption protects data from unauthorized access or disclosure in case of loss or theft of a mobile device.

Complex password policy for mobile devices, triggering of remote data wipe capabilities, and awareness training for mobile device users are useful measures to enhance data security on mobile devices, but they do not prevent data leakage as effectively as data encryption. A complex password policy can be bypassed by brute force attacks or password cracking tools. Remote data wipe capabilities depend on network connectivity and device power availability. Awareness training for mobile device users can reduce human errors or negligence, but it cannot guarantee compliance or behavior change. References: CISA Review Manual (Digital Version): Chapter 5 - Information Systems Operations and Business Resilience

最新問題**: 268**
職務の分離における弱点を検出するのに最も役立つ文書は次のどれですか?
A. システムフローチャート
B. データフロー図
C. プロセスフローチャート
D. エンティティ関係図
Answer: C (メーッセージを残す**)**
The best document for an IS auditor to use in detecting a weakness in segregation of duties is a process flowchart. A process flowchart is a diagram that illustrates the sequence of steps, activities, tasks, or decisions involved in a business process. A process flowchart can help detect a weakness in segregation of duties by showing who performs what actions or roles in a process, and whether there is any overlap or conflict of interest among them. The other options are not as useful as a process flowchart in detecting a weakness in segregation of duties, as they do not show who performs what actions or roles in a process. A system flowchart is a diagram that illustrates the components, functions, interactions, or logic of an information system. A data flow diagram is a diagram that illustrates how data flows from sources to destinations through processes, stores, or external entities. An entity-relationship diagram is a diagram that illustrates how entities (such as tables) are related to each other through attributes (such as keys) in a database. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

最新問題**: 269**
経営陣の反応に対して情報システム監査人がまずすべきことは何か
対面式の内部統制アンケートでは、重要な内部統制の
制御はもはや効果的ではないのですか?
A. 制御を実行するために必要なリソースを決定する
効果的。
B. 内部統制の全体的な有効性を検証します。
C. 制御の影響がなくなったことを確認します。
D. 他の補償制御の存在を確認します。

Answer: (解答を表示する**)**
The first thing that an IS auditor should do when management responses to an in-person internal control questionnaire indicate a key internal control is no longer effective is to ascertain the existence of other compensating controls. Compensating controls are alternative controls that provide reasonable assurance of achieving the same objective as the original control. The IS auditor should verify whether there are any compensating controls in place that can mitigate the risk of the key control being ineffective, and evaluate their adequacy and effectiveness. The other options are not the first steps, because they either require more information about the compensating controls, or they are actions to be taken after identifying and assessing the compensating controls. References: CISA Review Manual (Digital Version)1, Chapter 2, Section 2.2.3

最新問題**: 270**
セキュリティ パッチが自動的にダウンロードされ、運用サーバーに適用される場合に発生する最大のリスクは次のどれですか。
A. サポートドキュメントは更新されていません。
B. パッチのインストール中はマルウェア対策が無効になります。
C. パッチは重要度に関係なくインストールできます。
D. パッチにより重大なサービス障害が発生する可能性があります。
Answer: D (メーッセージを残す**)**
The greatest risk associated with security patches being automatically downloaded and applied to production servers is that patches may result in major service failures, as they may introduce new bugs, conflicts, or incompatibilities that could affect the functionality, performance, or availability of the servers12. Automatic patching may also bypass the testing and validation processes that are necessary to ensure the quality and reliability of the patches34.
References
1: Do you leave Windows Automatic Updates enabled on your production IIS server? - Server Fault1 2:
Azure now installs security updates on Windows VMs automatically3 3: Server Patch Management | Process of Server Patching - ManageEngine2 4: Windows Security Updates | Microsoft Patch Updates Guide - ManageEngine4

最新問題**: 271**
IS 監査人は、組織がコスト効率の良い方法でオンデマンドで新しいサーバーを追加できないことを発見しました。次のうち、監査人の最善の推奨事項はどれですか。
A. 既存システムの容量を増加します。
B. ハードウェアを新しいテクノロジーにアップグレードします。
C. IT 機能のために臨時契約労働者を雇用します。
D. 仮想環境を構築します。

Answer: (解答を表示する)
The best recommendation for an organization that is unable to add new servers on demand in a cost-efficient manner is to build a virtual environment. A virtual environment is a technology that allows multiple virtual machines to run on a single physical server, sharing its resources and capabilities. A virtual environment can help the organization add new servers on demand in a cost-efficient manner by reducing the need for hardware acquisition, maintenance, and power consumption. The other options are not as effective as building a virtual environment, as they do not address the root cause of the problem or provide the same benefits.
Increasing the capacity of existing systems is a short-term solution that can help improve the performance and availability of the current servers, but it does not enable the organization to add new servers on demand in a cost-efficient manner. Upgrading hardware to newer technology is a costly solution that can help enhance the functionality and reliability of the servers, but it does not enable the organization to add new servers on demand in a cost-efficient manner. Hiring temporary contract workers for the IT function is an irrelevant solution that can help supplement the IT staff's skills and knowledge, but it does not enable the organization to add new servers on demand in a cost-efficient manner.
References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3.1

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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**
請負業者のデータセンターへのアクセスを管理する最も効果的な方法は何ですか?
A. 訪問者の身元の確認
B. 訪問者のアクセスに対する管理者の承認
C. 訪問者が着用するバッジ識別
D. 訪問者のアクセスには付き添いが必要
Answer: (解答を表示する)

最新問題: **273**
IS 監査人は、社内のシステム開発ライフサイクル (SDLC) プロジェクトがユーザー仕様を満たしていないことを知りました。監査人は、まず次のどのフェーズの要件を調査する必要がありますか?
A. 構成フェーズ

B. ユーザートレーニングフェーズ
C. 品質保証 (QA) フェーズ
D. 開発フェーズ
Answer: C (メーッセージを残す)
The quality assurance (QA) phase is the phase where the IS auditor should first examine requirements from an in-house SDLC project that has not met user specifications. This is because the QA phase is the phase where the system is tested and verified against the user specifications and the design specifications to ensure that it meets the functional and non-functional requirements, as well as the quality standards and expectations. The QA phase involves various testing activities, such as unit testing, integration testing, system testing, acceptance testing, performance testing, security testing, etc., to identify and resolve any defects, errors, or deviations from the specifications12.
The configuration phase is not the phase where the IS auditor should first examine requirements from an in- house SDLC project that has not met user specifications. The configuration phase is the phase where the system is installed and configured on the target environment, such as hardware, software, network, etc., to prepare it for deployment and operation. The configuration phase may involve activities such as installation, customization, migration, integration, etc., to ensure that the system is compatible and interoperable with the existing infrastructure and systems34.
The user training phase is not the phase where the IS auditor should first examine requirements from an in- house SDLC project that has not met user specifications. The user training phase is the phase where the end- users are trained and educated on how to use the system effectively and efficiently. The user training phase may involve activities such as developing training materials, conducting training sessions, providing feedback and support, etc., to ensure that the users are familiar and comfortable with the system features and functions56.
The development phase is not the phase where the IS auditor should first examine requirements from an in- house SDLC project that has not met user specifications. The development phase is the phase where the system is coded and built based on the design specifications and the user specifications. The development phase may involve activities such as programming, debugging, documenting, etc., to create a working prototype or a final product of the system

最新問題**: 274**
IS 監査人は、アプリケーションの監査証跡が次の状態であることを確認する必要があります。
A. 十分なセキュリティを備えています。
B. すべてのデータベース レコードを記録します。
C. オンラインでアクセス可能
D. 運用効率に影響を与えない

Answer: A (メーッセージを残す)
An application's audit trail is a record of all actions or events that occur within or affect an application, such as user activities, system operations, data changes, errors, exceptions, etc. An audit trail can provide evidence and accountability for an application's functionality and performance, and support auditing, monitoring, troubleshooting, and investigation purposes. An IS auditor should ensure that an application's audit trail has adequate security, which means that it is protected from unauthorized access, modification, deletion, or disclosure. Adequate security can help ensure that an audit trail maintains its integrity, reliability, and availability, and prevents tampering or manipulation by attackers or insiders who want to hide their tracks or evidence of their actions. Logs all database records is a possible feature of an application's audit trail, but it is not the most important thing for an IS auditor to ensure, as logging all database records may not be necessary or feasible for some applications, and may generate excessive or irrelevant data that can affect the storage or analysis of the audit trail. Is accessible online is a possible feature of an application's audit trail, but it is not the most important thing for an IS auditor to ensure, as online accessibility may not be required or desirable for some applications, and may introduce security or privacy risks for the audit trail. Does not impact operational efficiency is a desirable outcome of an application's audit trail, but it is not the most important thing for an IS auditor to ensure, as operational efficiency may not be the primary objective or concern of an application's audit trail, and may depend on other factors or trade-offs such as storage capacity, performance speed, or data quality.

最新問題**: 275**
ファイアウォール ログの整合性を最も確実に保証するものは次のどれですか?
A. ログは毎月確認されます。
B. ログを表示するには、承認されたアクセスが必要です。
C. ログを変更できません。
D. ログはポリシーごとに保持されます。
Answer: (解答を表示する)
The best way to provide assurance of the integrity of a firewall log is to ensure that the log cannot be modified. A firewall log is a record of the traffic and events that occur at the firewall, which is a device or software that controls and filters the incoming and outgoing network traffic based on predefined rules and policies. The integrity of a firewall log means that the log is accurate, complete, consistent, and valid, and that it has not been altered, deleted, or corrupted by unauthorized or malicious parties. The IS auditor should verify that the firewall log has adequate controls to prevent or detect any modification of the log, such as encryption, hashing, digital signatures, write-once media, or tamper-evident seals. The other options are not as effective as ensuring that the log cannot be modified, because they either do not address the integrity of the log data, or they are monitoring or retention measures rather than preventive or detective controls. References:
CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.4

最新問題: **276**
フォローアップを計画しているとき、情報システム監査人は、運用管理者から、最近の組織変更によって以前に特定されたリスクに対処したため、アクション プランを実施する必要がなくなったことを知らされます。監査人は次に何をすべきでしょうか。
A. 変更により、リスクが対処されたかどうかを判断することが困難になったことを報告します。
B. 経営陣の主張を受け入れ、リスクに対処したことを報告します。
C. 変更によって対処が必要な新たなリスクが発生したかどうかを判断します。
D. 変更を確認し、リスクが対処されたかどうかを判断します。
Answer: B (メーッセージを残す**)**
When operational management informs the IS auditor that recent organizational changes have addressed previously identified risks and implementing the action plan is no longer necessary, the IS auditor should accept management's assertion and report that the risks have been addressed. However, it is essential to document this communication and ensure that there is evidence supporting management's claim. If there are any doubts or concerns, further investigation may be necessary. The auditor should not assume new risks without proper assessment or evidence1. References:
1(https://www.isaca.org/resources/isaca-journal/issues
/2016/volume-6/enhancing-the-audit-follow-up-process-using-cobit-5)

最新問題: **277**
IS 監査人が組織のサイバーセキュリティ インシデント対応の成熟度のレビューを計画しています。次の方法のうち、最も信頼性の高い結論を提供するものはどれでしょうか。
A. 判断的サンプリング
B. データ分析テスト
C. 可変サンプリング
D. コンプライアンステスト
Answer: (解答を表示する**)**
Compliance testing ensures that the organization's incident response processes align with established cybersecurity frameworks and policies. This methodology provides objective and reliable conclusions about the maturity of incident response capabilities.
* Judgmental Sampling (Option A): Relies on subjective judgment and is less reliable.
* Data Analytics Testing (Option B): Useful for identifying trends but may not assess process maturity comprehensively.
* Variable Sampling (Option C): Appropriate for statistical analysis but less effective in process maturity assessments.
Reference: ISACA CISA Review Manual, Job Practice Area 2: Information Systems Audit and Assurance.

最新問題**: 278**
内部ネットワーク セグメント間のファイアウォールは、次の方法でセキュリティを強化し、リスクを軽減します。
A. ネットワークセグメントを通過するすべてのパケットをジョギングする
B. ネットワークセグメント間を流れるすべてのトラフィックを検査し、セキュリティポリシーを適用する
C. ネットワーク参加者間のセッションの監視とレポート
D. 接続しているすべてのシステムで適切なセキュリティ制御が有効になっていることを確認します。
Answer: B (メーッセージを残す**)**
A firewall between internal network segments improves security and reduces risk by inspecting all traffic flowing between network segments and applying security policies. This will prevent unauthorized or malicious access, data leakage, or network attacks from compromising the network resources or data. Logging all packets passing through network segments may provide audit trails and evidence, but not prevent or mitigate security incidents. Monitoring and reporting on sessions between network participants may help to identify anomalous or suspicious activities, but not block or filter them. Ensuring all connecting systems have appropriate security controls enabled may enhance the overall network security posture, but not isolate or segregate different network segments. References: Info Technology & Systems Resources | COBIT, Risk, Governance ... - ISACA, section "Book COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution | Digital | English"

最新問題**: 279**
次の情報セキュリティ要件のうち、BYOD (個人所有デバイス) 環境で組織データの追跡を可能にするのはどれですか。
A. 従業員は、組織のデータを含むモバイルデバイスの紛失や盗難を直ちに報告する必要があります。
B. 従業員は、組織のモバイルデバイス許容使用ポリシーの承認に署名する必要があります。
C. 従業員は個人のデバイスを組織のモバイルデバイス管理プログラムに登録する必要があります。
Answer: C (メーッセージを残す**)**
The best way to track organizational data in a BYOD environment is to enroll the personal devices in the organization's mobile device management (MDM) program. This will allow the organization to monitor, control, and secure the data on the devices remotely. Employees must also report lost or stolen devices and sign the acceptable use policy, but these are not sufficient to enable tracking of data. References: Info Technology & Systems Resources | COBIT, Risk, Governance ... - ISACA, section "Book IT Control Objectives for Sarbanes-Oxley, 4th Edition | Digital | English"

最新問題: **280**
仮想環境におけるハイパーバイザーに関連する最大のリスクは次のどれですか?
A. 可用性の問題
B. 仮想スプロール
C. 単一障害点
D. パッチ不足
Answer: (解答を表示する**)**
A single point of failure is a component or system that, if it fails, will cause the entire system to stop functioning. In virtual environments, the hypervisor is the software layer that enables multiple virtual machines to run on a single physical host. If the hypervisor is compromised, corrupted, or unavailable, all the virtual machines running on that host will be affected. This can result in data loss, downtime, or security breaches.
References
ISACA CISA Review Manual, 27th Edition, page 254
Virtualization: What are the security risks?
What Is a Hypervisor? (Definition, Types, Risks)

最新問題: **281**
プログラマーが給与システム レポートの主要フィールドに不正な変更を加えました。この問題の原因として最も大きな影響を与えたと考えられるのは次のどの管理上の弱点でしょうか。
A. プログラマーはテストにユーザーを関与させませんでした。
B. ユーザー要件が文書化されていませんでした。
C. 給与ファイルは司書の管理下にありませんでした。
D. プログラマーは製品プログラムにアクセスできます。
Answer: D (メーッセージを残す**)**
The programmer having access to the production programs is the most likely control weakness that would have contributed to the unauthorized changes to the payroll system report. This is because the programmer could modify the production code without proper authorization, documentation, or testing, and bypass the change management process. This could result in errors, fraud, or data integrity issues in the payroll system.
The programmer should only have access to the development or test environment, and the production programs should be under the control of a librarian or a change manager.
References
ISACA CISA Review Manual, 27th Edition, page 254
4 Types of Internal Control Weaknesses
ACCT 4631 - Internal Auditing: CIA Quiz Topic 6 Flashcards

最新問題: **282**

品質管理システム (QMS) が有効であることを IT 管理者に最も強く保証できるのは次のどれですか。
A. ITの品質に満足している利害関係者の割合が高い
B. 高い割合でインシデントが迅速に解決される
C. 品質保証(QA)によってレビューされたITプロセスの割合が高い
D. 質の高いトレーニングに参加するIT従業員の割合が高い
Answer: (解答を表示する**)**
Stakeholder satisfaction is a key indicator of the effectiveness of a QMS, as it reflects the extent to which the QMS meets the expectations and priorities of the customers and other interested parties. A high percentage of stakeholder satisfaction implies that the QMS is delivering consistent and reliable products or services that meet the quality standards and requirements.
References
ISACA CISA Review Manual, 27th Edition, page 253
The Four Main Components of A Quality Management System
The Road to Developing an Effective Quality Management System (QMS)

最新問題**: 283**
組織の情報分類プロセスにおける IS 監査人の主な役割は次のどれですか?
A. 割り当てられた分類に従って情報資産を保護する
B. 割り当てられた分類に従って資産が保護されていることを検証する
C. 分類レベルが規制ガイドラインに準拠していることを確認する
D. 組織内の情報資産の分類レベルの定義
Answer: B (メーッセージを残す**)**
Validating that assets are protected according to assigned classification is the primary role of the IS auditor in an organization's information classification process. An IS auditor should evaluate whether the information security controls are adequate and effective in safeguarding the information assets based on their classification levels. The other options are not the primary role of the IS auditor, but rather the responsibilities of the information owners, custodians, or security managers. References:
* CISA Review Manual (Digital Version), Chapter 6, Section 6.2.31
* CISA Review Questions, Answers & Explanations Database, Question ID 206

最新問題**: 284**
定期的な年次監査の過去の結果を確認する際、情報システム監査人は、発見事項が報告されておらず、独立性が維持されていない可能性があることに気付きます。次のうちどれが監査人の最善の行動方針でしょうか?
A. 上級管理職に通知します。
B. 内部統制を再評価します。
C. 監査管理に通知します。

D. 独立性を保証するために過去の監査を再実行します。
Answer: C (メーッセージを残す**)**
If an IS auditor suspects that independence may not have been maintained in past audits, the best course of action is to inform audit management. Audit management has the responsibility and authority to address such issues. They can review the situation, determine if there was indeed a lack of independence, and decide on the appropriate actions to take123. While informing senior management, reevaluating internal controls, and re- performing past audits might be necessary at some point, the first step should be to inform audit management.

最新問題**: 285**
ソフトウェア開発のウォーターフォール ライフサイクル モデルは、次のどの状況に最も適していますか?
A. 保護要件は理解されています。
B. プロジェクトには時間的なプレッシャーが伴います。
C. このプロジェクトでは、オブジェクト指向設計アプローチを適用する予定です。
D. このプロジェクトでは新しいテクノロジーが使用されます。
Answer: (解答を表示する**)**
The waterfall life cycle model of software development is best suited for situations where the project requirements are well understood. The waterfall life cycle model is a sequential and linear approach to software development that consists of several phases, such as planning, analysis, design, implementation, testing, and maintenance. Each phase depends on the completion and approval of the previous phase before proceeding to the next phase. The waterfall life cycle model is best suited for situations where the project requirements are well understood, as it assumes that the requirements are clear, stable, and fixed at the beginning of the project, and do not change significantly throughout the project. The project is subject to time pressures is not a situation where the waterfall life cycle model of software development is best suited, as it may not be flexible or agile enough to accommodate changes or adjustments in the project schedule or timeline. The waterfall life cycle model may involve long delays or dependencies between phases, and may not allow for early feedback or delivery of software products. The project intends to apply an object-oriented design approach is not a situation where the waterfall life cycle model of software development is best suited, as it may not be compatible or effective with the object-oriented design approach. The object-oriented design approach is a technique that models software as a collection of interacting objects that have attributes and behaviors. The object-oriented design approach may require iterative and incremental development methods that allow for dynamic and adaptive changes in software design and functionality. The project will involve the use of new technology is not a situation where the waterfall life cycle model of software development is best suited, as it may not be able to cope with the uncertainty or complexity of new technology. The waterfall life cycle model

may not allow for sufficient exploration or experimentation with new technology, and may not be able to handle changes or issues that arise from new technology.

最新問題**: 286**
クラウドベースのメッセージングおよびコラボレーション プラットフォームの取得の計画段階で決定することが最も重要なのは次のどれですか?
A. ロールベースのアクセス制御ポリシー
B. プラットフォームにアップロードできるデータの種類
C. プラットフォームへのユーザーのオンボーディングとオフボーディングのプロセス
D. 管理者のアクティビティを確認するプロセス
Answer: B (メーッセージを残す**)**
The most important thing to determine during the planning phase of a cloud-based messaging and collaboration platform acquisition is the types of data that can be uploaded to the platform. This is because different types of data may have different security, privacy, and compliance requirements, depending on the nature, sensitivity, and value of the data. For example, personal data, financial data, health data, or intellectual property data may be subject to various laws and regulations that govern how they can be collected, stored, processed, and shared in the cloud. Therefore, it is essential to identify and classify the types of data that will be uploaded to the platform, and ensure that the platform meets the organization's policies and standards for data protection1.
The other options are not as important as the types of data that can be uploaded to the platform during the planning phase of a cloud-based messaging and collaboration platform acquisition. Option A, role-based access control policies, is a mechanism that defines who can access what data and resources on the platform based on their roles and responsibilities. Role-based access control policies are important for ensuring data security and accountability, but they can be designed and implemented after the platform is acquired2. Option C, processes for on-boarding and off-boarding users to the platform, are procedures that enable or disable user accounts and access rights on the platform. Processes for on-boarding and off-boarding users are important for managing user identities and lifecycles, but they can be developed and executed after the platform is acquired3. Option D, processes for reviewing administrator activity, are methods that monitor and audit the actions and events performed by administrators on the platform. Processes for reviewing administrator activity are important for detecting and preventing unauthorized or malicious activities, but they can be established and performed after the platform is acquired4.
References:
* Cloud Messaging and Collaboration Services - Maryland.gov DoIT4
* MessageBird acquires real-time notifications and in-app messaging platform Pusher for $35M | TechCrunch2
* Symphony to lead financial market communications with the acquisition of Cloud9 Technologies3

* Cloud messaging and collaboration | Sumo Logic

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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**
システム変換中のダウンタイムを最も効果的に最小限に抑えるのはどれですか?
A. 段階的アプローチ
B. 直接切り替え
C. パイロットスタディ
D. 並列実行
Answer: D (メーッセージを残す**)**
The most effective way to minimize downtime during system conversions is to use a parallel run. A parallel run is a method of system conversion where both the old and new systems operate simultaneously for a period of time until the new system is verified to be functioning correctly. This reduces the risk of errors, data loss, or system failure during conversion and allows for a smooth transition from one system to another.
References: CISA Review Manual, 27th Edition, page 467

最新問題: **288**
サイバーレジリエンスの主な目的は次のどれですか?
A. セキュリティ侵害の重大性を制限し、継続的な運用を維持する
B. サービス中断後に通常の運用を再開する
C. 運用への影響を最小限に抑えながら、インシデントから効率的かつ効果的に回復する
D. 潜在的な攻撃や業務の中断を防ぐため
Answer: A (メーッセージを残す**)**

最新問題: **289**
データ センター改修プロジェクトに関与する IS 監査人の最も適切な責任は次のどれですか。
A. プロジェクトに関与する責任者の独立したレビューの実施
B. 改修工事を行う業者の選定
C. プロジェクトが予定通りに進行し、マイルストーンが達成されることを確認する
D. データセンターの運用管理の実装

Answer: A (メーッセージを残す)
IS auditors primarily provide assurance and oversight. In this context, independent reviews ensure that those responsible for the renovation project are meeting their obligations, following best practices, and managing risks appropriately.
References:
ISACA's Code of Professional Ethics: Emphasizes the IS Auditor's duty to be independent and objective.
The Role of IS Audit: IS Auditors are not project managers but provide objective assessment and guidance regarding controls and risk mitigation within projects.
CISA Review Manual (27th Edition): May have sections discussing the role of IS auditors in infrastructure projects or similar initiatives.

最新問題**: 290**
クロスサイト スクリプティング (XSS) 攻撃は、次の方法で最も効果的に防止できます。
A. アプリケーション ファイアウォール ポリシー設定。
B. 3 層 Web アーキテクチャ。
C. 安全なコーディングプラクティス。
D. 業界共通のフレームワークの使用。
Answer: C (メーッセージを残す)
Secure coding practices are the best way to prevent cross-site scripting (XSS) attacks, because they can ensure that the web application validates and sanitizes user input and output data to prevent malicious scripts from being executed on the web browser. XSS attacks are a type of web application vulnerability that exploit the lack of input validation or output encoding in web pages that accept user input or display dynamic content. Application firewall policy settings, a three-tier web architecture, and use of common industry frameworks are not effective controls to prevent XSS attacks, because they do not address the root cause of the vulnerability in the web application code. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.4.2

最新問題**: 291**
火災警報システムがコンピュータ室に設置されています。火災警報制御パネルの最も効果的な場所は、
A. 無停電電源装置 (UPS) モジュールに最も近いコンピュータ ルーム
B. サーバーコンピュータに最も近いコンピュータルーム
C. システム管理者のオフィス
D. 建物の警備員が使用するブース
Answer: D (メーッセージを残す)
A fire alarm system is a device that detects and alerts people of the presence of fire or smoke in a building. A fire alarm control panel is the central unit that monitors and controls

the fire alarm system. The most effective location for the fire alarm control panel would be inside the booth used by the building security personnel.
This is because:
* The security personnel can quickly and easily access the fire alarm control panel in case of an emergency, and take appropriate actions such as notifying the fire department, evacuating the building, or resetting the system.
* The fire alarm control panel can be protected from unauthorized access, tampering, or damage by the security personnel, who can also monitor its status and performance regularly.
* The fire alarm control panel can be isolated from the computer room, which may be exposed to higher risks of fire or smoke due to the presence of electrical equipment, such as uninterruptible power supply (UPS) modules or server computers.
* The fire alarm control panel can be connected to the computer room through a dedicated communication line, which can ensure reliable and timely transmission of signals and information between the two locations.
References:
* [1]: Fire Alarm Control Panel - an overview | ScienceDirect Topics
* [2]: Fire Alarm Control Panel - What is it and how does it work? | Fire Protection Online
* [3]: Fire Alarm Control Panel Installation Guide - XLS3000 - Honeywell

最新問題**: 292**
組織のソフトウェア取得プロセスを監査する場合、情報システム監査人が組織にとってのソフトウェアのメリットを理解するための最良の方法は、
A. 実現可能性調査
B. ビジネスケース
C. 提案依頼書 (RFP)
D. IT戦略との整合
Answer: B (メーッセージを残す**)**
The best way for an IS auditor to understand the software benefits to the organization would be to review the business case, which is a document that provides the justification and rationale for acquiring a software solution based on its expected costs, benefits, risks, and alignment with the organization's goals and strategies. The business case helps to evaluate the feasibility and viability of the software acquisition and to support the decision-making process. A feasibility study is a document that analyzes the technical, operational, economic, legal, and social aspects of a software solution to determine its feasibility and suitability for the organization's needs, but it does not necessarily provide a clear indication of the software benefits to the organization. A request for proposal (RFP) is a document that solicits proposals from potential vendors or suppliers for a software solution based on the organization's requirements and specifications, but it does not necessarily provide a clear indication of the software benefits to the organization. The alignment with IT strategy is a factor that influences the software acquisition process and ensures that the software

solution supports and enables the organization's IT strategy, but it is not a document that can be reviewed by an IS auditor to understand the software benefits to the organization.
References: CISA Review Manual (Digital Version), Chapter 3: Information Systems Acquisition, Development & Implementation, Section 3.1:
Business Case Development

最新問題**: 293**
組織の情報セキュリティポリシーの妥当性を評価する際に、情報システム監査人が考慮すべき最も重要な事項は次のどれですか?
A. IT戦略計画との整合
B. IT 運営委員会の議事録
C. 業界のベストプラクティスに準拠
D. ビジネス目標
Answer: D (メーッセージを残す**)**
The most important consideration for an IS auditor when assessing the adequacy of an organization's information security policy is its alignment with the business objectives. The information security policy is a high-level document that defines the organization's vision, goals, principles, and responsibilities for protecting its information assets. The information security policy should support and enable the achievement of the business objectives, such as increasing customer satisfaction, enhancing competitive advantage, or complying with legal requirements. The information security policy should also be consistent with other relevant policies, standards, and frameworks that guide the organization's governance, risk management, and compliance activities.

最新問題**: 294**
情報資産が輸送中および廃棄中に適切に安全に保護されているかどうかを判断する際に、最も考慮すべき事項は次のどれですか。
A. 適切なラベル付けが不足している
B. 最近の意識啓発トレーニングが不足しています。
C. パスワード保護の欠如
D. 適切なデータ分類の欠如
Answer: D (メーッセージを残す**)**
The most concerning issue when determining if information assets are adequately safeguarded during transport and disposal is lack of appropriate data classification. Data classification is a process that assigns categories or levels of sensitivity to different types of information assets based on their value, criticality, or risk to the organization. Data classification can help safeguard information assets during transport and disposal by providing criteria and guidelines for identifying, labeling, handling, and protecting information assets according to their sensitivity. Lack of appropriate data classification can compromise the security and confidentiality of information assets during transport and

disposal by exposing them to unauthorized access, disclosure, theft, damage, or destruction. The other options are not as concerning as lack of appropriate data classification in safeguarding information assets during transport and disposal, as they do not affect the identification, labeling, handling, or protection of information assets according to their sensitivity. Lack of appropriate labeling is a possible factor that may increase the risk of misplacing, losing, or mishandling information assets during transport and disposal, but it does not affect the classification of information assets according to their sensitivity. Lack of recent awareness training is a possible factor that may affect the knowledge or behavior of staff involved in transporting or disposing of information assets, but it does not affect the classification of information assets according to their sensitivity. Lack of password protection is a possible factor that may affect the security or confidentiality of information assets stored on devices during transport and disposal, but it does not affect the classification of information assets according to their sensitivity. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.3.2

最新問題**: 295**
新しい生産システムの導入に伴うリスクを最も効果的に軽減できるのは次のどれですか?
A. リリース管理
B. 問題管理
C. 構成管理
D. インシデント管理
Answer: B (メーッセージを残す**)**

最新問題**: 296**
データベース管理システム (DBMS) のレコード ロック オプションは次の目的で使用されます。
A. レコードの同時更新のリスクを排除する
B. データベース管理者 (DBA) がユーザーのアクティビティを記録できるようにします。
C. ユーザーがレコード内の特定の値を変更することを制限します。
D. ユーザーが他のユーザーを自分のファイルから締め出すことを可能にします。
Answer: A (メーッセージを残す**)**
The record-locking option of a database management system (DBMS) serves to eliminate the risk of concurrent updates to a record by different users or transactions. Record locking is a technique of preventing simultaneous access to data in a database, to prevent inconsistent results1. For example, if two bank clerks try to update the same bank account for two different transactions, record locking can ensure that only one clerk can modify the record at a time, while the other has to wait until the lock is released. This way, the record will reflect both transactions correctly and avoid data corruption.
Record locking does not serve to allow database administrators (DBAs) to record the activities of users. This is a function of auditing or logging, which can track the actions

performed by users on the database2. Record locking does not affect the ability of DBAs to monitor or audit user activities.
Record locking does not serve to restrict users from changing certain values within records. This is a function of access control or authorization, which can enforce rules or policies on what data users can view or modify2. Record locking does not affect the permissions or privileges of users on the database.
Record locking does not serve to allow users to lock others out of their files. This is a function of encryption or password protection, which can secure files from unauthorized access or modification3. Record locking does not affect the security or confidentiality of files on the database.
References:
Record locking - Wikipedia1
Database security - Wikipedia2
File system permissions - Wikipedia3

最新問題**: 297**
コンピュータ システムに障害が発生する直前の状態にトランザクションと記録を復元するための適切なカットオフが確立されていることを最も確実に保証できるのは次のうちどれですか。
A. トランザクションファイルのバックアップコピーをオフサイトでローテーションする
B. データベース管理システム (DBMS) を使用して、部分的に処理されたトランザクションを動的にバックアウトする
C. システムコンソールログを電子形式で維持する
D. すべての伝送ラインでバイシンクロナス機能を確保する
Answer: B (メーッセージを残す**)**
The best way to ensure that a proper cutoff has been established to reinstate transactions and records to their condition just prior to a computer system failure is to use a database management system (DBMS) to dynamically back-out partially processed transactions. A DBMS is a software system that manages the creation, manipulation, retrieval, and security of data stored in a database. A DBMS can provide features such as transaction management, concurrency control, recovery management, and integrity management. A DBMS can dynamically back-out partially processed transactions by using mechanisms such as rollback segments, undo logs, or write-ahead logs. These mechanisms allow the DBMS to restore the database to a consistent state before the failure occurred.
References:
* CISA Review Manual (Digital Version)
* CISA Questions, Answers & Explanations Database

最新問題**: 298**
組織の目標を達成するために IT を最大限に活用する IT 戦略計画には、次の内容が含まれます。

A. 将来のニーズと現在の機能の比較。
B. リスクに基づいたプロジェクトのランキング。
C. エンタープライズ アーキテクチャ (EA) の影響。
D. 組織の予算にリンクされた IT 予算。
Answer: (解答を表示する**)**
An IT strategic plan that best leverages IT in achieving organizational goals will include enterprise architecture (EA) impacts. EA is the practice of analyzing, designing, planning, and implementing enterprise analysis to successfully execute on business strategies1. EA helps organizations structure IT projects and policies to align with business goals, to stay agile and resilient in the face of rapid change, and to stay on top of industry trends and disruptions1. EA also describes an organization's processes, information processes and personnel and other organizational subunits aligned with the organization's core goals and strategies2. By including EA impacts in the IT strategic plan, an organization can ensure that the IT initiatives are consistent with the business vision, objectives, and tactics, and that they support the desired business outcomes3.
A comparison of future needs against current capabilities, a risk-based ranking of projects, and IT budgets linked to the organization's budget are all important elements of an IT strategic plan, but they do not necessarily leverage IT in achieving organizational goals. A comparison of future needs against current capabilities can help identify gaps and opportunities for improvement, but it does not provide a clear direction or roadmap for how to achieve them. A risk-based ranking of projects can help prioritize the most critical and beneficial projects, but it does not ensure that they are aligned with the business strategy or that they deliver value to the stakeholders. IT budgets linked to the organization's budget can help allocate resources and monitor costs, but they do not reflect the impact or contribution of IT to the business performance or growth.
References:
Implement Agile IT Strategic Planning with Enterprise Architecture - The Open Group Blog
What is enterprise architecture? A framework for transformation | CIO Strategic Planning and Enterprise Architecture

最新問題**: 299**
データ カンターのスロート評価をレビューする IS 監査人は、次のような場合に最も懸念します。
A. 特定された脅威の一部は発生する可能性が低いです。
B. 特定されたすべての脅威は外部エンティティに関連しています。
C. 演習は現地管理者によって完了しました。
D. 近隣組織の業務も対象になりました。
Answer: B (メーッセージを残す**)**
An IS auditor reviewing the threat assessment for a data center would be most concerned if all identified threats relate to external entities. This indicates that the threat assessment

is incomplete and biased, as it ignores the potential threats from internal sources, such as employees, contractors, vendors, or authorized visitors. Internal threats can pose significant risks to the data center, as they may have access to sensitive information, systems, or facilities, and may exploit their privileges for malicious or fraudulent purposes. According to a study by IBM, 60% of cyberattacks in 2015 were carried out by insiders1
Some of the identified threats are unlikely to occur is not a cause for concern, as it shows that the threat assessment is comprehensive and realistic, and considers all possible scenarios, regardless of their probability. A threat assessment should not exclude any potential threats based on subjective judgments or assumptions, as they may still have a high impact if they materialize.
The exercise was completed by local management is not a cause for concern, as it shows that the threat assessment is conducted by the people who are most familiar with the data center's operations, environment, and risks. Local management may have more relevant and accurate information and insights than external parties, and may be more invested in the outcome of the threat assessment.
Neighboring organizations' operations have been included is not a cause for concern, as it shows that the threat assessment is holistic and contextual, and considers the interdependencies and influences of external factors on the data center's security. Neighboring organizations' operations may pose direct or indirect threats to the data center, such as physical damage, network interference, or shared vulnerabilities.
References:
* IBM Security Services 2016 Cyber Security Intelligence Index 1

最新問題**: 300**
施設の入り口に生体認証アクセス装置を設置する場合、どのような管理が行われますか?
A. 予防的
B. 抑止力
C. 修正
D. 探偵
Answer: (解答を表示する**)**
A biometric access device installed at the entrance to a facility is a type of preventive control. Preventive controls are designed to deter or prevent undesirable events from occurring12. They are proactive measures that aim to inhibit incidents before they happen12. In this case, the biometric access device prevents unauthorized individuals from gaining access to the facility by requiring unique biological characteristics for authentication12.
References:
Guide to Biometric Access Control & Door Lock Security - Avigilon
Biometric access control: meaning, types and implementation - Smowl

最新問題**: 301**

自動化されたソーシャル メディア アカウントの大規模なグループを利用して、データを盗んだり、スパムを送信したり、分散型サービス拒否 (DDoS) 攻撃を開始したりする脅威の種類はどれですか?
A. フィッシングの試み
B. マルウェアの共有
C. ボットネット攻撃
D. データマイニング
Answer: C (メーッセージを残す**)**

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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**: 302**
組織の IT 戦略がビジネス目標と一致していることを示す最良の証拠は次のどれですか?
A. 組織の変更に応じて IT 戦略が変更されます。
B. IT 戦略は経営幹部によって承認されます。
C. IT 戦略は、IT 運用のベスト プラクティスに基づいています。
D. IT戦略はビジネス戦略に大きな影響を与える
Answer: (解答を表示する**)**
The best evidence that an organization's IT strategy is aligned to its business objectives is that the IT strategy is approved by executive management. This implies that the IT strategy has been reviewed and validated by the senior leaders of the organization, who are responsible for setting and overseeing the business objectives. The IT strategy may be modified in response to organizational change, based on IT operational best practices, or have significant impact on the business strategy, but these are not sufficient indicators of alignment without executive approval. References: CISA Review Manual (Digital Version)1, Chapter 1, Section 1.2.1

最新問題**: 303**
IT ベンダーのサービス レベルを監視するための最適な基準は次のどれでしょうか?
A. サービス監査人のレポート
B. パフォーマンス メトリック
C. ベンダーへのサプライズ訪問
D. ベンダーへのインタビュー

Answer: (解答を表示する**)**
The best criteria for monitoring an IT vendor's service levels are the performance metrics, as they provide quantifiable and measurable indicators of how well the vendor is delivering the agreed-upon services, such as availability, reliability, quality, timeliness, and customer satisfaction. A service auditor's report is a document that provides an independent opinion on the vendor's controls and processes, but it may not reflect the actual service levels or performance. A surprise visit to the vendor may help to verify the vendor's compliance and operations, but it may not be feasible or effective for monitoring the service levels on a regular basis. An interview with the vendor may help to obtain feedback and insights from the vendor's perspective, but it may not be objective or reliable for monitoring the service levels. References: CISA Review Manual (Digital Version), Chapter 2: Governance and Management of IT, Section 2.4: IT Service Delivery and Support

最新問題**: 304**
銀行員による電信送金詐欺を防ぐための最良の方法はどれですか?
A. 独立した和解
B. 送金金額の再入力
C. 2要素認証制御
D. システム強制デュアルコントロール
Answer: (解答を表示する**)**
The best method to prevent wire transfer fraud by bank employees is system-enforced dual control. System- enforced dual control is a segregation of duties control that requires two or more individuals to perform or authorize a transaction or activity using a system that enforces this requirement. System-enforced dual control can prevent wire transfer fraud by requiring independent verification and approval of payment requests, amounts, and recipients by different bank employees using a system that does not allow any single employee to complete the transaction alone. The other options are not as effective as system-enforced dual control in preventing wire transfer fraud, as they do not involve independent checks or approvals using a system.
Independent reconciliation is a detective control that can help compare and confirm payment records with bank statements, but it does not prevent wire transfer fraud from occurring. Re-keying of wire dollar amounts is an input control that can help detect any errors or discrepancies in payment amounts, but it does not prevent wire transfer fraud from occurring. Two-factor authentication control is an access control that can help verify the identity and authorization of bank employees, but it does not prevent wire transfer fraud from occurring.
References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

最新問題**: 305**
IS 監査人が、外部データ プロバイダーから市場価格データをインポートするプロセスをレビューしています。監査人が最も重要と見なすべき次の調査結果はどれですか。

A. データの品質は監視されていません。
B. インポートされたデータは頻繁に破棄されません。
C. 転送プロトコルは暗号化されていません。
D. 転送プロトコルでは認証は必要ありません。
Answer: A (メーッセージを残す)
The most critical finding that the IS auditor should consider when reviewing processes for importing market price data from external data providers is that the quality of the data is not monitored. This is because market price data is essential for financial transactions, risk management, valuation and reporting, and any errors or inaccuracies in the data can have significant impact on the organization's performance, reputation and compliance. The IS auditor should ensure that the organization has established quality criteria and controls for the imported data, such as validity, completeness, timeliness, consistency and accuracy, and that the data is regularly checked and verified against these criteria. The other findings are also important, but not as critical as data quality. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.7

最新問題**: 306**
社内でシステムを開発する場合と比較して、ソフトウェア パッケージを取得すると、エンド ユーザーによるテストの必要性が高まります。
A. 排除
B. 変更なし
C. 増加
D. 減少
Answer: B (メーッセージを残す)
Compared to developing a system in-house, acquiring a software package means that the need for testing by end users is unchanged. This is because end users are still the ultimate customers and beneficiaries of the system, and they need to ensure that the software package meets their requirements, expectations, and satisfaction. End user testing, also known as user acceptance testing (UAT) or beta testing, is the final stage of testing performed by the user or client to determine whether the software can be accepted or not1. End user testing is important for both in-house developed and acquired software packages, as it helps to verify the functionality, usability, performance, and reliability of the system2. End user testing also helps to identify and resolve any defects, errors, or issues that may not have been detected by the developers or vendors3.
Therefore, option B is the correct answer.
Option A is not correct because end user testing is not eliminated by acquiring a software package. Even though the software package may have been tested by the vendor or supplier, it may still have bugs, compatibility issues, or configuration problems that need to be fixed before deployment4. Option C is not correct because end user testing is not increased by acquiring a software package. The scope and extent of end user testing

depend on various factors, such as the complexity, criticality, and customization of the system, and not on whether it is developed in-house or acquired. Option D is not correct because end user testing is not reduced by acquiring a software package. The software package may still require modifications or integrations to suit the specific needs and environment of the organization, and these changes need to be tested by the end users.
References:
Chapter 4 Methods of Software Acquisition5
What is User Acceptance Testing (UAT): A Complete Guide1
What Is End-to-End Testing? (With How-To and Example)3
How to Evaluate New Software in 5 Steps4
User Acceptance Testing (UAT) in ERP Projects
User Acceptance Testing for Packaged Software

最新問題**: 307**
過去に同様の内部監査で例外が報告されていないにもかかわらず、外部監査ではユーザー終了プロセスで繰り返し発生する例外が特定されました。今後内部監査プロセスを改善するための情報システム監査人の最善の行動方針は次のどれですか。
A. 制御自己評価 (CSA) の結果を確認します。
B. ユーザーの終了プロセスの変更を確認します。
C. 内部監査のサンプリング方法を確認します。
D. 今後のすべての監査にユーザー終了プロセスを含めます。
Answer: C (メーッセージを残す**)**

最新問題**: 308**
データ損失防止 (DLP) ツールを実装するための最も重要な前提条件は次のどれですか?
A. ユーザーに、会社全体の共有ドライブではなく、セキュリティで保護されたフォルダにファイルを保存するよう要求する
B. データ転送ログを確認してデータフローの履歴パターンを判断する
C. DLP ポリシーを開発し、ユーザーによる署名付き確認を要求する
D. 既存のデータがどこに存在するかを特定し、データ分類マトリックスを確立する
Answer: (解答を表示する**)**
A data loss prevention (DLP) tool is a software application that detects and prevents data breaches by monitoring and protecting sensitive data from unauthorized access, transfer, or use1. A DLP tool can help your organization comply with regulations, prevent insider threats, and protect your intellectual property.
Before implementing a DLP tool, the most important prerequisite is to identify where existing data resides and establish a data classification matrix. This is because you need to know what data you have, where it is stored, how sensitive it is, and who can access it. A data classification matrix is a framework that defines the categories and levels of data sensitivity, such as public, internal, confidential, or restricted2. By identifying and

classifying your data, you can determine the appropriate DLP policies and controls to apply to each type of data and prevent data loss or leakage.

