ISACA.CISA-JPN.v2026-10-20.q678

試験コード：	CISA-JPN
試験名称：	Certified Information Systems Auditor (CISA日本語版)
認証ベンダー：	ISACA
無料問題の数：	678
バージョン：	v2026-10-20
ページの閲覧量：	107
問題集の閲覧量：	7463

https://www.jpnshiken.com/shiken/ISACA.CISA-JPN.v2026-10-20.q678.html

質問: **1**
回帰テストはどのプロセスで最も一般的に使用されますか？
A. 単体テスト
B. システム変更
C. プログラム開発
D. ストレステスト
正解: **B** (コメントを発表する)

質問: **2**
統制目標を達成するためのIT統制の設計について、主に責任を負うのは誰ですか？
A. ビジネス管理
B. 内部監査人
C. ITマネージャー
D. リスク管理
正解: (正解を表示します)

質問: **3**
職務分掌に伴うリスクに対する以下の対応策のうち、初期費用が最も低いのはどれか？
A. リスク受容
B. リスク軽減
C. リスク移転
D. リスク軽減
正解: **A** (コメントを発表する)
Segregation of duties is a fundamental concept in cybersecurity and information security. It refers to the practice of dividing critical tasks and responsibilities among different individuals or roles within an organization to reduce the risk of fraud, error, or unauthorized activities1. Segregation of duties is designed to prevent unilateral actions within an organization's workflow, which can result in damaging events that would exceed the organization's risk tolerance2.

There are different types of responses to risk associated with segregation of duties, depending on the level of risk and the cost-benefit analysis. Some of the common responses are:
Risk acceptance: This means acknowledging a risk and deciding to tolerate it without taking any corrective actions. This response is usually chosen when the risk is low or the cost of mitigation is too high3.
Risk mitigation: This means taking steps ahead of time to lessen the effects of a risk and make it less likely to happen. Some examples of mitigation strategies are making backup plans, setting up early warning systems, and staying away from high-risk areas or activities4.
Risk transference: This means shifting the negative impact of a risk and/or the responsibility for managing the risk response to a third party. Some examples of transference strategies are outsourcing, insurance, or contracts5.
Risk reduction: This means reducing the probability and/or severity of the risk below a threshold of acceptability. Some examples of reduction strategies are implementing controls, policies, or procedures to prevent or detect risks6.
Based on these definitions, the response to risk associated with segregation of duties that would incur the lowest initial cost is A. Risk acceptance. This is because risk acceptance does not require any additional resources or actions to address the risk. However, risk acceptance also implies that the organization is willing to bear the consequences of the risk if it occurs, which could be costly in the long run.
Therefore, the correct answer to your question is A. Risk acceptance.

質問**: 4**
クラウドアクセスセキュリティブローカー(CASB)が脅威を効果的に検知し、対応できるようにするために、最も重要な対策は次のうちどれですか？
A. データ移動の監視
B. 長期CASB契約の実施
C. 情報セキュリティポリシーの見直し
D. ファイアウォールの有効性を評価する
正解**: A (**コメントを発表する**)**
ACloud Access Security Broker (CASB)ensuresvisibility, compliance, and securityof cloud applications, andmonitoring data movementis the key to detecting threats.
Option A (Correct):Monitoring data movementallows organizations todetect and preventunauthorized access, data exfiltration, and cloud-based threats.
Option B (Incorrect):Along-term contractdoes not inherentlyimprove security monitoring.
Option C (Incorrect):Reviewing policies helps withgovernance, but it does notactively detect threats.
Option D (Incorrect):Firewallsprotectnetwork perimeters, while CASBs focus oncloud security, making this anineffective measurefor CASB threat detection.

Reference:ISACA CISA Review Manual -Domain 5: Protection of Information Assets-CoversCASB, cloud security, and threat detection best practices.

質問: **5**
ある組織が、サードパーティベンダーからウェブベースのメールサービスを購入し、自社のメールサーバーインフラ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ものでしょうか？
A. サービスとしてのインフラストラクチャ(IaaS)
B. データベース ･アズ ･ア ･サービス (DBaaS)
C. プラットフォーム ･アズ ･ア ･サービス (PaaS)
D. サービスとしてのソフトウェア (SaaS)
正解: **D (**コメントを発表する**)**

質問: **6**
従業員による機密情報の意図しない漏洩に伴うリスクを軽減するための、IS監査担当者による最善の推奨事項は次のうちどれですか？
A. 侵入防御システム(IPS)およびファイアウォール
B. データ損失防止(DLP)技術
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
正解: **(**正解を表示します**)**
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

質問: **7**
会計担当者は、在庫レベルを記載したスプレッドシートを定期的に組織の財務報告システムにアップロードします。これらの転送は、社内開発者が作成したカスタマイズされたインターフェースを通じて実行されます。
インターフェースのレビュー中に IS 監査人が確認する必要がある最も重要なのは次のどれですか。
A. スプレッドシートのデータは財務システムに正しく記録されています。
B. 財務システムの転送は、会計担当者によって事前に定義された間隔で実行されます。

C. スプレッドシートにはマルウェアや悪意のあるマクロは含まれていません。
D. データ転送接続は全二重通信をサポートしていません。
正解: **(**正解を表示します**)**
Comprehensive and Detailed Explanation:
The primary audit concern is data integrity-ensuring that the data uploaded via the custom interface is accurately and completely transferred to the financial system.
* Option A directly addresses data accuracy and integrity.
* Option B (timing) is secondary compared to correctness.
* Option C (malware checks) is important but handled by security controls, not the primary audit concern here.
* Option D (duplex communication) is irrelevant to ensuring accurate financial records.
# ISACA Reference: CISA Review Manual 27th Edition, Domain 3, section on interface controls and audit considerations.

質問: **8**
組織の情報セキュリティポリシーの適切性を評価する際に、情報セキュリティ監査担当者にとって最も重要な考慮事項は次のうちどれですか？
A. IT運営委員会議事録
B. 事業目標
C. IT戦術計画との整合性
D. 業界のベストプラクティスへの準拠
正解: **(**正解を表示します**)**
The most important consideration for an IS auditor when assessing the adequacy of an organization's information security policy is the business objectives. An information security policy is a document that defines the organization's approach to protecting its information assets from internal and external threats. It should align with the organization's mission, vision, values, and goals, and support its business processes and functions1. An informationsecurity policy should also be focused on the business needs and requirements of the organization, rather than on technical details orspecific solutions2.
The other options are not as important as the business objectives, because they do not directly reflect the organization's purpose and direction. IT steering committee minutes are records of the discussions and decisions made by a group of senior executives who oversee the IT strategy and governance of the organization. They may provide some insights into the information security policy, but they are not sufficientto evaluate its adequacy3. Alignment with the IT tactical plan is a measure of how well the information security policy supports the short-term actions and projects that implement the IT strategy. However, the IT tactical plan itself shouldbe aligned with the business objectives, and not vice versa4. Compliance with industry best practice is a desirable quality of an information security policy, but it is not a guarantee of its effectiveness or suitability for the organization. Industry best practices are general guidelines or recommendations that may

not apply to every organization or situation. An information security policy should be customized and tailored to the specific context and needs of the organization. References: The 12 Elements of an Information Security Policy | Exabeam1
11 Key Elements of an Information Security Policy | Egnyte2
What is an IT steering committee? Definition, roles and responsibilities ...3 What is IT Strategy? Definition, Components and Best Practices | BMC ...4 IT Security Policy: Key Components and Best Practices for Every Business

質問: **9**
システム開発スタッフの新規メンバーに付与する場合、以下のアクセス権限のうちどれが最も大きなリスクをもたらしますか？
A. 本番プログラムライブラリへの書き込みアクセス
B. 開発データライブラリへの書き込みアクセス
C. 実行プログラムライブラリへのアクセス
D. 開発プログラムライブラリへのアクセスを実行します
正解: **(**正解を表示します**)**
Write access to production program libraries presents the greatest risk when granted to a new member of the system development staff. Production program libraries contain executable code that runs on live systems and supports critical business functions. Write access allows a user to modify or delete existing programs, or add new programs to the library. If a user were to make unauthorized or erroneous changes to production programs, it could cause serious disruptions, errors, or security breaches in the organization's operations.
Therefore, writeaccess to production program libraries should be restricted to authorized personnel only, and subject to strict change management controls.