最新問題**: 309**
次のどれが物理アクセスの予防管理の例ですか?
A. 建物へのすべての訪問者のログエントリを保存する
B. 建物に指紋ベースのアクセス制御システムを実装する
C. すべての出入り口に閉回路テレビ（CCTV）カメラを設置する
D. ワークステーションにログインするスタッフのインスタンスを記録するための集中ログサーバーを実装する
Answer: B (メーッセージを残す**)**
A preventive control is a control that aims to deter or prevent undesirable events from occurring. A fingerprint-based access control system for the building is an example of a preventive control for physical access, as it restricts unauthorized persons from entering the premises. Keeping log entries for all visitors to the building, installing CCTV cameras for all ingress and egress points, and implementing a centralized logging server to record instances of staff logging into workstations are examples of detective controls, which are controls that aim to discover or detect undesirable events that have already occurred.
References: IS Audit and Assurance Tools and Techniques, CISA Certification | Certified Information Systems Auditor | ISACA

最新問題**: 310**
組織では、従業員が個人のモバイル デバイスに機密データを保持することを許可しています。紛失または盗難にあったデバイスからのデータ漏洩のリスクを軽減するための最適な推奨事項は次のうちどれですか。
A. 従業員にセキュリティ意識向上トレーニングへの参加を義務付けます。
B. 重要なデータ ファイルをパスワードで保護します。
C. アクセス試行が複数回失敗した後に自動ワイプするように設定します。
D. デバイスの自動ロック機能を有効にします。
Answer: (解答を表示する**)**
The best recommendation to mitigate the risk of data leakage from lost or stolen devices that contain confidential data is to configure them to auto-wipe after multiple failed access attempts, as this would prevent unauthorized access and erase sensitive information from the device. Requiring employees to attend security awareness training, password protecting critical data files, or enabling device auto-lock function are also good practices, but they may not be sufficient or effective in preventing data leakage from lost or stolen devices.
References: CISA Review Manual (Digital Version), Chapter 5, Section 5.3

最新問題**: 311**

組織がデータ損失を予測するための最も効果的な方法はどれですか?
A. 従業員のインターネット アクセスを制限します。
B. データ分類手順を実装します。
C. ファイアウォールのログに異常がないか確認します。
D. 定期的にセキュリティ意識向上トレーニングを実施します。
Answer: D (メーッセージを残す)
Data loss can occur due to various reasons, such as accidental deletion, hardware failure, malware infection, theft, or unauthorized access. Data classification procedures can help to identify and protect sensitive data, but they are not sufficient to prevent data loss. The most effective way to protect against data loss is to conduct periodic security awareness training for employees, which can educate them on the importance of data security, the best practices for data handling and storage, and the common threats and risks to data.

最新問題**: 312**
IT バランスト スコアカードは、以下の監視に最も効果的な手段です。
A. エンタープライズ IT のガバナンス。
B. 制御の有効性。
C. 投資収益率 (ROI)。
D. 変更管理の有効性。
Answer: (解答を表示する)
An IT balanced scorecard is a strategic management tool that aligns IT objectives with business goals and measures the performance of IT processes using key performance indicators (KPIs). It is the most effective means of monitoring governance of enterprise IT, which is the process of ensuring that IT supports the organization's strategy and objectives. Governance of enterprise IT covers aspects such as IT value delivery, IT risk management, IT resource management, and IT performance measurement. An IT balanced scorecard can help monitor these aspects and provide feedback to improve IT governance. References: ISACA Frameworks: Blueprints for Success, CISA Review Manual (Digital Version)

最新問題**: 313**
IS 監査人が IT 施設のアウトソーシング契約をレビューしています。欠落している場合、監査人が最も懸念すべき事項は次のどれですか。
A. ハードウェア構成
B. アクセス制御の要件
C. ヘルプデスクの可用性
D. 境界ネットワーク セキュリティ図
Answer: B (メーッセージを残す)
The missing access control requirements should present the greatest concern to the IS auditor when reviewing a contract for the outsourcing of IT facilities. Access control

requirements are essential for ensuring the confidentiality, integrity, and availability of the outsourced IT resources and data. They specify the roles, responsibilities, and permissions of the outsourcing vendor and its staff, as well as the client and its users, in accessing and managing the IT facilities. They also define the security policies, standards, and procedures that the outsourcing vendor must follow to protect the IT facilities from unauthorized or malicious access, use, modification, or disclosure. Without clear and comprehensive access control requirements, the outsourcing contract may expose the client to significant risks of data breaches, compliance violations, service disruptions, or reputational damage.
Hardware configurations, help desk availability, and perimeter network security diagram are important aspects of an outsourcing contract, but they are not as critical as access control requirements. Hardware configurations describe the technical specifications and performance of the IT equipment that the outsourcing vendor will provide and maintain. Help desk availability defines the service levels and support channels that the outsourcing vendor will offer to the client and its users. Perimeter network security diagram illustrates the network architecture and security measures that the outsourcing vendor will implement to protect the IT facilities from external threats. These aspects can be verified or modified during the implementation or operation phases of the outsourcing contract, but access control requirements need to be established and agreed upon before signing the contract.
References:
ISACA, CISA Review Manual, 27th Edition, Chapter 5: Protection of Information Assets, Section 5.3:
Logical Access1
CIO.com, 7 tips for managing an IT outsourcing contract2
Brainhub.eu, 8 Tips for Managing an IT Outsourcing Contract

最新問題**: 314**
データ損失防止 (DLP) 監査の計画段階で、経営陣はモバイル コンピューティングに関する懸念を表明しています。IS 監査人が関連するリスクとして特定する必要があるのは次のうちどれですか。
A. クラウドの使用はITの可用性に悪影響を及ぼします
B. ユーザー意識向上トレーニングの必要性が増加
C. いつでもどこでもアクセスできることによる脆弱性の増加
D. IT インフラストラクチャとアプリケーションに対するガバナンスと監視の欠如
Answer: C (メーッセージを残す**)**
The associated risk of mobile computing that an IS auditor should identify during the planning phase of a data loss prevention (DLP) audit is increased vulnerability due to anytime, anywhere accessibility. Mobile computing refers to the use of portable devices, such as laptops, tablets, smartphones, or wearable devices, that can access data and applications over wireless networks from any location6. Mobile computing enables greater flexibility, productivity, and convenience for users, but also poses significant security

challenges for organizations. One of these challenges is increased vulnerability due to anytime, anywhere accessibility. This means that mobile devices are exposed to a higher risk of loss, theft, damage, or unauthorized access than stationary devices7. If mobile devices contain or access sensitive data without proper protection, such as encryption or authentication, they could result in data leakage or breach in case of compromise8. Therefore, an IS auditor should identify this risk as part of a DLP audit. The other options are less relevant or incorrect because:
* A. The use of cloud negatively impacting IT availability is not an associated risk of mobile computing that an IS auditor should identify during the planning phase of a DLP audit, as it is more related to cloud computing than mobile computing. Cloud computing refers to the delivery of computing services, such as data storage or processing, over the Internet from remote servers. Cloud computing may enable or support mobile computing by providing access to data and applications from any device or location, but it does not necessarily imply mobile computing. The use of cloud may negatively impact IT availability if there are disruptions or outages in the cloud service provider's network or infrastructure, but this is not a direct consequence of mobile computing.
* B. Increased need for user awareness training is not an associated risk of mobile computing that an IS auditor should identify during the planning phase of a DLP audit, as it is more of a control or mitigation measure than a risk. User awareness training refers to educating users about security policies, procedures, and best practices for using mobile devices and protecting data. User awareness training may help to reduce the risk of data loss or breach due to mobile computing by increasing user knowledge and responsibility, but it does not eliminate or prevent the risk.
* D. Lack of governance and oversight for IT infrastructure and applications is not an associated risk of mobile computing that an IS auditor should identify during the planning phase of a DLP audit, as it is more of a general or organizational risk than a specific or technical risk. Governance and oversight refer to the establishment and implementation of policies, standards, and procedures for managing IT resources and aligning them with business objectives. Lack of governance and oversight for IT infrastructure and applications may affect the security and performance of mobile devices and data, but it is not a direct or inherent result of mobile computing. References: Mobile Computing - ISACA, Mobile Computing Device Threats, Vulnerabilities and Risk Factors Are Ubiquitous - ISACA, Data Loss Prevention-Next Steps - ISACA, [Cloud Computing - ISACA], [Cloud Computing Risk Assessment - ISACA], [User Awareness Training - ISACA], [Governance and Oversight - ISACA]

最新問題**: 315**
IT ガバナンス監査中に、情報システム監査人は、IT ポリシーと手順が定期的にレビューおよび更新されていないことに気付きます。情報システム監査人が最も懸念するのは、ポリシーと手順が以下の点を満たしていない可能性があることです。
A. 現在の実践を反映します。

B. 新しいシステムとそれに伴うプロセスの変更を含めます。
C. 関連法の変更を組み込む。
D. 適切な品質保証 (QA) の対象となる。
Answer: A (メーッセージを残す)
The greatest concern for an IS auditor when reviewing IT policies and procedures that are not regularly reviewed and updated is that policies and procedures might not reflect current practices. Policies are documents that define the goals, objectives, and guidelines for an organization's information systems and resources. Procedures are documents that describe the steps, tasks, or activities for implementing or executing policies. Policies and procedures should be regularly reviewed and updated to ensure that they are relevant, accurate, consistent, and effective for the organization's information systems and resources. Policies and procedures that are not regularly reviewed and updated might not reflect current practices, as they might be outdated, obsolete, or incompatible with the current state or needs of the organization's information systems and resources. This can cause confusion, inconsistency, inefficiency, or noncompliance among users or stakeholders who rely on policies and procedures for guidance or direction. Policies and procedures might not include new systems and corresponding process changes is a possible concern for an IS auditor when reviewing IT policies and procedures that are not regularly reviewed and updated, but it is not the greatest one. Policies and procedures might not include new systems and corresponding process changes, as they might be unaware of or unresponsive to the introduction or modification of information systems or resources within the organization. This can cause gaps, overlaps, or conflicts among policies and procedures that affect different information systems or resources.

最新問題: **316**
情報システム監査人が監査業務のリスク評価を実施する際に考慮すべき最も重要なことはどれですか?
A. コントロールの設計
B. 業界標準とベストプラクティス
C. 前回の監査の結果
D. 前回の監査からの経過時間
Answer: C (メーッセージを残す)
The results of the previous audit are an important source of information for an IS auditor to consider when performing the risk assessment prior to an audit engagement, as they can provide insights into the current state and performance of the auditee, identify any issues or gaps that need to be followed up or addressed, and highlight any areas that require special attention or focus. The design of controls is an important factor to evaluate during an audit engagement, but it is not the most important thing to consider when performing the risk assessment prior to an audit engagement, as it does not reflect the actual implementation or effectiveness of the controls. Industry standards and best practices are useful benchmarks or guidelines for an IS auditor to compare or measure against during

an audit engagement, but they are not the most important thing to consider when performing the risk assessment prior to an audit engagement, as they may not be applicable or relevant to the specific context or objectives of the auditee. The amount of time since the previous audit is a relevant criterion to determine the frequency or timing of an audit engagement, but it is not the most important thing to consider when performing the risk assessment prior to an audit engagement, as it does not indicate the level or nature of risk associated with the auditee.

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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: **317**
セキュリティ インシデント プロセスを確認する IS 監査人は、インシデントは解決され終了しているものの、根本原因が調査されていないことに気付きました。この状況で最も重要な懸念事項は次のどれですか。
A. 従業員による虐待は報告されていません。
B. 学んだ教訓が適切に文書化されていない
C. 脆弱性が適切に対処されていない
D. セキュリティ インシデント ポリシーが古くなっています。
Answer: C (メーッセージを残す**)**
The major concern with the situation where security incidents are resolved and closed, but root causes are not investigated, is that vulnerabilities have not been properly addressed. Vulnerabilities are weaknesses or gaps in the security posture of an organization that can be exploited by threat actors to compromise its systems, data, or operations. If root causes are not investigated, vulnerabilities may remain undetected or unresolved, allowing attackers to exploit them again or use them as entry points for further attacks. This can result in repeated or escalated security incidents that can cause more damage or disruption to the organization.
The other options are not as major as the concern about vulnerabilities, but rather secondary or related issues that may arise from the lack of root cause analysis. Abuses by employees have not been reported is a concern that may indicate a lack of awareness, accountability, or monitoring of insider threats. Lessons learned have not been properly documented is a concern that may indicate a lack of improvement, learning, or feedback

from security incidents. Security incident policies are out of date is a concern that may indicate a lack of alignment, review, or update of security incident processes.
References:
* ISACA CISA Review Manual 27th Edition (2019), page 254
* Why Root Cause Analysis is Crucial to Incident Response (IR) - Avertium3
* Root Cause Analysis Steps and How it Helps Incident Response ...

最新問題**: 318**
組織が IT セキュリティ要件に影響を及ぼす可能性のある新しい規制を認識した場合、IS 監査人が最初に実行することを推奨すべき項目は次のうちどれですか。
A. 新しい規制に基づいてセキュリティ ポリシーを更新します。
B. 影響を受ける可能性があるシステムと IT 関連プロセスを特定します。
C. セキュリティ意識とトレーニング コンテンツにどのような影響が及ぶ可能性があるかを評価します。
D. 既存の IT コントロールの設計と有効性を確認します。
Answer: B (メーッセージを残す**)**
The first thing that an IS auditor should recommend when an organization is made aware of a new regulation that is likely to impact IT security requirements is to determine which systems and IT-related processes may be impacted. This is because the impact assessment is a crucial step to understand the scope and magnitude of the changes that the new regulation may entail, as well as the potential risks and gaps that need to be addressed. The impact assessment can help the organization to prioritize and plan the necessary actions and resources to comply with the new regulation in a timely and effective manner12.
Updating security policies based on the new regulation is not the first thing to do, because it requires a clear understanding of the impact and implications of the new regulation, which can only be obtained after conducting an impact assessment. Updating security policies without an impact assessment may result in incomplete, inconsistent, or ineffective policies that may not meet the regulatory requirements or the organizational needs12.
Evaluating how security awareness and training content may be impacted is not the first thing to do, because it is a secondary or supporting activity that depends on the results of the impact assessment and the policy updates. Evaluating security awareness and training content without an impact assessment or policy updates may result in inaccurate, outdated, or irrelevant content that may not reflect the regulatory requirements or the organizational expectations34.
Reviewing the design and effectiveness of existing IT controls is not the first thing to do, because it is a monitoring or assurance activity that follows the implementation of the changes based on the impact assessment and the policy updates. Reviewing IT controls without an impact assessment or policy updates may result in misleading, incomplete, or

invalid findings that may not capture the regulatory requirements or the organizational performance

最新問題**: 319**
次のどれが、販売時点管理 (POS) システムと総勘定元帳間のインターフェースが販売データを完全かつ正確に転送していることを情報システム監査人に保証するものですか?
A. 顧客の売上領収書の電子コピーが保管されます。
B. 月次銀行取引明細書は例外なく照合されます。
C. 夜間のバッチ処理がリアルタイム処理に置き換えられました。
D. POS インターフェースを介して転送されるデータは暗号化されます。
Answer: A (メーッセージを残す**)**
The best option to provide an IS auditor assurance that the interface between a point-of-sale (POS) system and the general ledger is transferring sales data completely and accurately is A. Electronic copies of customer sales receipts are maintained. Electronic copies of customer sales receipts are records of the transactions that occurred at the POS system, which can be compared with the data transferred to the general ledger. This can help detect any errors, omissions, or discrepancies in the data transfer process and ensure that the sales data is complete and accurate.
The other options are not as effective as A in providing assurance that the interface between the POS system and the general ledger is transferring sales data completely and accurately. B. Monthly bank statements are reconciled without exception. Monthly bank statements are records of the cash inflows and outflows of the organization, which may not match with the sales data recorded by the POS system and the general ledger.
For example, there may be delays, discounts, returns, or refunds that affect the cash flow but not the sales revenue. Therefore, reconciling monthly bank statements without exception does not necessarily mean that the sales data is complete and accurate. C. Nightly batch processing has been replaced with real-time processing. Nightly batch processing is a method of transferring data from the POS system to the general ledger in batches at a scheduled time, usually at night. Real-time processing is a method of transferring data from the POS system to the general ledger as soon as the transactions occur. Real-time processing may improve the timeliness and efficiency of the data transfer process, but it does not guarantee that the sales data is complete and accurate. There may still be errors, omissions, or discrepancies in the data transfer process that need to be detected and corrected. D. The data transferred over the POS interface is encrypted. Encryption is a process of transforming data into an unreadable form using a secret key or algorithm, so that only authorized parties can access the original data. Encryption protects the confidentiality and security of the data transferred over the POS interface, but it does not ensure that the sales data is complete and accurate.
There may still be errors, omissions, or discrepancies in the data transfer process that need to be detected and corrected.

References:
* ISACA, CISA Review Manual, 27th Edition, 2019, p. 2471
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription2
* Sales Audit Overview - Oracle3
* Notes on Audit of Ledgers - Guidelines to Auditors - Accountlearning

最新問題**: 320**
組織のデバイス インベントリを調整する担当者が実行した場合に、職務の分離 (SoD) に関する最大の懸念を引き起こすタスクは次のどれですか。
A. スペアパーツ用追跡装置
B. 従業員へのデバイスの発行
C. デバイスポリシーの作成
D. デバイスの発行の承認
Answer: (解答を表示する**)**

最新問題**: 321**
情報情報監査人は、経営陣が新しいシステムを運用モードで使用する前にテストすることを推奨しました。テスト計画を開発する際の管理者にとって最善のアプローチは、次のような処理パラメータを使用することです。
A. テスト ジェネレーターによってランダムに選択されます。
B. アプリケーションのベンダーによって提供されます。
C. ユーザーによってランダムに選択されます。
D. 実稼働エンティティと顧客によってシミュレートされます。
Answer: D (メーッセージを残す**)**
The best approach for management in developing a test plan is to use processing parameters that are simulated by production entities and customers. This is because using realistic data and scenarios can help to evaluate the functionality, performance, reliability, and security of the new system under actual operating conditions and expectations. Using processing parameters that are randomly selected by a test generator, provided by the vendor of the application, or randomly selected by the user may not be sufficient or representative of the production environment and may not reveal all the potential issues or defects of the new system. References: [ISACA CISA Review Manual 27th Edition], page 266.

最新問題**: 322**
IS 監査人は、パッチ ログから、対象範囲内の一部のシステムが定期的なパッチ適用スケジュールに準拠していないことを発見しました。監査人は次に何をすべきでしょうか?
A. IT 管理者にインタビューして、現在の手順を明確にします。
B. この発見を上級管理職に報告します。

C. 組織のパッチ管理ポリシーを確認します。
D. フォローアップ項目として行動計画を策定するよう要求します。
Answer: C (メーッセージを残す)
The IS auditor should review the organization's patch management policy to determine the expected frequency and scope of patching, as well as the roles and responsibilities of the patch management team. This will help the auditor assess the severity and impact of the non-compliance, and identify the root cause and possible remediation actions12.
References
1: How to Create a Patch Management Policy: Complete Guide 2: Free Patch Management Policy Template (+Examples)

最新問題**: 323**
監査対象者が、高リスクの発見事項に対する是正措置計画に予想よりも時間がかかることを示した場合、情報システム監査人が取るべき最善の行動はどれですか?
A. より長い目標日を受け入れ、監査システムに文書化します。
B. 期限切れの発見事項を監査委員会にエスカレーションします。
C. 暫定的な補償制御が実装されているかどうかを判断します。
D. 合意された期間内に修復が完了することを要求します。
Answer: C (メーッセージを残す)

最新問題**: 324**
IT とビジネス目標を整合させるための IT フレームワークを実装することで、最も効果的に対処できる懸念事項は次のどれですか。
A. 不正確なビジネス影響分析 (BIA)
B. 不十分なIT変更管理手法
C. ベンチマーク分析の欠如
D. 不十分なITポートフォリオ管理
Answer: D (メーッセージを残す)
An IT framework for alignment between IT and business objectives is a set of principles, guidelines, and practices that help an organization to ensure that its IT investments support its strategic goals, deliver value, manage risks, and optimize resources. One of the benefits of implementing such a framework is that it enables an effective IT portfolio management, which is the process of selecting, prioritizing, monitoring, and evaluating the IT projects and services that comprise the IT portfolio. An IT portfolio is a collection of IT assets, such as applications, infrastructure, data, and capabilities, that are aligned with the business needs and objectives. An IT portfolio management helps an organization to achieve the following outcomes:
* Align the IT portfolio with the business strategy and vision
* Balance the IT portfolio among different types of investments, such as innovation, growth, maintenance, and compliance

* Optimize the IT portfolio performance, value, and risk
* Enhance the IT portfolio decision-making and governance
* Improve the IT portfolio communication and transparency

Therefore, an inadequate IT portfolio management is a major concern that can be addressed by implementing an IT framework for alignment between IT and business objectives. An inadequate IT portfolio management can result in the following issues:

* Misalignment of the IT portfolio with the business needs and expectations
* Imbalance of the IT portfolio among competing demands and priorities
* Suboptimal use of the IT resources and capabilities
* Lack of visibility and accountability of the IT portfolio outcomes and impacts
* Poor communication and collaboration among the IT portfolio stakeholders

The other possible options are:

* Inaccurate business impact analysis (BIA): A BIA is a process of identifying and assessing the potential effects of a disruption or disaster on the critical business functions and processes. A BIA helps an organization to determine the recovery priorities, objectives, and strategies for its business continuity plan. A BIA is not directly related to an IT framework for alignment between IT and business objectives, although it may use some inputs from the IT portfolio management. Therefore, an inaccurate BIA is not a concern that can be effectively addressed by implementing an IT framework for alignment between IT and business objectives.
* Inadequate IT change management practices: IT change management is a process of controlling and managing the changes to the IT environment, such as hardware, software, configuration, or documentation. IT change management helps an organization to minimize the risks and disruptions caused by the changes, ensure the quality and consistency of the changes, and align the changes with the business requirements. IT change management is not directly related to an IT framework for alignment between IT and business objectives, although it may support some aspects of the IT portfolio management. Therefore, inadequate IT change management practices are not a concern that can be effectively addressed by implementing an IT framework for alignment between IT and business objectives.
* Lack of a benchmark analysis: A benchmark analysis is a process of comparing an organization's performance, processes, or practices with those of other organizations or industry standards. A benchmark analysis helps an organization to identify its strengths and weaknesses, set realistic goals and targets, and implement best practices for improvement. A benchmark analysis is not directly related to an IT framework for alignment between IT and business objectives, although it may provide some insights for the IT portfolio management. Therefore, lack of a benchmark analysis is not a concern that can be effectively addressed by implementing an IT framework for alignment between IT and business objectives.

References: 1: What is Portfolio Management? | Smartsheet 2: What Is Portfolio Management? - Definition from Techopedia 3: What Is Project Portfolio Management (PPM)? | ProjectManager.com 4: What Is Business Impact Analysis? |

Smartsheet 5: What Is Change Management? - Definition from Techopedia 6: Benchmarking - Wikipedia

最新問題**: 325**
データセンター内の物理的な情報資産を保護するために最も重要な前提条件は次のどれですか?
A. 情報資産を発注するスタッフと受領するスタッフの職務の分離
B. 展開された情報資産の完全かつ正確なリスト
C. オンサイトバックアップジェネレータの可用性とテスト
D. データ保護要件に関するITスタッフの知識
Answer: B (メーッセージを残す**)**
The most important prerequisite for the protection of physical information assets in a data center is a complete and accurate list of information assets that have been deployed. Information assets are any data, devices, systems, or software that have value for the organization and need to be protected from unauthorized access, use, disclosure, modification, or destruction4. A data center is a facility that houses various infor mation assets such as servers, storage devices, network equipment, etc., that support the organization's IT operations and services5. A complete and accurate list of information assets that have been deployed in a data center can help to identify and classify the assets based on their importance, sensitivity, or criticality for the organization. This can help to determine the appropriate level of protection and security measures that need to be applied to each asset. A complete and accurate list of information assets can also help to track and monitor the location, status, ownership, usage, configuration, maintenance, etc., of each asset. This can help to prevent or detect any unauthorized or inappropriate changes or movements of assets that may compromise their security or integrity.
Segregation of duties between staff ordering and staff receiving information assets, availability and testing of onsite backup generators, and knowledge of the IT staff regarding data protection requirements are also important prerequisites for the protection of physical information assets in a data center, but not as important as a complete and accurate list of information assets that have been deployed.
These factors are more related to the implementation and maintenance of security controls and procedures that depend on having a complete and accurate list of information assets as a starting point. References:
ISACA CISA Review Manual 27th Edition, page 308

最新問題**: 326**
IS 監査レポートに含めるべき最も重要な項目は次のどれですか?
A. 各監査観察に対する特定の技術ソリューション
B. 証拠が不十分なため、観察結果は調査結果として報告されなかった
C. さまざまなリスク領域に対処するためのロードマップ
D. 軽減されていないリスクのレベルとビジネスへの影響

Answer: D (メーッセージを残す)

最新問題: **327**
組織内でプライバシー関連の制御を実装する主な目的は次のどれですか?
A. 機密データの損失を防ぐため
B. 法律および規制の要件に準拠するため
C. 保存中のデータと転送中のデータを暗号化のために識別する
D. 個人にデータの使用に関する選択肢を提供する
Answer: B (メーッセージを残す)
The primary objective of implementing privacy-related controls within an organization is to comply with legal and regulatory requirements that protect the rights and interests of individuals whose personal data are collected, processed, stored, shared or disposed by the organization. Privacy-related controls are based on principles such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality and accountability. These principles aim to ensure that personal data are processed in a manner that respects the privacy of individuals and complies with the applicable laws and regulations in different jurisdictions. Preventing confidential data loss, identifying data at rest and data in transit for encryption, and providing options to individuals regarding use of their data are examples of specific privacy-related controls that support the primary objective of compliance. References: Privacy Regulatory Lookup Tool, CDPSE Official Review Manual, 2nd Edition

最新問題: **328**
外部レビュー中に、情報システム監査人は、組織内のシステムの重要性を分類する際に一貫性のないアプローチを観察しました。システムの重要性を決定するための主な要素として推奨されるべきものは次のどれですか?
A. 主要業績評価指標 (KPI)
B. 最大許容ダウンタイム (MAD)
C. リカバリポイント目標 (RPO)
D. 平均復旧時間 (MTTR)
Answer: B (メーッセージを残す)
The primary factor to determine system criticality within an organization is the maximum allowable downtime (MAD). MAD is the maximum time frame during which recovery must become effective before an outage compromises the ability of an organization to achieve its business objectives and/or survival. MAD reflects the business impact of a system outage on the organization's operations, reputation, compliance, and finances. MAD can help to prioritize system recovery efforts, allocate resources, and establish recovery objectives.

最新問題: **329**

内部監査チームは、別の国のサードパーティがホストする監査管理アプリケーションを使用するかどうかを決定しています。
ホストされたアプリケーションに給与監査文書をアップロードする場合に最も重要な考慮事項は何ですか?
A. 組織に影響を与える財務規制
B. アプリケーションがホストされているデータセンターの物理的なアクセス制御
C. 組織に影響を及ぼすプライバシー規制
D. ホスティングサービスプロバイダーがストレージに対して請求する単位あたりのコスト
Answer: (解答を表示する**)**
This is because privacy regulations are laws or rules that protect the personal information of individuals from unauthorized access, use, disclosure, or transfer by third parties. Payroll audit documentation may contain sensitive and confidential data, such as employee names, salaries, benefits, taxes, deductions, and bank accounts. If the audit management application is hosted by a third party in a different country, the organization may need to comply with the privacy regulations of both its own country and the host country, as well as any international or regional agreements or frameworks that apply. Privacy regulations may impose various requirements and obligations on the organization, such as obtaining consent from the data subjects, implementing appropriate security measures, notifying data breaches, and ensuring data quality and accuracy.
Privacy regulations may also grant various rights to the data subjects, such as accessing, correcting, deleting, or transferring their data. Failing to comply with privacy regulations may expose the organization to significant risks and consequences, such as legal actions, fines, sanctions, reputational damage, or loss of trust.
Some examples of privacy regulations affecting the organization are:
* The General Data Protection Regulation (GDPR), which is a comprehensive and strict privacy regulation that applies to any organization that processes personal data of individuals in the European Union (EU) or offers goods or services to them, regardless of where the organization or the data is located1.
* The California Consumer Privacy Act (CCPA), which is a broad and influential privacy regulation that applies to any organization that collects personal information of California residents and meets certain thresholds of revenue, data volume, or data sharing2.
* The Health Insurance Portability and Accountability Act (HIPAA), which is a sector-specific privacy regulation that applies to any organization that handles protected health information (PHI) of individuals in the United States, such as health care providers, health plans, or health care clearinghouses3.
Therefore, before using an audit management application hosted by a third party in a different country, the internal audit team should conduct a thorough assessment of the privacy regulations affecting the organization and ensure that they have adequate policies, procedures, and controls in place to comply with them.

最新問題**: 330**
次の活動のうち、IS 監査人が独立性を維持しながら、コントロール セールス評価 (CSA) を実施できるようにするものはどれですか。
A. 修復計画の実施
B. CSA を部分的に完了する
C. 修復計画の策定
D. CSAアンケートの作成
Answer: D (メーッセージを残す**)**
Developing the CSA questionnaire is an activity that would allow an IS auditor to maintain independence while facilitating a control self-assessment (CSA). An IS auditor can design and provide a CSA questionnaire to help the business units or process owners to evaluate their own controls and identify any issues or improvement opportunities. This will enable an IS auditor to support and guide the CSA process without compromising their objectivity or independence. The other options are activities that would impair an IS auditor's independence while facilitating a CSA, as they involve implementing, completing, or developing remediation actions for control issues. References:
* CISA Review Manual (Digital Version), Chapter 2, Section 2.41
* CISA Review Questions, Answers & Explanations Database, Question ID 215

最新問題**: 331**
IS 監査人は、エンタープライズ リソース プランニング (ERP) システムの実装後レビューを実施しています。
エンド ユーザーは、システムによって実行される重要な自動計算の精度について懸念を示しています。監査人の最初の行動は次のようになります。
A. システムの最近の変更を確認します。
B. ユーザー受け入れテスト (UAT) の完全性を確認します。
C. 結果を検証して、ユーザーの懸念の妥当性を判断します。
D. 初期のビジネス要件を確認します。
Answer: C (メーッセージを残す**)**
The IS auditor's first course of action should be to verify the results of the critical automatic calculations made by the system to determine the validity of user concerns. This is because the IS auditor needs to obtain sufficient and appropriate audit evidence to support the audit findings and conclusions. By verifying the results, the IS auditor can assess whether there are any errors or discrepancies in the system's calculations that could affect the accuracy and reliability of the financial data. The IS auditor can use various techniques to verify the results, such as re-performing the calculations, comparing them with expected values, or tracing them to source documents.

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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: **332**
システム変更のロールバック計画の主な目的はどれですか?
A. 必要に応じて変更を削除するための手順が存在することを確認する
B. 必要に応じてテストを再実行できるようにするため
C. 変更を実施する前にバックアップが存在することを確認する
D. システム変更が有効であることを確認する
Answer: A (メーッセージを残す**)**

最新問題: **333**
ある組織は、サードパーティ ベンダーから Web ベースの電子メール サービスを購入し、独自の電子メール サーバー インフラストラクチャを廃止することを決定しました。この組織の目的に最も適したクラウド コンピューティング環境はどのようなタイプでしょうか。
A. サービスとしてのプラットフォーム (PaaS)
B. サービスとしてのソフトウェア (SaaS)
C. サービスとしてのデータベース (DBaaS)
D. サービスとしてのインフラストラクチャ (IaaS)
Answer: B (メーッセージを残す**)**

最新問題: **334**
システム インターフェイスのデータの整合性を保証するのに役立つのは次のどれですか。
A. システムインターフェーステスト
B. ユーザー受け入れテスト (IJAT)
C. 検証チェック
D. 監査ログ
Answer: C (メーッセージを残す**)**
Validation checks are a type of data quality control that helps to ensure the integrity of data for a system interface. Validation checks verify that the data entered or transferred between systems is correct, consistent, and conforms to predefined rules or standards. Validation checks can prevent or detect errors, anomalies, or inconsistencies in the data that may affect the system's functionality, performance, or security.
Option C is correct because validation checks are a common and effective method of ensuring data integrity for a system interface. Validation checks can be performed at

various stages of the data lifecycle, such as input, processing, output, or storage. Validation checks can also be applied to different types of data, such as data types, codes, ranges, formats, consistency, and uniqueness.
Option A is incorrect because system interface testing is a type of software testing that verifies the interaction between two separate systems or components of a system. System interface testing does not directly ensure the integrity of data for a system interface, but rather the functionality and reliability of the interface itself.
System interface testing may use validation checks as part of its test cases, but it is not the same as validation checks.
Option B is incorrect because user acceptance testing (UAT) is a type of software testing that evaluates whether the system meets the user's expectations and requirements. UAT does not directly ensure the integrity of data for a system interface, but rather the usability and acceptability of the system from the user's perspective. UAT may use validation checks as part of its test scenarios, but it is not the same as validation checks.
Option D is incorrect because audit logs are records of events and activities that occur within a system or network. Audit logs do not directly ensure the integrity of data for a system interface, but rather provide evidence and accountability for the system's operations and security. Audit logs may use validation checks as part of their analysis or reporting, but they are not the same as validation checks.
References:
CISA Online Review Course1, Module 5: Protection of Information Assets, Lesson 4: Data Quality Management, slide 5-6.
CISA Review Manual (Digital Version)2, Chapter 5: Protection of Information Assets, Section 5.3: Data Quality Management, p. 281-282.
CISA Review Manual (Print Version), Chapter 5: Protection of Information Assets, Section 5.3: Data Quality Management, p. 281-282.
CISA Questions, Answers & Explanations Database3, Question ID: QAE_CISA_722.
Data Validation - Overview, Types, Practical Examples4
Data Validity: The Best Practice for Your Business5
Validation - Data validation6
What is Data Validation? Types, Techniques, Tools7

最新問題**: 335**
IS 監査人が組織のクラウド アクセス セキュリティ ブローカー (CASB) ソリューションをレビューしています。監査人が検証する必要がある最も重要な項目は次のうちどれですか。
A. クラウド サービスは分類されます。
B. ユーザーは集中管理されます。
C. クラウド プロセスは回復力があります。
D. ユーザーは定期的に再認証されます。

Answer: D (メーッセージを残す)
Periodic recertification of users ensures that only authorized individuals retain access to cloud services and helps identify and revoke access for users who no longer require it. This is a critical control for maintaining security and compliance in a cloud environment.
* Classifying Cloud Services (Option A): This is foundational but does not verify ongoing user access.
* Centrally Managing Users (Option B): While useful for consistency, it does not assess whether access rights are still valid.
* Ensuring Cloud Process Resilience (Option C): This focuses on operational continuity rather than access control.
Periodic recertification aligns with governance practices to ensure access rights remain appropriate over time.
Reference: ISACA CISA Review Manual, Job Practice Area 4: Protection of Information Assets.

最新問題**: 336**
新しい財務アプリケーションの開発では、情報システム監査人が最初に関与すべき事項は次のとおりです。
A. 制御設計。
B. 実現可能性調査。
C. アプリケーション設計。
D. システムテスト。
Answer: B (メーッセージを残す)
In the development of a new financial application, the IS auditor's first involvement should be in the feasibility study. A feasibility study is a preliminary analysis that evaluates the technical, operational, economic, and legal aspects of a proposed project or system. A feasibility study helps determine whether the project or system is viable, feasible, and desirable for the organization and its stakeholders.
The IS auditor's role in the feasibility study is to provide an independent and objective assessment of the project or system's risks, benefits, costs, and impacts. The IS auditor should also ensure that the feasibility study follows a structured and systematic approach, considers all relevant factors and alternatives, and complies with the organization's policies and standards. The IS auditor should also verify that the feasibility study is documented and communicated to the appropriate decision-makers.
The IS auditor's involvement in the feasibility study is important because it can help:
* Identify and mitigate potential risks and issues that could affect the project or system's success
* Evaluate and justify the project or system's alignment with the organization's strategy, goals, and value proposition
* Estimate and optimize the project or system's resources, budget, schedule, and quality

* Assess and enhance the project or system's security, reliability, performance, and usability
* Ensure that the project or system meets the expectations and requirements of the users and other stakeholders The other three options are not the first involvement of the IS auditor in the development of a new financial application, although they may be part of the subsequent stages of the development process. Control design is the process of defining and implementing controls that ensure the security, integrity, availability, and efficiency of the system. Application design is the process of specifying the functional and technical features of the system. System test is the process of verifying that the system meets the specifications and requirements.
Therefore, feasibility study is the best answer.
References:
* [Feasibility Study - ISACA]
* [IS Auditing Guideline G13 Performing an IS Audit Engagement - ISACA]

最新問題**: 337**
IS 監査人は、IT 管理者がバランスト スコアカードを使用して次のことを行うことを推奨する可能性が最も高いでしょう。
A. 組織が品質基準を満たしているかどうかを示します。
B. IT スタッフがパフォーマンス要件を満たしていることを確認します。
C. IT スタッフをトレーニングおよび教育します。
D. IT 機能とプロセスを評価します。
Answer: D (メーッセージを残す**)**
A balanced scorecard is a strategic planning framework that companies use to assign priority to their products, projects, and services; communicate about their targets or goals; and plan their routine activities1. The scorecard enables companies to monitor and measure the success of their strategies to determine how well they have performed. A balanced scorecard for IT management can help assess IT functions and processes by defining four perspectives: financial, customer, internal business process, and learning and growth2. These perspectives can help IT management align their IT objectives with the organization's vision and mission, identify and prioritize the key performance indicators (KPIs) for IT, and evaluate the effectiveness and efficiency of IT operations and services3.
References
1: Balanced Scorecard - Overview, Four Perspectives 2: The IT Balanced Scorecard (BSC) Explained - BMC Software 3: A BALANCED SCORECARD (BSC) FOR IT PERFORMANCE MANAGEMENT - SAS Support

最新問題**: 338**
監査目標が確立される主な根拠は次のうちどれですか?
A. 監査リスク

B. リスクの考慮
C. 以前の監査の評価
D. ビジネス戦略
Answer: (解答を表示する**)**
The primary basis on which audit objectives are established is the consideration of risks12. This involves identifying and assessing the risks that could prevent the organization from achieving its objectives12. The audit objectives are then designed to address these risks and provide assurance that the organization's controls are effective in managing them12. While audit risk, assessment of prior audits, and business strategy are important factors in the audit process, they are secondary to the fundamental requirement of considering risks12.
References:
Objectives of Auditing - Primary and Secondary Objectives of Auditing | Auditing Management Notes Audit Objectives | Primary and Subsidiary Audit Objectives - EDUCBA

最新問題**: 339**
支払い取引データが適切なユーザーに制限されるようにするための最良の方法はどれですか?
A. 2要素認証の実装
B. ネットワークセキュリティソフトウェアを使用してトランザクションへのアクセスを制限する
C. アプリケーションレベルでロールベースのアクセスを実装する
D. 機密性の高いアプリケーショントランザクションに単一のメニューを使用する
Answer: C (メーッセージを残す**)**
The best way to ensure payment transaction data is restricted to the appropriate users is implementing role- based access at the application level. Role-based access is a method of access control that assigns permissions or privileges to users based on their roles or functions within an organization or system. Role-based access can help ensure that payment transaction data is restricted to the appropriate users, by allowing only authorized users who have a legitimate need or purpose to access or use the payment transaction data, and preventing unauthorized or unnecessary access or use by other users.
Implementing two-factor authentication is a possible way to enhance the security and verification of user identities, but it is not the best way to ensure payment transaction data is restricted to the appropriate users, as it does not define what permissions or privileges users have on the payment transaction data. Restricting access to transactions using network security software is a possible way to protect the network communication and transmission of payment transaction data, but it is not the best way to ensure payment transaction data is restricted to the appropriate users, as it does not specify what actions or operations users can perform on the payment transaction data.
Using a single menu for sensitive application transactions is a possible way to simplify the user interface and navigation of payment transaction data, but it is not the best way to

ensure payment transaction data is restricted to the appropriate users, as it does not limit what users can access or use the payment transaction data.

最新問題**: 340**
次のどれがビジネスクリティカルなアプリケーションの監査の品質に最も貢献しますか?
A. 独立した外部監査人への監査の割り当て
B. アプリケーション所有者が報告した以前の調査結果を確認する
C. 開発チームが犯す一般的なコーディングエラーを特定する
D. 監査計画プロセスの早い段階でアプリケーション所有者を関与させる
Answer: (解答を表示する**)**
Involving the application owner early in the audit planning process is the best way to contribute to the quality of an audit of a business-critical application. The application owner has a deep understanding of the application and its business context, which can provide valuable insights for the audit. Early involvement can also help ensure that the audit is aligned with the business objectives and risks, and that any potential issues are identified and addressed promptly12.
References:
Business Critical Applications: An In-Depth Look
Framework for Audit Quality - IFAC

最新問題**: 341**
従業員による不適切な活動のリスクを軽減するための最も効果的な制御は次のどれですか?
A. ユーザーアクティビティの監視
B. 2要素認証
C. ネットワークセグメンテーション
D. アクセスの再認証
Answer: A (メーッセージを残す**)**
The answer A is correct because user activity monitoring is the most effective control to mitigate against the risk of inappropriate activity by employees. User activity monitoring (UAM) is the process of tracking and recording the actions and behaviors of users on devices, networks, or applications that belong to an organization. UAM can help to prevent, detect, and respond to insider threats, such as data theft, fraud, sabotage, or misuse of resources. UAM can also help to enforce policies, ensure compliance, and improve productivity and performance.
Some of the benefits of UAM are:
* Prevention: UAM can deter employees from engaging in inappropriate activity by making them aware that their actions are monitored and recorded. UAM can also prevent unauthorized access or use of sensitive data or resources by implementing access controls, encryption, or alerts.

* Detection: UAM can detect any anomalies, deviations, or violations in user activity by analyzing the data collected from various sources, such as logs, keystrokes, screenshots, or video recordings. UAM can also use artificial intelligence or machine learning to identify patterns, trends, or risks in user behavior.
* Response: UAM can respond to any incidents or issues related to user activity by notifying the relevant stakeholders, such as managers, security teams, or auditors. UAM can also provide evidence or proof of user activity for investigation or remediation purposes.

Some examples of UAM tools are:

* Teramind: Teramind is a cloud-based UAM platform that offers features such as user behavior analytics, risk scoring, policy enforcement, data loss prevention, and productivity optimization.
* Digital Guardian: Digital Guardian is a data protection platform that offers UAM capabilities such as endpoint detection and response, data classification and tagging, and threat hunting and incident response.
* XPLG: XPLG is a log management and analysis platform that offers UAM features such as log aggregation and correlation, user behavior profiling and anomaly detection, and real-time alerts and dashboards.

The other options are not as effective as option A. Two-factor authentication (option B) is a security mechanism that requires users to provide two pieces of evidence to verify their identity before accessing a system or resource. Two-factor authentication can enhance the security and privacy of user accounts, but it does not monitor or record the user activity after the authentication. Network segmentation (option C) is a technique that divides a network into smaller subnetworks based on criteria such as function, location, or security level. Network segmentation can improve the performance, security, and manageability of a network by reducing congestion, isolating threats, and enforcing policies. However, network segmentation does not track or record the user activity within each segment of the network. Access recertification (option D) is a process that verifies and validates the access rights of users to systems or resources periodically or on- demand. Access recertification can ensure that users have the appropriate level of access based on their roles and responsibilities, but it does not monitor or record the user activity with the access rights.

References:

* [User Activity Monitoring: Examples and Best Practices | SEON]
* Top 10 user activity monitoring tools: software features and tracking price - Dashly blog
* What is User Activity Monitoring? How It Works, Benefits, Best Practices and More - Digital Guardian
* What Is User Activity Monitoring? Learn the What, Why, and How - XPLG

最新問題: 342

IT 戦略計画をレビューする際に、情報システム監査人は以下の点が特定されているかどうかを考慮する必要があります。
A. IT スタッフの割り当て。
B. 使用されるプロジェクト管理方法論。
C. 主要な IT イニシアチブ。
D. 運用戦術計画へのリンク。
Answer: (解答を表示する**)**
In reviewing the IT strategic plan, the IS auditor should consider whether it identifies the major IT initiatives that are aligned with the organization's vision, mission, and objectives, and that support the business strategy and priorities12. The major IT initiatives should also be realistic, measurable, and achievable, and should have clear timelines, budgets, and responsibilities34.
References
1: IT Strategy Template for a Successful Strategic Plan | Gartner2 2: IT Strategy Template for a Successful Strategic Plan | Gartner4 3: Conduct a Strategic Plan Review & Assessment - Governance3 4: Time To Conduct A Strategy Review? Here's How To Get Started1

最新問題**: 343**
IS 監査人は、解雇された従業員のアクセス権を削除するプロセスが文書化されていないことを発見しました。この観察から得られる最も重要なリスクは何ですか?
A. 手順がベストプラクティスと一致しない可能性があります
B. 人事 (HR) レコードがシステム アクセスと一致しない可能性があります。
C. 不正アクセスを識別できません。
D. アクセス権が適切なタイミングで削除されない可能性があります。
Answer: D (メーッセージを残す**)**
The most significant risk from this observation is that access rights may not be removed in a timely manner. If the process for removing access for terminated employees is not documented, there is no clear guidance or accountability for who, how, when, and what actions should be taken to revoke the access rights of the employees who leave the organization. This could result in delays, inconsistencies, or omissions in removing access rights, which could allow terminated employees to retain unauthorized access to the organization's systems and data. This could compromise the security, confidentiality, integrity, and availability of the information assets. References:
* CISA Review Manual (Digital Version)
* CISA Questions, Answers & Explanations Database

最新問題**: 344**
データセンターの環境管理レビューの一環として消火システムを検査する場合、次のどれを考慮する必要がありますか?

A. インストールマニュアル
B. オンサイト交換の可用性
C. 保険適用範囲
D. メンテナンス手順
Answer: D (メーッセージを残す)
The correct answer is D. Maintenance procedures should be considered when examining fire suppression systems as part of a data center environmental controls review. Fire suppression systems are critical for protecting the data center equipment and personnel from fire hazards. Therefore, they should be regularly maintained and tested to ensure their proper functioning and compliance with safety standards. Maintenance procedures should include inspection, cleaning, replacement, and repair of the fire suppression system components, as well as documentation of the maintenance activities and results. Installation manuals, onsite replacement availability, and insurance coverage are not directly related to the fire suppression system performance and effectiveness, and therefore are not relevant for the audit review. References: CISA Review Manual (Digital Version)1, page 403.

最新問題**: 345**
内部監査チームと外部監査チームの両方がリソースを最適化するために同じアプローチをレビューしている、高リスク領域の IT 一般管理監査中ですか?
A. 外部監査によって実行された作業を内部監査テストに活用します。
B. 内部監査人と外部監査人の両方が同時に作業を実行するようにします。
C. 外部監査チームに内部監査作業を活用するよう要求します。
D. 一般統制監査を次の監査年度にロールフォワードします。
Answer: A (メーッセージを残す)
The best approach to optimize resources when both internal and external audit teams are reviewing the same IT general controls area is to leverage the work performed by external audit for the internal audit testing. This can avoid duplication of efforts, reduce audit costs and enhance coordination between the audit teams. The internal audit team should evaluate the quality and reliability of the external audit work before relying on it. Ensuring both the internal and external auditors perform the work simultaneously is not an efficient use of resources, as it would create redundancy and possible interference. Requesting that the external audit team leverage the internal audit work may not be feasible or acceptable, as the external audit team may have different objectives, standards and independence requirements. Rolling forward the general controls audit to the subsequent audit year is not a good practice, as it would delay the identification and remediation of any control weaknesses in a high-risk area. References: ISACA, CISA Review Manual, 27th Edition, 2018, page
247

最新問題: **346**
2 人のユーザーが同じデータベース レコードに同時にアクセスした場合に最も大きなリスクとなるのはどれですか。
A. エンティティの整合性
B. 参照整合性
C. 可用性の整合性
D. データの整合性
Answer: (解答を表示する**)**

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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: **347**
IS 監査人がフロントエンドの補助元帳とメイン元帳を検査しています。2 つのシステム間のアカウントのマッピングに欠陥がある場合、次のどれが最も懸念されるでしょうか。
A. 単一のジャーナルエントリの二重投稿
B. 新規ビジネス取引をサポートできない
C. アカウント属性の不正な変更
D. 財務報告の不正確さ
Answer: D (メーッセージを残す**)**
The greatest concern for an IS auditor if there are flaws in the mapping of accounts between a front-end subledger and a main ledger is the inaccuracy of financial reporting. A subledger is a detailed record of transactions for a specific account, such as accounts receivable, accounts payable, inventory, or fixed assets.
A main ledger is a summary record of all transactions for all accounts in an accounting system. The mapping of accounts between a subledger and a main ledger is the process of linking or reconciling the transactions in the subledger with the corresponding entries in the main ledger. If there are flaws in the mapping of accounts, such as missing, duplicated, or incorrect transactions, the main ledger may not reflect the true financial position and performance of the organization. This may lead to inaccurate financial reporting, which may affect decision making, compliance, auditing, taxation, and stakeholder confidence.
Double-posting of a single journal entry, inability to support new business transactions, and unauthorized alteration of account attributes are not the greatest concerns for an IS auditor if there are flaws in the mapping of accounts between a front-end subledger and a main

ledger. These are possible consequences or causes of flaws in the mapping of accounts, but they do not have as significant an impact as inaccuracy of financial reporting. Double-posting of a single journal entry may result in errors or discrepancies in the main ledger balances. Inability to support new business transactions may indicate limitations or inefficiencies in the accounting system design or configuration. Unauthorized alteration of account attributes may suggest weaknesses or breaches in access control or segregation of duties.

最新問題**: 348**
監査分析で使用されるテスト手順の品質と整合性を最もよく保証するものは次のどれですか?
A. 監査チームへのテスト手順のベストプラクティスの開発と伝達
B. 監査データリポジトリの開発と実装
C. 手続きの分散化と定期的なピアレビューの実施
D. 手順の集中化と変更管理の実装
Answer: D (メーッセージを残す**)**
The best way to ensure the quality and integrity of test procedures used in audit analytics is to centralize procedures and implement change control. Centralizing procedures means storing them in a common repository that can be accessed and updated by authorized users. Change control means implementing a process for tracking, reviewing, approving, and documenting any changes made to the procedures. This ensures that the procedures are consistent, accurate, reliable, and secure. References: CISA Review Manual, 27th Edition, page 401

最新問題**: 349**
IS 監査人がデータ変換プロジェクトをレビューしています。稼働開始前の監査人の最善の推奨事項は次のどれですか?
A. 構成ベースラインを確立します。
B. テスト手順とシナリオを確認します。
C. テスト スクリプトを自動化します。
D. 模擬変換テストを実施します。
Answer: D (メーッセージを残す**)**

最新問題**: 350**
サービスプロバイダーが顧客にセキュリティ侵害を通知していないことを発見した場合、情報システム監査人はまず何をすべきでしょうか?
A. 発見内容を法執行機関に通知します。
B. 第三者に顧客への通知を要求します。
C. 重要な発見事項を含む監査レポート。
D. 監査管理者に検出結果を通知します。

Answer: (解答を表示する**)**
The IS auditor should notify audit management of the finding first, as this is a significant issue that may affect the audit scope and objectives. The IS auditor should not notify law enforcement or require the third party to notify customers without consulting audit management first. The audit report with a significant finding should be issued after the audit is completed and the findings are validated. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 247

最新問題**: 351**
情報システム監査人が監査対象者との終了会議中に行うべき最も重要なことはどれですか?
A. レポートに記載されている事実が正しいことを確認する
B. 上級管理職に推奨事項を伝える
C. 推奨事項の実装日を指定します。
D. 是正措置を決定するための入力を要求します。
Answer: A (メーッセージを残す**)**
Ensuring that the facts presented in the report are correct is the most important thing for an IS auditor to do during an exit meeting with an auditee. An IS auditor should confirm that the audit findings and observations are accurate, complete, and supported by sufficient evidence, as well as that the auditee understands and agrees with them. This will help to avoid any misunderstandings or disputes later on, as well as to enhance the credibility and quality of the audit report. The other options are less important things for an IS auditor to do during an exit meeting, as they may involve communicating the recommendations to senior management, specifying implementation dates for the recommendations, or requesting input in determining corrective action. References:
* CISA Review Manual (Digital Version), Chapter 2, Section 2.5.21
* CISA Review Questions, Answers & Explanations Database, Question ID 222

最新問題**: 352**
デプロイメント プログラムの一環としてセキュア コード レビューが実施される際に、どのような種類の制御が実装されていますか?
A. 修正
B. 抑止力
C. 監視
D. 探偵
Answer: D (メーッセージを残す**)**

最新問題**: 353**
IS 監査人は、運用担当者が年度末の財務諸表に寄与するスクリプトを実行していなかったことを発見しました。次のうち、最も適切な推奨事項はどれですか。

A. 運用担当者を再訓練します。
B. 終了チェックリストを実装します。
C. 操作マニュアルを更新します。
D. 財務経験のあるスタッフを業務に投入します。
Answer: (解答を表示する**)**
The best recommendation for the IS auditor to make is to implement a closing checklist, as this will help to ensure that all the required tasks and scripts are performed and verified during the year-end closing process12. A closing checklist can also help to prevent errors, omissions, and delays that could affect the accuracy and timeliness of the financial statements3 .
References
1: Year-end closing procedures for GL - Dynamics GP | Microsoft Learn1 2: Year-end activities FAQ - Finance | Dynamics 365 | Microsoft Learn2 3: Year-End Closing Checklist: 10 Steps to Close Your Books3 :
Year End Closing Checklist: 7 Steps to Make it Easy

最新問題**: 354**
個人データの保持期間と破棄の条件は、によって決定される必要があります。
A. リスクマネージャー。
B. データベース管理者 (DBA)。
C. プライバシー マネージャー。
D. 事業主。
Answer: D (メーッセージを残す**)**
The business owner is the person or entity that has the authority and responsibility for defining the purpose and scope of the processing of personal data, as well as the expected outcomes and benefits. The business owner is also accountable for ensuring that the processing of personal data complies with the applicable laws and regulations, such as the General Data Protection Regulation (GDPR) or the Data Protection Act 2018 (DPA 2018). One of the requirements of the GDPR and the DPA 2018 is to adhere to the principle of storage limitation, which states that personal data should be kept for no longer than is necessary for the purposes for which it is processed1. This means that the business owner should determine and justify how long they need to retain personal data, based on factors such as:
The nature and sensitivity of the personal data
The legal or contractual obligations or rights that apply to the personal data The business or operational needs and expectations that depend on the personal data The risks and impacts that may arise from retaining or deleting the personal data The business owner should also establish and document the conditions and methods for the destruction of personal data, such as:
The criteria and triggers for deciding when to destroy personal data

The procedures and tools for securely erasing or anonymising personal data The roles and responsibilities for carrying out and overseeing the destruction of personal data The records and reports for verifying and evidencing the destruction of personal data Therefore, retention periods and conditions for the destruction of personal data should be determined by the business owner, as they are in charge of defining and managing the processing of personal data, as well as ensuring its compliance with the law.

最新問題**: 355**
次のどれが、IS 監査の専門家に監査機能を実行するための最適な指示情報源を提供しますか?
A. 監査憲章
B. IT運営委員会
C. 情報セキュリティポリシー
D. 監査のベストプラクティス
Answer: A (メーッセージを残す**)**
The audit charter is the document that defines the purpose, authority and responsibility of the IS audit function. It provides IS audit professionals with the best source of direction for performing audit functions, as it establishes the scope, objectives, reporting lines, independence, accountability and resources of the IS audit function. The IT steering committee is a governance body that oversees the strategic alignment, prioritization and direction of IT initiatives, but it does not provide specific guidance for IS audit functions. The information security policy is a document that defines the rules and principles for protecting information assets in the organization, but it does not cover all aspects of IS audit functions. Audit best practices are general guidelines and recommendations for conducting effective and efficient audits, but they are not binding or authoritative sources of direction for IS audit functions. References: CISA Review Manual (Digital Version) 1, Chapter 1: Information Systems Auditing Process, Section 1.1: Audit Charter.

最新問題**: 356**
継続的インテグレーション/継続的開発 (CI/CD) プロセスは、ソフトウェア障害のリスクを軽減するのにどのように役立ちますか?
A. ソフトウェアバージョンの簡単なロールバック
B. 小さな増分変更
C. 手動マイルストーンの削減
D. 自動ソフトウェアテスト
Answer: B (メーッセージを残す**)**
A continuous integration/continuous development (CI/CD) process helps to reduce software failure risk by enabling smaller incremental changes to the software code, rather than large and infrequent updates12. Smaller incremental changes allow developers to detect and fix errors, bugs, or vulnerabilities more quickly and easily, and to ensure that the software is always in a working state34. Smaller incremental changes also reduce the

complexity and uncertainty of the software development process, and improve the quality and reliability of the software product5.
References
1: What is CI/CD? Continuous integration and continuous delivery explained1 2: 5 CI/CD challenges-and how to solve them | TechBeacon4 3: Continuous Integration vs Continuous Delivery vs Continuous Deployment2 4: 7 CI/CD Challenges & their Must-Know Solutions | BrowserStack3 5: 5 common pitfalls of CI/CD-and how to avoid them | InfoWorld5

最新問題**: 357**
報告された監査問題に対する合意された是正措置のフォローアップをスケジュールする適切な時期を決定する際に、情報システム監査人に最も適したガイドとなるのは次のどれですか。
A. 進捗状況の更新によると、合意されたアクションの実施は順調に進んでいます。
B. 実装から制御操作の証拠を提供するのに十分な時間が経過しています。
C. ビジネス管理は、合意されたアクションの実施をスケジュールどおりに完了しました。
D. 規制当局は検査訪問のタイムラインを発表しました。
Answer: B (メーッセージを残す**)**
This is because the follow-up of agreed corrective actions for reported audit issues should be done after the auditee has had enough time to implement the corrective actions and demonstrate their effectiveness and sustainability. The follow-up audit should not be too soon or too late, but based on a reasonable and realistic timeframe that allows for adequate testing and verification of the control operation12.
Answer A. Progress updates indicate that the implementation of agreed actions is on track. is not the best answer, because progress updates are not sufficient to guide the follow-up audit timing. Progress updates are useful for monitoring and communicating the status and challenges of the corrective actions, but they do not provide conclusive evidence of the control operation. The follow-up audit should be based on actual results and outcomes, not on expectations or projections12.
Answer C. Business management has completed the implementation of agreed actions on schedule. is not the best answer, because the completion of the implementation of agreed actions is not enough to guide the follow-up audit timing. The completion of the implementation only indicates that the auditee has taken the necessary steps to address the audit issues, but it does not guarantee that the corrective actions are effective and sustainable. The follow-up audit should be based on the evaluation and validation of the control operation, not on the completion of the control implementation12.
Answer D. Regulators have announced a timeline for an inspection visit. is not the best answer, because the regulators' inspection visit is not relevant to guide the follow-up audit timing. The regulators' inspection visit is an external factor that may or may not coincide with the internal follow-up audit schedule. The follow-up audit should be based on the

internal audit plan and objectives, not on the external audit requirements or expectations12.

最新問題**: 358**
IS 監査人は、ローカル システムからクラウドへのエンタープライズ リソース プランニング (ERP) の移行を評価しています。
データの責任者は誰なのか
このプロジェクトでの分類は？
A. 情報セキュリティ担当者
B. データベース管理者 (DBA)
C. 情報所有者
D. データアーキテクト
Answer: C (メーッセージを残す**)**
The best option for the question is C, information owner. This is because:
The information owner is the person or entity that has the authority and responsibility for the business processes and functions that collect, use, store, and dispose of data1.
The information owner is accountable for ensuring that the data is handled in compliance with the applicable laws, regulations, policies, and standards, such as the GDPR and the PIPEDA1234.
The information owner is in the best position to determine the purpose and necessity of collecting and retaining data, as well as the risks and benefits associated with it1.
The information owner should consult with other stakeholders, such as the risk manager, the database administrator (DBA), and the privacy manager, to establish and implement appropriate data classification policies and procedures2.
Data classification is the process of organizing data in groups based on their attributes and characteristics, and then assigning class labels that describe a set of attributes that hold true for the corresponding data sets345.
Data classification helps organizations to identify, manage, protect, and understand their data, as well as to comply with modern data privacy regulations345.
Data classification also helps to determine appropriate user access levels, which means defining who can access, modify, share, or delete data based on their roles, responsibilities, and needs345.
Therefore, the information owner should be responsible for the data classification in an ERP migration project from local systems to the cloud (option C), as they have the authority and accountability for the data and its protection.
The other options are not correct because:
The information security officer (option A) is responsible for overseeing and coordinating the security policies and practices of the organization that involve data6. The information security officer should advise and assist the information owner on the best practices and standards for data security, but not determine the data classification.

The database administrator (DBA) (option B) is responsible for installing, configuring, monitoring, maintaining, and improving the performance of databases and data stores that contain data5. The DBA should support the information owner in implementing and enforcing the data classification policies and procedures, but not determine them.
The data architect (option D) is responsible for designing, modeling, and documenting the logical and physical structures of databases and data stores that contain data7. The data architect should collaborate with the information owner in creating and maintaining the data classification schema and metadata, but not determine them.

最新問題**: 359**
高度にセキュリティ保護されたエリアへの訪問者のアクセスを制御する最も効果的な方法はどれですか?
A. 訪問者は許可された人員の同伴が必要です。
B. 訪問者は生体認証を使用する必要があります。
C. 訪問者はセキュリティカメラによってオンラインで監視されます
D. 訪問者はデッドマンドアから入る必要があります。
Answer: A (メーッセージを残す**)**
The most effective control over visitor access to highly secured areas is to require visitors to be escorted by authorized personnel. This control ensures that visitors are supervised at all times and do not enter any restricted or sensitive areas without permission. It also allows authorized personnel to verify the identity, purpose, and clearance of the visitors, and to monitor their behavior and activities. Escorting visitors also reduces the risk of tailgating, piggybacking, or unauthorized duplication of access credentials.
Requiring visitors to use biometric authentication, monitoring visitors online by security cameras, and requiring visitors to enter through dead-man doors are all examples of technical controls that can enhance visitor access control, but they are not as effective as escorting visitors. Biometric authentication can provide a high level of identity verification, but it does not prevent visitors from accessing unauthorized areas or compromising security in other ways. Security cameras can provide a record of visitor movements and actions, but they may not deter or detect security breaches in real time. Dead-man doors can prevent unauthorized entry by requiring two-factor authentication, but they do not ensure that visitors are accompanied by authorized personnel.
References:
ISC Best Practices for Facility Access Control1
Visitor Management Best Practices From Top Organizations2
8 Best Practices for Setting Up a Visitor Management System3

最新問題**: 360**
組織のリスク管理プログラムの有効性を最もよく示すのは次のどれですか?
A. 固有のリスクが排除されます。

B. 残留リスクが最小限に抑えられます。
C. 制御リスクが最小限に抑えられます。
D. 全体的なリスクが定量化されます。
Answer: B (メーッセージを残す**)**
The effectiveness of a risk management program can be measured by how well it reduces the residual risk, which is the risk that remains after applying controls, to an acceptable level. Inherent risk is the risk that exists before applying any controls, and it cannot be eliminated completely. Control risk is the risk that the controls fail to prevent or detect a risk event, and it is a component of residual risk. Overall risk is not a meaningful metric for assessing the effectiveness of a risk management program, as it does not account for the impact and likelihood of different risk events. References: CISA Review Manual (Digital Version), Chapter 1, Section
1.2.2

最新問題**: 361**
ホワイト ボックス テスト方法は、次のどのテスト プロセスに適用できますか?
A. 社交性テスト
B. 統合テスト
C. ユーザー受け入れテスト (UAT)
D. 並列テスト
Answer: B (メーッセージを残す**)**

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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**: 362**
インターネット ファイアウォールの固有のセキュリティ上の弱点により、次のどの攻撃手法が成功しますか?
A. フィッシング
B. 暗号化されたパスワードの辞書攻撃を使用する
C. パケットを傍受してパスワードを表示する
D. サイトに過剰な数のパケットを送りつける
Answer: (解答を表示する**)**

Flooding the site with an excessive number of packets is an attack technique that will succeed because of an inherent security weakness in an Internet firewall. This type of attack is also known as a denial-of-service (DoS) attack or a distributed denial-of-service (DDoS) attack if it involves multiple sources. The aim of this attack is to overwhelm the network bandwidth or the processing capacity of the firewall or the target system, rendering it unable to respond to legitimate requests or perform its normal functions. An Internet firewall is a device or software that monitors and controls incoming and outgoing network traffic based on predefined rules. A firewall can block or allow traffic based on various criteria, such as source address, destination address, port number, protocol type, application type, etc. However, a firewall cannot prevent traffic from reaching its interface or distinguish between legitimate and malicious traffic based on its content or behavior. Therefore, a firewall is vulnerable to flooding attacks that exploit its limited resources.
Phishing is an attack technique that involves sending fraudulent emails or messages that appear to come from legitimate sources, such as banks, government agencies, online services, etc., in order to trick recipients into revealing their personal or financial information, such as passwords, credit card numbers, bank account details, etc., or into clicking on malicious links or attachments that can infect their systems with malware or ransomware.
Phishing does not exploit an inherent security weakness in an Internet firewall, but rather exploits human psychology and social engineering techniques. A firewall cannot prevent phishing emails or messages from reaching their intended targets, unless they contain some identifiable features that can be filtered out by the firewall rules. However, a firewall cannot detect or prevent users from responding to phishing emails or messages or from opening malicious links or attachments. Using a dictionary attack of encrypted passwords is an attack technique that involves trying to guess or crack passwords by using a list of common or likely passwords or by using a brute-force method that tries all possible combinations of characters. This type of attack does not exploit an inherent security weakness in an Internet firewall, but rather exploits weak or poorly chosen passwords or weak encryption algorithms. A firewall cannot prevent a dictionary attack of en crypted passwords, unless it has some mechanisms to detect and block repeated or suspicious login attempts or to enforce strong password policies. However, a firewall cannot protect passwords from being stolen or intercepted by other means, such as phishing, malware, keylogging, etc. Intercepting packets and viewing passwords is an attack technique that involves capturing and analyzing network traffic that contains sensitive information, such as passwords, credit card numbers, bank account details, etc., in order to use them for malicious purposes. This type of attack does not exploit an inherent security weakness in an Internet firewall, but rather exploits insecure or unencrypted network communication protocols or channels. A firewall cannot prevent packets from being intercepted and viewed by unauthorized parties, unless it has some mechanisms to encrypt or obfuscate the network traffic or to authenticate the source and destination of the traffic. However, a firewall cannot protect packets from being modified or tampered with by other means, such

as man-in-the- middle attacks, replay attacks, etc. References: ISACA CISA Review Manual 27th Edition, page 300

最新問題**: 363**
データセンター内の情報資産をベンダーによる盗難から保護するために最も効果的なのは次のどれですか?
A. ベンダーの活動を監視および制限する
B. ベンダーにアクセス カードを発行します。
C. データデバイスと情報ラベルを隠す
D. ポータブルデバイスおよびワイヤレスデバイスの使用を制限します。
Answer: A (メーッセージを残す**)**
The most effective control to protect information assets in a data center from theft by a vendor is to monitor and restrict vendor activities. A vendor may have legitimate access to the data center for maintenance or support purposes, but they may also have malicious intentions or be compromised by an attacker. By monitoring and restricting vendor activities, the organization can ensure that the vendor only performs authorized tasks and does not access or tamper with sensitive data or equipment. Issuing an access card to the vendor, concealing data devices and information labels, and restricting use of portable and wireless devices are also useful controls, but they are not as effective as monitoring and restricting vendor activities in preventing theft by a vendor. References:
* CISA Review Manual, 27th Edition, page 3381
* CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

最新問題**: 364**
組織がクラスタリングを使用する最も適切な理由はどれですか?
A. システムの応答時間を短縮する
B. 回復時間目標 RTO）を改善する
C. バックアップを高速化するため
D. システムの回復力を向上させる
Answer: (解答を表示する**)**
Clustering is a technique that groups multiple servers or nodes together to act as one system, providing high availability, scalability, and load balancing for applications or services. Clustering can improve system resiliency, which is the ability of a system to withstand or recover from failures or disruptions without compromising its functionality or performance. Clustering can achieve this by providing redundancy and fault tolerance for critical components or processes, enabling automatic failover and recovery in case of node failures, distributing workload among multiple nodes to avoid overloading or bottlenecks, and allowing dynamic addition or removal of nodes to meet changing demand or capacity needs. Clustering may also decrease system response time by improving performance and efficiency through load balancing and parallel processing, but this is not its primary purpose. Clustering may facilitate faster backups by enabling concurrent backup

operations across multiple nodes, but this is not its main benefit. Clustering may improve the recovery time objective (RTO), which is the maximum acceptable time for restoring a system or service after a disruption, by reducing the downtime and data loss caused by failures, but this is not the best reason for using clustering, as there may be other factors that affect the RTO, such as backup frequency, recovery procedures, and testing methods.

最新問題**: 365**
適切なデータ分類を効果的に実装することによる主な利点は次のどれですか?
A. 機密データに対するビジネスリスクの管理
B. 機密データの精度の向上
C. ビジネス要件を満たす能力
D. 機密データが暗号化されていることの保証
Answer: A (メーッセージを残す**)**

最新問題**: 366**
データ ウェアハウス (DW) 管理において、ソース システムからの変更によって発生するデータ品質の問題を防ぐ最善の方法は何ですか?
A. データ品質アラートを設定して、データ ウェアハウスとソース システム間の差異をチェックします。
B. 2つのシステム間の抽出/転送/ロード(ETL)プロセスの変更には承認が必要
C. データウェアハウスを影響分析に含める または ソースシステムの変更を含める）
D. 2つのシステム間の抽出/転送/ロード(ETL)プロセスの変更へのアクセスを制限する
Answer: C (メーッセージを残す**)**
Including the data warehouse in the impact analysis for any changes in the source system is the best way to prevent data quality issues caused by changes from a source system. A data warehouse is a centralized repository of integrated data from one or more source systems. An impact analysis is a technique of assessing the potential effects and consequences of a change on the existing system or environment. Including the data warehouse in the impact analysis can help to identify and mitigate any data quality issues that may arise from changes in the source system, such as data inconsistency, incompleteness, or inaccuracy. The other options are less effective ways to prevent data quality issues, as they may involve data quality alerts, approval for changes, or access restrictions. References:
* CISA Review Manual (Digital Version), Chapter 5, Section 5.41
* CISA Review Questions, Answers & Explanations Database, Question ID 226

最新問題**: 367**
自動化されたインターフェースを介して 2 つのシステム間の毎日のデータ フローを監査し、それが完全かつ正確であることを確認する場合、最も適切なテスト アプローチは次のどれですか。

A. インターフェースに適用されている暗号化標準がベストプラクティスに準拠していることを確認します。
B. インターフェース構成とシステムの出力例を検査します。
C. 25 日間のサンプルについて 2 つのシステム間のデータ調整を実行します。
D. 両システムのコードレビューを実施し、設計ドキュメントを検査します。
Answer: C (メーッセージを残す)
The most appropriate testing approach when auditing a daily data flow between two systems via an automated interface is to perform data reconciliation between the two systems for a sample of 25 days. Data reconciliation is a process of verifying that the data transferred from one system to another is complete and accurate, and that there are no discrepancies or errors in the data flow1. Data reconciliation can be performed by using generalized audit software, which is a type of computer-assisted audit technique (CAAT) that allows the IS auditor to perform various audit tasks on the data stored in different file formats and databases2. By performing data reconciliation for a sample of 25 days, the IS auditor can test the reliability and consistency of the data flow over a reasonable period of time, and identify any potential issues or anomalies that could affect the quality of the data or the functionality of the systems.
References
1: Data Flow Testing - GeeksforGeeks 2: Generalized Audit Software (GAS) - ISACA

最新問題**: 368**
監査フレームワークは、次の方法で IS 監査機能を支援します。
A. IS 監査機能の権限と責任を定義します。
B. 監査プログラムの実行方法の詳細を提供します。
C. 監査の実施に関する指示と情報を提供します。
D. 監査を完了するために必要な具体的な手順の概要
Answer: C (メーッセージを残す)
Audit frameworks can assist the IS audit function by providing direction and information regarding the performance of audits. Audit frameworks are sets of standards, guidelines, and best practices that help IS auditors plan, conduct, and report on their audit engagements. Audit frameworks can help IS auditors ensure the quality, consistency, and professionalism of their audit work, as well as comply with the expectations and requirements of the stakeholders and regulators. Audit frameworks can also help IS auditors address the specific challenges and risks of auditing information systems and technology.
Defining the authority and responsibility of the IS audit function is not a way that audit frameworks can assist the IS audit function, but rather a way that the IS audit charter can assist the IS audit function. The IS audit charter is a document that defines the purpose, scope, objectives, and authority of the IS audit function within the organization. The IS

audit charter can help IS auditors establish their role and position in relation to other functions and departments, as well as clarify their rights and obligations.
Providing details on how to execute the audit program is not a way that audit frameworks can assist the IS audit function, but rather a way that the audit methodology can assist the IS audit function. The audit methodology is a set of procedures and techniques that guide IS auditors in performing their audit tasks and activities. The audit methodology can help IS auditors apply a systematic and structured approach to their audit work, as well as use appropriate tools and methods to collect and analyze evidence.
Outlining the specific steps needed to complete audits is not a way that audit frameworks can assist the IS audit function, but rather a way that the audit plan can assist the IS audit function. The audit plan is a document that describes the scope, objectives, timeline, resources, and deliverables of a specific audit engagement. The audit plan can help IS auditors organize and manage their audit work, as well as communicate their expectations and responsibilities to the auditees.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019, p. 51 1
* Understanding Project Audit Frameworks - Wolters Kluwer 2
* How to Implement a Robust Audit Framework - Insights - Metricstream 3
* What Is The Internal Audit Function? An Accurate Definition Of The

最新問題**: 369**
不正なログオンを防止する最も信頼性の高い方法はどれですか?
A. 認証トークンの発行
B. 現在のセキュリティポリシーの強化
C. 営業時間外の使用を制限する
D. 自動パスワードジェネレータのインストール
Answer: A (メーッセージを残す**)**
Issuing authentication tokens is the most reliable method of preventing unauthorized logon, as it provides a strong form of authentication that requires users to present something they have (the token) and something they know (the personal identification number or PIN) to access the system. Authentication tokens are physical devices that generate a one-time password or code that changes periodically and is synchronized with the authentication server. This makes it difficult for attackers to steal or guess the credentials of legitimate users. Reinforcing current security policies, limiting after-hours usage and installing an automatic password generator are not as reliable as issuing authentication tokens, as they do not provide a strong form of authentication and may still be vulnerable to unauthorized logon attempts. References:
* : [Authentication Token Definition]
* : Authentication | ISACA

最新問題**: 370**

組織が緊急の変更を適切かつ透明性を持って処理していることを IS 監査人に示す最良の方法はどれですか?
A. 特別なログオン ID は、プログラマーに実稼働環境への永続的なアクセスを許可するために使用されます。
B. 緊急の変更は、実稼働ライブラリにすぐに適用されます。
C. アプリケーション操作マニュアルには、緊急修正によってシステムの整合性が損なわれないようにするための手順が記載されています。
D. 変更管理コントロールは遡及的に適用されます。
Answer: C (メーッセージを残す)

最新問題**: 371**
IS 監査人は、ビジネス経費請求システム内での不正を防止するプロセスを確認する任務を負っています。この確認に関与させるのに最も重要な関係者は次のうちどれですか。
A. 情報セキュリティ管理者
B. 品質保証（QA）マネージャー
C. 事業部幹部
D. ビジネスプロセスオーナー
Answer: D (メーッセージを残す)
The business process owner is the most important stakeholder to involve in the review of the processes that prevent fraud within a business expense claim system. This is because the business process owner is responsible for defining, implementing, and monitoring the business rules and policies that govern the expense claim process. The business process owner also has the authority and accountability to approve or reject expense claims, as well as to investigate and report any suspicious or fraudulent activities. The business process owner can provide valuable insights and feedback to the IS auditor on the effectiveness and efficiency of the current processes, as well as the potential risks and controls that need to be addressed12.
The information security manager is not the most important stakeholder because their role is mainly focused on ensuring the confidentiality, integrity, and availability of the information systems and data that support the expense claim process. The information security manager can help the IS auditor with assessing the technical aspects of the system, such as access controls, encryption, logging, and backup, but they may not have sufficient knowledge or authority over the business rules and policies that prevent fraud1.
The quality assurance (QA) manager is not the most important stakeholder because their role is mainly focused on ensuring the quality and reliability of the software applications and systems that support the expense claim process. The QA manager can help the IS auditor with testing and verifying the functionality and performance of the system, but they may not have sufficient knowledge or authority over the business rules and policies that prevent fraud1.

The business department executive is not the most important stakeholder because their role is mainly focused on overseeing the strategic objectives and financial performance of the business department that uses the expense claim system. The business department executive can help the IS auditor with understanding the business context and needs of the expense claim process, but they may not have sufficient knowledge or authority over the operational details and controls that prevent fraud

最新問題**: 372**
次の監査手順のうち、アプリケーション プログラムが設計どおりに機能していることを最も確実に保証できるのはどれですか。
A. 継続的監査モジュールの使用
B. 経営幹部へのインタビュー
C. アカウントの確認
D. プログラムドキュメントの確認
Answer: A (メーッセージを残す**)**
Using a continuous auditing module is an audit procedure that would provide the best assurance that an application program is functioning as designed. A continuous auditing module is a software tool that performs automated and continuous testing and monitoring of an application program's inputs, outputs, processes, and controls. A continuous auditing module can help to verify the accuracy, completeness, validity, reliability, and timeliness of the application program's data and transactions. A continuous auditing module can also help to identify and report any errors, anomalies, deviations, or exceptions in the application program's performance or compliance.
The other options are not as effective or relevant as using a continuous auditing module for providing assurance that an application program is functioning as designed. Interviewing business management is a technique for obtaining information and opinions from the users or owners of the application program, but it does not directly test or verify the functionality or quality of the application program. Confirming accounts is a technique for verifying the existence and accuracy of account balances or transactions, but it does not necessarily reflect the design or operation of the application program. Reviewing program documentation is a technique for examining the specifications, requirements, and procedures of the application program, but it does not provide evidence of the actual implementation or execution of the application program.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019, p. 2361
* Continuous audit and monitoring - PwC2

最新問題**: 373**
ネットワークアクティビティを監視するサードパーティのサービスプロバイダーの IS 監査を計画する場合、最初のステップは次のどれですか?
A. サードパーティの監視ログとインシデント処理を確認する

B. サードパーティプロバイダーの役割と責任を確認する
C. 組織のサードパーティ監視プロセスを評価する
D. 組織がプロバイダーと安全な接続を確立しているかどうかを確認します
Answer: (解答を表示する**)**
The first step when planning an IS audit of a third-party service provider that monitors network activities is to review the roles and responsibilities of the third-party provider. This will help to establish the scope, objectives, and expectations of the audit, as well as to identify any potential risks, issues, or gaps in the service level agreement (SLA) between the organization and the provider. Reviewing the third party's monitoring logs and incident handling, evaluating the organization's third-party monitoring process, and determining if the organization has a secure connection to the provider are important steps, but they should be performed after reviewing the roles and responsibilities of the provider.
References: CISA Review Manual (Digital Version)1, page 269.

最新問題**: 374**
IT 戦略文書をレビューする IS 監査人にとって、最も懸念されるのは次のどれでしょうか?
A. ターゲット アーキテクチャは技術レベルで定義されます。
B. 前年度の IT 戦略目標は達成されませんでした。
C. 戦略的な IT 目標は、最新の市場動向からのみ導き出されます。
D. 新しい取り組みの財務見積りが文書内で公開されます。
Answer: (解答を表示する**)**
The most concerning thing for an IS auditor reviewing an IT strategy document is that the strategic IT goals are derived solely from the latest market trends. An IT strategy document is a blueprint that defines how an organization will use technology to achieve its goals. It should be based on a thorough analysis of the organization's internal and external factors, such as its vision, mission, values, objectives, strengths, weaknesses, opportunities, threats, customers, competitors, regulations, and industry standards. An IT strategy document should also align with the organization's business strategy and reflect its unique needs and capabilities. If an IT strategy document is derived solely from the latest market trends, it may not be relevant or appropriate for the organization's specific situation. It may also lack coherence, consistency, feasibility, or sustainability.
The other options are not as concerning as option C. Target architecture is defined at a technical level is not a concern for an IS auditor reviewing an IT strategy document. Target architecture is the desired state of an organization's IT systems in terms of their structure, functionality, performance, security, interoperability, and integration. Defining target architecture at a technical level can help an IS auditor to understand how the organization plans to achieve its strategic IT goals and what technical requirements and standards it needs to follow. The previous year's IT strategic goals were not achieved is not a concern for an IS auditor reviewing an IT strategy document. The previous year's IT strategic goals are the outcomes that the organization intended to accomplish with its IT initiatives in the

past year. Not achieving these goals may indicate some challenges or gaps in the organization's IT performance or execution. However, this does not necessarily affect the quality or validity of the current IT strategy document. An IS auditor should focus on evaluating whether the current IT strategy document is realistic, measurable, achievable, relevant, and time-bound.
Financial estimates of new initiatives are disclosed within the document is not a concern for an IS auditor reviewing an IT strategy document. Financial estimates are projections of the costs and benefits of new initiatives that are part of the IT strategy document. Disclosing financial estimates within the document can help an IS auditor to assess whether the new initiatives are aligned with the organization's budget and resources and whether they provide value for money. References: IT Strategy Template for a Successful Strategic Plan | Gartner, Definitive Guide to Developing an IT Strategy and Roadmap - CioPages, An Example of a Well-Developed IT Strategy Plan - Resolute

最新問題**: 375**
エンタープライズ暗号化インフラストラクチャを構築またはアップグレードする場合、成長するビジネス環境にとって最も重要な要件は次のどれですか?
A. サービス検出
B. スケーラブルなアーキテクチャとシステム
C. バックアップと復元機能
D. ネットワークスロットリング
Answer: (解答を表示する**)**

最新問題**: 376**
レビュー中に、情報システム監査人は、企業ユーザーがインターネットに接続された任意の Web ブラウザーからクラウドベースのアプリケーションやデータにアクセスできることを発見しました。不正アクセスを防止するための監査人の最善の推奨事項は次のどれですか。
A. 侵入検知システム (IDS) を実装する。
B. セキュリティ ポリシーと手順を更新します。
C. 多要素認証を実装します。
D. すべてのコンピューティング デバイスで強力なマルウェア対策制御を活用します。
Answer: C (メーッセージを残す**)**
The best recommendation to prevent unauthorized access to cloud-based applications and data is to implement multi-factor authentication (MFA). MFA is a method of verifying the identity of a user by requiring two or more pieces of evidence, such as a password, a code sent to a phone, or a biometric factor. MFA adds an extra layer of security to prevent unauthorized access, even if the user's password is compromised or stolen. MFA can also help comply with data privacy and security regulations, such as the General Data

Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA).
The other options are not as effective as MFA in preventing unauthorized access. An intrusion detection system (IDS) is a tool that monitors network traffic and alerts administrators of suspicious or malicious activity, but it does not prevent access by itself. Updating security policies and procedures is a good practice, but it does not ensure that users follow them or that they are enforced. Utilizing strong anti-malware controls on all computing devices can help protect against malware infections, but it does not prevent users from accessing cloud-based applications and data from any Internet-connected web browser.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019, p. 2471
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription2
* What Is Cloud Security? | Google Cloud3
* 5 Cloud Application Security Best Practices | Snyk4

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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: **377**
データ漏洩を防ぐために、組織の BYOD (個人所有デバイスの持ち込み) ポリシーに含めるべき最良の推奨事項は次のどれですか?
A. 従業員に BYOD デバイス上のデータに関するプライバシー権を放棄するよう要求します。
B. BYODデバイスに多要素認証を要求する。
C. 紛失または盗難にあった BYOD デバイスを報告する従業員の責任を指定します。
D. 登録された BYOD デバイスのみがネットワークにアクセスできるようにします。
Answer: (解答を表示する**)**
The best recommendation to include in an organization's bring your own device (BYOD) policy to help prevent data leakage is to require multi-factor authentication on BYOD devices. BYOD is a practice that allows employees to use their own personal devices, such as smartphones, tablets, or laptops, to access the organization's network, data, and systems. Data leakage is a risk that involves the unauthorized or accidental disclosure or

transfer of sensitive or confidential data from the organization to external parties or devices.
Multi-factor authentication is a security measure that requires users to provide two or more pieces of evidence to verify their identity and access rights, such as passwords, tokens, biometrics, or codes. Multi-factor authentication can help prevent data leakage by reducing the likelihood of unauthorized access to the organization's data and systems through BYOD devices, especially if they are lost, stolen, or compromised. The other options are not as effective as requiring multi-factor authentication on BYOD devices, because they either do not prevent data leakage directly, or they are reactive rather than proactive measures. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.3

最新問題: **378**
IS 監査人が特定のベンダーの買掛金取引のサンプルを分析し、平均取引の 5 倍の値を持つ 1 つの取引を特定しました。監査人が次に行うべきことは何ですか。
A. 差異を直ちに監査委員会に報告する
B. 監査対象者に差異の説明を求める
C. サンプルサイズを母集団の100%に増やす
D. サンプル集団から取引を除外する
Answer: (解答を表示する**)**
An IS auditor is analyzing a sample of accounts payable transactions for a specific vendor and identifies one transaction with a value five times as high as the average transaction. The next step that the auditor should do is to request an explanation of the variance from the auditee. This is because the variance may indicate an error, fraud, or an unusual but legitimate transaction that requires further investigation. The auditor should not report the variance immediately to the audit committee without verifying its cause and significance. The auditor should not increase the sample size to 100% of the population without considering the cost-benefit analysis and the sampling methodology. The auditor should not exclude the transaction from the sample population without justification, as it may affect the validity and reliability of the audit results. References:
CISA Review Manual (Digital Version), [ISACA Auditing Standards]

最新問題: **379**
大規模な金融機関に対する継続的な監査に最適なプロセスは次のどれでしょうか?
A. 災害復旧システムにおける暗号化標準のテスト
B. リアルタイムデータシステムのアクセス制御の検証
C. システム間の並列テストの実行
D. ヘルプデスク指標のパフォーマンスの検証
Answer: B (メーッセージを残す**)**
The best process for continuous auditing for a large financial institution is validating access controls for real- time data systems. This is because access controls are critical for ensuring the confidentiality, integrity, and availability of the financial data that is processed

and transmitted by the real-time data systems. Real-time data systems are systems that provide timely and accurate information to support decision-making and transactions in a dynamic and complex environment. Examples of real-time data systems in the financial sector include payment systems, trading platforms, risk management systems, and fraud detection systems.
Continuous auditing of access controls can help detect and prevent unauthorized access, data leakage, data manipulation, or data loss that could compromise the security, reliability, or compliance of the real-time data systems.
Testing encryption standards on the disaster recovery system is not the best process for continuous auditing for a large financial institution. Encryption standards are important for protecting the data stored or transmitted by the disaster recovery system, which is a system that provides backup and recovery capabilities in case of a disruption or disaster. However, testing encryption standards is not a continuous process, but rather a periodic or event-driven process that can be performed as part of the disaster recovery plan testing or validation.
Performing parallel testing between systems is not the best process for continuous auditing for a large financial institution. Parallel testing is a process of comparing the results of two or more systems that perform the same function or task, such as a new system and an old system, or a primary system and a backup system.
Parallel testing can help verify the accuracy, consistency, and compatibility of the systems. However, parallel testing is not a continuous process, but rather a temporary or transitional process that can be performed as part of the system implementation or migration.
Validating performance of help desk metrics is not the best process for continuous auditing for a large financial institution. Help desk metrics are indicators that measure the efficiency, effectiveness, and quality of the help desk service, which is a service that provides technical support and assistance to the users of information systems and technology. Help desk metrics can include metrics such as response time, resolution time, customer satisfaction, and service level agreement (SLA) compliance. Validating performance of help desk metrics can help evaluate and improve the help desk service. However, validating performance of help desk metrics is not a continuous auditing process, but rather a continuous monitoring process that can be performed by the help desk management or quality assurance team.
References:
* All eyes on: Continuous auditing - KPMG Global 1
* Internal audit's role at financial institutions: PwC 2
* The Fed - Supervisory Policy and Guidance Topics - Large Banking ... 3
* Continuous Audit: Definition, Steps, Advantages and Disadvantages 4

最新問題: 380
予期せぬ電力増加の影響を受けやすい地域では、次のうちどれが最も効果的にシステムを保護しますか?