質問: **10**
情報システムの取得、開発、導入プロセスをレビューするIS監査担当者にとって、以下のうちどれが最も懸念すべき事項でしょうか？
A. データ所有者はデータ変換ツールの使用方法についてトレーニングを受けていません。
B. 導入後の教訓検証は実施されませんでした。
C. システムの導入は、通常、請負業者によって行われます。
D. 閲覧可能なシステムドキュメントがありません。
正解: **(**正解を表示します**)**

質問: **11**
IS監査担当者が組織のリスク管理プログラムをレビューしています。以下のうち、企業のITリスク許容度を決定する主要な要因となるべきものはどれですか？
A. 戦略目標
B. 投資収益率(ROI)

C. 制御を導入するコスト
D. リスク事象の発生確率
正解: **A (**コメントを発表する**)**
An organization ' s IT risk appetite should be primarily driven by its strategic objectives. The risk appetite defines the amount and type of risk the organization is willing to pursue or retain to achieve its goals.
Aligning risk appetite with strategic objectives ensures that risk-taking is consistent with the organization ' s mission and vision. While ROI, cost of controls, and the likelihood of risk events are important considerations in risk management, they are factors evaluated within the context of the overarching strategic objectives.
References:
ISACA CISA Review Manual, 28th Edition, Chapter 2: Governance and Management of IT.

質問: **12**
ソフトウェアライセンス監査において、以下のうち最も重要なものはどれですか？
A. 判断サンプリング
B. 実質的テスト
C. コンプライアンステスト
D. ストップ -オア -ゴー -サンプリング
正解: **(**正解を表示します**)**
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 examiningtransactions, 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 itdoes notverify 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 orbalances" and compliance testing as "testing performed to obtain audit evidence on theoperating effectiveness of controls." 1 According to the ISACA IT Audit and Assurance Guideline G15 Software License Management, "The objective of a software license auditis 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

質問: **13**
被監査企業が、高リスクの指摘事項に対する是正措置計画の策定に予想よりも時間がかかると表明した場合、IS監査担当者が取るべき最善の行動は次のうちどれでしょうか？
A. 期限切れの発見事項を監査委員会に報告する。
B. より長い目標日を受け入れ、監査システムに記録します。
C. 合意された期間内に是正措置を完了することを要求します。
D. 暫定的な補償制御が実施されているかどうかを判断します。
正解: **(**正解を表示します**)**

質問: **14**
ビジネスアプリケーションシステムに保存されている機密情報の不正な取得を防止するために、次のうちどれが最も適切ですか？
A. アクセス制御にシングルサインオンを適用する
B. 職務分掌を実施する。
C. 内部データアクセスポリシーを適用します。
D. デジタル署名の使用を強制します。
正解: **(**正解を表示します**)**
The most appropriate control to prevent unauthorized retrieval of confidential information stored in a business application system is to enforce an internal data access policy. A data access policy defines who can access what data, under what conditions and for what purposes. It also specifies the roles and responsibilities of data owners, custodians and users, as well as the security measures and controls to protect data confidentiality, integrity and availability. By enforcing a data access policy, the organization can ensure that only authorized personnel can retrieve confidential informationfrom the business application system. Applying single sign-on for access control, implementing segregation of duties and enforcing the use of digital signatures are also useful controls, but they are not sufficient to prevent unauthorized data retrieval without a clear and comprehensive data access policy.
References:
CISA Review Manual, 27th Edition, page 2301
CISA Review Questions, Answers and Explanations Database - 12 Month Subscription2

質問: **15**
組織のITポリシーが効果的に実施されていることを確認するために、IS監査担当者が最も適切なアプローチは次のうちどれですか？
A. 組織の外部認証を確認する。
B. 業界標準と比較してポリシーをベンチマークする。
C. 従業員がポリシーをどの程度遵守しているかを判断する。