A. 電圧レギュレータ
B. ジェネレータ
C. 代替電源ライン
D. サーキットブレーカー
Answer: (解答を表示する**)**

最新問題**: 381**
エンドユーザー コンピューティング (EUC) における複雑な計算の意図しない変更に関連するリスクを軽減するための最良の方法はどれですか?
A. 独立した第三者にソース計算をレビューしてもらう
B. 安全なライブラリから EUC プログラムのコピーを実行する
C. 複雑なパスワード制御を実装する
D. 手動計算によるEUC結果の検証
Answer: B (メーッセージを残す**)**
The best way to mitigate the risk associated with unintentional modifications of complex calculations in end- user computing (EUC) is to execute copies of EUC programs out of a secure library. This will ensure that the original EUC programs are protected from unauthorized changes and that the copies are run in a controlled environment. A secure library is a repository of EUC programs that have been tested, validated, and approved by the appropriate authority. Executing copies of EUC programs out of a secure library can also help with version control, backup, and recovery of EUC programs. Having an independent party review the source calculations, implementing complex password controls, and verifying EUC results through manual calculations are not as effective as executing copies of EUC programs out of a secure library, as they do not prevent or detect unintentional modifications of complex calculations in EUC. References: End-User Computing (EUC) Risks: A Comprehensive Guide, End User Computing (EUC) Risk Management

最新問題**: 382**
IS 監査人がアウトソーシングされたヘルプデスクのサービス管理をレビューしています。サービス プロバイダーがこの機能をどのように効果的に実行しているかを示す最適な指標は次のどれですか。
A. 処理された通話数
B. 通話記録のレビュー
C. チケットの平均年齢
D. 顧客満足度評価
Answer: D (メーッセージを残す**)**

最新問題**: 383**

ネットワーク デバイス管理を監査する際に、IS 監査人が検証する必要がある最も重要な項目は次のどれですか。
A. サービス アカウントを通じてデバイスにアクセスすることはできません。
B. バックアップ ポリシーにはデバイス構成ファイルが含まれます。
C. すべてのデバイスに最新のセキュリティ パッチが適用されています。
D. すべてのデバイスは保護されたネットワーク セグメント内に配置されています。
Answer: (解答を表示する**)**
The most important thing for an IS auditor to validate when auditing network device management is that all devices have current security patches assessed. This is because security patches are essential for fixing known vulnerabilities and preventing unauthorized access, data breaches, or denial-of-service attacks on the network devices. If the network devices are not patched regularly, they may expose the network to various cyber threats and compromise the confidentiality, integrity, and availability of the network services and data12.
Devices cannot be accessed through service accounts is not the most important thing to validate because service accounts are typically used for automated tasks or processes that require privileged access to network devices. Service accounts can be secured by using strong passwords, limiting their permissions, and monitoring their activities. However, service accounts alone do not protect the network devices from external or internal attacks that exploit unpatched vulnerabilities3.
Backup policies include device configuration files is not the most important thing to validate because backup policies are mainly used for restoring the network devices in case of failure, disaster, or corruption. Backup policies can help with recovering the network functionality and data, but they do not prevent the network devices from being compromised or attacked in the first place. Backup policies should be complemented by security policies that ensure the network devices are patched and protected4.
All devices are located within a protected network segment is not the most important thing to validate because network segmentation is a technique that divides the network into smaller subnets or zones based on different criteria, such as function, security level, or access control. Network segmentation can help isolate and contain the impact of a potential attack on a network device, but it does not prevent the attack from happening. Network segmentation should be combined with security patching and other security measures to ensure the network devices are secure.

最新問題**: 384**
物理的な破壊が現実的でない場合、ハードディスク上の機密データを処分する最も効果的な手段は次のどれですか?
A. 複数回上書きする
B. ディスクの暗号化
C. 再フォーマット

D. ファイルを順番に削除する
Answer: A (メーッセージを残す**)**
The correct answer is A. Overwriting multiple times. Overwriting is a method of securely erasing data from a hard disk by replacing the existing data with random or meaningless data, making it difficult or impossible to recover the original data1. Overwriting multiple times, also known as multiple-pass overwriting, is a more effective way of disposing of sensitive data than overwriting once, as it reduces the possibility of residual traces of data that could be recovered by advanced techniques2. Overwriting multiple times can be done by using specialized software tools that follow certain standards or algorithms, such as the US Department of Defense's DoD 5220.22-M or the Gutmann method3.

最新問題**: 385**
次のどれがハッカーによる攻撃のリスクに対して最も効果的でしょうか?
A. トンネリング
B. 暗号化
C. メッセージの検証
D. ファイアウォール
Answer: B (メーッセージを残す**)**
The best guard against the risk of attack by hackers is encryption. Encryption is the process of transforming data into an unreadable format using a secret key or algorithm. Encryption can protect data in transit and at rest from unauthorized access, modification, or disclosure by hackers. Encryption can also ensure the authenticity and integrity of data by using digital signatures or hashes.
Tunneling, message validation, and firewalls are not the best guards against the risk of attack by hackers.
Tunneling is a technique that encapsulates one network protocol within another to create a secure connection between two endpoints. Message validation is a process that verifies the format, content, and origin of a message before accepting it. Firewalls are devices or software that filter network traffic based on predefined rules. These controls may help reduce the exposure or impact of hacker attacks, but they do not provide the same level of protection as encryption.

最新問題**: 386**
IS 監査人が社内ソフトウェア開発ソリューションのリリース管理プロセスをレビューしています。ソフトウェア バージョンが本番環境と同じになる可能性が最も高いのはどの環境ですか?
A. ステージング
B. テスト
C. 統合
D. 開発
Answer: (解答を表示する**)**

A staging environment is a replica of the production environment that is used to test and verify software before deploying it to production. A staging environment is most likely to have the same software version as production, as it mimics the real-world conditions and configurations that will be encountered in production.
A testing environment is a separate environment that is used to perform various types of testing on software, such as functional testing, performance testing, security testing, etc. A testing environment may not have the same software version as production, as it may undergo frequent changes or updates based on testing results or feedback. An integration environment is a separate environment that is used to combine and test software components or modules from different developers or sources, to ensure that they work together as expected.
An integration environment may not have the same software version as production, as it may involve different versions or branches of software from different sources. A development environment is a separate environment that is used by developers to create and modify software code. A development environment may not have the same software version as production, as it may contain unfinished or untested code that has not been released yet.

最新問題**: 387**
サイバー攻撃が発生したときに、拡散のリスクを軽減できるセキュリティ対策は次のどれですか?
A. データ損失防止 (DLP) システム
B. ネットワークセグメンテーション
C. 境界ファイアウォール
D. Web アプリケーション ファイアウォール (WAF)
Answer: B (メーッセージを残す**)**

最新問題**: 388**
脆弱性スキャンが侵入テストよりも優れている最大の利点は次のどれですか?
A. テストでは偽陽性結果の数が少なくなります
B. ネットワーク帯域幅がより効率的に利用される
C. カスタム開発されたアプリケーションをより正確にテストできます
D. テストプロセスを自動化して、大規模な資産グループをカバーできます。
Answer: D (メーッセージを残す**)**
The greatest advantage of vulnerability scanning over penetration testing is that the testing process can be automated to cover large groups of assets. Vulnerability scanning is an automated, high-level security test that reports its findings of known vulnerabilities in systems, networks, applications, and devices. Vulnerability scanning can be performed frequently, quickly, and efficiently to scan a large number of assets and identify potential weaknesses that need to be addressed. Vulnerability scanning can also help organizations comply with security standards and regulations, such as PCI DSS1.

The other options are not as advantageous as option D, as they may not reflect the true benefits or limitations of vulnerability scanning compared to penetration testing. The testing produces a lower number of false positive results, but this is not necessarily true, as vulnerability scanning may report vulnerabilities that are not exploitable or relevant in the context of the organization. Network bandwidth is utilized more efficiently, but this may not be a significant advantage, as vulnerability scanning may still consume considerable network resources depending on the scope and frequency of the scans. Custom-developed applications can be tested more accurately, but this is also not true, as vulnerability scanning may not be able to detect complex or unknown vulnerabilities that require manual analysis or exploitation.
References:
* 1: Vulnerability scanning vs penetration testing: What's the difference? | TechRepublic
* 2: Vulnerability Scanning vs. Penetration Testing - Fortinet
* 3: Penetration Test Vs Vulnerability Scan | Digital Defense
* 4: Penetration Testing vs. Vulnerability Scanning: What's the difference?
* 5: Penetration Testing vs. Vulnerability Scanning | Secureworks
* 6: PCI DSS Quick Reference Guide - PCI Security Standards Council

最新問題**: 389**
監査レポートをプロジェクト運営委員会に発行する前に、最初に評価する必要があるのは誰ですか?
A. プロジェクトスポンサー
B. 監査委員会
C. IS監査マネージャー
D. ビジネスオーナー
Answer: C (メーッセージを残す**)**

最新問題**: 390**
ファイアウォール ルール内で有効にした場合、次のサービスのうちどれが最も大きなリスクをもたらすでしょうか?
A. 簡易メール転送プロトコル (SMTP)
B. シンプル オブジェクト アクセス プロトコル (SOAP)
C. ハイパーテキスト転送プロトコル (HTTP)
D. ファイル転送プロトコル (FTP)
Answer: D (メーッセージを残す**)**
File transfer protocol (FTP) is a service that allows users to transfer files between computers over a network.
If enabled within firewall rules, FTP would present the greatest risk, as it can expose sensitive data to unauthorized access, modification, or deletion. FTP does not provide encryption or authentication, which makes it vulnerable to eavesdropping, spoofing, and tampering attacks. Simple mail transfer protocol (SMTP), simple object access protocol

(SOAP), and hypertext transfer protocol (HTTP) are also services that can be used to exchange data over a network, but they have more security features than FTP, such as encryption, authentication, or validation. References: CISA Review Manual (Digital Version)

最新問題: **391**
組織の過去四半期の IT プロセス パフォーマンス レポートを確認する IS 監査人にとって、最も懸念すべき事項は次のどれですか。
A. 指標が業界ベンチマークと一致していない
B. 利害関係者のレビューなしに指標が定義された
C. 主要業績評価指標 (KPI) はわずか 1 か月で達成されました
D. パフォーマンスレポートには専門用語が多すぎる
Answer: C (メーッセージを残す**)**

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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: **392**
アプリケーション プログラミング インターフェイス (API) 統合実装に関連する盗聴のリスクを軽減するための、情報システム監査人の最善の推奨事項は次のどれですか。
A. API エンドポイントをマスクします。
B. Simple Object Access Protocol (SOAP) を実装します。
C. 拡張マークアップ言語 (XML) ファイルを暗号化します。
D. トランスポート層セキュリティ (TLS) を実装します。
Answer: D (メーッセージを残す**)**

最新問題: **393**
サードパーティのサービスプロバイダーの情報セキュリティ管理が有効であることを示す最良の証拠は次のどれですか?
A. サービスプロバイダーの外部監査人によるコントロールの監査レポート
B. サービスプロバイダーのセキュリティ構成管理のドキュメント
C. サービスプロバイダーの情報セキュリティ担当者とのインタビュー
D. サービスプロバイダーのポリシーと手順のレビュー
Answer: A (メーッセージを残す**)**

An audit report of the controls by the service provider's external auditor provides the best evidence that a third-party service provider's information security controls are effective. An external auditor is an independent and objective party that can assess the design and operating effectiveness of the service provider' s information security controls based on established standards and criteria. An external auditor can also provide an opinion on the adequacy and compliance of the service provider's information security controls, as well as recommendations for improvement.
Documentation of the service provider's security configuration controls is a source of evidence that a third- party service provider's information security controls are effective, but it is not the best evidence.
Documentation of the security configuration controls can show the settings and parameters of the service provider's information systems and networks, but it may not reflect the actual implementation and operation of the controls. Documentation of the security configuration controls may also be outdated, incomplete, or in accurate.
An interview with the service provider's information security officer is a source of evidence that a third-party service provider's information security controls are effective, but it is not the best evidence. An interview with the information security officer can provide insights into the service provider's information security strategy, policies, and procedures, but it may not verify the actual performance and compliance of the information security controls. An interview with the information security officer may also be biased, subjective, or misleading.
A review of the service provider's policies and procedures is a source of evidence that a third-party service provider's information security controls are effective, but it is not the best evidence. A review of the policies and procedures can show the service provider's information security objectives, requirements, and guidelines, but it may not demonstrate the actual execution and enforcement of the information security controls. A review of the policies and procedures may also be insufficient, inconsistent, or outdated.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019, p. 284
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

最新問題: **394**
監査観察を修正するために合意された経営対応のフォローアップ活動をスケジュールする際に、情報システム監査人が最も考慮すべき事項は次のどれですか?
A. 修復による事業中断
B. IT予算の制約
C. 責任あるIT担当者の可用性
D. 元の調査結果のリスク評価
Answer: D (メーッセージを残す)

The most important consideration for an IS auditor when scheduling follow-up activities for agreed-upon management responses to remediate audit observations is the risk rating of original findings. The risk rating of original findings is an assessment of the potential impact or likelihood of an audit issue or observation on the organization's objectives, operations, or reputation. The risk rating of original findings can help determine the priority and urgency of follow-up activities for agreed-upon management responses to remediate audit observations by ensuring that high-risk issues are addressed first and more frequently than low-risk issues.
The other options are not as important as the risk rating of original findings in scheduling follow-up activities for agreed-upon management responses to remediate audit observations, as they do not reflect the significance or severity of audit issues or observations. Business interruption due to remediation is a possible consequence of implementing corrective actions to address audit issues or observations, but it does not indicate the priority or urgency of follow-up activities. IT budgeting constraints is a possible factor that may affect the availability or feasibility of resources for implementing corrective actions to address audit issues or observations, but it does not indicate the priority or urgency of follow-up activities. Availability of responsible IT personnel is a possible factor that may affect the accountability or responsiveness of staff for implementing corrective actions to address audit issues or observations, but it does not indicate the priority or urgency of follow-up activities. References: CISA Review Manual (Digital Version), Chapter 2, Section 2.4

最新問題**: 395**
データ品質に関連する IT 管理リスクを受け入れるかどうかの決定は、以下の者が責任を負う必要があります。
A. 情報セキュリティチーム。
B. IS 監査マネージャー。
C. 最高情報責任者 (CIO)。
D. 事業主。
Answer: D (メーッセージを残す**)**
The decision to accept an IT control risk related to data quality should be the responsibility of the business owner. The business owner is the person who has the authority and accountability for the business process that relies on the data quality. The business owner should understand the impact of data quality issues on the business objectives, performance, and compliance. The business owner should also be involved in defining the data quality requirements, assessing the data quality risks, and implementing the data quality controls or mitigation strategies.

最新問題**: 396**

次のどれが最も品質保証 (QA) チームの独立性を危険にさらし、利益相反につながる可能性がありますか?
A. テストの前提とソリューション設計をクロスチェックする
B. 適切なドキュメントを保証するためにコードを検査する
C. テストプロセス中にコーディングエラーを修正する
D. 開発方法論への準拠の確保
Answer: C (メーッセージを残す**)**

最新問題**: 397**
SQL インジェクションの脆弱性に対処するための最善のコントロールは何ですか?
A. Unicode 翻訳
B. セキュア ソケット レイヤー (SSL) 暗号化
C. 入力検証
D. デジタル署名
Answer: C (メーッセージを残す**)**
Input validation is the best control to address SQL injection vulnerabilities, because it can prevent malicious users from entering SQL commands or statements into input fields that are intended for data entry, such as usernames or passwords. SQL injection is a technique that exploits a security vulnerability in an application's software by inserting SQL code into a query string that can execute commands on a database server. Unicode translation, SSL encryption, and digital signatures are not effective controls against SQL injection, because they do not prevent or detect SQL code injection into input fields. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.4.2

最新問題**: 398**
新しいプライバシー法に対する組織の対応を確認する際に、情報システム監査人が最初に評価すべきことは何ですか?
A. 個人情報の収集を制限するための実施計画
B. 同様の要件を含む可能性のある他の国のプライバシー法
C. 法律遵守を達成するための運用計画
D. プライバシーコンポーネントを含むシステムの分析
Answer: D (メーッセージを残す**)**
The first thing that an IS auditor should evaluate when reviewing an organization's response to new privacy legislation is the analysis of systems that contain privacy components. Privacy components are elements of a system that collect, process, store, or transmit personal information that is subject to privacy legislation. An analysis of systems that contain privacy components should identify what types of personal information are involved, where they are located, how they are used, who has access to them, and what risks or threats they face. An analysis of systems that contain privacy components is

essential for determining the scope and impact of the new privacy legislation on the organization's systems and processes.
The other options are not as important as option D. An implementation plan for restricting the collection of personal information is a possible action, but not the first thing to evaluate, when reviewing an organization's response to new privacy legislation. An implementation plan for restricting the collection of personal information is a document that outlines how an organization will comply with the principle of data minimization, which states that personal information should be collected only for specific and legitimate purposes and only to the extent necessary for those purposes. An implementation plan for restricting the collection of personal information should be based on an analysis of systems that contain privacy components. Privacy legislation in other countries that may contain similar requirements is a possible source of reference, but not the first thing to evaluate, when reviewing an organization's response to new privacy legislation. Privacy legislation in other countries that may contain similar requirements is a set of laws or regulations that governs the protection of personal information in other jurisdictions that may have comparable or compatible standards or expectations as the new privacy legislation. Privacy legislation in other countries that may contain similar requirements may provide guidance or best practices for complying with the new privacy legislation. However, privacy legislation in other countries that may contain similar requirements should not be used as a substitute for an analysis of systems that contain privacy components.
An operational plan for achieving compliance with the legislation is a possible deliverable, but not the first thing to evaluate, when reviewing an organization's response to new privacy legislation. An operational plan for achieving compliance with the legislation is a document that describes how an organization will implement and maintain the necessary policies, procedures, controls, and measures to comply with the new privacy legislation. An operational plan for achieving compliance with the legislation should be derived from an analysis of systems that contain privacy components. References: Privacy law - Wikipedia, Data Protect ion and Privacy Legislation Worldwide | UNCTAD, Data minimization - Wikipedia

最新問題: **399**
IS 監査人がエンタープライズ ガバナンスをレビューしたところ、テクノロジー リスク ガバナンスの組織構造が定義されていないことがわかりました。この構造の欠如に関して最も懸念されるのは次のうちどれですか。
A. ソフトウェア開発者は不適切な技術を採用する可能性があります。
B. プロジェクト マネージャーは、組織のリスク許容度を超えるテクノロジ リスクを受け入れる場合があります。
C. 技術リスクに関する主要な意思決定主体が特定されていない
D. 組織のセキュリティ標準に対する明確な承認機関が存在しません。
Answer: C (メーッセージを残す**)**

The greatest concern with the lack of structure for technology risk governance is C. Key decision-making entities for technology risk have not been identified. Technology risk governance is the process of establishing and maintaining the policies, roles, responsibilities, and accountabilities for managing technology risks within an organization1. Technology risk governance requires a clear organizational structure that defines who has the authority and responsibility to make decisions, set objectives, allocate resources, monitor performance, and ensure compliance for technology risk management2. Without such a structure, an organization may face the following challenges:
Lack of alignment and integration between technology and business strategies, leading to suboptimal outcomes and missed opportunities.
Lack of clarity and consistency in technology risk identification, assessment, mitigation, and reporting, leading to gaps and overlaps in risk coverage and exposure.
Lack of communication and collaboration among different stakeholders involved in technology risk management, leading to conflicts and inefficiencies.
Lack of oversight and accountability for technology risk management activities and results, leading to poor quality and reliability.

最新問題**: 400**
内部ネットワーク上の不正なワイヤレス アクセス ポイントの存在を検出するのに最も効果的なのは次のうちどれですか。
A. 継続的なネットワーク監視
B. 定期的なネットワーク脆弱性評価
C. 電子アクセスログの確認
D. 物理的なセキュリティレビュー
Answer: (解答を表示する**)**
The most effective method for detecting the presence of an unauthorized wireless access point on an internal network is A. Continuous network monitoring. This is because continuous network monitoring can capture and analyze all the wireless traffic in the network and identify any rogue or spoofed devices that may be connected to the network without authorization. Continuous network monitoring can also alert the system administrator of any suspicious or anomalous activities on the network and help to locate and remove the unauthorized wireless access point quickly.
Periodic network vulnerability assessments (B) can also help to detect unauthorized wireless access points, but they are not as effective as continuous network monitoring, because they are performed at fixed intervals and may miss some devices that are added or removed between the assessments. Review of electronic access logs can provide some information about the devices that access the network, but they may not be able to detect devices that use fake or stolen credentials or devices that do not generate any logs.
Physical security reviews (D) can help to prevent unauthorized physical access to the network ports or devices, but they may not be able to detect wireless access points that are hidden or disguised as legitimate devices.

最新問題: **401**
災害復旧計画 (DRP) のテストが成功したかどうかを判断するための最良の方法はどれですか?
A. 事前に設定されたテスト目標が達成されたかどうかを分析します。
B. バックアップ データ センターでテストを実行します。
C. 主要担当者の参加を評価します。
D. オフサイト バックアップ ファイルをテストします。
Answer: A (メーッセージを残す**)**
The best way to determine whether a test of a disaster recovery plan (DRP) was successful is to analyze whether predetermined test objectives were met. Test objectives are specific, measurable, achievable, relevant, and time-bound (SMART) goals that define what the test aims to accomplish and how it will be evaluated. Test objectives should be aligned with the DRP objectives and scope, and should cover aspects such as recovery time objectives (RTOs), recovery point objectives (RPOs), critical business functions, roles and responsibilities, communication channels, backup systems, and contingency procedures. By comparing the actual test results with the expected test objectives, the IS auditor can measure the effectiveness and efficiency of the DRP and identify any gaps or weaknesses that need to be addressed.

最新問題: **402**
IS 監査人は、組織が選択した IT オペレーティング システム ソフトウェアをより深く理解したいと考えています。
次のどれをレビューするのが最も役立つでしょうか?
A. サービスレベル契約 (SLA)
B. プロジェクト運営委員会憲章
C. エンタープライズ アーキテクチャ (EA)
D. IT監査レポート
Answer: (解答を表示する**)**

最新問題: **403**
IS 監査人は、現在も定期的に使用されているソフトウェア システムが何年も古く、サポートされていないことを発見しました。監査対象者は、ソフトウェアが現在のバージョンで実行されるまで 6 か月かかると述べています。サポートされていないバージョンのソフトウェアの使用に関連する即時のリスクを軽減する最善の方法は次のどれですか。
A. ソフトウェア システムの古いバージョンにすべてのパッチが適用されていることを確認します。
B. 古いソフトウェア システム上の未使用のポートをすべて閉じます。
C. 古いソフトウェア システムに到達しようとするネットワーク トラフィックを監視します。

D. 古くなったソフトウェア システムをメイン ネットワークから分離します。
Answer: D (メーッセージを残す**)**
The best way to reduce the immediate risk associated with using an unsupported version of the software is to segregate the outdated software system from the main network. This will limit the exposure of the system to potential attacks and prevent it from compromising other systems on the network. Segregating the system will also reduce the impact of any security incidents that may occur on the system.
Monitoring network traffic attempting to reach the outdated software system (option C) is not the best way to reduce the risk, as it will not prevent or stop any attacks on the system. It will only provide visibility into the network activity and alert the auditee of any suspicious or malicious traffic.
Verifying all patches have been applied to the software system's outdated version (option A) and closing all unused ports on the outdated software system (option B) are also not the best ways to reduce the risk, as they will not address the underlying issue of using an unsupported version of the software. Patches and ports may still have vulnerabilities that are not fixed by the vendor, and attackers may exploit them to gain access to the system. Therefore, option D is the correct answer.
References:
* Introduction (Part 1 of 7: Mitigating Risks of Unsupported Operating Systems)
* Summary (Part 7 of 7: Mitigating Risks of Unsupported Operating Systems)
* Upgrade, Retire, or Replace Unsupported Software (Part 4 of 7: Mitigating Risks of Unsupported Operating Systems)

最新問題**: 404**
システム開発プロジェクトは、継続的な人員不足により遅延が発生しています。実装時にシステムの品質を最も確実に保証できる戦略は次のどれですか?
A. すべての開発スタッフに残業代とボーナスを支給します。
B. 新しいシステム開発ツールを活用して生産性を向上します。
C. システム開発を迅速化するために IS スタッフを採用します。
D. 最初の目標日にコア機能のみを提供します。
Answer: (解答を表示する**)**
The strategy that would provide the greatest assurance of system quality at implementation is delivering only the core functionality on the initial target date. This strategy can help avoid compromising the quality of the system by focusing on the essential features that meet the user needs and expectations. Delivering only the core functionality can also help reduce the scope creep, complexity, and testing efforts of the system development project.
Implementing overtime pay and bonuses for all development staff, utilizing new system development tools to improve productivity, and recruiting IS staff to expedite system development are not strategies that would provide the greatest assurance of system

quality at implementation. These strategies may help speed up the system development process, but they may also introduce new risks or challenges such as burnout, learning curve, integration issues, or communication gaps. These risks or challenges may adversely affect the quality of the system.

最新問題**: 405**
情報システム監査人が総勘定元帳システムのデータの品質を確認するよう依頼されました。次のうちどれが監査人に最も有意義な結果をもたらすでしょうか?
A. システムの脆弱性評価
B. ソースドキュメントに対する整合性チェック
C. ビジネスオーナーと最大のアカウント価値について話し合う
D. システム所有者およびオペレーターへのインタビュー
Answer: B (メーッセージを残す**)**

最新問題**: 406**
データ損失防止 (DLP) ツールの実装前レビューを実施する情報システム監査人にとって、最も懸念されるのは次のどれでしょうか。
A. ツールはブロック モードではなくモニター モードで実装されています。
B. クローラーは機密データを検出するために使用されます。
C. ディープ パケット インスペクションにより、転送中のデータ パケットが開かれます。
D. 暗号化キーは集中管理されていません。
Answer: (解答を表示する**)**
A data loss prevention (DLP) tool implemented in monitor mode only observes and logs potential data leakage but does not actively prevent it. This leaves the organization vulnerable to data breaches, making it the most critical concern in a pre-implementation review.
* Crawlers for Sensitive Data (Option B): While crawlers may pose a performance impact, they are essential for discovering sensitive data.
* Deep Packet Inspection (Option C): Though it introduces privacy considerations, it is a standard DLP functionality for inspecting data in transit.
* Encryption Key Management (Option D): While important for security, improper management does not immediately prevent DLP functionality.
Reference: ISACA CISA Review Manual, Job Practice Area 4: Protection of Information Assets.

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の

GoShiken.com CISA-JPN 問題集をゲットする人はこちら:
https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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: **407**
エンティティの内部リソースを保護するためにファイアウォールで使用されるのは次のどれですか?
A. リモート アクセス サーバー
B. セキュア ソケット レイヤー (SSL)
C. インターネット プロトコル (IP) アドレスの制限
D. フェイルオーバーサービス
Answer: C (メーッセージを残す**)**
Internet Protocol (IP) address restrictions are used in a firewall to protect the entity's internal resources by allowing or denying access to specific IP addresses or ranges of IP addresses based on predefined rules.
Remote access servers, Secure Sockets Layers (SSLs), and failover services are not directly related to firewall protection, but rather to other aspects of network security, such as authentication, encryption, and availability. References: CISA Review Manual (Digital Version), Chapter 5: Protection of Information Assets, Section 5.2: Network Security Devices and Technologies

最新問題: **408**
インシデント対応チームは、ネットワーク サブネットでウイルスが発生したことを通知されました。次のステップは次のどれですか。
A. ダメージを最小限に抑えることに重点を置きます。
B. インシデントを文書化します。
C. 侵害されたシステムが完全に機能していることを確認します。
D. 影響を受けるシステムを削除して復元します。
Answer: A (メーッセージを残す**)**

最新問題: **409**
データ変換プロセス中に組織のデータ分類ポリシーが確実に保持されるようにするための最良の方法はどれですか?
A. データ分類コントロールをデータ セットにマップします。
B. 抽出、変換、ロード (ETL) ツールへのアクセスを制御します。
C. すべてのビジネス アプリケーションにわたってデータ検出演習を実施します。
D. データ作成時にメタデータに分類ラベルを実装します。
Answer: D (メーッセージを残す**)**
Data classification is the process of tagging data according to its type, sensitivity, and value to the organization. Data transformation is the process of changing the structure and

format of data to make it usable for analysis and visualization. Both processes are important for data security and compliance, but they also pose some challenges.
One of the challenges is to ensure that the organization's data classification policies are preserved during the process of data transformation. This means that the data should retain its original classification level and labels after it is transformed, and that the appropriate controls and protections are applied to the transformed data.
The best way to ensure this is to implement classification labels in metadata during data creation (D).
Metadata is data that describes other data, such as its source, format, content, and context. By adding classification labels to metadata, the data can be easily identified and tracked throughout its lifecycle, including during data transformation. The labels can also help enforce the proper access rights and encryption standards for the data, regardless of its state or location.

最新問題**: 410**
内部監査機能の内部品質保証 (QA) を実行する主な理由は、次の点を確認することです。
A. 監査リソースが最も効果的に使用されます。
B. 内部監査活動は監査基準と監査方法論に準拠しています。
C. 監査機能は適切に管理されており、パフォーマンス メトリックを満たしています。
D. 監査における固有のリスクが最小限に抑えられます。
Answer: (解答を表示する**)**
The primary reason to perform internal QA for an internal audit function is to ensure that the internal audit activity adheres to the Definition of Internal Auditing and the International Standards for the Professional Practice of Internal Auditing (Standards) issued by the Institute of Internal Auditors (IIA), as well as the internal audit methodology and policies of the organization. A QA program enables an evaluation of the internal audit activity's performance, efficiency, effectiveness, and value, and identifies opportunities for improvement. A QA program also helps to enhance the credibility and reputation of the internal audit function among the stakeholders.
References
Quality Assurance - The Institute of Internal Auditors or The IIA
Benefits of a quality assurance review for internal audit
Optimize your internal audit function with a quality assurance review ...

最新問題**: 411**
インターネット プロトコル セキュリティ (IPsec) アーキテクチャを実装する場合、アプリケーション配信に関与するサーバーは次のようになります。
A. トランスポート層セキュリティ (TLS) 経由で通信します。
B. 許可されたユーザーによる許可されていないアクティビティをブロックします。
C. パブリック ファイアウォール経由でのみチャネルにアクセスできます。

D. 認証によるチャネル アクセス。
Answer: A (メーッセージを残す**)**
When implementing Internet Protocol security (IPsec) architecture, the servers involved in application delivery communicate via Transport Layer Security (TLS), which is a protocol that provides encryption and authentication for data transmitted over a network. IPsec operates at the network layer and provides security for IP packets, while TLS operates at the transport layer and provides security for TCP connections. Blocking authorized users from unauthorized activities, channeling access only through the public-facing firewall, and channeling access through authentication are not functions of IPsec architecture. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.4.2

最新問題**: 412**
ジョブがジョブスケジュールに従って完了したかどうかを IS 監査人が評価するのに最も適しているのは、次のどれですか。
A. データベーススケジュール
B. コンソールログ
C. 例外ログ
D. システムスケジュール
Answer: (解答を表示する**)**

最新問題**: 413**
設計段階のプロジェクトが組織の目標を満たすかどうかを判断する際に、ビジネスケースと比較するのに最適なものは何ですか?
A. 実施計画
B. プロジェクト予算規定
C. 要件分析
D. プロジェクト計画
Answer: (解答を表示する**)**
Requirements analysis should be the best thing to compare against the business case when determining whether a project in the design phase will meet organizational objectives, because it defines the functional and non-functional specifications of the project deliverables that should satisfy the business needs and expectations. Requirements analysis can help evaluate whether the project design is aligned with the business case and whether it can achieve the desired outcomes and benefits. Implementation plan, project budget provisions, and project plan are also important aspects of a project in the design phase, but they are not as relevant as requirements analysis for comparing against the business case. References: CISA Review Manual (Digital Version), Chapter 4, Section 4.2.1

最新問題**: 414**

心臓ケア組織は、モノのインターネット (IoT) デバイスを利用して、リアルタイムの患者モニタリングと高度な診断を通じて患者の転帰を改善しています。これらのデバイスを企業ネットワーク トラフィックから分離するのに最も役立つのは次のどれですか。
A. 内部ファイアウォール
B. ブロックチェーン技術
C. コンテンツフィルタリングプロキシ
D. ゼロトラストアーキテクチャ
Answer: A (メーッセージを残す)
Internal firewalls are highly effective for isolating Internet of Things (IoT) devices from corporate network traffic. By segmenting the network and restricting communication between devices and the main corporate infrastructure, internal firewalls help mitigate the risk of lateral movement and data breaches caused by compromised IoT devices.
* Blockchain Technology (Option B): This is useful for ensuring data integrity but not for network isolation.
* Content Filtering Proxy (Option C): This is designed to manage web traffic and does not provide network segmentation.
* Zero Trust Architecture (Option D): While Zero Trust provides robust access controls, internal firewalls are more directly suited for traffic isolation.
Reference: ISACA CISA Review Manual, Job Practice Area 4: Protection of Information Assets.

最新問題**: 415**
サイバー攻撃が発生したときに、拡散のリスクを軽減できるセキュリティ対策は次のどれですか?
A. 境界ファイアウォール
B. データ損失防止 (DLP) システム
C. Web アプリケーション ファイアウォール
D. ネットワークセグメンテーション
Answer: (解答を表示する)
Network segmentation is the best security measure to reduce the risk of propagation when a cyberattack occurs, because it divides the network into smaller subnetworks that are isolated from each other and have different access controls and security policies. This limits the spread of malicious traffic and prevents attackers from accessing sensitive data or systems in other segments. A perimeter firewall, a data loss prevention (DLP) system, and a web application firewall are also useful security measures, but they do not prevent propagation within the network as effectively as network segmentation does. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.3

最新問題**: 416**
次のどれがビジネスと IT の連携にとって最大の課題となるでしょうか?

A. 取締役会への最高情報責任者 (CIO) の関与の欠如
B. 新規ビジネスプロジェクトを実行するためのIT予算が不十分
C. ビジネス戦略策定における情報セキュリティの関与の欠如
D. 最高情報責任者 (CIO) が議長を務める IT 運営委員会
Answer: A (メーッセージを残す)
The greatest challenge to the alignment of business and IT is the lack of chief information officer (CIO) involvement in board meetings. The CIO is the senior executive responsible for overseeing the IT strategy, governance, and operations of the organization, and ensuring that they support the business objectives and needs. The CIO should be involved in board meetings to communicate the value and contribution of IT to the organization, to align the IT vision and direction with the business strategy and priorities, and to advocate for the IT resources and investments required to achieve the desired outcomes. The lack of CIO involvement in board meetings can result in a disconnect between business and IT, a loss of trust and confidence in IT, and missed opportunities for innovation and value creation. The other options are not as challenging as the lack of CIO involvement in board meetings, because they either do not affect the strategic alignment of business and IT, or they can be addressed by other means such as collaboration, negotiation, or escalation.
References:
CISA Review Manual (Digital Version)1, Chapter 1, Section 1.2.1

最新問題**: 417**
監査リスクを最もよく表しているのはどれですか?
A. 同社は虚偽の告発で訴えられています。
B. 財務報告書には検出されていない重大な誤りが含まれている可能性があります。
C. 従業員が資金を不正流用していた。
D. 主要従業員は2年間休暇を取っていません。
Answer: (解答を表示する)
The best description of an audit risk is that the financial report may contain undetected material errors. Audit risk is the risk that the auditor expresses an inappropriate opinion on the financial report when it contains material misstatements or errors. Audit risk consists of three components: inherent risk, control risk, and detection risk. Inherent risk is the susceptibility of an assertion or a control to a material misstatement or error due to factors such as complexity, volatility, fraud, or human error. Control risk is the risk that a material misstatement or error will not be prevented or detected by the internal controls. Detection risk is the risk that the auditor's procedures will not detect a material misstatement or error that exists in an assertion or a control.
References:
* CISA Review Manual (Digital Version)
* CISA Questions, Answers & Explanations Database

最新問題**: 418**
第三者が関与する共同開発活動中に組織の独自のコードを最もよく保護する方法は次のどれですか?
A. 作業明細書 (SOW)
B. 秘密保持契約 (NDA)
C. サービスレベル契約 (SLA)
D. プライバシー同意書
Answer: B (メーッセージを残す**)**
A nondisclosure agreement (NDA) is the best way to protect an organization's proprietary code during a joint- development activity involving a third party. An NDA is a legal contract that binds the parties involved in a joint-development activity to keep confidential any information, data or materials that are shared or exchanged during the activity. An NDA specifies what constitutes confidential information, how it can be used, disclosed or protected, how long it remains confidential, what are the exceptions and remedies for breach of confidentiality, and other terms and conditions. An NDA can help to protect an organization's proprietary code from being copied, modified, distributed or exploited by unauthorized parties without its consent or knowledge. The other options are not as effective as option B, as they do not address confidentiality issues specifically. A statement of work (SOW) is a document that defines the scope, objectives, deliverables, tasks, roles, responsibilities, timelines and costs of a joint-development activity, but it does not cover confidentiality issues explicitly. A service level agreement (SLA) is a document that defines the quality, performance and availability standards and metrics for a service provided by one party to another party in a joint-development activity, but it does not cover confidentiality issues explicitly. A privacy agreement is a document that defines how personal information collected from customers or users is collected, used, disclosed and protected by one party or both parties in a joint-development activity, but it does not cover confidentiality issues related to proprietary code. References: CISA Review Manual (Digital Version) , Chapter 3: Information Systems Acquisition, Development & Implementation, Section 3.2: Project Management Practices.

最新問題**: 419**
大規模組織向けのデータ損失防止 (DLP) ソリューションを開発する場合、最初に実行すべきステップは次のうちどれですか。
A. データのインベントリと分類の演習を実施します。
B. 企業全体で承認されたデータワークフローを特定する_
C. 機密データの使用に対する脅威分析を実施します。
D. DLPポリシーとテンプレートを作成する
Answer: A (メーッセージを残す**)**
The first step when developing a DLP solution for a large organization is to conduct a data inventory and classification exercise. This step involves identifying and locating all the data

assets that the organization owns, generates, or handles, and assigning them to different categories based on their sensitivity, value, and regulatory requirements1. Data inventory and classification is essential for DLP because it helps to determine the scope and objectives of the DLP solution, as well as the appropriate level of protection and monitoring for each data category2. Data inventory and classification also enables the organization to prioritize its DLP efforts based on the risk and impact of data loss or leakage3.
Option B is not correct because identifying approved data workflows across the enterprise is a subsequent step after conducting data inventory and classification. Data workflows are the processes and channels through which data are created, stored, accessed, shared, or transmitted within or outside the organization4. Identifying approved data workflows helps to define the normal and legitimate use of data, as well as to detect and prevent unauthorized or anomalous data activities5. However, before identifying approved data workflows, the organization needs to know what data it has and how it should be classified.
Option C is not correct because conducting a threat analysis against sensitive data usage is another subsequent step after conducting data inventory and classification. Threat analysis is the process of identifying and assessing the potential sources, methods, and impacts of data loss or leakage incidents. Threat analysis helps to design and implement effective DLP controls and countermeasures based on the risk profile of each data category. However, before conducting threat analysis, the organization needs to know what data it has and how it should be classified.
Option D is not correct because creating the DLP policies and templates is the final step after conducting data inventory and classification, identifying approved data workflows, and conducting threat analysis. DLP policies and templates are the rules and configurations that specify how the DLP solution should monitor, detect, report, and respond to data loss or leakage events. DLP policies and templates should be aligned with the organization's business needs, regulatory obligations, and risk appetite. However, before creating the DLP policies and templates, the organization needs to know what data it has, how it should be classified, how it should be used, and what threats it faces.
References:
Data Inventory & Classification: The First Step in Data Protection1
Data Classification: What It Is And Why You Need It2
How to Prioritize Your Data Loss Prevention Strategy in 20203
What Is Data Workflow? Definition & Examples4
How to Identify Data Workflows for Your Business5
Threat Analysis: A Comprehensive Guide for Beginners
How to Conduct a Threat Assessment for Your Business
What Is Data Loss Prevention (DLP)? Definition & Examples
How to Create Effective Data Loss Prevention Policies

最新問題: 420

ファイアウォールが外部からの攻撃からネットワークを効果的に保護するためには、どのような基本的な慣行に従う必要がありますか?
A. すべての外部通信はファイアウォール経由で行う必要があります。
B. ファイアウォールは非武装地帯 (DMZ) に配置する必要があります。
C. 必須の外部サービスのみを許可する必要があります。
D. 外部情報のフィルターを定義する必要があります。
Answer: (解答を表示する**)**

最新問題**: 421**
新しい Web サーバーをサポートするハードウェアを取得するための組織の実現可能性調査において、次のどれが省略されると最も懸念されるでしょうか。
A. 買収資金調達の代替案
B. 潜在的ベンダーの財務安定性
C. 潜在的なベンダーの評判
D. 利用可能な製品の費用便益分析
Answer: D (メーッセージを残す**)**
The most important part of a feasibility study is the economics1. A cost-benefit analysis of available products is crucial as it helps to understand the economic viability of the project1. It compares the costs of the project with the benefits it is expected to deliver, which is essential for making informed decisions1. Omitting this could lead to investments in hardware that may not provide the expected returns or meet the organization's needs.
References:
The Components of a Feasibility Study - ProjectEngineer

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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**: 422**
次のどれが電子メール メッセージで送信された情報の機密性を保護しますか?
A. セキュアハッシュアルゴリズム1(SHA-1)
B. デジタル署名
C. 暗号化
D. デジタル証明書
Answer: C (メーッセージを残す**)**

Encryption is the process of transforming information into an unreadable form using a secret key, so that only authorized parties can access it. Encryption would protect the confidentiality of information sent in email messages, as it would prevent unauthorized parties from intercepting and reading the messages. Secure Hash Algorithm 1 (SHA-1) is a cryptographic hash function that produces a fixed-length output from an input.
SHA-1 does not encrypt information, but rather verifies its integrity by detecting any changes or modifications. Digital signatures are electronic signatures that use encryption and hash functions to authenticate the identity of the sender and the integrity of the message. Digital signatures do not protect the confidentiality of information, but rather ensure its authenticity and non-repudiation. Digital certificates are electronic documents that contain the public key and identity information of an entity, such as a person, organization or device. Digital certificates are issued by trusted third parties called certificate authorities (CAs). Digital certificates do not protect the confidentiality of information, but rather enable secure communication and encryption by verifying the identity and public key of an entity. References:
* : [Encryption Definition]
* : [Secure Hash Algorithm 1 (SHA-1) Definition]
* : [Digital Signature Definition]
* : [Digital Certificate Definition]

最新問題**: 423**
IS 監査人は、組織の事業継続計画 (BCP) が過去 18 か月間更新されておらず、組織が最近生産工場を閉鎖したことを知りました。監査人が取るべき最善の行動は次のどれですか。
A. ビジネス影響分析 (BIA) が組織の構造とコンテキストに適合しているかどうかを判断します。
B. 工場で使用されている技術の種類と、それが BCP にどのような影響を与えるかを判断します。
C. リカバリ時間目標 (R TO) への影響を判断するためのテストを実行します。
D. 工場の閉鎖による操業へのリスクを評価します。
Answer: A (メーッセージを残す**)**
The IS auditor should first determine whether the business impact analysis (BIA) is current with the organization's structure and context. The BIA is a critical component of the BCP and should reflect the current state of the organization. If the BIA is not up-to-date, it may not accurately reflect the impact of a disruption to the organization's operations, including the closure of a production plant12.
References: ISACA's Information Systems Auditor Study Materials1

最新問題**: 424**
意味のある推奨事項や調査結果を作成するために、情報システム監査人が決定し理解する必要がある最も重要なのは次のどれですか?

A. 根本原因
B. 責任者
C. 影響
D. 基準
Answer: (解答を表示する**)**
Root cause is the most important thing for an IS auditor to determine and understand to develop meaningful recommendations for findings. A root cause is the underlying factor or condition that leads to a problem or issue. A finding is a statement that describes a problem or issue identified during an audit. A recommendation is a suggestion or advice that aims to address or resolve a finding. To develop meaningful recommendations for findings, an IS auditor should determine and understand the root cause of each finding, as this can help to identify the most effective and appropriate actions to prevent or correct the problem or issue. The other options are not as important as determining and understanding the root cause, as they do not directly address or resolve the finding.
References: CISA Review Manual, 27th Edition, page 434

最新問題**: 425**
マルチテナント クラウド環境でデータ漏洩防止を最も効果的に実施できる方法はどれですか?
A. 監視ツールは、ダウンタイムが発生した場合に警告するように設定されています
B. 四半期ごとに包括的なセキュリティレビューが実行されます。
C. 異なるテナントのデータはデータベーススキーマによって分離されます
D. テナントはデータ分類ポリシーを実装する必要がある
Answer: (解答を表示する**)**
Data leakage prevention (DLP) is the process of preventing unauthorized access, disclosure, or transfer of sensitive data. In a multi-tenant cloud environment, where multiple customers share the same infrastructure and resources, DLP is a critical challenge. One of the best methods to enforce DLP in such an environment is to require tenants to implement data classification policies. Data classification policies define the types and levels of sensitivity of data, and the corresponding security controls and measures to protect them. By implementing data classification policies, tenants can ensure that their data is properly labeled, encrypted, segregated, and monitored according to their specific requirements and compliance standards. This can help prevent data leakage from accidental or malicious actions by other tenants, cloud service providers, or external parties.
References:
* 2: How Do I Secure my Data in a Multi-Tenant Cloud Environment? | Thales
* 3: Protecting Sensitive Customer Data in a Cloud-Based Multi-Tenant Environment | Saturn Cloud
* 4: Microsoft 365 isolation controls - Microsoft Service Assurance

最新問題**: 426**
金融アプリケーションにおけるトランザクションの有効性に関する最も信頼性の高い監査証拠を提供するのは次のどれですか?
A. ウォークスルーレビュー
B. 実質的なテスト
C. コンプライアンステスト
D. 設計ドキュメントのレビュー
Answer: B (メーッセージを残す**)**
Substantive testing provides the most reliable audit evidence on the validity of transactions in a financial application. Substantive testing is an audit procedure that examines the financial statements and supporting documentation to see if they contain errors or misstatements. Substantive testing can help to verify that the transactions recorded in the financial application are authorized, complete, accurate, and properly classified. Substantive testing can include methods such as vouching, confirmation, analytical procedures, or physical examination.