D. ITセキュリティ侵害が増加しているかどうかを判断する。
正解: **C** (コメントを発表する)
The correct answer is C. Determine the level of employee adherence to the policies.
To obtain assurance that IT policies have been effectively implemented, the auditor must determine whether employees actually follow the policies in daily operations. A policy may be well written, approved, and aligned with standards, but it is not effectively implemented unless users, administrators, managers, and process owners comply with it.
ISACA guidance on policy compliance explains that assurance over compliance requires collecting sufficient information through methods such as direct observation, metrics, corroboration, tests, controls, audits, self- assessments, and critical questioning. ISACA's CISA Exam Content Outline also includes evaluating the organization's management of IT policies and practices, including compliance with legal and regulatory requirements.
Option A is not the best answer because external certifications may provide some comfort, but they do not prove that the organization's own employees are consistently following internal IT policies.
Option B is not the best answer because benchmarking shows whether policies are well designed compared with industry standards. It does not prove that the policies are implemented or followed.
Option D is not the best answer because security breaches are lagging indicators. A lack of breaches does not prove policy effectiveness, and an increase in breaches may be caused by many factors unrelated to policy implementation.
This question maps mainly to Governance and Management of IT because IT policies, standards, procedures, practices, and compliance with those practices are part of IT governance.
References: ISACA CISA Exam Content Outline, Domain 2; ISACA article on determining policy compliance.

質問: **16**
上級監査人が、下級監査人が作成した作業書類を精査している。その書類には、被監査企業が問題を修正したと述べた後に、指摘事項が削除されたことが示されている。上級監査人が取るべき最も適切な行動は次のうちどれか？
A. 被監査者に再テストを依頼する
B. 記載されている作業書類を承認する
C. 調査結果を復活させる
D. この問題を監査責任者に照会する
正解: (正解を表示します)
The senior auditor's most appropriate course of action is to have the finding reinstated, because the auditee's claim of correcting the problem is not sufficient evidence to support the removal of the finding. The auditor should verify that the corrective action has been implemented effectively and that it has resolved the underlying issue or risk. The auditor should also document the evidence andresults of the verification in the work papers. The

other options are not appropriate, because they either accept the auditee's claim without verification, delegate the responsibility to the auditee or escalate the issue unnecessarily.
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,section12062

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu　**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **17**
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. ギャップ分析を実施する。
B. コントロール自己評価(CSA)を実施する。
C. 成熟度モデルを開発する。
D. 主要業績指標(KPI)を評価する。
正解: **C** (コメントを発表する)

質問: **18**
経理部門内で男性社員を適切に隔離するために、次のうちどの管理策が最も効果的ですか？
A. 取引の監査証跡が存在することを保証する
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基づいてプログラムの機能を制限します
正解: (正解を表示します)
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 and Explanations Database,Question ID 223

質問: **19**
IS監査担当者は、経営陣の回答に対してまず何をすべきでしょうか？
対面式の内部統制質問票は、重要な内部統制を示す。
制御はもはや効果的ではないのか？
A. 制御を効果的にするために必要なリソースを決定します。
B. 内部統制の全体的な有効性を検証します。
C. コントロールが無効になった場合の影響を確認します。
D. 他の補償制御の存在を確認する。
正解: **(**正解を表示します**)**
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 theyeither 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

質問: **20**
組織の新たに導入され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IS監査担当者にとって、以下の調査結果のうちどれが最も懸念すべきでしょうか？
A. 新入社員のみがプログラムへの参加を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は確立されていません。
C. 従業員は結果を即座に通知されません
D. プログラムの更新時期はまだ決定されていません
正解: **(**正解を表示します**)**
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 alsoissues 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

質問: **21**
マルチテナントクラウド環境において、データ漏洩防止を最も効果的に実現す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アラートを発するように設定されています。
B. 包括的なセキュリティレビューが四半期ごとに実施されます。
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ります
正解: **(**正解を表示します**)**
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

質問: **22**
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する。
C. インシデントの影響を受けたシステムを隔離します。
D. 根本原因分析を開始します。
正解: **A (**コメントを発表する**)**
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