最新問題**: 427**
グローバル組織のポリシーでは、すべてのワークステーションを毎日マルウェアスキャンする必要があると規定されています。このポリシーへの継続的な準拠の最良の証拠を IS 監査人に提供するには、次のうちどれがよいでしょうか。
A. 侵入テストの結果
B. 管理証明
C. マルウェア対策ツールの監査ログ
D. 最近のマルウェアスキャンレポート
Answer: C (メーッセージを残す**)**
Anti-malware tool audit logs would provide an IS auditor with the best evidence of continuous compliance with the global organization's policy that states that all workstations must be scanned for malware each day. Anti-malware tool audit logs are records that capture the activities and events related to the anti-malware software installed on the workstations, such as scan schedules, scan results, updates, alerts, and actions taken1. These logs can help the IS auditor to verify that the anti-malware software is functioning properly, that the scans are performed regularly and effectively, and that any malware incidents are detected and resolved in a timely manner2. Anti-malware tool audit logs can also help the IS auditor to identify any gaps or weaknesses in the anti-malware policy or implementation, and to provide recommendations for improvement3.
The other options are not the best evidence of continuous compliance with the anti-malware policy. Penetration testing results are reports that show the vulnerabilities and risks of the workstations and network from an external or internal attacker's perspective4. While penetration testing can help to assess the security posture and resilience of the organization, it does not provide information on the daily anti-malware scans or their

outcomes. Management attestation is a statement or declaration from the management that they have complied with the anti-malware policy5. While management attestation can demonstrate commitment and accountability, it does not provide objective or verifiable evidence of compliance. Recent malware scan reports are documents that show the summary or details of the latest anti-malware scans performed on the workstations. While recent malware scan reports can indicate the current status and performance of the anti-malware software, they do not provide historical or comprehensive evidence of compliance.
References:
Malwarebytes Anti-Malware (MBAM) log collection and threat reports ...
Malicious Behavior Detection using Windows Audit Logs
PCI Requirement 5.2 - Ensure all Anti-Virus Mechanisms are Current ...
Management Attestation - an overview | ScienceDirect Topics
How to Read a Malware Scan Report | Techwalla

最新問題**: 428**
許可されたアクセスの意図しない誤用を軽減するための最も効果的な制御は次のどれですか?
A. 許容使用ポリシーの年次承認
B. ユーザーアクセスログの定期的な監視
C. セキュリティ意識向上トレーニング
D. 正式な懲戒処分
Answer: C (メーッセージを残す**)**
The most effective control to mitigate unintentional misuse of authorized access is security awareness training. This is because security awareness training can educate users on the proper use of their access rights, the potential consequences of misuse, and the best practices to protect the confidentiality, integrity, and availability of information systems. Security awareness training can also help users recognize and avoid common threats such as phishing, malware, and social engineering.
Annual sign-off of acceptable use policy, regular monitoring of user access logs, and formalized disciplinary action are not the most effective controls to mitigate unintentional misuse of authorized access. These controls may help deter or detect intentional misuse, but they do not address the root cause of unintentional misuse, which is often a lack of knowledge or awareness of security policies and procedures.

最新問題**: 429**
情報システム監査人は、退職した従業員の多くが買掛金システムから削除されていないことに気づきました。リスクを評価するために決定することが最も重要なのは次のどれですか?
A. 管理者によるユーザーアクセスレビューの頻度
B. 買掛金システムに関連する侵入試行の頻度

C. 退職した従業員のアクセスを終了するプロセス
D. 退職した従業員が実際にシステムにアクセスできるかどうか
Answer: D (メーッセージを残す**)**

最新問題**: 430**
IS 監査人は、ベンダーが廃業し、エスクローに古いバージョンのソース コードが保管されていることを発見しました。監査人が組織に対して推奨する最善策は何でしょうか。
A. 現在の問題を論議する新しいアプリケーションを分析する
B. ビジネスリスクを判断するための分析を実行する
C. エスクローバージョンを最新のものにします。
D. 既存のコードを使用してアプリケーションをサポートするためのメンテナンス計画を作成する
Answer: C (メーッセージを残す**)**
This means that the organization should obtain the source code from the escrow agent and compare it with the current version of the application that they are using. The organization should then identify and apply any changes or updates that are missing or different in the escrow version, so that it matches the current version.
This way, the organization can ensure that they have a complete and accurate copy of the source code that reflects their current needs and requirements.
Bringing the escrow version up to date can help the organization to avoid or reduce the risks and costs associated with using an outdated or incompatible version of the source code. For example, an older version of the source code may have bugs, errors, or vulnerabilities that could affect the functionality, security, or performance of the application. An older version of the source code may also lack some features, enhancements, or integrations that could improve the usability, efficiency, or value of the application. An older version of the source code may also not comply with some standards, regulations, or contracts that could affect the quality, reliability, or legality of the application1.
The other options are not as good as bringing the escrow version up to date for the organization. Option A, analyzing a new application that meets the current requirements, is a possible option but it may be more time- consuming, expensive, and risky than updating the existing application. The organization may have to go through a complex and lengthy process of selecting, acquiring, implementing, testing, and migrating to a new application, which could disrupt their operations and performance. The organization may also have to deal with compatibility, interoperability, or data quality issues when switching to a new application2. Option B, performing an analysis to determine the business risk, is a necessary step but not a recommendation for the organization. The organization should already be aware of the business risk of using an application whose vendor has gone out of business and whose escrow has an older version of the source code. The organization should focus on finding and implementing a solution to mitigate or eliminate this risk3. Option D, developing a maintenance plan to support the application using the existing code, is not a feasible option because it assumes that the organization has access to the

existing code. However, this is not the case because the vendor has gone out of business and the escrow has an older version of the source code. The organization cannot support or maintain an application without having a complete and accurate copy of its source code.
References:
* How Important Is Source Code Escrow - ISACA1
* The What and Why of Source Code Escrow2
* Unlocking Source Code In Escrow 2023: A Guide To Secure Software3

最新問題**: 431**
大量の視聴者が見込まれるライブ ストリーミング期間中にストリーミング サイトがサービスを継続して提供できるかどうかを検証するための最適なアプローチは次のうちどれですか。
A. 負荷テスト
B. ファジング
C. 障害の等級付け
D. ユーザビリティテスト
Answer: A (メーッセージを残す**)**

最新問題**: 432**
組織の災害復旧計画 (DRP) を評価する情報システム監査人にとって、最も懸念すべき事項は次のどれですか?
A. DRP は IT 部門によって開発されました。
B. DRP は過去 3 年間テストされていません。
C. DRP は 2 年間更新されていません。
D. DRP には、主要システムの復旧時間目標 (RTO) が含まれていません。
Answer: B (メーッセージを残す**)**
The DRP is a set of procedures and resources that enable an organization to restore its critical IT functions and operations in the event of a disaster or disruption. The DRP should be tested regularly to ensure its effectiveness, validity, and readiness. Testing the DRP can help to identify and resolve any gaps, issues, or weaknesses in the plan, as well as to evaluate the performance and capability of the recovery team and resources. If the DRP has not been tested during the past three years, it may not reflect the current IT environment, business requirements, or recovery objectives, and it may fail to meet the expectations and needs of the stakeholders.
References
ISACA CISA Review Manual, 27th Edition, page 255
Disaster Recovery Plan Testing: The Ultimate Checklist
What is a Disaster Recovery Plan (DRP) and How Do You Write One?

最新問題**: 433**

組織の IT サービス デスク機能に潜在的な問題があることを最もよく示すのは次のどれですか。
A. 文書化されていない操作手順
B. 職務の分離の欠如
C. ユーザーリクエストのバックログが多すぎる
D. 主要業績評価指標 (KPI) の欠如
Answer: C (メーッセージを残す)
An IT service desk is a function that provides technical support and assistance to the users of an organization' s IT systems and services. An IT service desk typically handles issues such as software installation, hardware troubleshooting, network connectivity, password reset, system configuration, and user training. An IT service desk aims to ensure that the IT systems and services are available, reliable, secure, and efficient for the users.
One of the best indications that there are potential problems within an organization's IT service desk function is an excessive backlog of user requests. A backlog is a list of user requests that have not been resolved or completed by the IT service desk within a specified time frame. An excessive backlog means that the IT service desk is unable to meet the demand or expectations of the users, and that the users are experiencing delays, dissatisfaction, or frustration with the IT service desk.
An excessive backlog of user requests can indicate various problems within the IT service desk function, such as:
* Insufficient staff, resources, or capacity to handle the volume or complexity of user requests
* Ineffective processes, procedures, or tools for managing, prioritizing, or resolving user requests
* Lack of skills, knowledge, or training among the IT service desk staff to deal with different types of user requests
* Poor communication, collaboration, or coordination among the IT service desk staff or with other IT functions or stakeholders
* Low quality, performance, or security of the IT systems or services that cause frequent or recurring user issues Therefore, an excessive backlog of user requests is the best indication that there are potential problems within an organization's IT service desk function.
References:
* What is an IT Service Desk? Definition and Functions - Indeed
* The Most Common IT Help Desk Issues - SherpaDesk
* 18 Common IT Help Desk Problems and Solutions - E-Pulse Blog

最新問題**: 434**
IS 監査人は、ユーザーが特定の映画を視聴する可能性を予測する機械学習モデルをレビューしています。監査人にとって最も懸念されるのは次のどれでしょうか。

A. モデルの開発にはオープンソースのプログラミング言語が使用されました。
B. 異なる集団から抽出されたデータを使用してモデルをテストしたところ、精度が低下しました。
C. モデルをトレーニングするためのデータセットは信頼できないソースから取得されました。
D. モデルは、トレーニング データと同じ母集団から抽出されたデータを使用してテストされました。
Answer: (解答を表示する**)**

最新問題**: 435**
プロジェクト チームは、既存のビジネス アプリケーションの代替を開発するために、アジャイル アプローチに切り替えることを決定しました。保護監査の有効性を確保するために、IS 監査人が最初に行うべきことは何ですか。
A. アジャイル プロセスを以前の方法論と比較します。
B. 既存のアジャイルプロセス制御を特定し評価する
C. 従うべき特定のアジャイル方法論を理解します。
D. ビジネスプロセスオーナーにインタビューしてビジネス要件のリストを作成する
Answer: (解答を表示する**)**
Understanding the specific agile methodology that will be followed is the first step that an IS auditor should do to ensure the effectiveness of the project audit. An IS auditor should familiarize themselves with the agile approach, principles, practices, and tools that will be used by the project team, as well as the roles and responsibilities of the project stakeholders. This will help the IS auditor to identify and assess the relevant risks and controls for the project audit. The other options are not the first steps that an IS auditor should do, but rather possible subsequent actions that may depend on the specific agile methodology. References:
* CISA Review Manual (Digital Version), Chapter 4, Section 4.3.21
* CISA Review Questions, Answers & Explanations Database, Question ID 211

最新問題**: 436**
経営陣による実装後のレビューが効果的であったことを情報システム監査人に最もよく示すのは次のどれですか?
A. 学んだ教訓は文書化され、適用されました。
B. ビジネスおよび IT 関係者が実装後のレビューに参加しました。
C. 実装後レビューは、システム開発ライフサイクル (SDLC) の正式なフェーズです。
D. 内部監査のフォローアップは何も発見されずに完了しました。
Answer: A (メーッセージを残す**)**
The best indication to an IS auditor that management's post-implementation review was effective is that lessons learned were documented and applied, as this shows that the management has identified and addressed the issues and gaps that arose during the

implementation, and has improved the processes and practices for future projects. Business and IT stakeholders participating in the post-implementation review is a good practice, but it does not guarantee that the review was effective or that the outcomes were implemented. Post- implementation review being a formal phase in the system development life cycle (SDLC) is a requirement, but it does not ensure that the review was effective or that the outcomes were implemented. Internal audit follow-up being completed without any findings is a desirable result, but it does not indicate that the management's post-implementation review was effective or that the outcomes were implemented.
References:
CISA Review Manual (Digital Version), Chapter 3: Information Systems Acquisition, Development and Implementation, Section 3.2: Project Management Practices1

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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**: 437**
仮想マシンに暗号化されずに保存されたデータの機密性と整合性を保護するための最も効果的な制御は次のどれですか?
A. 仮想マシンの保存されたイメージとスナップショットへのアクセスを監視します。
B. 仮想マシンのイメージとスナップショットへのアクセスを制限します。
C. 仮想マシンイメージとスナップショットの作成を制限します。
D. 仮想マシンの論理アクセス制御を定期的に確認します。
Answer: (解答を表示する**)**
The most effective control for protecting the confidentiality and integrity of data stored unencrypted on virtual machines is to monitor access to stored images and snapshots of virtual machines. Images and snapshots are copies of virtual machines that can be used for backup, restoration, or cloning purposes. If data stored on virtual machines are unencrypted, they may be exposed or compromised if unauthorized or malicious users access or copy the images or snapshots. Therefore, monitoring access to stored images and snapshots can help detect and prevent any unauthorized or suspicious activities, and provide audit trails for accountability and investigation.
Restricting access to images and snapshots of virtual machines, limiting creation of virtual machine images and snapshots, and reviewing logical access controls on virtual machines regularly are not the most effective controls for protecting the confidentiality and integrity of

data stored unencrypted on virtual machines. These controls may help reduce the risk or impact of data exposure or compromise, but they do not provide sufficient visibility or assurance of data protection. Restricting access to images and snapshots may not prevent authorized users from abusing their privileges or credentials. Limiting creation of virtual machine images and snapshots may not address the existing copies that may contain sensitive data. Reviewing logical access controls on virtual machines regularly may not reflect the actual access activities on images and snapshots.

最新問題**: 438**
組織は機密情報をパスワード保護されたファイルに保存し、そのファイルは共有フォルダに置かれています。攻撃者はソーシャル エンジニアリングによってパスワードを入手し、この情報を盗みました。
次のどれを実装すれば、組織は将来この種のインシデントを最も効果的に防止できるでしょうか?
A. 多要素認証 (MFA)
B. 従業員向けセキュリティ意識向上プログラム
C. ビジネスマネージャーによるアクセス履歴ログの確認
D. パスワード保護を伴うファイル暗号化
Answer: B (メーッセージを残す**)**
Social engineering exploits human vulnerabilities, and the most effective mitigation is training employees to recognize and respond to these threats. Security awareness programs help build a culture of vigilance, equipping employees with the knowledge to identify phishing attempts, suspicious behavior, and other social engineering tactics.
* Multi-factor Authentication (MFA) (Option A): Enhances access control but does not address the human vulnerability to social engineering.
* Access History Log Review (Option C): Useful for post-incident analysis but does not prevent incidents.
* File Encryption with Password Protection (Option D): Adds security layers but is ineffective if the password is compromised.
Reference: ISACA CISA Review Manual, Job Practice Area 4: Protection of Information Assets.

最新問題**: 439**
組織の脆弱性スキャンプログラムの有効性を評価する情報システム監査人にとって、最も懸念すべきことはどれですか。
A. 特定された脆弱性に対処するために取られた手順が正式に文書化されていない
B. 解決を確実にする権限を持つ個人に結果が報告されない
C. 組織の脆弱性スキャンスケジュールで要求される頻度よりも低い頻度でスキャンが実行されます
D. 結果は上級管理職によって承認されない

Answer: B (メーッセージを残す)
The finding that should be of greatest concern to an IS auditor assessing the effectiveness of an organization' s vulnerability scanning program is that results are not reported to individuals with authority to ensure resolution. This indicates a lack of accountability and communication for vulnerability management, which may result in unresolved or delayed remediation of identified vulnerabilities. This may expose the organization to increased risk of cyberattacks or breaches. The other findings are also concerning, but not as much as this one, because they may affect the completeness, accuracy or timeliness of the vulnerability scanning process, but not necessarily its effectiveness. References:
* ISACA, CISA Review Manual, 27th Edition, chapter 4, section 4.41
* ISACA, COBIT 2019 Framework: Introduction and Methodology, section 3.2

最新問題**: 440**
IT プロジェクトのプライバシーに関する懸念の範囲を評価する際に考慮すべき最も重要なのは次のどれですか?
A. データの所有権
B. 適用される法律および規制
C. ビジネス要件とデータフロー
D. エンドユーザーのアクセス権
Answer: B (メーッセージを残す)
When assessing the scope of privacy concerns for an IT project, the most important factor to consider is the applicable laws and regulations. These laws and regulations define the legal requirements for data privacy and protection that the project must comply with. They can vary greatly depending on the jurisdiction and the type of data being processed, and non-compliance can result in significant penalties123. While data ownership, business requirements and data flows, and end-user access rights are also important considerations, they are typically guided by these legal requirements.
References: ISACA's Information Systems Auditor Study Materials1

最新問題**: 441**
ある組織には、IT 戦略委員会と IT 運営委員会の両方があります。IT 運営委員会の議事録を確認する際、情報システム監査人は、委員会が次の事項を確認できることを期待します。
A. IT 投資のリスクとリターンを比較しました。
B. ビジネスに対する IT の貢献を評価しました。
C. 戦略的 IT 目標の達成状況を確認しました。
D. プロジェクトに適切なリソースを取得して割り当てました。
Answer: (解答を表示する)

最新問題**: 442**

IS 監査人が組織のデータ損失防止 (DLP) 制御の運用上の有効性を評価するための最も信頼性の高い方法はどれですか?
A. 機密ファイルが個人の USB デバイスに送信されないことを確認します。
B. 業界のベストプラクティスに基づいてデータ分類レベルを確認します。
C. すべてのコンピュータ システムに最新の DLP ソフトウェアがインストールされていることを確認します。
D. インタビューを実施して、データ保護の脆弱性の可能性を特定します。
Answer: A (メーッセージを残す)

最新問題**: 443**
ある組織では、従業員が仕事で個人のモバイル デバイスを使用することを許可しています。従業員のプライバシーを侵害することなく情報セキュリティを最もよく維持できるのは次のうちどれですか。
A. デバイスにセキュリティソフトウェアをインストールする
B. デバイス上の作業環境と個人スペースを区切る
C. ユーザーがアプリケーションを追加できないようにする
D. 勤務時間中に個人目的でデバイスを使用することを制限する
Answer: B (メーッセージを残す)
Partitioning the work environment from personal space on devices. This would best maintain information security without compromising employee privacy by creating a separate and secure area on the personal mobile devices for work-related data and applications. This way, the organization can protect its information from unauthorized access, loss, or leakage, while respecting the employees' personal data and preferences on their own devices.
The other options are not as effective as option B in balancing information security and employee privacy.
Option A, installing security software on the devices, is a good practice but may not be sufficient to prevent data breaches or comply with regulatory requirements. Option C, preventing users from adding applications, is too restrictive and may interfere with the employees' personal use of their devices. Option D, restricting the use of devices for personal purposes during working hours, is impractical and difficult to enforce.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription
* Personal Cellphone Privacy at Work1
* Protecting your personal information and privacy on a company phone2
* Mobile Devices and Protected Health Information (PHI)3
* Using your personal phone for work? Here's how to separate your apps and data4
* 9 Ways to Improve Mobile Security and Privacy in the Age of Remote Work5

最新問題: **444**
次のコントロールのうち、買掛金部門内の適切な人員分離を最も確実に保証するものはどれですか?
A. トランザクションの監査証跡が存在することを確認する
B. 更新プログラムへのアクセスを買掛金担当者のみに制限する
C. 作成されたすべてのトランザクションレコードに作成者のユーザーIDをフィールドとして含める
D. ユーザーのセキュリティプロファイルに従ってプログラム機能を制限する
Answer: D (メーッセージを残す)
Restricting program functionality according to user security profiles is the best control for ensuring appropriate segregation of duties within an accounts payable department. An IS auditor should verify that the access rights and permissions of the accounts payable staff are based on their roles and responsibilities, and that they are not able to perform incompatible or conflicting functions such as creating, approving, or paying invoices. This will help to prevent fraud, errors, or abuse of authority within the accounts payable process.
The other options are less effective controls for ensuring segregation of duties, as they may involve audit trails, access restrictions, or user identification. References:
* CISA Review Manual (Digital Version), Chapter 6, Section 6.31
* CISA Review Questions, Answers & Explanations Database, Question ID 223

最新問題: **445**
IS 監査人がアプリケーション システムの実装後レビューを実行するよう割り当てられています。次のどれが監査人の独立性を損なうでしょうか。
A. 監査人は、システムの開発中に特定の制御を実装しました。
B. 監査人はベストプラクティスに関するアドバイスを提供しました。
C. 監査人は運用上の責任を負わずにプロジェクトチームのメンバーとして参加した
D. 監査人は監査専用の組み込み監査モジュールを設計した。
Answer: A (メーッセージを残す)
The auditor implemented a specific control during the development of the system. This would impair the auditor's independence, as it would create a self-review threat, which is a situation where an auditor has to evaluate or review the results of his or her own work or judgment1. A self-review threat may compromise the auditor's objectivity and impartiality, as the auditor may be biased or influenced by his or her own involvement or interest in the system1. The auditor may also face a conflict of interest or a loss of credibility if he or she has to report on any issues or deficiencies related to the control he or she implemented.

最新問題: **446**

定期的な社内ソフトウェア ライセンスのレビュー中に、情報システム監査人は、従業員がビジネス ソフトウェアの重要な部分のライセンス キーを共有している事例を発見しました。監査人の最善の行動は次のうちどれですか?
A. ソフトウェア ライセンス監視ツールの使用を推奨します。
B. 追加のソフトウェア ライセンス キーの購入を推奨します。
C. 共有ソフトウェアライセンスのユーザーの必要性を検証する
D. ライセンス契約で共有使用が許可されているかどうかを確認します。
Answer: D (メーッセージを残す)
The auditor's best course of action after discovering instances where employees shared license keys to critical pieces of business software is to verify whether the licensing agreement allows shared use. A licensing agreement is a contract between the software provider and the user that defines the terms and conditions of using the software, including the number, type, and scope of licenses granted. Some licensing agreements may allow shared use of license keys among multiple users or devices, while others may prohibit or restrict such use. By verifying the licensing agreement, the auditor can determine whether the employees violated the contract or not, and whether there are any legal or financial risks or implications for the organization.
The other options are not as appropriate as option D, as they may not address the root cause of the issue or provide a comprehensive solution. Recommending the utilization of software licensing monitoring tools may help prevent or detect future instances of license key sharing, but it does not resolve the current situation or ensure compliance with the licensing agreement. Recommending the purchase of additional software license keys may be unnecessary or wasteful if the licensing agreement already allows shared use or if there are unused licenses available. Validating user need for shared software licenses may help identify the reasons or motivations behind license key sharing, but it does not justify or excuse such behavior if it violates the licensing agreement.
References:
* 9: Best License Management Software 2023 | Capterra
* 10: Best 10 Software License Management Tools in 2023 | Zluri
* 11: Top 10 Software License Tracking Tools | Zluri
* 12: Top 5 Software License Tracking Solutions in 2023 - DNSstuff

最新問題**: 447**
情報システム監査人が、会社の幹部が従業員に業務目的でソーシャル ネットワーキング サイトの使用を奨励していることを発見しました。次の推奨事項のうち、データ漏洩のリスクを軽減するのに最も役立つものはどれですか。
A. 従業員によるポリシー承認と秘密保持契約 (NDA)の署名の義務付け
B. 機密データに対する強力なアクセス制御を確立する
C. 従業員にソーシャルネットワーキングサイトの使用に関する教育とガイドラインを提供する

D. 従業員のソーシャル ネットワーキングの使用状況を監視する
Answer: C (メーッセージを残す**)**
The best recommendation to reduce the risk of data leakage from employee use of social networking sites for business purposes is to provide education and guidelines to employees on use of social networking sites.
Education and guidelines can help employees understand the benefits and risks of using social media for business purposes, such as enhancing brand awareness, engaging with customers, or sharing industry insights.
They can also inform employees about the dos and don'ts of social media etiquette, such as respecting privacy, protecting intellectual property, avoiding conflicts of interest, or complying with legal obligations.
Education and guidelines can also raise awareness of potential data leakage scenarios, such as phishing attacks, malicious links, fake profiles, or oversharing sensitive information, and provide tips on how to prevent or respond to them.

最新問題**: 448**
IT ポートフォリオ管理のレビューを実施する際に、最も重要な考慮事項は次のどれですか?
A. 各プロジェクトの責任をITチームメンバーに割り当てる
B. ベストプラクティスと業界で承認された方法論の遵守
C. ITポートフォリオのリスクを最小限に抑え、価値を最大化するための制御
D. ビジネス部門がITポートフォリオについて議論する会議の頻度
Answer: C (メーッセージを残す**)**
Controls to minimize risk and maximize value for the IT portfolio should be the most important consideration when conducting a review of IT portfolio management, because they ensure that the IT portfolio aligns with the business strategy, objectives, and priorities, and that the IT investments deliver optimal benefits and outcomes. Assignment of responsibility for each project to an IT team member, adherence to best practice and industry approved methodologies, and frequency of meetings where the business discusses the IT portfolio are also relevant aspects of IT portfolio management, but they are not as important as controls to minimize risk and maximize value. References: CISA Review Manual (Digital Version), Chapter 1, Section 1.2.3

最新問題**: 449**
取引データの正確性をテストする場合、より小さいサンプル サイズの使用を正当化する最も適切な状況は次のうちどれですか。
A. IS 監査スタッフは高いレベルの経験を持っています。
B. 母集団にはエラーがないことが期待されます。
C. 職務の適切な分離が実施されています。
D. データはユーザーが直接変更できます。

Answer: B (メーッセージを残す)

The best situation that justifies the use of a smaller sample size when testing the accuracy of transaction data is B. It is expected that the population is error-free. The sample size is the number of items selected from the population for testing. The sample size depends on various factors, such as the level of confidence, the tolerable error rate, the expected error rate, and the variability of the population. A smaller sample size means that fewer items are tested, which reduces the cost and time of testing, but also increases the sampling risk (the risk that the sample is not representative of the population).

One of the factors that affects the sample size is the expected error rate, which is the auditor's best estimate of the proportion of errors in the population before testing. A higher expected error rate means that more errors are likely to be found in the population, which requires a larger sample size to provide sufficient evidence for the auditor's conclusion. A lower expected error rate means that fewer errors are likely to be found in the population, which allows a smaller sample size to provide sufficient evidence for the auditor's conclusion.

Therefore, if it is expected that the population is error-free (i.e., the expected error rate is zero or very low), a smaller sample size can be justified.

The other situations do not justify the use of a smaller sample size when testing the accuracy of transaction data. A. The IS audit staff has a high level of experience. The IS audit staff's level of experience does not affect the sample size, but rather their ability to design and execute the sampling procedures and evaluate the results. The IS audit staff's level of experience may affect their judgment in selecting and applying sampling methods, but it does not change the statistical or mathematical principles that determine the sample size. B.

Proper segregation of duties is in place. Proper segregation of duties is an internal control that helps prevent or detect errors or fraud in transaction processing, but it does not affect the sample size. The sample size is based on the characteristics of the population and the objectives of testing, not on the controls in place. Proper segregation of duties may reduce the likelihood or impact of errors or fraud in transaction processing, but it does not eliminate them completely. Therefore, proper segregation of duties does not justify a smaller sample size when testing the accuracy of transaction data. C. The data can be directly changed by users. The data's ability to be directly changed by users does not justify a smaller sample size, but rather a larger one. The data' s ability to be directly changed by users increases the risk of errors or fraud in transaction processing, which requires a larger sample size to provide sufficient evidence for the auditor's conclusion. The data's ability to be directly changed by users also increases the variability of the population, which affects the sample size.

References:

* ISACA, CISA Review Manual, 27th Edition, 2019, p. 2471
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription2

* Audit Sampling - AICPA3
* How to choose a sample size (for the statistically challenged)

最新問題: **450**
災害復旧監査中に、情報システム監査人はビジネス影響分析 (BIA) が実施されていないことを発見しました。監査人はまず
A. ビジネス影響分析 (BIA) を実行します。
B. 経営陣に中間レポートを発行します。
C. 現在の災害復旧機能への影響を評価します。
D. 追加のコンプライアンス テストを実施します。
Answer: C (メーッセージを残す**)**
The first step that an IS auditor should take when finding that a business impact analysis (BIA) has not been performed is to evaluate the impact on current disaster recovery capability. A BIA is a process that identifies and analyzes the potential effects of disruptions to critical business functions and processes. A BIA helps determine the recovery priorities, objectives, and strategies for the organization. Without a BIA, the disaster recovery plan may not be aligned with the business needs and expectations, and may not provide adequate protection and recovery for the most critical assets and activities. Therefore, an IS auditor should assess how the lack of a BIA affects the current disaster recovery capability and identify any gaps or risks that need to be addressed.
Performing a BIA, issuing an intermediate report to management, and conducting additional compliance testing are not the first steps that an IS auditor should take when finding that a BIA has not been performed.
These steps may be done later in the audit process, after evaluating the impact on current disaster recovery capability. Performing a BIA is not the responsibility of the IS auditor, but of the business owners and managers. Issuing an intermediate report to management may be premature without sufficient evidence and analysis. Conducting additional compliance testing may not be relevant or necessary without a clear understanding of the disaster recovery requirements and objectives.

最新問題: **451**
データベース セキュリティ監査から得られた次の結果のうち、重大なセキュリティ侵害のリスクが最も大きいものはどれですか?
A. レガシー データは削除されていません。
B. 管理者アカウントのパスワードには有効期限が設定されていません。
C. デフォルト設定は変更されていません。
D. データベース アクティビティのログ記録が完了していません。
Answer: B (メーッセージを残す**)**
Admin accounts typically have the highest level of privileges and access to sensitive data. If the passwords for these accounts are not set to expire, it increases the risk of

unauthorized access and potential security breaches. This is especially true if an admin's credentials are compromised, as the attacker could have ongoing access to critical systems and data1.
References:
Database Auditing - Satori

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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: **452**
IS 監査人は、ネットワーク セキュリティ レビューの現場調査フェーズを完了し、初期段階の次の調査結果を準備していますが、最も高いリスクとしてランク付けする必要がありますか?
A. ネットワーク侵入テストは実行されません
B. ネットワーク ファイアウォール ポリシーは情報セキュリティ担当者によって承認されていません。
C. ネットワーク ファイアウォール ルールが文書化されていません。
D. ネットワーク デバイスのインベントリが不完全です。
Answer: A (メーッセージを残す**)**
The finding that should be ranked as the highest risk is that network penetration tests are not performed.
Network penetration tests are simulated cyberattacks that aim to identify and exploit the vulnerabilities and weaknesses of the network security controls, such as firewalls, routers, switches, servers, and devices.
Network penetration tests are essential for assessing the effectiveness and resilience of the network security posture, and for providing recommendations for improvement and remediation. If network penetration tests are not performed, the organization may not be aware of the existing or potential threats and risks to its network, and may not be able to prevent or respond to real cyberattacks, which can result in data breaches, service disruptions, financial losses, reputational damage, and legal or regulatory penalties. The other findings are also important, but not as risky as the lack of network penetration tests, because they either do not directly affect the network security controls, or they can be addressed by documentation or approval processes.
References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.4

最新問題: **453**
情報システム監査人は、リソースの制約により、データベース管理者（DBA）が本番環境への変更の開発と実行の責任を負っていることを発見しました。監査人が最初に行うべきことはどれですか？
A. 別のDBAが変更を行えるかどうかを判断する
B. 職務分掌違反の可能性を報告する
C. 補償制御が存在するかどうかを識別する
D. 実装前に変更管理プロセスが遵守されていることを確認する
Answer: (解答を表示する**)**
A database administrator (DBA) is responsible for maintaining the integrity, security and performance of the database systems. A DBA who is also responsible for developing and executing changes into the production environment may have a conflict of interest and pose a risk to the data quality and availability. Therefore, the IS auditor should first identify whether any compensating controls exist to mitigate this risk, such as independent reviews, approvals, audits or monitoring of the changes. Determining whether another DBA could make the changes, reporting a potential segregation of duties violation and ensuring a change management process is followed prior to implementation are possible actions that the auditor could take after identifying the compensating controls or the lack thereof.
References:
* : Database Administrator (DBA) Definition
* : Segregation of Duties | ISACA
* : [Compensating Control Definition]

最新問題: **454**
継続的な監査に最も適しているのはどれですか?
A. 低額取引
B. リアルライム取引
C. 不正取引
D. 手動トランザクション
Answer: B (メーッセージを残す**)**
Continuous auditing is a method of performing audit-related activities on a real-time or near real-time basis.
Continuous auditing is best suited for real-time transactions, such as online banking, e-commerce, or electronic funds transfer, that require immediate verification and assurance. Low-value transactions are not necessarily suitable for continuous auditing, as they may not pose significant risks or require frequent monitoring. Irregular transactions are not suitable for continuous auditing, as they may not occur frequently or consistently enough to justify the use of continuous auditing techniques. Manual transactions are not suitable for continuous auditing, as they may not be captured or processed by automated systems that enable continuous auditing. References:

* CISA Review Manual, 27th Edition, pages 307-3081
* CISA Review Questions, Answers & Explanations Database, Question ID: 253

最新問題: **455**
システム開発プロジェクトの詳細設計フェーズで IS 監査人が決定する必要がある最も重要な項目は次のどれですか?
A. プログラムのコーディング標準が遵守されている
B. 受け入れテスト基準が開発されました
C. データ変換手順が確立されました。
D. 設計は上級管理職によって承認されました。
Answer: B (メーッセージを残す**)**
The most important thing for an IS auditor to determine during the detailed design phase of a system development project is that acceptance test criteria have been developed. Acceptance test criteria define the expected functionality, performance and quality of the system, and are used to verify that the system meets the user requirements and specifications. The IS auditor should ensure that the acceptance test criteria are clear, measurable and agreed upon by all stakeholders. Program coding standards have been followed is something that the IS auditor should check during the coding or testing phase, not the detailed design phase.
Data conversion procedures have been established or the design has been approved by senior management are things that the IS auditor should verify during the implementation phase, not the detailed design phase. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 323

最新問題: **456**
企業内の財務システムの監査に統制依存型のアプローチを使用する必要があるかどうかを判断するには、どの IS 監査作業の順序が最も適切ですか?
A. 財務取引の詳細な調査とそれに続く総勘定元帳の検討
B. 主要な財務アプリケーションのレビューとそれに続く IT ガバナンス プロセスのレビュー
C. 一般的なISコントロールのレビューに続いてアプリケーションコントロールのレビュー
D. アプリケーション制御のレビューとそれに続く主要なビジネスプロセス制御のテスト
Answer: C (メーッセージを残す**)**

最新問題: **457**
ある組織が、新しい規制要件の検討に応じてデータ損失防止 (DLP) システムを実装しています。システムの設計を評価するのに最も役立つのは次のどれでしょうか。
A. データ侵害の履歴
B. システムマニュアル
C. エンタープライズ アーキテクチャ (EA)

D. 業界の動向
Answer: C (メーッセージを残す**)**

最新問題**: 458**
IS 監査人は、2 週間ごとにローカル データベース サーバーのバックアップを実行し、データのバックアップと復元の手順を管理する正式なポリシーを持たない組織を監査しています。次の調査結果のうち、組織にとって最も大きなリスクとなるものはどれですか。
A. データのバックアップ頻度が不十分
B. データバックアップポリシーがない
C. オフサイトデータバックアップの欠如
D. 定期的なデータ復元テストの欠如
Answer: A (メーッセージを残す**)**

最新問題**: 459**
データ分類プログラムを実装する際に最も重要なのは次のどれですか?
A. データ分類レベルを理解する
B. データの所有権の正式化
C. プライバシーポリシーの作成
D. 安全なストレージ容量の計画
Answer: B (メーッセージを残す**)**
Data classification is the process of organizing data into categories based on its sensitivity, value, and risk to the organization. Data classification helps to ensure that data is protected according to its importance and regulatory requirements. Data classification also enables data owners to make informed decisions about data access, retention, and disposal.
To implement a data classification program, it is most important to formalize data ownership. Data owners are the individuals or business units that have the authority and responsibility for the data they create or use. Data owners should be involved in defining the data classification levels, assigning the appropriate classification to their data, and ensuring that the data is handled according to the established policies and procedures. Data owners should also review and update the data classification periodically or when there are changes in the data or its usage.
The other options are not as important as formalizing data ownership when implementing a data classification program. Understanding the data classification levels is necessary, but it is not sufficient without identifying the data owners who will apply them. Developing a privacy policy is a good practice, but it is not specific to data classification. Planning for secure storage capacity is a technical consideration, but it does not address the business and legal aspects of data classification.
References:
* ISACA, CISA Review Manual, 27th Edition, 2020, page 247
* Data Classification: What It Is and How to Implement It

最新問題: **460**
組織のインシデント対応プログラムの有効性を示す最良の指標は次のどれですか?
A. 成功した侵入テストの数
B. 保護されているビジネスアプリケーションの割合
C. セキュリティイベントごとの財務的影響
D. セキュリティ脆弱性パッチの数
Answer: C (メーッセージを残す)
The best indicator of the effectiveness of an organization's incident response program is the financial impact per security event. This metric measures the direct and indirect costs associated with security incidents, such as loss of revenue, reputation damage, legal fees, recovery expenses, and fines. By reducing the financial impact per security event, the organization can demonstrate that its incident response program is effective in mitigating the consequences of security breaches and restoring normal operations as quickly as possible.
Number of successful penetration tests, percentage of protected business applications, and number of security vulnerability patches are indicators of the security posture of the organization, but they do not reflect the effectiveness of the incident response program.
References: ISACA Journal Article: Measuring Incident Response Effectiveness

最新問題: **461**
探偵管理の継続的な悪化の結果として最も大きな影響をもたらすのは次のどれですか?
A. ログの保存スペースの需要増加
B. 根本原因分析の有効性の低下
C. 全体的な回復時間の短縮
D. セキュリティログの誤検出数の増加
Answer: (解答を表示する)

最新問題: **462**
ある組織は、プライマリデータセンターのすべてのストレージデバイスを新しい大容量のユニットに交換しました。交換されたデバイスは、古いユニットを交換するために災害復旧サイトに設置されました。情報システム監査人の主な懸念は、
A. リカバリサイトのデバイスはストレージ要件を処理できる
B. 古いストレージデバイスと新しいストレージデバイスの両方にハードウェア保守契約が締結されています
C. 調達は企業方針と手順に準拠していた
D. 移転計画は関係者全員に伝えられた
Answer: A (メーッセージを残す)
An IS auditor's primary concern would be whether the recovery site devices can handle the storage requirements. The storage requirements are determined by the amount and type

of data that needs to be backed up and restored in case of a disaster at the primary data center. The recovery site devices should have enough capacity, performance, reliability, and compatibility to meet these requirements.
If the recovery site devices cannot handle the storage requirements, then there is a risk that some data may not be backed up properly or may not be available for recovery when needed. This could result in data loss, corruption, or inconsistency, which could affect the business continuity and integrity of the organization.
Therefore, an IS auditor should verify that:
* The recovery site devices have sufficient storage space to accommodate all the data that needs to be backed up from the primary data center.
* The recovery site devices have adequate bandwidth and speed to transfer and access data efficiently and effectively.
* The recovery site devices have appropriate security features and controls to protect data from unauthorized access or modification.
* The recovery site devices are compatible with the primary data center devices in terms of hardware, software, format, and protocol.
References:
* 10: What Is a Disaster Recovery Site? Hot, Cold & Warm Site
* 11: Disaster recovery site - What is the ideal distance to mitigate risks? - Advisera
* 12: Offsite Data Backup Storage vs Disaster Recovery (DR) - LINBIT

最新問題**: 463**
紛失した会社所有のモバイル デバイスへの不正アクセスのリスクを最小限に抑えるための最適な制御は次のどれですか。
A. パスワード/PIN保護
B. デバイス追跡ソフトウェア
C. デバイスの暗号化
D. 定期バックアップ
Answer: (解答を表示する**)**
The best control to minimize the risk of unauthorized access to lost company-owned mobile devices is device encryption. Device encryption is a process that transforms data on a device into an unreadable format using a cryptographic key. Device encryption protects the data stored on the device from being accessed by unauthorized parties, even if they bypass the password or PIN protection. Device encryption can also prevent data leakage if the device is disposed of or recycled without proper data sanitization. Password or PIN protection is a basic control that prevents unauthorized access to the device by requiring a secret code or pattern to unlock it. However, password or PIN protection can be easily compromised by brute force attacks, shoulder surfing, or social engineering. Device tracking software is a tool that allows the device owner or administrator to locate, lock, or wipe the device remotely in case of loss or theft. However, device tracking software depends on the device's network connectivity and GPS functionality, which may not be

available or reliable in some situations. Periodic backup is a process that copies the data from the device to another storage location for recovery purposes. Periodic backup can help restore the data in case of loss or damage of the device, but it does not prevent unauthorized access to the data on the device itself. References: CISA Review Manual (Digital Version), Chapter 5: Protection of Information Assets, Section 5.4: Mobile Devices

最新問題**: 464**
IS 監査マネージャーは、組織の給与計算アプリケーションのアップグレードを担当するプロジェクト マネージャーを一時的に監督する任務を負っていました。監査部門に戻った監査マネージャーは、給与計算アプリケーションの実装を検証するための監査を実施するよう依頼されました。監査マネージャーは、監査部門で IT プロジェクト管理の経験を持つ唯一の人物です。最善の対応策は何でしょうか。
A. 上級 IS 監査人がプロジェクトを管理し、IS 監査マネージャーが最終レビューを実行します。
B. 監査を独立した資格のあるリソースに外注します。
C. IT プロジェクト管理の経験が不足しているにもかかわらず、割り当てを別の監査マネージャーに転送します。
D. 適切な経験を持つ人が他にいないため、監査を管理します。
Answer: B (メーッセージを残す**)**

最新問題**: 465**
ある組織が最近、VoIP (Voice-over IP) 通信システムを実装しました。次のうち、情報システム監査人が主に懸念すべきものはどれですか?
A. 音声通信とデータ通信の両方における単一障害点
B. 内部トラフィックに仮想プライベートネットワーク (VPN) を使用できない
C. 音声とデータ通信の統合の欠如
D. パケットの破棄による音声品質の低下
Answer: A (メーッセージを残す**)**
The IS auditor's primary concern when an organization has recently implemented a Voice-over IP (VoIP) communication system is a single point of failure for both voice and data communications. VoIP is a technology that allows voice communication over IP networks such as the internet. VoIP can offer benefits such as lower costs, higher flexibility, and better integration with other applications. However, VoIP also introduces risks such as dependency on network availability, performance, and security. If both voice and data communications share the same network infrastructure and devices, then a single point of failure can affect both services simultaneously and cause significant disruption to business operations. Therefore, the IS auditor should evaluate the availability and redundancy of the network components and devices that support VoIP communication. The other options are not as critical as a single point of failure for both voice and data communications, as they do not pose a direct threat to business continuity. References: CISA Review Manual,

27th Edition, page 385

最新問題: **466**
IT ガバナンス機関は、IT サービスの提供が一貫して効果的なプロセスに基づいているかどうかを判断したいと考えています。次のうち、最適なアプローチはどれですか。
A. 主要業績評価指標 (KPI) を評価します。
B. ギャップ分析を実施します。
C. 成熟度モデルを開発します。
D. 制御自己評価 (CSA) を実装します。
Answer: C (メーッセージを残す**)**

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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: **467**
コンピュータのパフォーマンスを分析するときに最も役立つのは次のどれでしょうか?
A. 容量使用率を測定する統計指標
B. 応答時間に対するユーザーの不満に関する運用レポート
C. リソース使用を最適化するためのシステムソフトウェアのチューニング
D. オフピーク時の使用率と応答時間のレポート
Answer: A (メーッセージを残す**)**
Computer performance is the measure of how well a computer system can execute tasks and applications within a given time frame. Computer performance can be affected by various factors, such as hardware specifications, software configuration, network conditions, and user behavior. To analyze computer performance, it is important to use statistical metrics that can quantify the capacity utilization of the system resources, such as CPU, memory, disk, and network. These metrics can help identify the bottlenecks, inefficiencies, and anomalies that may degrade the performance of the system. Examples of such metrics include CPU utilization, memory usage, disk throughput, network bandwidth, and response time.
The other options are not as useful as statistical metrics when analyzing computer performance. An operations report of user dissatisfaction with response time is a subjective measure that may not reflect the actual performance of the system. Tuning of system software to optimize resource usage is a corrective action that can improve

performance, but it is not a method of analysis. A report of off-peak utilization and response time is a limited snapshot that may not capture the peak performance or the average performance of the system.
References:
* What is Computer Performance?
* How to Measure Computer Performance

最新問題**: 468**
IS 監査人は、リスク管理プラクティスが適用されていることを確認するために、イベント ログ集約システムを確認するように求められています。監査人が最も懸念すべき事項は次のどれですか。
A. ログ フィードはバッチ プロセスによってアップロードされます。
B. ログ データに対して完全性テストは実行されていません。
C. ログデータは正規化されていません。
D. データ暗号化標準は考慮されていません。
Answer: B (メーッセージを残す**)**
The IS auditor should be most concerned if completeness testing has not been performed on the log data, as this could indicate that some logs are missing, corrupted, or tampered with, and that the log aggregation system is not reliable or accurate12. Completeness testing is a process of verifying that all the logs generated by the source systems are successfully collected, transferred, and stored by the log aggregation system, and that there are no gaps or inconsistencies in the log data34. Completeness testing is essential for ensuring the integrity and validity of the log data, and for supporting the risk management practices of the organization.
References
1: Log Aggregation: How it Works, Methods, and Tools - Exabeam2 2: Log Aggregation & Monitoring Relation in Cybersecurity4 3: Log Aggregation: What It Is & How It Works | Datadog3 4: Data Flow Testing
- GeeksforGeeks1

最新問題**: 469**
機密性の高い顧客データを含む無人ラップトップが人事オフィスから複数盗まれました。再発に備えてデータを保護するための情報システム監査人の最善の推奨事項は次のどれでしょうか?
A. ディスクドライブを暗号化します。
B. 2要素認証を要求する
C. 物理的なセキュリティを強化する
D. ケーブルロックの使用を義務付ける
Answer: A (メーッセージを残す**)**

According to the CISA - Certified Information Systems Auditor Study Guide1, the correct answer to your question is A. Encrypt the disk drive. This is because encryption is a logical security measure that can protect data even if the physical device is stolen or lost. Encryption makes the data unreadable and inaccessible without the proper key or password. The other options are not as effective as encryption in this scenario. Two- factor authentication is a user authentication method that requires two pieces of evidence to verify the user's identity, such as a password and a code sent to a phone. However, this does not prevent unauthorized access to the data if the laptop is already logged in or if the attacker can bypass the authentication. Enhancing physical security is a preventive measure that can reduce the risk of theft, but it does not guarantee that theft will not occur or that the data will be safe if it does. Requiring the use of cable locks is another preventive measure that can deter thieves, but it can also be easily cut or removed by a determined attacker.