質問: **23**
データ保護のためにデータ所有権を割り当てる主な理由は、以下の点を確立するためである。
A. 信頼性。
B. 説明責任。
C. 権限、
D. トレーサビリティ。
正解: **(**正解を表示します**)**

質問: **24**
以下の戦略のうち、データ保持に関する慣行を損なうことなく、データストレージを最も最適化できるのはどれですか？
A. 電子メールで送信されるファイル添付ファイルのサイズを制限する
B. 1年以上前のメールを自動的に削除します
C. 30日後にメールを仮想メール保管庫に移動する
D. 従業員が大容量のメールをフラッシュドライブに保存できるようにする
正解: **(**正解を表示します**)**
The best strategy to optimize data storage without compromising data retention practices is to limit the size of file attachments being sent via email. This strategy can reduce the amount of storage space required for email messages, as well as the network bandwidth consumed by email traffic. File attachments can be large and often contain redundant or unnecessary information that can be compressed, converted, or removed before sending. By limiting the size of file attachments, the sender can encourage the use of more efficient formats, such as PDF or ZIP, or alternative methods of sharing files, such as cloud storage or web links. This can also improve the security and privacy of email communications, as large attachments may pose a higher risk of being intercepted, corrupted, or infected by malware.
References:
Data Storage Optimization: What is it and Why Does it Matter?
Data storage optimization 101: Everything you need to know

質問: **25**
IS監査人が、サードパーティベンダーの主要業績評価指標(KPI)の報告をレビューします。監査人が最も懸念すべき所見は次のうちどれですか？
A. KPIデータは分析されていません
B. KPIが明確に定義されていない
C. 一部のKPIは文書化されていません
D. KPIは一度も更新されていません

正解: **B (**コメントを発表する**)**
KPIs are not clearly defined is the most concerning finding for an IS auditor, because it implies that the third- party vendor does not have a clear understanding of what constitutes success or failure in their performance.
This can lead to inaccurate or misleading reporting, poor decision making, and lack of accountability. KPIs should be SMART (specific, measurable, achievable, relevant, and time-bound) and aligned with the business objectives and expectations of the stakeholders12. References: 1: CISAReview Manual (Digital Version), Chapter 5, Section 5.3.2 2: CISA Online Review Course, Module 5, Lesson 3

質問: **26**
ある組織が、特定の業務プロセスを対象とした統制自己評価(CSA)プログラムの導入を計画しています。このプログラムにおいて、内部監査チームの役割として適切なのは次のうちどれでしょうか？
A. 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施する。
B. 自己評価プロセスについて経営陣に助言する。
C. 経営陣がプロセス管理を効果的に評価するためのテスト手順を設計する。
D. CSAの対象となるビジネスプロセスを、今後の監査計画から除外する。
正解: **(**正解を表示します**)**
Theinternal audit team's roleinControl Self-Assessment (CSA)is toindependently validatemanagement's assessment to ensure accuracy and effectiveness.
Perform Testing to Validate Management's Assessment (Correct Answer - A) Ensures that self-assessments are reliable and comply with policies.
Example:Internal audit conducts sample tests to verify self-reported compliance.
Advising Management (Incorrect - B)
The audit teamreviewsrather than advises management.
Designing Testing Procedures (Incorrect - C)
Management should design CSA procedures, not auditors.
De-Scoping Business Processes (Incorrect - D)
Internal auditshould notreduce audit scope due to CSAs.
References:
ISACA CISA Review Manual
COBIT 2019: Control Self-Assessment

質問: **27**
クレジットカード会社が顧客明細書の印刷を外部委託することを決定しました。同社にとって最も重要な確認事項は以下のとおりです。
A. プロバイダーは代替のサービス拠点を持っています。
B. 契約には、サービス水準の不足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、会社のセキュリティ管理と一致しています。

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。
正解: **(**正解を表示します**)**
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 isbecause 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

質問: **28**
取引処理システムは総勘定元帳と連携しています。データ分析の結果、一部の取引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を実施したと述べていますが、情報システム監査担当者は、今後この連携が正しく機能していることを検証するために、どのような対策を推奨すべきでしょうか？
A. 定期的な照合を実行します。
B. システム修正について、システム所有者の承認を得てください。
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。
正解: **A (**コメントを発表する**)**
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)