最新問題**: 470**
組織のセキュリティ チームが、複数の脆弱なアプリケーションを含むシミュレートされた実稼働環境を作成しました。このような環境を作成する主な目的は何でしょうか。
A. 侵入検知システム (IDS) をテストする
B. セキュリティ管理者にトレーニングを提供する
C. サイバー攻撃のデジタル証拠を収集する
D. 攻撃者を誘い出してその行動を研究するため
Answer: (解答を表示する**)**
The primary purpose of creating a simulated production environment with multiple vulnerable applications is D: To attract attackers in order to study their behavior. This is also known as a honeypot, which is a decoy system that mimics a real target and lures attackers into revealing their techniques, tools, and motives1. A honeypot can help the organization's security team to improve their defense strategies, identify new threats, and collect digital evidence of cyberattacks1.

最新問題**: 471**
インターネット接続とローカル通信ループの冗長な組み合わせを提供するリカバリ施設は、どのタイプの通信継続性の例ですか?
A. 音声回復
B. 代替ルーティング
C. 長距離ネットワークの多様性
D. ラストマイル回線保護
Answer: D (メーッセージを残す**)**
Recovery facilities providing a redundant combination of Internet connections to the local communications loop is an example of last-mile circuit protection. Last-mile circuit protection is a type of telecommunications continuity that ensures the availability and redundancy of the final segment of the network that connects the end-user to the service

provider. The local communications loop, also known as the local loop or subscriber line, is the physical link between the customer premises and the nearest central office or point of presence of the service provider. By having multiple Internet connections from different providers or technologies, such as cable, DSL, fiber, wireless, or satellite, the recovery facilities can avoid losing connectivity in case one of the connections fails or is disrupted by a disaster5.
References:
* 9: Last Mile Redundancy - How to Ensure Business Continuity - Multapplied Networks

最新問題: **472**
プロジェクトのリスク管理の実践を見直す際に、最も懸念されるのは次の調査結果のうちどれでしょうか?
A. 正式なマイルストーンの承認はありません。
B. 進行中の問題は正式には追跡されません。
C. 定性的なリスク分析は更新されていません。
D. プロジェクト管理ソフトウェアは使用されていません。
Answer: B (メーッセージを残す**)**

最新問題: **473**
IS 部門は、コスト収益比、ユーザー満足度、コンピュータのダウンタイムに基づいて毎月評価されます。これは、アプリケーションとして最適です。
A. リスクフレームワーク
B. バランストスコアカード
C. バリューチェーン分析
D. 制御自己評価 (CSA)
Answer: (解答を表示する**)**
A balanced scorecard is a framework that translates the IT strategy into measurable objectives, indicators, targets, and initiatives across four perspectives: financial, customer, internal process, and learning and growth.
A balanced scorecard helps to monitor and evaluate how well the IT function is delivering value to the organization, achieving its strategic goals, and improving its capabilities and competencies. The other options are not the primary uses of a balanced scorecard, because they either focus on specific aspects of IT rather than the overall performance, or they are not directly related to the IT strategy.

最新問題: **474**
クラウド サービス プロバイダーを使用して顧客データを処理する組織にとって、最も重要なプライバシーの考慮事項は次のどれですか。
A. 顧客に通知せずに個人情報をサービスプロバイダーに転送することはできません。

B. サービスプロバイダーに転送された顧客データは、規制当局に報告する必要があります。
C. データのプライバシーは、組織に適用される規制に従って管理する必要があります。
D. データのプライバシーは、業界標準とベストプラクティスに従って監視する必要があります。
Answer: B (メーッセージを残す**)**

最新問題**: 475**
ソフトウェア開発プロジェクトの初期段階をレビューする際に、情報システム監査人が最も懸念するのは次のどれでしょうか?
A. プログラムコードをサポートする技術文書が不足している
B. 各スプリントの終了時にすべての要件が完了していない
C. ユーザー要件の背後にある受け入れ基準の欠如。
D. 詳細なユニットおよびシステムテスト計画の欠如
Answer: C (メーッセージを残す**)**
User requirements are statements that describe what the users expect from the software system in terms of functionality, quality, and usability. They are essential inputs for the software development process, as they guide the design, implementation, testing, and deployment of the system. Therefore, an IS auditor's greatest concern when reviewing the early stages of a software development project would be the lack of acceptance criteria behind user requirements. Acceptance criteria are measurable conditions that define when a user requirement is met or satisfied. They help ensure that the user requirements are clear, complete, consistent, testable, and verifiable. Without acceptance criteria, it would be difficult to evaluate whether the system meets the user expectations and delivers value to the organization. Technical documentation, such as program code, is usually produced in later stages of the software development process. Completion of all requirements at the end of each sprint is not mandatory in agile software development methods, as long as there is a prioritized backlog of requirements that can be delivered incrementally. A detailed unit and system test plan is also important for ensuring software quality, but it depends on well-defined user requirements and acceptance criteria. References: Information Systems Acquisition, Development & Implementation, CISA Review Manual (Digital Version)

最新問題**: 476**
ある組織は、選択されたビジネス プロセスに対して統制自己評価 (CSA) プログラムを実装することを計画しています。このプログラムに対する内部監査チームの役割は次のどれでしょうか。
A. 経営陣がプロセス制御を効果的に評価するためのテスト手順を設計します。
B. CSA がカバーするビジネス プロセスを将来の監査計画から除外します。
C. 経営陣の自己評価の正確性を検証するためのテストを実行します。

D. 自己評価プロセスについて経営陣にアドバイスします。
Answer: D (メーッセージを残す)

最新問題**: 477**
予測のために複数の販売取引データベースからデータを収集するミドルウェア アプリケーションが効果的に動作していることを最も確実に保証するものは次のどれですか。
A. 継続的な監査
B. 手動チェック
C. 例外レポート
D. 自動調整
Answer: A (メーッセージを残す)
Continuous auditing provides the greatest assurance that a middleware application compiling data from multiple sales transaction databases for forecasting is operating effectively12. Continuous auditing involves the use of automated tools to continuously monitor and audit a system's operations12. This allows for real- time identification and resolution of issues, ensuring that the system is always functioning as expected12. It also provides ongoing assurance about the integrity and reliability of the data being compiled by the middleware application12.
References:
5 Data Integration Methods and Strategies | Talend
What Is Middleware? Definition, Architecture, and Best Practices

最新問題**: 478**
母集団内で比較的少ないエラーが見つかると予想される場合に使用する最適なサンプリング方法はどれですか?
A. 可変サンプリング
B. 判断的サンプリング
C. 停止または実行サンプリング
D. 検出サンプリング
Answer: D (メーッセージを残す)
Discovery sampling is a type of statistical sampling that's used when the expected error rate in the population is very low1. This method is designed to discover at least one instance of an attribute or condition in a population1. It's often used in auditing to uncover fraud or noncompliance with rules and regulations1.
References:
What are sampling methods and how do you choose the best one?

最新問題**: 479**
次のアプローチのうち、データ分析を利用して新しいアカウント作成プロセスのテストを容易にするものはどれですか?

A. 無効な生年月日で新しいアカウント申請を送信しようとしました。
B. 生年月日フィールドの要件については、ビジネス要件ドキュメントを確認してください。
C. 過去 1 か月間に提出された新規アカウント申請に無効な生年月日が含まれていないか確認します。
D. 生年月日フィールドの要件の設定を評価する
Answer: C (メーッセージを残す)
Data analytics is the process of collecting, transforming, analyzing, and visualizing data to gain insights and support decision making1. Data analytics can be used to facilitate the testing of a new account creation process by applying various techniques and methods to evaluate the quality, functionality, performance, and security of the process. One of the approaches that would utilize data analytics to test the new account creation process is to review new account applications submitted in the past month for invalid dates of birth.
This approach would involve the following steps:
Extract the data of new account applications from the source system, such as a database or a web service, using appropriate tools and methods.
Transform and clean the data to ensure its accuracy, completeness, consistency, and validity, using techniques such as data profiling, data cleansing, data mapping, and data validation2.
Analyze the data to identify any anomalies, errors, or outliers in the date of birth field, using methods such as descriptive statistics, exploratory data analysis, hypothesis testing, or anomaly detection3.
Visualize the data to present the findings and insights in a clear and understandable way, using tools and techniques such as charts, graphs, dashboards, or reports.
By reviewing new account applications submitted in the past month for invalid dates of birth, the tester can use data analytics to:
Verify if the new account creation process is working as expected and meets the business requirements and specifications for the date of birth field.
Detect any defects or issues in the new account creation process that may cause invalid dates of birth to be accepted or rejected incorrectly.
Measure and monitor the performance and reliability of the new account creation process in terms of data quality, accuracy, and completeness.
Evaluate and improve the test coverage and effectiveness of the new account creation process by identifying any gaps or risks in the test cases or scenarios.
Therefore, option C is the correct answer.
Option A is not correct because attempting to submit new account applications with invalid dates of birth is not a data analytics approach, but a functional testing approach that involves executing test cases or scenarios manually or automatically to validate the behavior and functionality of the new account creation process.
Option B is not correct because reviewing the business requirements document for date of birth field requirements is not a data analytics approach, but a requirements analysis

approach that involves examining and understanding the needs and expectations of the stakeholders for the new account creation process.
Option D is not correct because evaluating configuration settings for date of birth field requirements is not a data analytics approach, but a configuration testing approach that involves verifying if the settings and parameters of the new account creation process are correct and consistent with the requirements.
References:
What is Data Analytics? Definition & Examples1
Data Transformation: Definition & Examples2
Data Analysis: Definition & Examples3
Data Visualization: Definition & Examples
Functional Testing: Definition & Examples
Requirements Analysis: Definition & Examples
Configuration Testing: Definition & Examples

最新問題**: 480**
ロボティクス ･プロセス ･オートメーション (RPA) の実装を監査する際に、情報システム監査人が最初に行うべきことはどれですか?
A. ソリューション アーキテクチャ全体を評価します。
B. ロボットが実行するアクティビティのシーケンスを分析します。
C. ロボットが使用する資格情報とその保存場所を識別します。
D. ロボットによって自動化されるビジネス プロセスを理解します。
Answer: (解答を表示する**)**

最新問題**: 481**
IS 監査人は、組織のデータ損失防止 (DLP) システムがベンダーのデフォルト設定を使用して違反を特定するように構成されていることを発見しました。監査人の主な懸念事項は次のようになります。
A. 組織のリスク プロファイルに応じて、違反レポートが保持されない場合があります。
B. 多数の誤検知違反が報告される可能性があります。
C. 違反は組織のリスク プロファイルに従って分類されない可能性があります。
D. 違反報告は適時に確認されない可能性があります。
Answer: C (メーッセージを残す**)**

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

https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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: **482**
データ センターの物理アクセス ログ システムは、各訪問者の身分証明書番号と訪問者の写真を記録します。システムの有効性に関するコンプライアンス テストを実施する情報システム監査人にとって、次のサンプリング方法のうち最も役立つものはどれですか。
A. クォータサンプリング
B. 無作為抽出
C. 属性サンプリング
D. 可変サンプリング
Answer: C (メーッセージを残す**)**
Attribute sampling is a method of audit sampling that is used to test the effectiveness of controls by measuring the rate of deviation from a prescribed procedure or attribute. Attribute sampling is suitable for testing compliance with the data center's physical access log system, as the auditor can compare the identification document numbers and photos of the visitors with the records in the system and determine whether there are any discrepancies or errors. Attribute sampling can also provide an estimate of the deviation rate in the population and allow the auditor to draw a conclusion about the operating effectiveness of the control.
Variable sampling, on the other hand, is a method of audit sampling that is used to estimate the amount or value of a population by measuring a characteristic of interest, such as monetary value, quantity, or size.
Variable sampling is not appropriate for testing compliance with the data center's physical access log system, as the auditor is not interested in estimating the value of the population, but rather in testing whether the system is operating as intended.
Quota sampling and haphazard sampling are both examples of non-statistical sampling methods that do not use probability theory to select a sample. Quota sampling involves selecting a sample based on certain criteria or quotas, such as age, gender, or location. Haphazard sampling involves selecting a sample without any specific plan or method. Both methods are not suitable for testing compliance with the data center's physical access log system, as they do not ensure that the sample is representative of the population and do not allow the auditor to measure the sampling risk or project the results to the population.
Therefore, attribute sampling is the most useful sampling method for an IS auditor conducting compliance testing for the effectiveness of the data center's physical access log system.
References:
* Audit Sampling - What Is It, Methods, Example, Advantage, Reason
* ISA 530: Audit sampling | ICAEW

最新問題: **483**
CFO は、月末報告中に財務システムが何度も減速したため、IT 容量管理の監査を要求しました。この監査をプログラムに含める前に考慮すべき最も重要なことは何でしょうか。
A. システムの遅延により手動処理の使用頻度が高まるかどうか
B. システムのパフォーマンスが組織に重大なリスクをもたらすかどうか
C. ステークホルダーが監査に協力する意思があるかどうか
D. 内部監査員が監査を実施するために必要なスキルを持っているかどうか
Answer: B (メーッセージを残す)
The most important thing to consider before including an audit of IT capacity management in the program is whether the system's performance poses a significant risk to the organization. IT capacity management is a process that ensures that IT resources are sufficient to meet current and future business needs, and that they are optimized for cost and performance. A poor IT capacity management can result in system slowdowns, outages, failures, or breaches, which can affect the availability, reliability, security, and efficiency of IT services and business processes. Therefore, before conducting an audit of IT capacity management, the auditor should assess the potential impact and likelihood of these risks on the organization's objectives, reputation, compliance, and customer satisfaction.
Whether system delays result in more frequent use of manual processing (option A) is not the most important thing to consider before including an audit of IT capacity management in the program, as it is only one possible consequence of poor IT capacity management. Manual processing can introduce errors, delays, inefficiencies, and inconsistencies in the data and reports, which can affect the quality and accuracy of financial information. However, manual processing is not the only or the worst outcome of poor IT capacity management; there may be other more severe or frequent risks that need to be considered.
Whether stakeholders are committed to assisting with the audit (option C) is also not the most important thing to consider before including an audit of IT capacity management in the program, as it is a factor that affects the feasibility and effectiveness of the audit, not the necessity or priority of it. Stakeholder commitment is important for ensuring that the auditor has access to relevant information, documents, data, and personnel, as well as for facilitating communication, collaboration, and feedback during the audit process. However, stakeholder commitment is not a sufficient reason to conduct an audit of IT capacity management; there must be a clear risk-based rationale for selecting this area for audit.
Whether internal auditors have the required skills to perform the audit (option D) is also not the most important thing to consider before including an audit of IT capacity management in the program, as it is a factor that affects the quality and credibility of the audit, not the urgency or importance of it. Internal auditors should have the appropriate knowledge, skills, and experience to perform an audit of IT capacity management, which may include technical, business, analytical, and communication skills. However, internal auditors can

also acquire or supplement these skills through training, coaching, consulting, or outsourcing.
Therefore, internal auditors' skills are not a decisive factor for choosing this area for audit.
Therefore, option B is the correct answer.
References:
* Guide to IT Capacity Management | Smartsheet
* ISO 27001 capacity management: How to implement control A.12.1.3 - Advisera
* ISO 27002:2022 - Control 8.6 - Capacity Management

最新問題**: 484**
実装後のレビューの主な焦点は、次のことを確認することです。
A. エンタープライズ アーキテクチャ (EA) に準拠しています。
B. ユーザー要件が満たされています。
C. 受け入れテストは適切に実行されました。
D. ユーザーのアクセス制御は適切に設計されています。
Answer: (解答を表示する**)**
The primary focus of a post-implementation review is to verify that user requirements have been met. User requirements are specifications that define what users need or expect from a system or service, such as functionality, usability, reliability, etc. User requirements are usually gathered and documented at the beginning of a project, and used as a basis for designing, developing, testing, and implementing a system or service. A post-implementation review is an evaluation that assesses whether a system or service meets its objectives and delivers its expected benefits after it has been implemented. The primary focus of a post- implementation review is to verify that user requirements have been met, as this can indicate whether the system or service satisfies the user needs and expectations, provides value and quality to the users, and supports the user goals and tasks. Enterprise architecture (EA) has been complied with is a possible focus of a post-implementation review, but it is not the primary one. EA is a framework that defines how an organization's business processes, information systems, and technology infrastructure are aligned and integrated to support its vision and strategy. EA has been complied with, as this can indicate whether the system or service fits with the organization's current and future state, and follows the organization's standards and principles. Acceptance testing has been properly executed is a possible focus of a post-implementation review, but it is not the primary one. Acceptance testing is a process that verifies whether a system or service meets the user requirements and expectations before it is accepted by the users or stakeholders. Acceptance testing has been properly executed, as this can indicate whether the system or service has been tested and validated by the users or stakeholders, and whether any issues or defects have been identified and resolved.
User access controls have been adequately designed is a possible focus of a post-implementation review, but it is not the primary one. User access controls are mechanisms

that ensure that only authorized users can access or use a system or service, and prevent unauthorized access or use. User access controls have been adequately designed, as this can indicate whether the system or service has appropriate security and privacy measures in place, and whether any risks or threats have been mitigated.

最新問題**: 485**
新しいコード開発における職務分離の競合に対する最適な補償制御は次のどれですか?
A. 変更承認委員会に開発者を追加する
B. 少数の人がコードをデプロイする権限を持っている
C. 実装後の変更レビュー
D. ステージング環境の作成
Answer: C (メーッセージを残す**)**
A post-implementation change review is the best compensating control against segregation of duties conflicts in new code development. This process involves a thorough review of the changes after they have been implemented to ensure that they meet their objectives and that the stakeholders are satisfied with the results1.
It provides an opportunity to identify and correct any issues or conflicts that may have arisen during the development and implementation process. While other options like adding developers to the change approval board, limiting code deployment access to a small number of people, and creating staging environments can also serve as compensating controls, a post-implementation change review provides a more comprehensive and effective control mechanism21.
References:
Review and Close Change process ST 2 5 - Micro Focus
Change Management for SOC: Risks, Controls, Audits, Guidance

最新問題**: 486**
ある組織が、データ分類スキームに従ってデータベース テーブルを分類したいと考えています。IS 監査人の観点から見ると、テーブルは次の基準に基づいて分類する必要があります。
A. テーブルにアクセスできるエンドユーザーの数。
B. テーブル内の列名の説明。
C. テーブルの更新頻度。
D. 各単一テーブルの特定の機能内容。
Answer: D (メーッセージを残す**)**

最新問題**: 487**
IS リソースの最も効率的な使用を効果的に促進する課金方法は次のとおりです。
A. 特定の使用状況に結び付けられる特定の料金。
B. 完全な動作能力を達成するための総使用率。

C. 実際に発生した費用を超える残余収入。
D. 料金を吸収する能力に基づいた割り当て。
Answer: A (メーッセージを残す**)**
The charging method for IS resources is the way that the IS function allocates its costs to the users or business units that consume its services. The charging method can affect the behavior and incentives of the users and the IS function, as well as the efficiency and effectiveness of the IS resources. Therefore, choosing an appropriate charging method is an important decision for the IS function and its stakeholders.
One of the possible charging methods is to charge specific costs that can be tied back to specific usage. This means that the IS function tracks and measures the actual consumption of each user or business unit for each IS service, and charges them accordingly. For example, if a user uses 10 GB of storage space, 5 hours of CPU time, and 100 MB of network bandwidth, the IS function will charge them based on the unit costs of these resources. This charging method has the advantage of encouraging the most efficient use of IS resources, as it provides clear and accurate feedback to the users about their consumption and costs, and motivates them to optimize their usage and avoid waste or overuse. This charging method also aligns the interests of the IS function and the users, as both parties benefit from reducing costs and improving efficiency.
The other possible charging methods are:
* Total utilization to achieve full operating capacity: This means that the IS function charges a fixed amount to each user or business unit based on their proportion of the total operating capacity of the IS resources. For example, if a user or business unit has 10% of the total computing power allocated to them, they will pay 10% of the total IS costs. This charging method has the disadvantage of discouraging efficient use of IS resources, as it does not reflect the actual consumption or usage of each user or business unit, and does not provide any incentive to reduce costs or improve efficiency. This charging method also creates a mismatch between the interests of the IS function and the users, as the IS function benefits from increasing costs and capacity, while the users bear the burden of paying for them.
* Residual income in excess of actual incurred costs: This means that the IS function charges a markup or profit margin on top of its actual incurred costs to each user or business unit. For example, if a user or business unit consumes $100 worth of IS resources, the IS function will charge them $120, where $20 is the residual income for the IS function. This charging method has the disadvantage of discouraging efficient use of IS resources, as it increases the costs for the users and reduces their value for money. This charging method also creates a conflict between the interests of the IS function and the users, as the IS function benefits from increasing costs and profits, while the users suffer from paying more than they should.
* Allocations based on the ability to absorb charges: This means that the IS function charges different amounts to different users or business units based on their ability to pay or their profitability. For example, if a user or business unit is more profitable or has a

higher budget than another user or business unit, they will pay more for the same amount of IS resources. This charging method has the disadvantage of discouraging efficient use of IS resources, as it does not reflect the actual consumption or usage of each user or business unit, and does not provide any incentive to reduce costs or improve efficiency. This charging method also creates an unfair and arbitrary distribution of costs among the users or business units, as some pay more than others for no valid reason. References: 1: Charging Methods for IT Services - IT Process Wiki 2: IT Chargeback Methods - CIO Wiki 3: IT Chargeback - Wikipedia

最新問題: **488**
ネットワーク アナリストが営業時間外にネットワークを監視し、重要なサーバーを侵害しようとするブルート フォース攻撃と思われるアクティビティを検出しました。アラートを確認して正確性を確認した後、次に何をすべきでしょうか。
A. 影響を受けるシステムを分離します。
B. インシデント対応計画を呼び出します。
C. 根本原因分析を実行します。
D. 実行したすべての手順を書面によるレポートに記録します。
Answer: (解答を表示する**)**

最新問題: **489**
監査業務中に発見された問題の修復における情報システム監査人の主な役割は次のとおりです。
A. 更新されたポリシーを経営陣に提示し、承認を得ます。
B. 問題の責任を負い、修復作業を監督します。
C. 調査結果を説明し、一般的なアドバイスを提供します。
D. ソリューションを提供することで監査対象者の管理を支援します。
Answer: (解答を表示する**)**

最新問題: **490**
IT リソースの支出が計画されたプロジェクト支出と一致しているかどうかを判断するための最良の方法は何ですか?
A. 達成価値分析 (EVA)
B. 投資収益率（ROI）分析
C. ガントチャート
D. クリティカルパス分析
Answer: A (メーッセージを残す**)**
The best method to determine if IT resource spending is aligned with planned project spending is earned value analysis (EVA). EVA is a technique that compares the actual cost, schedule, and scope of a project with the planned or budgeted values. EVA can help

to measure the project progress and performance, and identify any variances or deviations from the baseline plan1.
EVA uses three basic values to calculate the project status: planned value (PV), earned value (EV), and actual cost (AC). PV is the amount of work that was expected to be completed by a certain date, according to the project plan. EV is the amount of work that was actually completed by that date, measured in terms of the budgeted cost. AC is the amount of money that was actually spent to complete the work by that date1.
By comparing these values, EVA can determine if the project is on track, ahead, or behind schedule and budget. EVA can also calculate various indicators, such as cost variance (CV), schedule variance (SV), cost performance index (CPI), and schedule performance index (SPI), to quantify the magnitude and direction of the variances. EVA can also forecast the future performance and completion of the project, based on the current trends and assumptions1.
The other options are not as effective as EVA in determining if IT resource spending is aligned with planned project spending. Option B, return on investment (ROI) analysis, is a technique that evaluates the profitability or efficiency of an investment, by comparing the benefits or revenues with the costs. ROI analysis can help to justify or prioritize a project, but it does not measure the actual progress or performance of the project against the plan2. Option C, Gantt chart, is a tool that displays the tasks, durations, dependencies, and milestones of a project in a graphical format. Gantt chart can help to plan and monitor a project schedule, but it does not show the actual cost or scope of the project3. Option D, critical path analysis, is a technique that identifies the longest sequence of tasks or activities that must be completed on time for the project to finish on schedule. Critical path analysis can help to optimize and control a project schedule, but it does not account for the actual cost or scope of the project4.
References:
* Earned Value Analysis & Management (EVA/EVM) - Definition & Formulae1
* Return on Investment (ROI) Formula2
* What Is a Gantt Chart?3
* Critical Path Method for Project Management

最新問題**: 491**
監査報告書の草案の議論中に、IT 管理者は、情報システム監査人が無効と結論付けた制御に対してプロセスが実装されているという適切な証拠を提供しました。監査人の最善の処置は次のどれですか。
A. 新しいコントロールはフォローアップ中に評価されることをIT管理者に説明する
B. 結論を変更する前に監査を再実行します。
C. IT 管理者によって提供された証拠に基づいて結論を変更します。
D. レポートで IT 管理者が実行したアクションに関するコメントを追加します。
Answer: B (メーッセージを残す**)**

The auditor's best action when IT management provides suitable evidence for a control that had been concluded as ineffective is to re-perform the audit before changing the conclusion. This means that the auditor should verify the validity, completeness, and timeliness of the evidence provided by IT management and test the effectiveness of the new control in meeting the audit objectives. The auditor should not change the conclusion based on evidence provided by IT management without re-performing the audit, as this could compromise the auditor's independence and objectivity. The auditor should also not explain to IT management that the new control will be evaluated during follow-up or add comments about the action taken by IT management in the report, as these actions do not address the original audit finding. References: CISA Review Manual, 27th Edition, page 439

最新問題**: 492**
BYOD (個人所有デバイスの持ち込み) ポリシーで許可されているデバイスに関連する組織のネットワークへのリスクを軽減するための最良の方法はどれですか?
A. 個人用デバイスを IT スタッフによって確認する必要があります。
B. すべてのネットワーク スイッチでポート セキュリティを有効にします。
C. ネットワーク アクセス制御システムを実装します。
D. ポリシーでデバイスにウイルス対策ソフトウェアが必須であることを確認します。
Answer: C (メーッセージを残す**)**
The best way to mitigate risk to an organization's network associated with devices permitted under a BYOD policy is to implement a network access control system, as this will allow the organization to monitor, authenticate, and authorize the devices that connect to the network, and to enforce security policies and compliance requirements12. A network access control system can help to prevent unauthorized or compromised devices from accessing sensitive data or resources, and to detect and isolate any potential threats or vulnerabilities34.
References
1: Network Access Control (NAC) - ISACA 2: Network Access Control (NAC) - Cisco 3: BYOD Security Risks: 6 Ways to Protect Your Organization - ReliaQuest5 4: How to Mitigate BYOD Risks and Challenges - CIOReview6

最新問題**: 493**
ピアツーピア (P2P) コンピューティング環境でファイル転送の整合性を確保するための効果的な方法はどれですか?
A. 環境内のピア間で共有されるパケットを暗号化します。
B. 環境内のクライアント コンピューターをジャンプ サーバーに接続します。
C. 転送される各ファイルにメッセージ認証コードを関連付けます。
D. ファイルが侵入検知システム (IDS) を介して転送されていることを確認します。
Answer: (解答を表示する**)**

最新問題: **494**
組織の災害復旧計画 (DRP) を確認する情報システム監査人にとって、最も懸念すべき事項は次のどれですか?
A. DRP は上級管理職によって正式に承認されていません。
B. DRP はエンドユーザーに配布されていません。
C. IT インフラストラクチャのアップグレード以降、DRP は更新されていません。
D. DRP には重要なサーバーのみの回復手順が含まれています。
Answer: C (メーッセージを残す**)**
The greatest concern for an IS auditor reviewing an organization's disaster recovery plan (DRP) is that the DRP has not been updated since an IT infrastructure upgrade. This could render the DRP obsolete or ineffective, as it may not reflect the current configuration, dependencies or recovery requirements of the IT systems. The IS auditor should ensure that the DRP is reviewed and updated regularly to align with any changes in the IT environment. The DRP has not been formally approved by senior management is a concern for an IS auditor reviewing an organization's DRP, but it is not as critical as ensuring that the DRP is up to date and valid. The DRP has not been distributed to end users or the DRP contains recovery procedures for critical servers only are issues that relate to the communication or scope of the DRP, but not to its validity or effectiveness.
References: ISACA, CISA Review Manual, 27th Edition, 2018, page 389

最新問題: **495**
IS 監査人は、ローン承認のための機械学習アルゴリズム ベースのシステムをレビューしており、アルゴリズムの偏りをテストするためのデータ セットを準備しています。監査人のテスト データ セットに含めるべき最も重要なのは次のどれですか。
A. あらゆる年齢層の応募者
B. 重複レコード
C. 不完全なレコードと不正な形式のデータ
D. さまざまな地域や所得レベルの応募者
Answer: (解答を表示する**)**

最新問題: **496**
インシデント対応計画のテーブルトップ演習の主な利点は次のどれですか?
A. インシデント対応プログラムの成熟度を示します。
B. インシデントが発生する可能性を低減します。
C. 動作環境の欠陥を特定します。
D. チームの対応準備に対する信頼を高めます。
Answer: D (メーッセージを残す**)**
The primary benefit of a tabletop exercise for an incident response plan is to increase confidence in the team's response readiness (D). A tabletop exercise is a simulated

scenario that tests the effectiveness and efficiency of the incident response plan and team. It allows the team to practice their roles and responsibilities, review their procedures and tools, and identify and resolve any gaps or issues in their response process. A tabletop exercise can help the team to improve their skills, knowledge, and communication, and to prepare for real incidents1.

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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: **497**
次のコントロールのうち、システム構成を通じて最もよく実装されるものはどれですか?
A. 臨時従業員のネットワーク ユーザー アカウントは 90 日後に期限切れになります。
B. アプリケーション ユーザー アクセスは、適切性について 180 日ごとに確認されます。
C. 主要レポートの財務データは、完全性と正確性を保つためにソース システムまで追跡されます。
D. コンピュータ運用担当者は毎日バッチ処理ジョブを開始します。
Answer: A (メーッセージを残す)
This control is best implemented through system configuration because it can be enforced automatically by setting a parameter in the network operating system or directory service. This ensures that temporary workers do not have access to the network beyond their authorized period, and reduces the risk of unauthorized or malicious use of their accounts12.
References1: Configuration and Change Management - CISA2: What is IT Governance? - Definition from Techopedia

最新問題: **498**
次の活動のうち、組織内に存在する可能性のある個人への依存関係に関して、情報システム監査人に最も多くの洞察を提供するものはどれですか?
A. 休暇パターンの見直し
B. ユーザーアクティビティログの確認
C. 上級IT管理者へのインタビュー
D. ITプロセスを役割にマッピングする
Answer: D (メーッセージを残す)

Mapping IT processes to roles is an activity that provides an IS auditor with the most insight regarding potential single person dependencies that might exist within the organization. Single person dependencies occur when only one person has the knowledge, skills, or access rights to perform a critical IT function.
Mapping IT processes to roles can help to identify such dependencies and assess their impact on the continuity and security of IT operations. The other activities do not provide as much insight into single person dependencies, as they do not show the relationship between IT processes and roles. References: CISA Review Manual, 27th Edition, page 94

最新問題**: 499**
主要なシステムアップグレードの実装後レビューを実行する情報システム監査人にとって、最も懸念すべき事項は次のどれですか?
A. 変更承認は正式に文書化されていません。
B. オブジェクト コードには開発グループがアクセスできます。
C. 変更は開発グループによって本番環境にプロモートされます。
D. 開発者はテスト環境にアクセスできます。
Answer: C (メーッセージを残す**)**

最新問題**: 500**
従業員による機密情報の不注意な開示に関連するリスクを軽減するための、情報システム監査人の最善の推奨事項は次のどれですか?
A. 侵入防止システム (IPS) とファイアウォール
B. データ損失防止 (DLP) テクノロジー
C. 暗号化保護
D. メールフィッシングシミュレーション演習
Answer: B (メーッセージを残す**)**
DLP technologies are designed to prevent the unauthorized transmission or leakage of sensitive data, such as PII, intellectual property, or financial information, by employees or other insiders. DLP technologies can monitor, detect, and block data in motion, data at rest, and data in use across various channels, such as email, web, cloud, or removable devices. DLP technologies can also help enforce data security policies and compliance requirements.
References
ISACA CISA Review Manual, 27th Edition, page 253
The role of disclosures in risk assessment and mitigation
Mitigate Risk Strategy for Information Management

最新問題**: 501**
シグネチャベースの侵入検知システム (LDS) の有効性を示す最良の指標は次のどれですか?

A. 誤検出数の増加
B. これまで特定されていなかったインシデントの検出数の増加
C. 未知の侵入者の増加
D. 内部報告された重大なインシデント数の増加
Answer: B (メーッセージを残す**)**
Signature-based intrusion detection systems (IDS) are systems that compare network traffic with predefined patterns of known attacks, called signatures. The effectiveness of signature-based IDS depends on how well they can detect new or unknown attacks that are not in their signature database. Therefore, an increase in the number of detected incidents not previously identified is the best indicator of the effectiveness of signature-based IDS, as it shows that they can recognize novel or modified attacks.

最新問題**: 502**
ある企業では、すべてのプログラム変更要求 (PCR) が承認され、すべての変更が自動的に記録されることを要求しています。次の IS 監査手順のうち、生産プログラムに許可されていない変更が加えられたかどうかを最も適切に判断できるのはどれですか。
A. 完全なPCRフォームのサンプルをすべてのプログラム変更のログにトレースします
B. ソースコード比較ソフトウェアを使用して、前回の監査日以降にサンプルプログラムに変更が加えられたかどうかを判断します。
C. プログラム変更プロセス全体を通じてPCRのサンプルを確認し、適切な承認を得る
D. ログから完成したPCRフォームまでのプログラム変更のサンプルをトレースします。
Answer: (解答を表示する**)**
The best way to determine whether unauthorized changes have been made to production programs is to use source code comparison software to compare the current version of the programs with the previous version or the approved version. This will identify any changes that have been made without proper authorization or documentation. Tracing PCRs to logs or vice versa will only verify that the authorized changes have been recorded, but not detect any unauthorized changes. References: Standards, Guidelines, Tools and Techniques
- ISACA, section "IS Audit and Assurance Tools and Techniques"

最新問題**: 503**
年次内部監査計画の策定に携わっている情報システム監査人は、最高情報責任者 (CIO) が、前年度の多数の推奨事項に対処するためにさらに時間が必要であるため、翌年度は情報システム監査を行わないよう要求していることを知ります。監査人が最初に行うべきことは、次のどれですか。
A. 監査計画について話し合うために監査管理者にエスカレーションする
B. 最高執行責任者（COO）に通知し、監査計画のリスクについて話し合う
C. 次年度の計画からIS監査を除外する
D. クラン内のIS監査の数を増やす

Answer: A (メーッセージを残す)
The auditor should first escalate to audit management to discuss the audit plan. This is because the audit plan should be based on a risk assessment and aligned with the organization's objectives and strategies. The auditor should not accept the CIO's request without proper justification and approval from the audit management, who are responsible for ensuring the audit plan's quality and independence. The auditor should also communicate the potential risks and implications of not conducting IS audits in the upcoming year, such as missing new or emerging threats, vulnerabilities, or compliance issues. References:
* CISA Review Manual (Digital Version), Chapter 2, Section 2.11
* CISA Online Review Course, Domain 1, Module 1, Lesson 22

最新問題**: 504**
リスク管理の観点から、大規模で複雑なデータセンターの IT インフラストラクチャを実装する場合、次のうちどれが最適なアプローチでしょうか?
A. 展開前に新しいインフラストラクチャをシミュレートする
B. プロトタイピングと 1 フェーズの展開
C. 段階的なフェーズに基づいた展開計画
D. 概念実証に成功したビッグバン展開
Answer: C (メーッセージを残す)
The best approach from a risk management perspective when implementing a large and complex data center IT infrastructure is to use a deployment plan based on sequenced phases, as this will allow the organization to break down the project into manageable and measurable stages, and to monitor and control the progress, quality, and outcomes of each phase12. A phased deployment plan can also help to reduce the risks of errors, failures, or disruptions that could affect the entire infrastructure, and to implement corrective actions or contingency plans as needed34.
References
1: Data Center Project Planning: A Guide to Success2 2: Data Center Project Planning: A Guide to Success4 3: Data Center Migration: A Step-by-Step Guide3 4: Data Center Migration: A Step-by-Step Guide1

最新問題**: 505**
ある組織が新しいデータ損失防止 (DLP) ツールを導入しています。次のうちどれが、組織が誤検知アラートを減らすのに最も効果的でしょうか?
A. デフォルトのポリシーとツールルールセットを使用する
B. 限定されたルールセットの設定
C. モニターモードでツールを展開する
D. 検出ポイントの数を減らす
Answer: B (メーッセージを残す)

To reduce false positive alerts, it is essential to carefully configure a limited set of rules tailored to the organization's specific data loss prevention needs. This ensures that the DLP tool accurately identifies true positives and reduces the occurrence of false alarms.
References
* ISACA CISA Review Manual 27th Edition, Page 304-305 (DLP Tool Configuration)

最新問題: **506**
コンピューターフォレンジック監査は、次のどの状況に最も関連しますか?
A. IT 環境における不十分な制御
B. 取引データの不一致
C. サーバーパッチが不足しています
D. サーバーのハッキングによるデータ損失
Answer: D (メーッセージを残す**)**
A computer forensic audit is a process of collecting, preserving, analyzing, and presenting digital evidence from electronic devices in a legally admissible manner. It is most relevant in situations where data loss due to hacking of servers occurs, as it can help to identify the source, method, and extent of the attack, as well as recover the lost or damaged data. The other options are not as suitable for a computer forensic audit, as they relate to internal control issues, data quality issues, or system maintenance issues, which can be addressed by other types of audits or reviews. References: CISA Review Manual (Digital Version), Domain 4: Information Systems Operations and Business Resilience, Section 4.5 Computer Forensics1

最新問題: **507**
IT 意思決定における投資収益率 (ROI) アナリストの利点の 1 つは、次の点です。
A. 間接費を配分するための基準。
B. 機器の交換にかかる費用。
C. 推定所有コスト。
D. 財源を配分するための基準。
Answer: D (メーッセージを残す**)**
One benefit of return on investment (ROI) analysis in IT decision making is that it provides the basis for allocating financial resources. ROI analysis is a method of evaluating the profitability or cost-effectiveness of an IT project or investment by comparing the expected benefits with the required costs. ROI analysis can help IT decision makers prioritize and justify their IT initiatives, allocate their financial resources optimally, and demonstrate the value contribution of IT to the organization's goals and objectives. Basis for allocating indirect costs, cost of replacing equipment, and estimated cost of ownership are not benefits of ROI analysis in IT decision making. These are more inputs or outputs of ROI analysis that could be used to calculate or estimate the costs or benefits of an IT project or investment. References: [ISACA CISA Review Manual 27th Edition], page 307

最新問題: **508**
アプリケーション プログラミング インターフェイス (API) クエリを通じてデータが公開されるリスクを軽減するには、次の設計上の考慮事項のうちどれが最も重要ですか?
A. データ保持
B. データの最小化
C. データ品質
D. データの整合性
Answer: B (メーッセージを残す**)**
The answer B is correct because data minimization is the most important design consideration to mitigate the risk of exposing data through application programming interface (API) queries. An API is a set of rules and protocols that allows different software components or systems to communicate and exchange data. API queries are requests sent by users or applications to an API to retrieve or manipulate data. For example, a user may query an API to get information about a product, a service, or a location.
Data minimization is the principle of collecting, processing, and storing only the minimum amount of data that are necessary for a specific purpose. Data minimization can help to reduce the risk of exposing data through API queries by limiting the amount and type of data that are available or accessible through the API.
Data minimization can also help to protect the privacy and security of the data subjects and the data providers, as well as to comply with the relevant laws and regulations.
Some of the benefits of data minimization for API design are:
* Privacy: Data minimization can enhance the privacy of the data subjects by ensuring that only the data that are relevant and essential for the API purpose are collected and processed. This can prevent unnecessary or excessive collection or disclosure of personal or sensitive data, such as names, addresses, phone numbers, email addresses, etc. Data minimization can also help to comply with the privacy laws and regulations that require data protection by design and by default, such as GDPR (General Data Protection Regulation) or CCPA (California Consumer Privacy Act).
* Security: Data minimization can improve the security of the data providers by reducing the attack surface and the potential damage of a data breach. If less data are stored or transmitted through the API, there are fewer opportunities for attackers to access or compromise the data. Data minimization can also help to implement security controls such as encryption, access control, or logging more efficiently and effectively.
* Performance: Data minimization can increase the performance of the API by optimizing the use of resources and bandwidth. If less data are stored or transmitted through the API, there are less storage space and network traffic required. Data minimization can also help to improve the speed and reliability of the API responses.
Some of the techniques for data minimization in API design are:
* Define clear and specific purposes for the API and document them in the API specification or documentation.

* Identify and classify the data that are needed for each purpose and assign them appropriate labels or levels, such as public, internal, confidential, or restricted.
* Implement filters or parameters in the API queries that allow users or applications to specify or limit the data fields or attributes they want to retrieve or manipulate.
* Use pagination or throttling in the API responses that limit the number or size of data items returned per request.
* Use anonymization or pseudonymization techniques that remove or replace any identifying information from the data before sending them through the API.
Some examples of web resources that discuss data minimization in API design are:
* Data Minimization in Web APIs - World Wide Web Consortium (W3C)
* Adding Privacy by Design in Secure Application Development
* Chung-ju/Data-Minimization: A repository of related papers. - GitHub

最新問題**: 509**
従業員がパブリック ソーシャル ネットワーキング サイトを使用する場合、組織にとって最も大きなリスクとなるのは次のどれですか。
A. クロスサイトスクリプティング (XSS)
B. 著作権侵害
C. ソーシャルエンジニアリング
D. 組織に関する否定的な投稿
Answer: C (メーッセージを残す**)**
Social engineering is the manipulation of people to perform actions or divulge confidential information. It is a common technique used by attackers to gain unauthorized access to systems or data. Employees who use public social networking sites may be vulnerable to social engineering attacks, such as phishing, baiting, or pretexting, which pose the greatest risk to the organization's security. The other options are not as serious as social engineering, as they relate to web application vulnerabilities, intellectual property rights, and reputation management, which are less likely to compromise the organization's assets or operations. References: CISA Review Manual (Digital Version), Domain 5: Protection of Information Assets, Section 5.3 Security Awareness Training1

最新問題**: 510**
機密データを含む外部向けシステムは、ユーザーが読み取り専用権限または管理者権限を持つように構成されています。システムのほとんどのユーザーは管理者アクセス権を持っています。この状況に関連する最大のリスクは次のどれですか?
A. ユーザーはアプリケーション ログをエクスポートできます。
B. ユーザーは機密データを閲覧できます。
C. ユーザーは許可されていない変更を行うことができます。
D. ユーザーはオープンライセンスのソフトウェアをインストールできます。
Answer: C (メーッセージを残す**)**

The greatest risk associated with having most users with administrator access to an externally facing system containing sensitive data is that users can make unauthorized changes to the system or the data, which could compromise the integrity, confidentiality, and availability of the system and the data. Users can export application logs, view sensitive data, and install open-licensed software are also risks, but they are not as severe as unauthorized changes. References: ISACA CISA Review Manual 27th Edition Chapter 4

最新問題: **511**
次のどれが是正制御ですか?
A. 機器開発テストと製造の分離
B. データ処理における重複計算の検証
C. 分離のためのユーザーアクセス権の見直し
D. 緊急対応計画の実行
Answer: D (メーッセージを残す**)**
A corrective control is a control that aims to restore normal operations after a disruption or incident has occurred. Executing emergency response plans is an example of a corrective control, as it helps to mitigate the impact of an incident and resume business functions.
Separating equipment development testing and production is a preventive control, as it helps to avoid errors or unauthorized changes in production systems.
Verifying duplicate calculations in data processing is a detective control, as it helps to identify errors or anomalies in data processing. Reviewing user access rights for segregation is also a detective control, as it helps to detect any violations of segregation of duties principles. References: ISACA, CISA Review Manual,
27th Edition, 2018, page 64

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら:
https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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: **512**
来年にどの IS 監査を実施するかを選択するための主な基準は何でしょうか?
A. 上級管理職の要請
B. 前年度の監査結果
C. 組織のリスク評価
D. 以前の監査範囲と範囲

Answer: C (メーッセージを残す)
The primary basis for selecting which IS audits to perform in the coming year is the organizational risk assessment. An organizational risk assessment is a formal process for identifying, evaluating, and controlling risks that may affect the achievement of the organization's goals and objectives3. An organizational risk assessment can help IS auditors prioritize and plan their audit activities based on the level of risk exposure and impact of each area or process within the organization. An organizational risk assessment can also help IS auditors align their audit objectives and criteria with the organization's strategy and performance indicators. Senior management's request, prior year's audit findings, and previous audit coverage and scope are also possible bases for selecting which IS audits to perform in the coming year, but not as primary as the organizational risk assessment. These factors are more secondary or supplementary sources of information that can help IS auditors refine or adjust their audit plan based on specific needs or issues identified by management or previous audits. However, these factors may not reflect the current or emerging risks that may affect the organization's operations or performance.
References: ISACA CISA Review Manual 27th Edition, page 295

最新問題**: 513**
IS 監査人は、知的財産と特許を担当する事業部門のコラボレーション ツールに関連するセキュリティ管理をレビューしています。次の観察事項のうち、監査人が最も注意すべきものはどれですか。
A. 知的財産や特許を扱う部門に研修が行われていなかった
B. コンテンツ フィルタリングのログ記録と監視が有効になっていません。
C. 従業員はコラボレーション ツールを通じて社外のユーザーとファイルを共有できます。
D. コラボレーションツールはホストされており、インターネットブラウザ経由でのみアクセスできます。
Answer: B (メーッセージを残す)
The observation that should be of most concern to the auditor when reviewing security controls related to collaboration tools for a business unit responsible for intellectual property and patents is that employees can share files with users outside the company through collaboration tools. Collaboration tools are software or hardware devices that enable users to communicate, cooperate, and coordinate with each other on a common task or project. Collaboration tools can facilitate information sharing and knowledge exchange among users, but they can also pose security risks if not properly controlled or managed. Employees can share files with users outside the company through collaboration tools, as this can compromise the security and confidentiality of intellectual property and patents, which are valuable and sensitive assets of the organization. Employees may share files with unauthorized or untrusted users who may misuse or disclose the intellectual property and patents, either intentionally or unintentionally. This can cause harm or damage to the organization, such as loss of competitive advantage,

reputation, revenue, or legal rights. Training was not provided to the department that handles intellectual property and patents is a possible observation that could indicate a security issue related to collaboration tools for a business unit responsible for intellectual property and patents, but it is not the most concerning one. Training is an activity that educates and instructs users on how to use collaboration tools effectively and securely, such as how to access, share, store, and protect information using collaboration tools. Training was not provided to the department that handles intellectual property and patents, as this can affect the awareness and competence of users on collaboration tools, and increase the likelihood of errors or mistakes that may compromise the security or quality of information. However, this observation may not be directly related to collaboration tools, as it may apply to any information system or resource used by the department. Logging and monitoring for content filtering is not enabled is a possible observation that could indicate a security issue related to collaboration tools for a business unit responsible for intellectual property and patents, but it is not the most concerning one. Logging and monitoring are processes that record and analyze the events or activities that occur on an information system or network, such as user actions, system operations, data changes, errors, alerts, etc. Content filtering is a technique that blocks or allows access to certain types of information based on predefined criteria or rules, such as keywords, categories, sources, etc. Logging and monitoring for content filtering is not enabled, as this can affect the auditability, accountability, and visibility of collaboration tools, and prevent detection or investigation of security incidents or violations related to information sharing using collaboration tools. However, this observation may not be specific to collaboration tools, as it may affect any information system or network that uses content filtering. The collaboration tool is hosted and can only be accessed via an Internet browser is a possible observation that could indicate a security issue related to collaboration tools for a business unit responsible for intellectual property and patents, but it is not the most concerning one. A hosted collaboration tool is a type of cloud-based service that provides collaboration functionality over the Internet without requiring installation or maintenance on local devices. An Internet browser is a software application that enables users to access and interact with web-based content or services. The collaboration tool is hosted and can only be accessed via an Internet browser, as this can affect the availability and reliability of collaboration tools, and introduce security or privacy risks for information sharing using collaboration tools. However, this observation may not be unique to collaboration tools, as it may apply to any cloud-based service that uses an Internet browser.

最新問題**: 514**
監査フレームワーク中、情報システム監査チームは、従業員が個人用デバイスを会社所有のコンピューターに接続することを許可されていることを確認します。監査人は、データ損失を防ぐために適切なセキュリティ制御が実施されていることをどのように検証するのが最善でしょうか?

A. ウォークスルーを実施して、従業員がデバイスを接続して機密データを転送した結果を確認します。
B. データ損失および該当するモバイル デバイスのユーザー受け入れポリシーへの準拠を確認します。
C. データ損失防止 (DLP) ツールが組織によって適切に構成されていることを確認します。
D. 従業員が適切なモバイル デバイスのセキュリティ意識向上トレーニングを受けていることを確認します。
Answer: (解答を表示する**)**
The best way to validate that appropriate security controls are in place to prevent data loss is to review compliance with data loss and applicable mobile device user acceptance policies. This will ensure that the organization has established clear rules and guidelines for employees to follow when connecting their personal devices to company-owned computers. A walk-through, a DLP tool configuration, and a security awareness training are not sufficient to validate the effectiveness of the controls, as they may not cover all possible scenarios and risks. References: IT Audit Fundamentals Certificate Resources

最新問題**: 515**
IS 監査人は、新しいネットワーク接続によってインターネットと社内のエンタープライズ リソース プランニング (ERP) システム間の通信が可能になったことを発見しました。この観察結果を経営陣に提示する際に含めるべき主なビジネス インパクトは次のどれですか。
A. ネットワークパフォーマンスの低下
B. 脅威の増大
C. ERP システムのデータ品質の低下
D. 規制当局からの罰金の可能性が増加
Answer: B (メーッセージを残す**)**

最新問題**: 516**
情報情報監査マネージャーが報告書の提出前に上級情報情報監査人が行った作業をレビューする主な理由は次のうちどれですか?
A. 結論が適切にサポートされていることを確認する
B. フィールドワーク中に適切なサンプリング方法が使用されたことを確認するには
C. 作業が適切に文書化され、提出されていることを確認するため
D. 作業が業界標準に従って確実に行われるようにするため
Answer: A (メーッセージを残す**)**
The primary reason for an IS audit manager to review the work performed by a senior IS auditor prior to presentation of a report is to ensure the conclusions are adequately supported. The IS audit manager is responsible for overseeing and supervising the audit process, ensuring the quality and consistency of the audit work, and approving the audit report and recommendations. The IS audit manager should review the work performed by the senior IS auditor to verify that the audit objectives, scope, and criteria have been met,

that the audit evidence is sufficient, reliable, and relevant, and that the audit conclusions are logical, objective, and based on the audit evidence. The IS audit manager should also ensure that the audit report is clear, concise, accurate, and complete, and that it communicates the audit findings, conclusions, and recommendations effectively to the intended audience. The other options are not the primary reason for an IS audit manager to review the work performed by a senior IS auditor prior to presentation of a report, because they either relate to specific aspects or stages of the audit work rather than the overall outcome, or they are part of the senior IS auditor's responsibility rather than the IS audit manager's. References: CISA Review Manual (Digital Version)1, Chapter 2, Section 2.2.5

最新問題: **517**
組織のセキュリティ情報およびイベント管理 (SIEM) ソリューションを確認する際に最も懸念されるのは次のどれですか。
A. SIEM レポートがカスタマイズされます。
B. SIEM構成は毎年見直される
C. SIEM は分散化されています。
D. SIEM レポートはアドホックです。
Answer: (解答を表示する**)**
The greatest concern that the IS auditor should have when reviewing an organization's security information and event management (SIEM) solution is that the SIEM is decentralized. This is because a decentralized SIEM can pose challenges for collecting, correlating, analyzing and reporting on security events and incidents from multiple sources and locations. A decentralized SIEM can also increase the complexity and cost of maintaining and updating the SIEM components, as well as the risk of inconsistent or incomplete security monitoring and response. The IS auditor should recommend that the organization adopts a centralized or hybrid SIEM architecture that can provide a holistic and integrated view of the security posture and activities across the organization. The other findings are not as concerning as a decentralized SIEM, because they can be addressed by implementing best practices and standards for SIEM reporting and configuration. References:
CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.4

最新問題: **518**
IS 監査人は、最近導入されたアプリケーションに、テスト環境から不適切な更新アクセス権が残っている開発者が多数いることを発見しました。更新アクセス権の移行を最も効果的に防止するには、次のうちどれが効果的でしょうか。
A. ユーザーのプロビジョニングのためのロールベースのマトリックスを確立する
B. システム開発ライフサイクル (SDLC) 内に、稼働前にアクセスをクリーンアップするステップを含める

C. アプリケーション所有者にアプリケーションセキュリティの責任を負わせる
D. 品質保証 (QA) 環境でのユーザー アクセス権の再割り当て
Answer: B (メーッセージを残す**)**

最新問題**: 519**
システム管理者がネットワーク管理者としての責任を負うことに伴うリスクを軽減するための最も効率的な制御は次のどれですか?
A. 管理者は予告なしの監査の対象となります。
B. 管理者は重要な変更を行うために一時的なアクセス権を取得する必要があります。
C. 管理者はデューデリジェンス契約に署名する必要があります。
D. 管理者は重要な変更に対して追加の承認を要求する必要があります。
Answer: D (メーッセージを残す**)**

最新問題**: 520**
データ漏洩を防ぐためにスマートデバイスのセキュリティを強化する最善の方法はどれですか?
A. 組織の機密データへのアクセス ログをタイムリーに確認します。
B. 従業員にセキュリティ手順を正式に承認するよう要求します。
C. スマート デバイスに強力なセキュリティ設定を適用します。
D. BYOD (個人所有デバイスの持ち込み) セキュリティ手順に使用制限を含めます。
Answer: C (メーッセージを残す**)**

最新問題**: 521**
組織のプライバシー プログラムの確立を支援する内部監査の適切な手順は次のどれですか。
A. 新しい規制によってもたらされるリスクの分析
B. 個人データを保護するための制御の設計
C. 組織内でのプライバシーに関する役割の定義
D. 個人データの使用を監視する手順の開発
Answer: (解答を表示する**)**
Analyzing risks posed by new regulations is an appropriate role of internal audit in helping to establish an organization's privacy program. An internal auditor can provide assurance and advisory services on the compliance and effectiveness of the privacy program, as well as identify and assess the potential risks and impacts of new or changing privacy regulations. The other options are not appropriate roles of internal audit, but rather the responsibilities of the management, the information security officer, or the privacy officer.
References:
* CISA Review Manual (Digital Version), Chapter 7, Section 7.4.21
* CISA Review Questions, Answers & Explanations Database, Question ID 216

最新問題: **522**
次の文書のうち、IT 監査組織内の役割と責任を明記する必要があるのはどれですか?
A. 組織図
B. 監査担当者
C. 契約書
D. 年間監査計画
Answer: (解答を表示する**)**
The audit charter is a document that defines the purpose, scope, authority, and responsibility of an IT audit organization. The audit charter should specify roles and responsibilities within an IT audit organization, such as who is accountable for approving the audit plan, who is responsible for conducting the audits, who is authorized to access the audit evidence, and who is accountable for reporting the audit results. The organizational chart, the engagement letter, and the annual audit plan are also important documents for an IT audit organization, but they do not specify roles and responsibilities as clearly and comprehensively as the audit charter.

最新問題: **523**
組織がインシデント対応チームの有効性を向上させるために最も効果的なのは次のうちどれですか?
A. 定期的なテストを実施し、学んだ教訓を取り入れる
B. 平均解決時間の増加と主要業績評価指標 (KPI) メトリックの公開
C. インシデント対応手順を周知し、チームメンバーによる署名付き承認を要求する
D. チームメンバー全員が情報システム技術を理解していることを確認する
Answer: (解答を表示する**)**
Conducting periodic testing and incorporating lessons learned is the best way to improve the effectiveness of an incident response team. This allows the team to practice their response procedures, identify any gaps or weaknesses in their response, and learn from their mistakes. It also helps to keep the team's skills sharp and up-to-date. The lessons learned from these tests can then be used to improve the team's procedures and performance12. While understanding information systems technology, disseminating incident response procedures, and publishing KPI metrics can contribute to the effectiveness of the team, they do not provide the same level of continuous improvement as periodic testing and learning from experience.

最新問題: **524**
情報セキュリティ プログラムの成功に最も重要なのは次のどれですか?
A. 情報セキュリティとIT目標の整合
B. 情報セキュリティに対する経営陣の取り組み
C. ビジネスと情報セキュリティの統合
D. 情報セキュリティに対するユーザーの責任

Answer: B (メーッセージを残す)
The correct answer is B. Management's commitment to information security.
Management's commitment to information security is the most critical factor for the success of an information security program, as it provides the leadership, support, and resources needed to establish and maintain a secure environment.
Management's commitment to information security can be demonstrated by:
Setting the vision, mission, and goals for information security, and aligning them with the organization's strategies and objectives1.
Establishing and enforcing the policies, standards, and procedures for information security, and ensuring compliance with relevant laws and regulations1.
Allocating sufficient budget, staff, and technology for information security, and investing in training and awareness programs2.
Promoting a culture of security within the organization, and engaging with stakeholders and partners to foster trust and collaboration2.

最新問題**: 525**
実装後のレビューを実施する際に決定することが最も重要なのは次のどれですか?
A. ソリューションアーキテクチャがIT標準に準拠しているかどうか
B. 成功基準が達成されたかどうか
C. プロジェクトが承認された予算内で完了したかどうか
D. チームで行われたレッスンが文書化されているかどうか
Answer: (解答を表示する)
The most important thing to determine when conducting a post-implementation review is whether success criteria have been achieved. A post-implementation review is a process of evaluating the results and outcomes of a project or initiative after it has been completed and implemented. The success criteria are the measurable indicators that define what constitutes a successful project or initiative in terms of its objectives, benefits, quality, performance, and stakeholder satisfaction. The IS auditor should verify whether the success criteria have been achieved by comparing the actual results and outcomes with the expected or planned ones, and by assessing whether they meet or exceed the expectations and requirements of the stakeholders. The IS auditor should also identify any gaps, issues, or risks that may affect the sustainability or scalability of the project or initiative, and provide recommendations for improvement or remediation. The other options are not as important as determining whether success criteria have been achieved when conducting a post- implementation review, because they either focus on specific aspects or components of the project or initiative rather than the overall value proposition, or they are part of the pre-implementation or implementation phases rather than the post-implementation phase. References: CISA Review Manual (Digital Version)1, Chapter 4, Section 4.2.3

最新問題**: 526**

アウトソーシングされたプロバイダーのサービスが適切に管理されていることを示す最良の証拠は次のどれですか?
A. サービス レベル アグリーメント (SLA) に準拠していない場合は、適切な措置が講じられます。
B. 社内のパフォーマンス基準は企業戦略と一致しています。
C. サービス レベル契約 (SLA) には、不履行に対する罰則が含まれます。
D. ベンダーはパフォーマンスを証明するために履歴データを提供します。
Answer: A (メーッセージを残す**)**

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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: **527**
IT 関連の顧客サービス プロジェクトをレビューする IS 監査人にとって、最も懸念されるのは次のどれでしょうか。
A. プロジェクトのリスクが組織のリスク許容度を超えています。
B. 期待されるビジネス価値は定性的な言葉で表現されます。
C. プロジェクトを実行するには追加の投資が必要になります。
D. 組織は提案されたサービスを最初に提供します。
Answer: A (メーッセージを残す**)**

最新問題: **528**
IS 監査人は、3 か月以内に廃止されるレガシー アプリケーションが、現在のポリシーで確立されたセキュリティ要件を満たせないことを特定しました。この問題に対処する最善の方法 (または監査人) は何ですか?
A. 要件を満たすためにアプリケーションにパッチを適用することを推奨します。
B. ポリシー非準拠について IT ディレクターに通知します。
C. 経営陣がリスクを受け入れるためのポリシー例外を承認したことを確認します。
D. アプリケーションは 3 か月以内に廃止されるため、何もする必要はありません。
Answer: (解答を表示する**)**
The best way for the auditor to address this issue is to verify management has approved a policy exception to accept the risk. A policy exception is a formal authorization that allows a deviation from the established policy requirements for a specific situation or period of time. A policy exception should be based on a risk assessment that evaluates the impact

and likelihood of the potential threats and vulnerabilities, as well as the cost and benefit of the alternative controls. A policy exception should also be documented, approved, and monitored by management.
Recommending the application be patched to meet requirements is not the best way for the auditor to address this issue. Patching the application may not be feasible, cost-effective, or timely, given that the application will be decommissioned in three months. Patching the application may also introduce new risks or errors that could affect the functionality or performance of the application.
Informing the IT director of the policy noncompliance is not the best way for the auditor to address this issue.
Informing the IT director of the policy noncompliance may not resolve the issue or mitigate the risk, especially if the IT director is already aware of the situation and has decided to accept it. Informing the IT director of the policy noncompliance may also create unnecessary conflict or tension between the auditor and the auditee.
Taking no action since the application will be decommissioned in three months is not the best way for the auditor to address this issue. Taking no action may expose the organization to significant risks or consequences, such as data breaches, regulatory fines, or reputational damage, if the application is compromised or exploited by malicious actors. Taking no action may also violate the auditor's professional standards and responsibilities, such as due care, objectivity, and reporting.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019, p. 289
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription
* Cybersecurity Engineering for Legacy Systems: 6 Recommendations - SEI Blog
* How to Secure Your Company's Legacy Applications - iCorps

最新問題**: 529**
IS 監査人は、あるデータベース管理システム (DBMS) から別のシステムへの移行に伴うリスクを評価しています。変更全体を通じてシステムの整合性を確保するのに最も役立つのは次のうちどれですか。
A. 同じデータ分類を維持する
B. 同じデータ入力を保持する
C. 同じデータ構造を維持する
D. 同じデータインターフェースを維持する
Answer: C (メーッセージを残す**)**
The most helpful thing to ensure the integrity of the system throughout the change when moving from one database management system (DBMS) to another is preserving the same data structure. A DBMS is a software system that manages and manipulates data stored in a database, such as creating, updating, querying, deleting, etc. A database is a collection of structured or organized data that can be accessed or manipulated by a

DBMS. A data structure is a way of organizing or arranging data in a database, such as tables, columns, rows, keys, indexes, etc. Preserving the same data structure when moving from one DBMS to another can help ensure the integrity of the system throughout the change, by maintaining the consistency and accuracy of data in the database, and avoiding any errors or issues that may arise from incompatible or inconsistent data structures between different DBMSs. Preserving the same data classifications is a possible thing to ensure the integrity of the system throughout the change when moving from one DBMS to another, but it is not the most helpful one. Data classifications are categories or labels that define the level of sensitivity or importance of data in a database, such as public, confidential, secret, etc. Data classifications can help protect the security and privacy of data in the database by applying appropriate controls or restrictions on data access or use based on their classifications. Preserving the same data classifications when moving from one DBMS to another can help ensure the integrity of the system throughout the change by preventing unauthorized or inappropriate access or use of data in the database. However, this may not be directly related to the DBMS change, as it may apply to any data migration or transfer process. Preserving the same data inputs is a possible thing to ensure the integrity of the system throughout the change when moving from one DBMS to another, but it is not the most helpful one. Data inputs are sources or methods that provide data to a database, such as user inputs, sensors, files, etc. Data inputs can affect the quality and validity of data in the database by introducing errors or inconsistencies in data entry or collection. Preserving the same data inputs when moving from one DBMS to another can help ensure the integrity of the system throughout the change by reducing errors or inconsistencies in data input or collection.

最新問題**: 530**
さまざまなプログラムで使用されているさまざまなテクノロジーの概要を把握するために、情報システム監査人が最初にインタビューする必要があるスタッフは次のうちどれですか?
A. テクニカルアーキテクト
B. プログラムマネージャー
C. エンタープライズアーキテクト
D. ソリューションアーキテクト
Answer: C (メーッセージを残す**)**

最新問題**: 531**
安全なサーバー ルームには、スタッフがバッジを使用して入退室するたびに名前、日付、および時刻の情報を記録するバッジ リーダー システムがあります。システム ログを確認すると、IS 監査人は、一部の従業員が部屋に入ったが退室していないという記録に気付きました。次のうち、推奨する最も効果的な補償制御はどれですか。
A. 玄関に防犯カメラを設置する

B. 生体認証アクセス制御システムへの変更
C. 入口と出口に監視付きマントラップを実装する
D. 入口と出口で二要素認証を要求する
Answer: C (メーッセージを残す**)**
A monitored mantrap at entrance and exit points would be the most effective compensating control in this scenario. A mantrap is a physical security access control system comprising a small space having two sets of interlocking doors such that the first set of doors must close before the second set opens. By implementing a monitored mantrap, unauthorized access can be prevented and it can ensure that all individuals are logged when they enter and exit the server room12.
References: ISACA's Information Systems Auditor Study Materials3

最新問題**: 532**
データセンターへの訪問者のアクセスを制御するために最も効果的なのは次のどれですか?
A. 訪問者は許可された従業員によって案内されます
B. 入場申請の事前承認
C. 訪問者は到着時にフロントデスクでサインインします
D. 施設の監視には閉回路テレビ（CCTV）が使用される
Answer: A (メーッセージを残す**)**
The most effective way for controlling visitor access to a data center is to ensure that visitors are escorted by an authorized employee, as this prevents unauthorized or malicious actions by the visitors and provides accountability and supervision. Pre-approval of entry requests, visitors signing in at the front desk upon arrival, and closed-circuit television (CCTV) are also useful measures, but they are not as effective as escorting visitors, as they do not prevent or detect unauthorized or malicious actions by the visitors in real time. References: CISA Review Manual (Digital Version), Chapter 5: Protection of Information Assets, Section 5.1: Physical Access Controls1

最新問題**: 533**
次の監査まで修復テストを延期する最も適切な理由は次のうちどれですか?
A. 監査を実施し、スケジュールに同意した監査人が組織を退職しました。
B. 観察の相対的な重要性を考慮すると、管理者の計画されたアクションで十分です。
C. 被監査者の経営陣は、監査人によって報告されたすべての観察を受け入れました。
D. 監査環境は大幅に変化しました。
Answer: D (メーッセージを残す**)**
Deferring remediation testing until the next audit is justified only when there are significant changes in the audit environment that affect the relevance or validity of the audit observations and recommendations. For example, if there are changes in the business processes, systems, regulations, or risks that require a new audit scope or approach. The

other options are not valid justifications for deferring remediation testing, as they do not address the timeliness or quality of the audit follow-up process. The auditor who conducted the audit and agreed with the timeline has left the organization does not affect the responsibility of the audit function to ensure that remediation testing is performed as planned. Management's planned actions are sufficient given the relative importance of the observations does not guarantee that management will actually implement those actions or that they will be effective in addressing the audit issues. Auditee management has accepted all observations reported by the auditor does not eliminate the need for verification of remediation actions by an independent party. References: CISA Review Manual (Digital Version), Chapter 2, Section 2.4

最新問題: **534**
IS 監査人は、リソースの制約により、いくつかの重要なパッチがタイムリーに適用されていないことを発見しました。この状況で組織にとって最大のリスクは次のどれですか?
A. システムはベンダーによってサポートされていない可能性があります。
B. 既知のセキュリティ脆弱性は軽減されない可能性があります。
C. システムがユーザーの要件を満たしていない可能性があります。
D. 異なるシステムでは互換性がない可能性があります。
Answer: B (メーッセージを残す)

最新問題: **535**
IS 監査人は、ファイアウォールが時代遅れでベンダーによってサポートされていないことを発見しました。監査人が次に取るべき行動は次のどれですか?
A. 緩和制御を報告します。
B. 組織のセキュリティ体制を報告します。
C. ファイアウォールの値を決定します。
D. ファイアウォールを交換しない場合のリスクを判断します。
Answer: D (メーッセージを残す)
The IS auditor's next course of action after finding that firewalls are outdated and not supported by vendors should be to determine the risk of not replacing the firewall. Outdated firewalls may have known vulnerabilities that can be exploited by attackers to bypass security controls and access the network. They may also lack compatibility with newer technologies or standards that are required for optimal network performance and protection. Not replacing the firewall could expose the organization to various threats, such as data breaches, denial-of-service attacks, malware infections, or regulatory non-compliance. The IS auditor should assess the likelihood and impact of these threats and quantify the risk level for management to make informed decisions.

最新問題: **536**

データ損失防止 (DLP) ソリューションを評価する際に、保存中のデータに関連するリスクに最もよく対処できる機能はどれですか?
A. アクセスポリシーの適用
B. スキャンファイルの印刷
C. ストレージスキャン技術
D. ファイル移動検出
Answer: C (メーッセージを残す**)**

最新問題**: 537**
組織の情報セキュリティ ポリシーは、主に次の点に基づいて策定する必要があります。
A. エンタープライズ アーキテクチャ (EA)。
B. 業界のベストプラクティス。
C. リスク管理プロセス。
D. 過去の情報セキュリティインシデント。
Answer: C (メーッセージを残す**)**

最新問題**: 538**
IS 監査人の観点から、組織に導入されたソフトウェアの不完全なインベントリに関連する最大のリスクは次のどれでしょうか?
A. 重要なサーバー上の未使用のポートを閉じることができない
B. 組織内の未使用のライセンスを特定できない
C. 更新されたセキュリティパッチを展開できない
D. 導入されたソフトウェアのコストを決定できない
Answer: C (メーッセージを残す**)**
The greatest risk associated with an incomplete inventory of deployed software in an organization is the inability to deploy updated security patches. Security patches are updates that fix vulnerabilities or bugs in software that could be exploited by attackers. Without an accurate inventory of software versions and config urations, it is difficult to identify and apply the relevant patches in a timely manner, which exposes the organization to increased security risks. Inability to close unused ports on critical servers, inability to identify unused licenses within the organization, and inability to determine the cost of deployed software are not as critical as security risks. References: ISACA CISA Review Manual 27th Edition, page 308

最新問題**: 539**
外部レビュー中に、情報システム監査人は、組織内のシステムの重要性を分類する際に一貫性のないアプローチを観察しました。システムの重要性を決定するための主な要素として推奨されるべきものは次のどれですか?
A. 主要業績評価指標 (KPI)
B. リカバリポイント目標 (RPO)

C. 最大許容ダウンタイム (MAD)
D. 平均復旧時間 (MTTR)
Answer: C (メーッセージを残す**)**

最新問題**: 540**
ある組織は、2 人の IS 監査人を任命して、システムの実装を監査しました。監査人の 1 人は IT 関連の学位を持ち、もう 1 人はビジネスの学位を持っています。IS 監査の熟練度基準を満たすために最も重要なのは次のどれですか。
A. メンバーの 1 人が世界的に認められた監査認定を取得している限り、基準は満たされます。
B. 新しいスタッフを支援するために、技術的な共同ソーシングを使用する必要があります。
C. チーム メンバーの割り当ては、個人の能力に基づいて行う必要があります。
D. 監督者が新しい監査人の作業をレビューする限り、基準は満たされます。
Answer: C (メーッセージを残す**)**
Team member assignments based on individual competencies is the most important factor to meet the IS audit standard for proficiency. Proficiency is the ability to apply knowledge, skills and experience to perform audit tasks effectively and efficiently. The IS audit standard for proficiency requires that IS auditors must possess the knowledge, skills and discipline to perform audit tasks in accordance with applicable standards, guidelines and procedures. Team member assignments based on individual competencies is a way to ensure that each IS auditor is assigned to audit tasks that match their level of proficiency, and that the audit team as a whole has sufficient and appropriate proficiency to conduct the audit. The other options are not as important as option C, as they do not ensure that the IS auditors have the required proficiency to perform audit tasks.
Having a globally recognized audit certification is a way to demonstrate proficiency in IS auditing, but it does not guarantee that the IS auditor has the specific knowledge, skills and experience needed for a particular audit task or system. Technical co-sourcing is a way to supplement the proficiency of the IS audit team by hiring external experts or consultants to perform certain audit tasks or functions, but it does not replace the need for internal IS auditors to have adequate proficiency. Having a supervisor review the new auditors' work is a way to ensure quality and accuracy of the audit work, but it does not ensure that the new auditors have the necessary proficiency to perform audit tasks independently or competently. References: CISA Review Manual (Digital Version) , Chapter 1: Information Systems Auditing Process, Section 1.4: Audit Skills and Competencies.

最新問題**: 541**
災害復旧計画 (DRP) を機密として分類する最も重要な理由はどれですか?
A. データ分類ポリシーに準拠していることを確認します。
B. 計画を不正な変更から保護します。

C. ビジネス継続性のベストプラクティスに準拠します。
D. 攻撃につながる可能性のあるデータ漏洩のリスクを軽減します。
Answer: D (メーッセージを残す**)**
The most important reason to classify a disaster recovery plan (DRP) as confidential is to reduce the risk of data leakage that could lead to an attack. A DRP contains sensitive information about the organization's IT infrastructure, systems, processes, and procedures for recovering from a disaster. If this information falls into the wrong hands, it could be exploited by malicious actors to launch targeted attacks, sabotage recovery efforts, or extort ransom. Therefore, a DRP should be protected from unauthorized access, disclosure, modification, or destruction.
The other options are not as important as reducing the risk of data leakage that could lead to an attack:
* Ensuring compliance with the data classification policy is a good practice, but it is not a sufficient reason to classify a DRP as confidential. The data classification policy should reflect the level of risk and impact associated with each type of data, and a DRP should be classified as confidential based on its potential harm if compromised.
* Protecting the plan from unauthorized alteration is a valid concern, but it is not a primary reason to classify a DRP as confidential. A DRP should be protected from unauthorized alteration by implementing access controls, audit trails, version control, and change management processes.
Classifying a DRP as confidential may deter some unauthorized alterations, but it does not prevent them.
* Complying with business continuity best practice is a desirable goal, but it is not a compelling reason to classify a DRP as confidential. Business continuity best practice may recommend classifying a DRP as confidential, but it does not mandate it. The decision to classify a DRP as confidential should be based on a risk assessment and a cost-benefit analysis.

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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**: 542**
次のテクノロジーのうち、デバイス間のデータ送信の最大範囲が最も狭いのはどれですか?
A. Wi-Fi
B. Bluetooth

C. 長期進化 (LTE)
D. 近距離無線通信 (NFC)
Answer: (解答を表示する**)**
The technology that has the smallest maximum range for data transmission between devices is near-field communication (NFC). NFC is a short-range wireless technology that enables two devices to communicate when they are in close proximity, usually within a few centimeters. NFC is commonly used for contactless payments, smart cards, and device pairing. According to the Bluetooth Technology Website1, the effective range of NFC is less than a meter, while the other technologies have much longer ranges. Wi-Fi can reach up to 100 meters indoors and 300 meters outdoors2. Bluetooth can reach up to 800 feet with Bluetooth 5.0 specification3. Long-term evolution (LTE) can reach up to several kilometers depending on the cell tower and the device4.
References:
* 5: What is Wi-Fi? - Definition from WhatIs.com
* 6: Understanding Bluetooth Range | Bluetooth Technology Website
* 7: What is Bluetooth Range? What You Need to Know
* 8: How far can LTE signals travel? - Quora

最新問題**: 543**
新しく開発されたアプリケーションの有効性を評価する最良の方法は次のとおりです。
A. 実装後のレビューを実行します。
B. 負荷テストの結果を分析します。
C. 安全なコードレビューを実行します。
D. 受け入れテストの結果を確認します。
Answer: D (メーッセージを残す**)**
The best way to evaluate the effectiveness of a newly developed application is to review acceptance testing results. Acceptance testing is a process of verifying that the application meets the specified requirements and expectations of the users and stakeholders. Acceptance testing results can provide evidence of the functionality, usability, reliability, performance, security and quality of the application. Performing a post- implementation review, analyzing load testing results, and performing a secure code review are also important activities for evaluating an application, but they are not as comprehensive or conclusive as acceptance testing results.
References: Info Technology & Systems Resources | COBIT, Risk, Governance ... - ISACA, IT Governance and Process Maturity

最新問題**: 544**
IS 監査人は、Web アプリケーションの検証コントロールがパフォーマンス向上のためにサーバー側からブラウザーに移動されていることを発見しました。これにより、攻撃が成功する可能性が高くなります。

A. フィッシング。
B. サービス拒否 (DoS)
C. 構造化クエリ言語 (SQL) インジェクション
D. バッファオーバーフロー
Answer: C (メーッセージを残す)
Moving validation controls from the server side into the browser would most likely increase the risk of a successful attack by structured query language (SQL) injection. SQL injection is a technique that exploits a security vulnerability in an application's database layer by inserting malicious SQL statements into user input fields. Validation controls are used to check and filter user input before sending it to the database. If these controls are moved to the browser, they can be easily bypassed or modified by an attacker, who can then execute arbitrary SQL commands on the database. References: CISA Review Manual, 27th Edition, page 361

最新問題**: 545**
システム開発ライフサイクル (SDLC) をレビューしている IS 監査人が、ビジネス ケースの要件がないことに気付きました。次のどれが組織にとって最大の懸念事項でしょうか?
A. プロジェクトのコストが設定された予算を超えています。
B. ビジネス リソースが最適に割り当てられていません。
C. ベンダー選択基準が十分に評価されていません。
D. プロジェクトのビジネスへの影響が適切に分析されていません。
Answer: B (メーッセージを残す)

最新問題**: 546**
ソフトウェア ライセンス監査中に最も重要なのは次のどれですか?
A. 判断的サンプリング
B. 実質的なテスト
C. コンプライアンステスト
D. 停止または実行サンプリング
Answer: (解答を表示する)
Substantive testing is the most important type of testing during software license audits, as it provides evidence of the accuracy and completeness of the software inventory and licensing records. Substantive testing involves examining transactions, balances, and other data to verify their validity, existence, accuracy, and valuation.
Compliance testing, on the other hand, is more focused on assessing the adequacy and effectiveness of internal controls over software licensing, such as policies, procedures, and monitoring mechanisms.
Compliance testing alone cannot provide sufficient assurance that the software license audit objectives are met, as it does not verify the actual software usage and compliance

status. Judgmental sampling and stop-or- go sampling are methods of selecting samples for testing, not types of testing themselves. *References:
According to the ISACA IT Audit and Assurance Standards, Guidelines and Tools and Techniques for IS Audit and Assurance Professionals, section 1206 Testing, "The IS audit and assurance professional should perform sufficient testing to obtain sufficient appropriate evidence to support conclusions reached." 1 The section also defines substantive testing as "testing performed to obtain audit evidence to detect material misstatements in transactions or balances" and compliance testing as "testing performed to obtain audit evidence on the operating effectiveness of controls." 1 According to the ISACA IT Audit and Assurance Guideline G15 Software License Management, "The objective of a software license audit is to provide management with an independent assessment relating to compliance with software license agreements." 2 The guideline also states that "substantive tests should be performed on a sample basis to verify that all software installed on devices within scope has been appropriately licensed." 2

最新問題: **547**
次の非監査活動のうち、情報システム監査人の独立性と客観性を損なう可能性があるものはどれですか?
A. ITプロジェクト管理フレームワークに関するアドバイスの提供
B. サードパーティの顧客満足度調査の評価
C. 組織が採用している安全なソフトウェア開発ガイドラインを確認する
D. 新しいクラウドベースの労働力管理システムのセキュリティ制御の設計
Answer: D (メーッセージを残す**)**

最新問題: **548**
次の物理的な制御のうち、許可された個人だけがデータセンターにアクセスできることを最も確実に保証するものはどれですか?
A. データセンターは警備員によって巡回されています。
B. データセンターへのアクセスはビデオカメラで監視されています。
C. アクセスを許可する前にIDバッジを表示する必要があります
D. データセンターへのアクセスはマントラップによって制御されます。
Answer: (解答を表示する**)**
Access to the data center is controlled by a mantrap provides the greatest assurance that only authorized individuals can access a data center. A mantrap is a physical security device that consists of a small space with two sets of interlocking doors, such that the first set of doors must close before the second set opens1. A mantrap prevents unauthorized entry by requiring authentication at both doors, such as biometric scanners, card readers, or PIN codes. A mantrap also prevents tailgating, which is the act of following an authorized person into a restricted area without proper authorization2. A mantrap can also detect and trap intruders who attempt to force their way through the doors.

The other options are less effective physical controls for data center access. The data center is patrolled by a security guard is a deterrent measure, but it does not prevent unauthorized access by itself. A security guard may not be able to monitor all entry points, or may be distracted, bribed, or overpowered by intruders. Access to the data center is monitored by video cameras is a detective measure, but it does not prevent unauthorized access either. Video cameras can record the activities of intruders, but they cannot stop them from entering or alert the security personnel in real time. ID badges must be displayed before access is granted is a preventive measure, but it relies on human verification, which can be prone to errors or manipulation. ID badges can also be lost, stolen, or forged by intruders.
References:
Mantrap (access control) - Wikipedia1
Tailgating (security) - Wikipedia2

最新問題**: 549**
情報システム監査人が監査において重要性の概念を適用することが最も重要なのはいつですか?
A. 監査業務を計画する際
B. フィールドワークのための情報を収集する場合
C. 規制要件違反が判明した場合
D. 監査対象者からの表明を評価する場合
Answer: A (メーッセージを残す**)**
The concept of materiality is most important for an IS auditor to apply when planning an audit engagement, because it helps the auditor to determine the scope, objectives, procedures and resources of the audit.
Materiality is the degree to which an omission or misstatement of information could affect the users' decisions or the achievement of the audit objectives. By applying the concept of materiality, the auditor can focus on the most significant and relevant areas of the audit and avoid wasting time and effort on trivial or immaterial matters. The other options are not as important as planning an audit engagement, because they are either based on or affected by the materiality assessment done during the planning phase. References:
* ISACA, CISA Review Manual, 27th Edition, chapter 1, section 1.31
* ISACA, IT Audit and Assurance Standards, Guidelines and Tools and Techniques for IS Audit and Assurance Professionals, section 12022

最新問題**: 550**
フォローアップ監査の主な目的は次のとおりです。
A. リスク プロファイルが変更されたかどうかを評価します。
B. 推奨事項の妥当性を評価します。
C. ポリシーへの準拠を確認します。

D. 推奨事項に基づいて実行されたアクションの妥当性を判断します。
Answer: D (メーッセージを残す)

最新問題**: 551**
次の指標のうち、Web アプリケーションのパフォーマンスを最もよく示す指標はどれですか。
A. HTTPサーバーのエラー率
B. サーバースレッド数
C. 平均応答時間
D. サーバーの稼働時間
Answer: C (メーッセージを残す)
The best indicator of the performance of a web application is the average response time. This metric measures how long it takes for the web server to process and deliver a request from the client. It reflects the user's perception of how fast or slow the web application is, and it affects the user's satisfaction, engagement, and conversion. A low average response time means that the web application is responsive and efficient, while a high average response time means that the web application is sluggish and unreliable.
HTTP server error rate, server thread count, and server uptime are not as good indicators of the performance of a web application as the average response time. HTTP server error rate measures how often the web server fails to handle a request and returns an error code, such as 404 (Not Found) or 500 (Internal Server Error).
This metric indicates the reliability and availability of the web application, but it does not capture how fast or slow the web application is. Server thread count measures how many concurrent requests the web server can handle at a given time. This metric indicates the scalability and capacity of the web application, but it does not capture how long each request takes to process. Server uptime measures how long the web server has been running without interruption. This metric indicates the stability and resilience of the web application, but it does not capture how well the web application performs during that time.
References:
10 Key Application Performance Metrics & How to Measure Them - Stackify1 Measuring performance - Learn web development | MDN2 Understanding the Basics of Web Performance | BrowserStack3
14 Important Website Performance Metrics You Should Be Analyzing4
Top 8 Web Application Performance Metrics | MetricFire Blog5
Web Performance Monitoring: A How to Guide for Developers - Stackify6

最新問題**: 552**
適切な担当者がインシデントにタイムリーに対応できるようにするには、次のどれが最も役立ちますか?
A. インシデント管理ログの完了

B. 緊急メッセージを放送する
C. 専用のインシデント対応チームの必要性
D. インシデントエスカレーション手順の実装
Answer: D (メーッセージを残す**)**
Implementing incident escalation procedures is the best way to ensure that an incident receives attention from appropriate personnel in a timely manner, because it defines the roles and responsibilities, communication channels, and escalation criteria for handling different types of incidents34. Incident escalation procedures help to prioritize and coordinate the response efforts and ensure that the incident is resolved by the most qualified and authorized personnel. Completing the incident management log, broadcasting an emergency message, and requiring a dedicated incident response team are not sufficient to ensure that an incident receives attention from appropriate personnel in a timely manner, because they do not specify how to escalate the incident based on its severity, impact, or complexity. References: 3: CISA Review Manual (Digital Version), Chapter 6, Section 6.3.2 4: CISA Online Review Course, Module 6, Lesson 3

最新問題**: 553**
法医学調査中に収集された電子証拠が将来の法的手続きで証拠として認められることを保証するために最も重要なのは次のどれですか?
A. 専門的に認定された法医学調査員のみに証拠へのアクセスを制限する
B. 法医学調査全体を通じて担当者による証拠の取り扱いを文書化する
C. ハードドライブのイメージではなく、元のハードドライブに対して調査手順を実行する
D. 独立した第三者に法医学調査を依頼する
Answer: (解答を表示する**)**
The most important factor to ensure that electronic evidence collected during a forensic investigation will be admissible in future legal proceedings is to document evidence handling by personnel throughout the forensic investigation. Documentation is essential to establish the chain of custody, prove the integrity and authenticity of the evidence, and demonstrate compliance with legal and ethical standards. Documentation should include information such as the date, time, location, source, destination, method, purpose, result, and authorization of each action performed on the evidence. Documentation should also include any observations, findings, assumptions, limitations, or exceptions encountered during the investigation. References:
* CISA Review Manual (Digital Version)
* CISA Questions, Answers & Explanations Database

最新問題**: 554**
組織が内部ネットワークに保存されているデータを分類する主な理由は何ですか?
A. データ保持ポリシーを決定する
B. データ保護要件を実装するため
C. 組織のデータポリシーに準拠するため

D. 業界のベストプラクティスに従う
Answer: B (メーッセージを残す**)**
The primary reason for an organization to classify the data stored on its internal networks is to implement data protection requirements1234. Data classification helps organizations understand what data they have, its characteristics, and what security and privacy requirements it needs to meet so that the necessary protections can be achieved3. While determining data retention policy56, complying with the organization's data policies27, and following industry best practices891011 are important aspects of data classification, they are secondary to the fundamental requirement of implementing data protection requirements.
References:
What Is Data Classification & Why Is It Important? - RiskOptics
Data Classification Policy: Definition, Examples, & Free Template - Hyperproof Data Classification Policy: Benefits, Examples, and Techniques - Satori What is a Data Classification Policy? - Digital Guardian Data Classification and Practices - NIST Data Classification as a Catalyst for Data Retention and Archiving ...
What is data classification? - Cloud Adoption Framework
Data Classification - Data Security Policies | ITS Policies ...
IMPLEMENTING DATA CLASSIFICATION PRACTICES - NIST
Best Practices for Data Classification | Forcepoint

最新問題**: 555**
データ保持ポリシーを実装する最も適切な理由はどれですか?
A. 災害復旧手順の復旧ポイント目標（RPO）を確立する
B. 情報の保存と保護に関連する責任を制限する
C. 組織内でのデータ処理に関するビジネス目標を文書化する
D. IT部門外でデータ保護の責任と所有権を割り当てる
Answer: (解答を表示する**)**
The best reason to implement a data retention policy is to limit the liability associated with storing and protecting information. A data retention policy is a business' established protocol for maintaining information, typically defining what data needs to be retained, the format in which it should be kept, how long it should be stored for, whether it should eventually be archived or deleted, who has the authority to dispose of it, and what procedure to follow in the event of a policy violation1. A data retention policy can help an organization to:
Comply with legal and regulatory requirements that mandate the retention and disposal of certain types of data, such as financial records, health records, or personal data Reduce the risk of data breaches, theft, loss, or corruption by minimizing the amount of data stored and ensuring proper security measures are in place Save costs and resources by optimizing the use of storage space and reducing the need for backup and recovery operations Enhance operational efficiency and performance by eliminating unnecessary or

outdated data and improving data quality and accessibility Support business continuity and disaster recovery plans by ensuring critical data is available and recoverable in case of an emergency Facilitate audit trails and investigations by providing evidence of data authenticity, integrity, and provenance Therefore, by implementing a data retention policy, an organization can limit its liability associated with storing and protecting information, as well as improve its data governance and management practices.
References:
Data Retention Policy 101: Best Practices, Examples & More

最新問題: **556**
エンドユーザー コンピューティング (EUC) によって生成されたレポートに依存する場合、最も大きなリスクは次のどれですか。
A. データが不正確な可能性があります。
B. レポートが効率的に機能しない可能性があります。
C. レポートがタイムリーでない可能性があります。
D. 履歴データが利用できない可能性があります。
Answer: A (メーッセージを残す**)**
End-user computing (EUC) is a system in which users are able to create working applications besides the divided development process of design, build, test and release that is typically followed by software engineers1. Examples of EUC tools include spreadsheets, databases, low-code/no-code platforms, and generative AI applications2. EUC tools can provide flexibility, efficiency, and innovation for the users, but they also pose significant risks if not properly managed and controlled3.
The greatest risk when relying on reports generated by EUC is that the data may be inaccurate. Data accuracy refers to the extent to which the data in the reports reflect the true values of the underlying information4.
Inaccurate data can lead to erroneous decisions, misleading analysis, unreliable reporting, and compliance violations. Some of the factors that can cause data inaccuracy in EUC reports are:
Lack of rigorous testing: EUC tools may not undergo the same level of testing and validation as IT-developed applications, which can result in errors, bugs, or inconsistencies in the data processing and output3.
Lack of version and change control: EUC tools may not have a clear record of the changes made to them over time, which can create confusion, duplication, or loss of data. Users may also modify or overwrite the data without proper authorization or documentation3.
Lack of documentation and reliance on end-user who developed it: EUC tools may not have sufficient documentation to explain their purpose, functionality, assumptions, limitations, and dependencies. Users may also rely on the knowledge and expertise of the original developer, who may not be available or may not have followed best practices3.

Lack of maintenance processes: EUC tools may not have regular updates, backups, or reviews to ensure their functionality and security. Users may also neglect to delete or archive obsolete or redundant data3.
Lack of security: EUC tools may not have adequate access controls, encryption, or authentication mechanisms to protect the data from unauthorized access, modification, or disclosure. Users may also store or share the data in insecure locations or devices3.
Lack of audit trail: EUC tools may not have a traceable history of the data sources, inputs, outputs, calculations, and transformations. Users may also manipulate or falsify the data without detection or accountability3.
Overreliance on manual controls: EUC tools may depend on human intervention to input, verify, or correct the data, which can introduce errors, delays, or biases. Users may also lack the skills or training to use the EUC tools effectively and efficiently3.
The other options are not as great as data inaccuracy when relying on EUC reports. Reports may not work efficiently, reports may not be timely, and historical data may not be available are all potential risks associated with EUC tools, but they are less severe and less frequent than data inaccuracy. Moreover, these risks can be mitigated by improving the performance, scheduling, and storage of the EUC tools. However, data inaccuracy can have a pervasive and lasting impact on the quality and credibility of the reports and the decisions based on them. Therefore, option A is the correct answer.
References:
What is Data Accuracy?
What Is End User Computing (EUC) Risk?
End-user computing
End-User Computing (EUC) Risks: A Comprehensive Guide

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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: **557**
小規模な IS 部門で職務の分離が不十分な場合、最適な補償制御は次のどれですか?
A. 身元調査
B. ユーザー意識向上トレーニング
C. トランザクションログの確認
D. 必須休日
Answer: C (メーッセージを残す)

The best compensating control when segregation of duties is lacking in a small IS department is transaction log review. Transaction log review can help detect any unauthorized or fraudulent activities performed by IS staff who have access to multiple functions or systems. Transaction log review can also provide an audit trail for accountability and investigation purposes. The other options are not as effective as transaction log review in compensating for the lack of segregation of duties. Background checks are preventive controls that can help screen potential employees for any criminal records or dishonest behavior, but they do not prevent existing employees from abusing their access privileges. User awareness training is a detective control that can help educate users on how to report any suspicious or abnormal activities in the IS environment, but it does not monitor or verify the actions of IS staff. Mandatory holidays are deterrent controls that can discourage IS staff from engaging in fraudulent activities by requiring them to take periodic leave, but they do not prevent or detect such activities when they occur. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

最新問題**: 558**
組織の海外におけるサイバーセキュリティ規制への準拠を監査する計画を立てる際に最も役立つのは次のどれですか?
A. 監査の優先順位を決定し、運用リスクが最も大きい国に焦点を当てます。
B. 最も厳しい要件を持つ国のサイバーセキュリティ規制に従ってください。
C. 各国の監査チームからの調査結果の報告を標準化するテンプレートを開発する
D. さまざまな規制要件を組織のITガバナンスフレームワークにマッピングする
Answer: (解答を表示する**)**
The most useful thing to do when planning to audit an organization's compliance with cybersecurity regulations in foreign countries is to map the different regulatory requirements to the organization's IT governance framework. This is because an IT governance framework is a roadmap that defines the methods used by an organization to implement, manage and report on IT governance within said organization1. IT governance helps align business and IT strategies using a solid and formal framework2. By mapping the different regulatory requirements to the IT governance framework, the auditor can:
Identify the commonalities and differences among the various cybersecurity regulations that apply to the organization's operations in different countries.
Assess the level of compliance and maturity of the organization's IT governance practices against each regulatory requirement.
Evaluate the risks and gaps associated with non-compliance or partial compliance with any of the regulatory requirements.
Recommend appropriate actions or improvements to enhance the organization's IT governance and cybersecurity posture.
Option D is correct because mapping the different regulatory requirements to the organization's IT governance framework is a systematic and effective way to plan and conduct an audit of compliance with cybersecurity regulations in foreign countries.

最新問題: **559**
侵入テストを計画する際に最初に行うべきことはどれですか?
A. 秘密保持契約 (NDA) を実行します。
B. 脆弱性の報告要件を決定します。
C. テスト範囲を定義します。
D. テストに対する管理者の同意を得る。
Answer: D (メーッセージを残す)
The first step when planning a penetration test is to obtain management consent for the testing. This is because a penetration test involves simulating a cyberattack against the organization's systems and networks, which may have legal, ethical, and operational implications. Without proper authorization from management, a penetration test may violate laws, policies, contracts, or service level agreements. Management consent also helps define the objectives, scope, and boundaries of the test, as well as the roles and responsibilities of the testers and the stakeholders. Obtaining management consent for the testing also demonstrates due care and due diligence on the part of the testers and the organization.
Executing nondisclosure agreements (NDAs), determining reporting requirements for vulnerabilities, and defining the testing scope are important steps when planning a penetration test, but they are not the first step.
These steps should be done after obtaining management consent for the testing, as they depend on the approval and involvement of management and other parties.

最新問題: **560**
組織が情報セキュリティ意識向上プログラムの有効性を判断するために最も効果的なのは次のどれですか?
A. トレーニングの質に対するユーザー満足度の測定
B. ソーシャルエンジニアリング演習の結果を評価する
C. セキュリティスタッフのパフォーマンス評価の見直し
D. ヘルプデスクへの通話数の分析
Answer: B (メーッセージを残す)
The effectiveness of an information security awareness program is best measured by assessing real-world behavior rather than subjective feedback or indirect metrics. Social engineering exercises simulate real-world attack scenarios, testing whether employees can identify and respond appropriately to security threats. This directly evaluates the program's impact on employee behavior and awareness.
* Measuring User Satisfaction (Option A): While useful for feedback, satisfaction does not measure the effectiveness of awareness in preventing security incidents.
* Reviewing Security Staff Performance Evaluations (Option C): This focuses on staff capabilities rather than the awareness program's effectiveness.

* Analyzing Help Desk Calls (Option D): This might provide insight into recurring issues but does not directly measure the program's success in changing user behavior.
Conducting social engineering exercises aligns with best practices for assessing organizational security awareness.
Reference: ISACA CISA Review Manual, Job Practice Area 2: Information Systems Audit and Assurance.

最新問題**: 561**
システムが RFID を使用する場合、IS 監査人が最も注意すべき点は次のどれですか?
A. プライバシー
B. 保守性
C. スケーラビリティ
D. 否認防止
Answer: A (メーッセージを残す**)**
RFID stands for Radio Frequency Identification, and it is a technology that uses radio waves to identify or track objects that have a small chip (RFID tag) attached to them. RFID tags can store various types of information, such as serial numbers, product codes, or personal data. RFID readers can scan the tags from a distance and access the information without physical contact1.
RFID has many benefits for different applications, such as inventory management, supply chain optimization, asset tracking, and access control. However, RFID also poses some challenges and risks for information security and privacy. Some of these risks are:
Privacy: RFID tags can be read by unauthorized or malicious parties, who can collect personal or sensitive data without the knowledge or consent of the tag owners. This can lead to identity theft, profiling, tracking, or surveillance2. For example, a hacker could scan an RFID-tagged passport or credit card and steal the personal information or financial details of the owner3.
Communication attacks: RFID systems are vulnerable to various types of attacks that target the wireless communication between the tags and the readers. These include eavesdropping, jamming, spoofing, replaying, cloning, or modifying the data transmitted by the tags or the readers4. For example, an attacker could intercept the data from an RFID tag and alter it before sending it to the reader, causing false or misleading information to be recorded.
Mafia fraud: This is a type of attack where an adversary acts as a man-in-the-middle and relays the information between two legitimate parties. This can allow the adversary to bypass authentication or authorization mechanisms and gain access to restricted areas or resources. For example, an attacker could use a device to relay the signal from an RFID-tagged car key to the car's ignition system and start the car without having the physical key.

最新問題**: 562**

データ移行プロジェクトの最初のステップは次のどれですか?
A. 新しいシステムでビジネスプロセスをどのように実行すべきかに関する決定の検討
B. 現在のデータベースのデータのクリーンアップを完了して不整合を解消します
C. 新しいシステムのデータ構造を理解する
D. データ変換スクリプトの作成
Answer: C (メーッセージを残す)
Data migration is the process of moving data from one system to another, which may involve changes in storage, database, or application. To perform a successful data migration, it is essential to understand the data structure of the new system, which defines how the data is organized, stored, and accessed. Understanding the new system's data structure will help determine the following aspects of the data migration project:
The scope and requirements of the data migration, such as what data needs to be migrated, how much data needs to be migrated, and what are the quality and performance expectations.
The data mapping and transformation rules, such as how the data elements from the source system correspond to the data elements in the target system, and what transformations or conversions are needed to ensure compatibility and consistency.
The data validation and testing methods, such as how to verify that the migrated data is accurate, complete, and functional in the new system, and how to identify and resolve any errors or issues.
Therefore, understanding the new system's data structure is a crucial first step in a data migration project, as it lays the foundation for the subsequent steps of data extraction, transformation, loading, validation, and testing.

最新問題**: 563**
現場作業の過程で、内部 IS 監査員は新しく導入されたアプリケーション内に重大な脆弱性を発見しました。監査員が取るべき最善の行動は何でしょうか?
A. 結果を外部監査人に報告します。
B. 発見した内容をレポートに記録します。
C. その他の潜在的な脆弱性を特定します。
D. IT 管理者に通知します。
Answer: D (メーッセージを残す)

最新問題**: 564**
データを保存するためにクラウド プロバイダーに移動するかどうかを決定する際に、最初に考慮すべき事項は次のうちどれですか。
A. データ保存コスト
B. データ分類
C. ベンダークラウド認定
D. サービスレベル契約 (SLA)

Answer: (解答を表示する**)**
Data classification is the first consideration when deciding whether data should be moved to a cloud provider for storage because it determines the level of protection and security required for the data. Data classification also helps to identify the legal and regulatory requirements that apply to the data, such as privacy, retention and disposal policies. Data storage costs, vendor cloud certification and service level agreements (SLAs) are important factors to consider, but they are secondary to data classification. References: CISA Review Manual (Digital Version) 1, Chapter 5, Section 5.3.2

最新問題**: 565**
次のコントロールのうち、データベース管理者 (DBA) によって実行されるデータ抽出クエリが監視されるようにするのに役立つものはどれですか。
A. DBAのアクティビティログを確認する
B. DBA アクティビティへのアクセスを制限する
C. 定期的なアクセスレビューの実行
D. データベースアクセスのログを保存する
Answer: A (メーッセージを残す**)**

最新問題**: 566**
テクノロジーと電子記録の進歩により、IS 監査人は電子メールのみで業務を完了しました。IS 監査人が侵害した可能性のあるのは次のどれですか?
A. 熟練度
B. 適切な専門家の配慮
C. 十分な証拠
D. レポート
Answer: B (メーッセージを残す**)**
Due professional care is the obligation of an IS auditor to exercise the appropriate level of skill, competence, and diligence in performing an audit. It also requires the IS auditor to comply with the relevant standards, guidelines, and ethical principles of the profession. Completing an engagement by email only may compromise due professional care, as it may limit the IS auditor's ability to obtain sufficient and appropriate evidence, to communicate effectively with the auditee and other stakeholders, and to perform adequate quality assurance and review procedures. The other options are not as relevant as due professional care, as they relate to specific aspects of an audit, such as proficiency (the knowledge and skills of the IS auditor), sufficient evidence (the quantity and quality of the audit evidence), and reporting (the presentation and communication of the audit results). References: CISA Review Manual (Digital Version), Domain 1: The Process of Auditing Information Systems, Section 1.2 ISACA IT Audit and Assurance Standards

最新問題**: 567**

組織は、すべての部門で遵守される成熟したリスク管理プラクティスを開発しました。監査チームがこのリスク管理の成熟度を活用するための最も効果的な方法は何ですか?
A. 経営陣に代わってリスク対応を実施する
B. 監査計画のためのリスクレジスタの統合
C. リスクに関する経営陣への保証の提供
D. 監査リスクの特定と評価のワークショップの促進
Answer: (解答を表示する**)**
The most effective way for the audit team to leverage the risk management maturity of the organization is to integrate the risk register for audit planning purposes. The risk register is a document that records the identified risks, their likelihood, impact, and mitigation strategies for a project or an organization. By using the risk register, the audit team can align their audit objectives, scope, and procedures with the organization's risk profile and priorities. This will help the audit team to provide more value-added and relevant assurance and recommendations to the management and stakeholders.
Some of the web sources that support this answer are:
* Audit Maturity And Risk Management | Ideagen
* Building a Mature Enterprise Risk Management Plan | AuditBoard
* CISA Certified Information Systems Auditor - Question0551

最新問題**: 568**
RSA 暗号化を使用して作成されたデジタル署名によって提供される制御を最も危険にさらす可能性のあるものはどれですか?
A. ダイジェストを使用してハッシュ関数を反転する
B. 平文メッセージの改ざん
C. 受信者の公開鍵を解読する
D. 送信者の秘密鍵を取得する
Answer: D (メーッセージを残す**)**
A digital signature is a cryptographic technique that verifies the authenticity and integrity of a message or document, by using a hash function and an asymmetric encryption algorithm. A hash function is a mathematical function that transforms any input data into a fixed-length output value called a digest, which is unique for each input. An asymmetric encryption algorithm uses two keys: a public key and a private key.
The public key can be shared with anyone, while the private key must be kept secret by the owner. To create a digital signature, the sender first applies a hash function to the plaintext message to generate a digest. Then, the sender encrypts the digest with their private key to produce the digital signature. To verify the digital signature, the receiver decrypts the digital signature with the sender's public key to obtain the digest. Then, the receiver applies the same hash function to the plaintext message to generate another digest. If the two digests match, it means that the message has not been altered and that it came from the sender. The security of a digital signature depends on the secrecy of the sender's private key. If an attacker obtains the sender's private key, they can create fake

digital signatures for any message they want, thus compromising the control provided by the digital signature. Reversing the hash function using the digest is not possible, as hash functions are designed to be one-way functions that cannot be inverted. Altering the plaintext message will result in a different digest after applying the hash function, which will not match with the decrypted digest from the digital signature, thus invalidating the digital signature. Deciphering the receiver's public key is not relevant, as public keys are meant to be publicly available and do not affect the security of digital signatures.

最新問題**: 569**
脆弱性スキャン プロセスの完全性を判断する際に検証することが最も重要なのは次のどれですか。
A. 組織のシステム インベントリは最新の状態に保たれます。
B. 脆弱性スキャンの結果が CISO に報告されます。
C. 組織は脆弱性の特定にクラウドホスト型スキャンツールを使用しています
D. 脆弱性スキャンツールへのアクセスは定期的に確認されます
Answer: A (メーッセージを残す**)**
The completeness of the vulnerability scanning process depends on the accuracy and currency of the organization's systems inventory, which is a list of all the hardware and software assets that are owned or used by the organization. A complete and up-to-date systems inventory can help ensure that all the systems are identified and scanned for vulnerabilities, and that no system is missed or overlooked. Vulnerability scanning results are reported to the CISO is a good practice for ensuring accountability and visibility of the vulnerability management process, but it is not the most important thing to verify when determining the completeness of the vulnerability scanning process, as reporting does not guarantee that all the systems are scanned. The organization is using a cloud-hosted scanning tool for identification of vulnerabilities is a possible option for conducting vulnerability scanning, but it is not the most important thing to verify when determining the completeness of the vulnerability scanning process, as the type of scanning tool does not affect the scope or coverage of the scanning. Access to the vulnerability scanning tool is periodically reviewed is a critical control for ensuring the security and integrity of the vulnerability scanning tool, but it is not the most important thing to verify when determining the completeness of the vulnerability scanning process, as access review does not ensure that all the systems are scanned.

最新問題**: 570**
データ分析を使用する際に情報情報監査人が最も懸念すべき点は次のうちどれですか?
A. データセットには無関係なフィールドが含まれています
B. データ ソースに整合性がありません
C. データは監査人によって抽出されませんでした
D. データ分析ソフトウェアはオープンソースです
Answer: (解答を表示する**)**

最新問題: **571**
セキュリティ メトリック ダッシュボードの実装によって対処できる経営幹部の懸念事項は次のどれですか。
A. セキュリティプログラムの有効性
B. セキュリティインシデントと業界ベンチマーク
C. セキュリティに割り当てられた合計時間数
D. 誤検出の総数
Answer: A (メーッセージを残す**)**
The executive management concern that could be addressed by the implementation of a security metrics dashboard is the effectiveness of the security program. A security metrics dashboard is a tool that provides a visual representation of key performance indicators (KPIs) and key risk indicators (KRIs) related to the organization's information security objectives and activities. A security metrics dashboard can help executive management monitor and evaluate the performance and value delivery of the security program, identify strengths and weaknesses, assess compliance with policies and standards, and support decision making and improvement initiatives. Security incidents vs. industry benchmarks, total number of hours budgeted to security, and total number of false positives are not executive management concerns that could be addressed by the implementation of a security metrics dashboard. These are more operational or technical aspects of information security that could be measured and reported by other means, such as incident reports, budget reports, or log analysis. References: [ISACA CISA Review Manual 27th Edition], page 302

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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: **572**
IS 監査人は、主要システムのキャパシティ管理が IT 部門によって実行されており、ビジネスからの情報提供がないことを発見しました。監査人の主な懸念事項は次のとおりです。
A. 機器を最大限に活用できなかった
B. ビジネスの容量ニーズの予期せぬ増加。
C. データセンターの過剰なストレージ容量のコスト
D. 将来のビジネス プロジェクトの資金調達への影響。

Answer: B (メーッセージを残す)
The auditor's primary concern when capacity management for a key system is being performed by IT with no input from the business would be an unanticipated increase in business's capacity needs. This could result in performance degradation, service disruption or customer dissatisfaction if IT is not able to provide sufficient capacity to meet the business demand. Failure to maximize the use of equipment, cost of excessive data center storage capacity or impact to future business project funding are secondary concerns that relate to resource optimization or budget allocation, but not to service delivery or customer satisfaction. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 374

最新問題**: 573**
IT インターフェース制御のレビューにより、受信システムに転送されないレコードを識別して修正するプロセスが組織にないことが判明しました。次のうち、IS 監査人の最善の推奨事項はどれですか?
A. データファイルの自動暗号化、復号化、電子署名を有効にする
B. システム間のデータの自動調整を実行するソフトウェアを実装する
C. コーダーがシステム間のデータの手動調整を実行する
D. システム間のデータ転送を可能な限り自動化する
Answer: D (メーッセージを残す)
The best recommendation for an organization that does not have a process to identify and correct records that do not get transferred to the receiving system is to implement software to perform automatic reconciliations of data between systems. This will ensure that the data integrity and completeness are maintained and that any errors or discrepancies are detected and resolved in a timely manner. Enabling encryption, decryption, and electronic signing of data files may enhance the data security and authenticity, but not the data accuracy or consistency. Having coders perform manual reconciliation of data between systems may be prone to human errors and inefficiencies. Automating the transfer of data between systems as much as feasible may reduce the chances of data loss or corruption, but not eliminate them completely. References: IS Audit and Assurance Standards, section "Standard 1202: Risk Assessment in Planning"

最新問題**: 574**
次のどれが買掛金システムにおける予防管理の例ですか?
A. システムでは、システムのマスターベンダーリストに含まれているベンダーへの支払いのみが許可されます。
B. システムとそのデータのバックアップは毎晩実行され、定期的にテストされます。
C. システムは、スタッフが請求書の合計と比較するために使用する毎日の支払い概要レポートを作成します。
D. 支払部門の全メンバーにポリシーと手順が明確に伝達されている

Answer: A (メーッセージを残す)
The system only allows payments to vendors who are included in the system's master vendor list is an example of a preventative control in an accounts payable system. A preventative control is a control that aims to prevent errors or irregularities from occurring in the first place. By restricting payments to vendors who are authorized and verified in the master vendor list, the system prevents unauthorized or fraudulent payments from being made. The other options are examples of other types of controls, such as backup (recovery), reconciliation (detective), and communication (directive) controls. References: CISA Review Manual, 27th Edition, page 223

最新問題**: 575**
次のファイアウォールのタイプのどれが、ハッカーの侵入に対して最も高いレベルの制御を提供しますか?
A. 回線ゲートウェイ
B. アプリケーションレベルゲートウェイ
C. スクリーニングルーター。
D. パケットフィルタリングルーター
Answer: B (メーッセージを残す)

最新問題**: 576**
監査報告書の草案の議論中に、IT 管理者は、情報システム監査人によって効果がないという結論が出されたコントロールに対してプロセスが実装されたことを示す適切な証拠を提供しました。監査人の最善のアクションは次のどれですか。
A. 新しいコントロールはフォローアップ中に評価されることをIT管理者に説明する
B. レポートにIT管理が行ったアクションに関するコメントを追加する
C. IT 管理者が提供した証拠に基づいて結論を変更する
D. 結論を変更する前に監査を再実行します
Answer: D (メーッセージを残す)
The auditor's best action is to re-perform the audit before changing the conclusion, because the auditor needs to obtain sufficient and appropriate evidence to support the audit opinion. The evidence provided by IT management may not be reliable or relevant, and it may not reflect the actual effectiveness of the control during the audit period. Therefore, the auditor should verify the evidence independently and test the control again to ensure that it meets the audit criteria and objectives. The other options are not appropriate, because they either ignore or accept the evidence provided by IT management without verification, which may compromise the quality and integrity of the audit. References:
* ISACA, CISA Review Manual, 27th Edition, chapter 1, section 1.51
* ISACA, IT Audit and Assurance Standards, Guidelines and Tools and Techniques for IS Audit and Assurance Professionals, section 12062

最新問題: **577**
IT プロジェクトの利益実現計画で指定された望ましい成果を達成するための説明責任を促進するための最良の推奨事項は次のどれですか?
A. プロジェクト マネージャーが利益実現計画を管理するための正式な権限を持っていることを確認します。
B. プロジェクトと同じプログラム内の他のプロジェクト間の依存関係を文書化します。
C. 利益実現計画のあらゆる側面の実施と追跡について、IT 部門が責任を持つようにします。
D. 計画内で特定された各メリットに対して、責任、対策、およびタイムラインを割り当てます。
Answer: D (メーッセージを残す**)**

最新問題: **578**
組織のプライバシー ポリシーを確認する際に、情報システム監査人が調査する上で最も重要なのは次のどれですか。
A. 個人データの収集について規制当局から明示的な許可があるかどうか
B. 組織が個人データを収集する正当な目的
C. 個人情報を第三者のサービスプロバイダーと共有することが禁止されているかどうか
D. 個人データを保護するために組織が選択した暗号化メカニズム
Answer: (解答を表示する**)**
The most important thing for an IS auditor to examine when reviewing an organization's privacy policy is its legitimate purpose for collecting personal data. A legitimate purpose is a clear and specific reason for collecting personal data that is necessary for the organization's business operations or legal obligations, and that respects the rights and interests of the data subjects. A legitimate purpose is the basis for establishing a lawful and fair processing of personal data, and it should be communicated to the data subjects in the privacy policy. The other options are not as important as the legitimate purpose in reviewing the privacy policy.
Explicit permission from regulators to collect personal data is not always required, as there may be other lawful bases for data collection, such as consent, contract, or public interest. Sharing of personal information with third-party service providers is not prohibited, as long as there are adequate safeguards and agreements in place to protect the data. The encryption mechanism selected by the organization for protecting personal data is a technical control that can enhance data security, but it does not determine the legality or fairness of data collection. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.3.2

最新問題: **579**

患者が治療のためにどこにいても患者データにアクセスできるようにしたい、複数の拠点を持つ医療機関にとって最も効率的なソリューションは次のどれですか?
A. Infrastructure as a Service (IaaS) プロバイダー
B. サービスとしてのソフトウェア (SaaS) プロバイダー
C. ネットワークセグメンテーション
D. 動的ローカリゼーション
Answer: (解答を表示する**)**
The answer B is correct because Software as a Service (SaaS) provider is the most efficient solution for a multi-location healthcare organization that wants to be able to access patient data wherever patients present themselves for care. SaaS is a cloud computing model that allows users to access software applications over the internet, without having to install, maintain, or update them on their own devices or servers. SaaS providers host and manage the software applications and the underlying infrastructure, and handle any issues such as security, availability, and performance.
SaaS can offer several benefits for a multi-location healthcare organization, such as:
* Accessibility: SaaS applications can be accessed from any device and location that has an internet connection, which enables the healthcare organization to access patient data across different facilities and regions, and provide seamless and coordinated care to the patients.
* Scalability: SaaS applications can scale up or down according to the demand and usage of the healthcare organization, which allows the organization to accommodate fluctuations in patient volume, data volume, or service requirements.
* Cost-effectiveness: SaaS applications are usually offered on a subscription or pay-per-use basis, which reduces the upfront and ongoing costs of purchasing, installing, and maintaining software licenses, hardware, and IT staff.
* Security: SaaS providers are responsible for ensuring the security and privacy of the software applications and the data they store, which can help the healthcare organization comply with the relevant regulations and standards, such as HIPAA (Health Insurance Portability and Accountability Act) or GDPR (General Data Protection Regulation).
Some examples of SaaS providers that offer solutions for healthcare organizations are:
* Epic: Epic is a leading provider of electronic health record (EHR) systems that enable healthcare organizations to store, manage, and share patient data across different settings and specialties. Epic also offers cloud-based solutions that allow healthcare organizations to access Epic's software applications over the internet, without having to host them on their own servers.
* Salesforce Health Cloud: Salesforce Health Cloud is a cloud-based platform that helps healthcare organizations connect with patients, providers, payers, and partners. Salesforce Health Cloud enables healthcare organizations to manage patient relationships, coordinate care teams, engage patients through personalized journeys, and leverage data and analytics to improve outcomes and efficiency.

* DocuSign: DocuSign is a cloud-based platform that enables users to sign, send, and manage documents electronically. DocuSign can help healthcare organizations streamline workflows, reduce errors, and enhance compliance by automating the process of obtaining signatures for consent forms, contracts, prescriptions, referrals, and other documents.
The other options are not as efficient as option B. Infrastructure as a Service (IaaS) provider (option A) is a cloud computing model that provides users with access to computing resources such as servers, storage, network, and operating systems over the internet. IaaS can offer some benefits such as flexibility, scalability, and cost-effectiveness for a multi-location healthcare organization, but it also requires more technical expertise and management from the organization than SaaS. The organization would still need to install, configure, update, and secure the software applications that run on the IaaS infrastructure. Network segmentation (option C) is a technique that divides a network into smaller subnetworks based on criteria such as function, location, or security level. Network segmentation can improve the performance, security, and manageability of a network by reducing congestion, isolating threats, and enforcing policies. However, network segmentation alone does not enable a multi-location healthcare organization to access patient data wherever patients present themselves for care. The organization would still need a software solution that can store, manage, and share patient data across different segments of the network. Dynamic localization (option D) is a process that adapts the content and functionality of a software application to suit the preferences and needs of users in different locations or regions. Dynamic localization can enhance the user experience and satisfaction by providing relevant information in local languages, currencies, formats, and regulations.
However, dynamic localization does not address the core issue of accessing patient data wherever patients present themselves for care. The organization would still need a software solution that can store, manage, and share patient data across different locations or regions.
References:
* Epic
* Salesforce Health Cloud
* DocuSign

最新問題**: 580**
組織の IT 部門と内部 IS 監査機能はすべて最高情報責任者 (CIO) に報告します。この報告構造に関連する最大の懸念事項は次のどれですか。
A. 監査結果が不正確になる可能性
B. IS監査の独立性の侵害
C. IS監査リソースが他のIT機能と共有されている
D. IS 監査は他の監査機能から分離されている
Answer: B (メーッセージを残す**)**

The greatest concern with the IT department and internal IS audit function both reporting to the CIO is the potential compromise of IS audit independence. Auditor independence refers to the impartiality and objectivity of an auditor in conducting an audit, free from conflicts of interest and bias1. It is crucial for ensuring the quality and reliability of financial reporting1. If the IS audit function reports to the CIO, who also oversees the IT department, it could create a conflict of interest that might compromise the impartiality and objectivity of the IS audit function.
References:
Auditor Independence - What is it, Rules, Importance, Examples

最新問題**: 581**
サービスベンダーがクライアントの要求に応じて制御レベルを維持していることを確認するための最も効果的な方法はどれですか?
A. 合意された基準を使用して、定期的にオンサイト評価を実施します。
B. ベンダーとのサービス レベル契約 (SLA) を定期的に確認します。
C. ベンダーの IT システムの予告なしの脆弱性評価を実施します。
D. ベンダーのコントロール自己評価 (CSA) の証拠を取得します。
Answer: A (メーッセージを残す**)**
The most effective method to verify that a service vendor keeps control levels as required by the client is to conduct periodic on-site assessments using agreed-upon criteria. On-site assessments can provide direct evidence of whether the vendor's controls are operating effectively and consistently in accordance with the client's expectations and requirements. Agreed-upon criteria can ensure that the assessments are objective, relevant, and reliable. The other options are not as effective as on-site assessments in verifying the vendor's control levels. Periodically reviewing the SLA with the vendor can help monitor whether the vendor meets its contractual obligations and service standards, but it does not provide assurance of whether the vendor's controls are adequate or sufficient. Conducting an unannounced vulnerability assessment of vendor's IT systems can help identify any weaknesses or gaps in the vendor's security controls, but it may violate the terms and conditions of the vendor-client relationship or cause operational disruptions. Obtaining evidence of the vendor's CSA can provide some indication of whether the vendor's controls are self-monitored and reported, but it does not verify whether the vendor's controls are independent or accurate. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.4

最新問題**: 582**
小規模な IT 部門では DevOps を採用しており、これによりこのグループのメンバーはコードを本番環境にデプロイし、リリースを自動化するために開発アクセスを維持できます。次のうち、最も効果的な制御はどれですか。
A. 開発に参加していないチームメンバーによるデプロイ前の承認を強制します。

B. DevOps チームは、同じコードを開発および展開していないことを示すポリシー承認を毎年提供します。
C. 年次トレーニングでは、開発者とコード展開者の間の分離を維持する必要性を強調します。
D. IT コンプライアンス マネージャーは、同じ人物がコードを開発および展開していないことを確認するために、毎週レビューを実行します。
Answer: A (メーッセージを残す**)**
The most effective control to maintain segregation of duties in a DevOps environment is A. Enforce approval prior to deployment by a member of the team who has not taken part in the development. Segregation of duties (SoD) is a principle that requires multiple actors to complete a task to reduce the risk of fraud, error, or abuse1. In a DevOps environment, where developers and operators work together to deliver software faster and more reliably, SoD may seem to be incompatible or impractical. However, SoD can still be achieved by implementing controls that ensure that no single person can develop, test, and deploy code without oversight or review2.
Enforcing approval prior to deployment by a member of the team who has not taken part in the development is an effective control that ensures that code changes are verified and validated by a peer before they are released to production. This control can help prevent or detect any unauthorized or malicious modifications, errors, or vulnerabilities in the code, and ensure that the code meets the quality and security standards3. This control can also promote collaboration and feedback among the team members, and improve the transparency and accountability of the software delivery process3.

最新問題**: 583**
生産スケジュールのレビュー中に、情報システム監査人は、スタッフが必須の運用手順を遵守していないことに気付きました。監査人の次のステップは次のようになります。
A. 監査レポートに非準拠を含めます。
B. 手順に従わなかった理由を特定します。
C. 監査作業書類に不適合事項を記載します。
D. 違反を特定する監査覚書を発行します。
Answer: B (メーッセージを残す**)**

最新問題**: 584**
IS 監査人は、最近本番環境に導入されたオンライン販売システムで、セキュリティ テストがすべて完了していないことに気付きました。監査人が取るべき最善の行動は次のどれですか。
A. ビジネスへの露出度を決定する
B. 今後のテスト活動を適切に調整する
C. セキュリティインシデントの監視を強化する
D. セキュリティテストを実行するために第三者を雇う

Answer: (解答を表示する**)**
The IS auditor's best course of action when reviewing the use of an outsourcer for disposal of storage media is to determine exposure to the business. Storage media, such as hard disks, tapes, flash drives, or CDs, may contain sensitive or confidential information that needs to be protected from unauthorized access, disclosure, or misuse. The IS auditor should verify that the outsourcer has a process that appropriately sanitizes the media before disposal, such as wiping, degaussing, shredding, or incinerating, and that the process is effective and compliant with the organization's policies and standards. The IS auditor should also assess the potential impact and risk to the business if the storage media is not properly sanitized or disposed of, such as data breaches, reputational damage, legal or regulatory penalties, or loss of competitive advantage. The other options are not the best course of action, because they either do not address the root cause of the problem, or they are reactive rather than proactive measures. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.7

最新問題**: 585**
プログラムのソース コードに加えられた変更の監査証跡を維持するための最良の方法はどれですか。
A. ソースコード内に詳細を埋め込みます。
B. ファイルの命名規則を標準化します。
C. 自動バージョン管理を活用します。
D. 変更記録の詳細を文書化します。
Answer: C (メッセージを残す**)**
Automated version control systems are the best method to maintain an audit trail of changes made to the source code of a program. They automatically track and manage changes to the source code over time, allowing you to see what changes were made, when they were made, and who made them1. This provides a clear and detailed audit trail that can be invaluable for debugging, understanding the evolution of the code, and ensuring accountability23.

最新問題**: 586**
組織のインシデント管理プロセスの設計を評価する情報システム監査人にとって、最も懸念されるのは次のどれでしょうか?
A. サービス管理基準が遵守されていません。
B. インシデントを解決するのに予想される時間が指定されていません。
C. 指標は上級管理職に報告されません。
D. 優先順位付け基準が定義されていません。
Answer: D (メッセージを残す**)**
he design of an incident management process should include prioritization criteria to ensure that incidents are handled according to their impact and urgency. Without

prioritization criteria, the organization may not be able to allocate resources effectively and respond to incidents in a timely manner. Expected time to resolve incidents, service management standards, and metrics reporting are important aspects of incident management, but they are not as critical as prioritization criteria for the design of the process. References:
ISACA Journal Article: Incident Management: A Practical Approach

有効な **CISA-JPN** 問題集は GoShiken.com が提供された合格しやすい CISA-JPN 試験問題集！ GoShiken.com が最新の **CISA-JPN** 試験問題集を提供しています。GoShiken.com CISA-JPN 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA-JPN 問題集をゲットする人はこちら: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**139430%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**: 587**
組織の許容使用ポリシーに記載されている次の記述のうち、情報資産の保護に関連するデータ分類標準との整合性を最もよく示しているのはどれですか。
A. パブリック ネットワーク経由で送信される情報資産はすべて、経営幹部の承認が必要です。
B. すべての情報資産は、組織のシステムに保存されるときに暗号化する必要があります。
C. 情報資産には正当な理由のある者のみがアクセスできる必要があります。
D. すべての情報資産には、従業員による適切な取り扱いを容易にするために、明確に定義されたレベルが割り当てられます。
Answer: B (メーッセージを残す**)**
The statement that BEST demonstrates alignment with data classification standards related to the protection of information assets is D. All information assets will be assigned a clearly defined level to facilitate proper employee handling. Data classification involves categorizing information assets based on their sensitivity, importance, and usage. Assigning clearly defined levels (such as public, internal, confidential, etc.) to information assets ensures that appropriate security controls are applied based on their classification. By doing so, organizations can manage access, encryption, and other protective measures effectively12.
References:
1. IFRC. "Information Security: Acceptable Use Policy."
1(https://www.ifrc.org/sites/default/files/2021-11
/IFRC-Information-Security-Acceptable-Use-Policy.pdf)
2. UNSW Sydney. "Data Classification Standard."
2(https://www.unsw.edu.au/content/dam/pdfs/governance

/policy/2022-01-policies/datastandard.pdf)
3. Digital Guardian. "What is a Data Classification Policy?"
3(https://www.digitalguardian.com/blog/what- data-classification-policy)
4. Microsoft Service Trust Portal. "Data classification & sensitivity label taxonomy."
4(https://learn.microsoft.
com/en-us/compliance/assurance/assurance-data-classification-and-labels)
5. Clark University ITS Policies. "Data Classification - Data Security Policies."
5(https://www2.clarku.edu
/offices/its/policies/data_classification.cfm)

最新問題**: 588**
トップダウン成熟度モデルプロセスを利用した結果は次のどれでしょうか?
A. 類似のプロセスの有効性を同業者とベンチマークする手段
B. 企業内の他のプロセスの有効性を比較する手段
C. タイムリーなレビューを確実にするために、より古く、より確立されたプロセスを特定する
D. 改善の余地が最も大きいプロセスの特定
Answer: D (メーッセージを残す**)**
A top-down maturity model process is a method of assessing and improving the maturity level of a process or a set of processes within an organization. A maturity level is a measure of how well-defined, controlled, measured, and optimized a process is. A top-down maturity model process starts with defining the desired maturity level and then identifying the gaps and improvement opportunities for each process. This helps prioritize the processes that need the most attention and improvement. Therefore, a result of utilizing a top- down maturity model process is identification of processes with the most improvement opportunities.
A means of benchmarking the effectiveness of similar processes with peers, a means of comparing the effectiveness of other processes within the enterprise, and identification of older, more established processes to ensure timely review are not results of utilizing a top-down maturity model process. These are possible benefits or objectives of using other types of maturity models or assessment methods, but they are not specific to a top-down approach.

最新問題**: 589**
組織の情報セキュリティ ポリシーを見直す必要があることを最もよく示すのは次のどれですか。
A. 監査報告書における低リスクの発見事項の数が多い
B. 年間ITリスク評価の完了
C. 経営陣が承認した例外の増加
D. ビジネス取引の複雑化
Answer: C (メーッセージを残す**)**

最新問題: **590**
アプリケーション テストを自動化する主な利点は次のとおりです。
A. テストの一貫性を提供します。
B. より柔軟性を高めます。
C. すべての手動テストプロセスを置き換えます。
D. コードのレビューにかかる時間を短縮します。
Answer: (解答を表示する**)**
The primary benefit of automating application testing is to provide test consistency. Automated testing can ensure that the same test cases are executed in the same manner and order every time, which can improve the reliability and accuracy of the test results. Providing more flexibility, replacing all manual test processes, and reducing the time to review code are possible benefits of automating application testing, but they are not the primary benefit. References:
* ISACA, CISA Review Manual, 27th Edition, 2020, p. 3091
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

最新問題: **591**
アプリケーション コンテナ インフラストラクチャに固有のリスクとなるのは次のどれですか。
A. 共有レジストリ
B. ホストオペレーティングシステム
C. 共有データ
D. 共有カーネル
Answer: (解答を表示する**)**
Application containers are a form of operating system virtualization that share the same kernel as the host operating system. This means that any vulnerability or compromise in the kernel can affect all the containers running on the same host, as well as the host itself. Additionally, containers may have privileged access to the kernel resources and functions, which can pose a risk of unauthorized or malicious actions by the container processes. Therefore, securing the kernel is a critical aspect of application container security.
Shared registries (option A) are not an inherent risk in the application container infrastructure, but they are a potential risk that depends on how they are configured and managed. Shared registries are repositories that store and distribute container images. They can be public or private, and they can have different levels of security and access controls. Shared registries can pose a risk of exposing sensitive data, distributing malicious or vulnerable images, or allowing unauthorized access to images. However, these risks can be mitigated by using secure connections, authentication and authorization mechanisms, image signing and scanning, and encryption.

Host operating system (option B) is not an inherent risk in the application container infrastructure, but it is a potential risk that depends on how it is configured and maintained. Host operating system is the underlying platform that runs the application containers and provides them with the necessary resources and services.
Host operating system can pose a risk of exposing vulnerabilities, misconfigurations, or malware that can affect the containers or the host itself. However, these risks can be mitigated by using minimal and hardened operating systems, applying patches and updates, enforcing security policies and controls, and isolating and monitoring the host.
Shared data (option C) is not an inherent risk in the application container infrastructure, but it is a potential risk that depends on how it is stored and accessed. Shared data is the information that is used or generated by the application containers and that may be shared among them or with external entities. Shared data can pose a risk of leaking confidential or sensitive data, corrupting or losing data integrity, or violating data privacy or compliance requirements. However, these risks can be mitigated by using secure storage solutions, encryption and decryption mechanisms, access control and auditing policies, and backup and recovery procedures.
Therefore, option D is the correct answer.
References:
* Application Container Security Guide | NIST
* CSA for a Secure Application Container Architecture
* Application Container Security: Risks and Countermeasures

最新問題**: 592**
不正な支払いを防ぐ最善の方法は、ベンダーの設定と以下の間で職務の分離を実施することです。
A. 支払い処理。
B. 給与処理。
C. 調達。
D. 製品登録。
Answer: A (メーッセージを残す**)**
Segregation of duties is a key internal control that aims to prevent fraud and errors by ensuring that no single individual has the authority to execute two or more conflicting sensitive transactions or functions. In the accounts payable vendor payment cycle, segregation of duties involves separating the tasks of vendor setup, procurement, invoice approval, and payment processing1. This way, an employee cannot create a fictitious vendor and issue a payment to themselves or their accomplices without being detected by another person. Therefore, the best way to prevent fraudulent payments is to implement segregation of duties between the vendor setup and payment processing. References: 1: Segregation of Duties in the Accounts Payable Vendor Payment Cycle for SMBs - Now With a Podcast! - Debra R Richardson : What is Separation of duties

- University of California, Berkeley

最新問題: **593**
プログラマーが給与システム レポートの重要なフィールドに不正な変更を加えました。次のどの制御の弱点がこの問題に最も寄与していると考えられますか?
A. プログラマーはテストにユーザーを参加させなかった
B. ユーザー要件が文書化されていません
C. プログラマーは製品プログラムにアクセスできる
D. 給与ファイルは司書の管理下にありませんでした
Answer: C (メーッセージを残す**)**
The programmer having access to the production programs is a control weakness that would have contributed most to the problem of unauthorized changes to key fields in a payroll system report. This is because it violates the principle of segregation of duties, which requires that different individuals or groups perform different functions related to system development, testing, implementation, and operation. Allowing programmers to access production programs increases the risk of errors, fraud, or malicious actions that may compromise the integrity, availability, or confidentiality of the system or its data. The other options are not as significant as having access to production programs, as they relate to other aspects of system development or maintenance, such as user involvement in testing (which affects user satisfaction and acceptance), user requirements documentation (which affects system functionality and quality), and payroll files control (which affects data security and accuracy). References: CISA Review Manual (Digital Version), Domain 3:
Information Systems Acquisition, Development and Implementation, Section 3.2 Project Management Practices

Valid CISA-JPN Dumps shared by GoShiken.com for Helping Passing CISA-JPN Exam! GoShiken.com now offer the **newest CISA-JPN exam dumps**, the GoShiken.com CISA-JPN exam **questions have been updated** and **answers have been corrected** get the **newest** GoShiken.com CISA-JPN dumps with Test Engine here: https://www.goshiken.com/ISACA/CISA-JPN-mondaishu.html (**1394** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)