質問: **29**
IS 監査人は、実装以来テストされていない 2 つのビジネス クリティカルなシステム間のデータ転送の整合性を確認するように依頼されました。監査を計画するのに最も役立つ情報は次のどれですか。
A. システム変更ログ
B. IT テストのポリシーと手順
C. 以前のシステムインターフェーステスト記録
D. 品質保証 (QA) テスト
正解: **(**正解を表示します**)**

質問: **30**
組織内に内部IS監査機能を維持することの最大の利点は次のうちどれですか？
A. 勧告の独立性と公平性の向上
B. 年間を通じてIS監査スタッフの可視性と対応能力が向上しました。
C. 経営陣と提言について交渉する能力
D. ビジネスとプロセスへの理解を深める
正解: **(**正解を表示します**)**

質問: **31**
システム開発プロセスで品質保証 (QA) を実行する主な目的はどれですか?
A. 開発されたシステムが他のシステムとうまく統合されるようにする
B. 開発されたシステムがビジネス要件を満たしていることを確認する
C. 新しいシステムの高レベルの要件を決定するのに役立ちます
D. 期待された利益が実現されていることを確認する
正解: **B (**コメントを発表する**)**

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com

CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu 「**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **32**
次のうち、シャドウITの例はどれですか？
A. IT部門の承認なしにクラウドベースの注文管理ツールを使用している従業員
B. 従業員が会社支給のノートパソコンを使用して個人の銀行情報にアクセスする
C. IT部門の承認を得ずに、従業員が個人用メールを使用して顧客と連絡を取っている。
D. 勤務時間中に会社支給のタブレットを使ってソーシャルメディアにアクセスする従業員
正解: **(**正解を表示します**)**
Shadow IT refers to the use of IT systems, devices, software, or services without explicit organizational approval. This often occurs when employees or departments adopt tools that bypass official IT governance structures.
Using a Cloud-Based Order Management Tool Without Approval (Option A)is a clear example of shadow IT because the employee is circumventing established IT policies to implement a solution independently.
Accessing Personal Banking Information on a Company-Provided Laptop (Option B)is a potential misuse of resources but does not qualify as shadow IT since it does not involve unauthorized technology.
Using Personal Email for Client Communication (Option C)may violate communication policies but is not related to the adoption of unapproved IT systems.
Accessing Social Media on a Company-Provided Tablet (Option D)is improper use of a company asset but does not involve unauthorized IT tools.
Shadow IT introduces risks such as data breaches, lack of compliance, and inefficiencies due to lack of integration with official systems. Organizations should have clear policies and monitoring mechanisms to address such risks.
Reference:ISACA CISA Review Manual, Job Practice Area 1: Governance and Management of IT.

質問: **33**
組織のデータ分類プロセスに関して、最も大きな懸念事項は次のうちどれですか？
A. データ分類プロセスは過去1年間更新されていません。
B. データ分類プロセスを管理するために使用されるシステムが同期されていません。
C. データ分類プロセスが業界標準に準拠していません。
D. 記録管理を担当するユーザーは、データ分類プロセスを認識していません。
正解: **(**正解を表示します**)**

質問: **34**

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
正解: **A** (コメントを発表する)
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 reviewthe work performed by a seniorIS 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 thanthe IS audit manager's. References: CISA Review Manual (Digital Version)
1, Chapter 2, Section 2.2.5

質問: **35**
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、以下を確認することです。
A. 付与されたアクセス権限。
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. アクセス制御システムのログ設定。
正解: (正解を表示します)
The best way to determine whether programmers have permission to alter production data is to review the access rights that have been granted. In audit terms, the question is asking whether the programmers are authorized to perform a specific action in production. The most direct evidence of that authorization is the actual privileges assigned to their accounts or roles. ISACA access-control guidance consistently focuses on granted access, segregation of duties, and restricting direct production or database access.
Option A is correct because granted rights directly show whether programmers can update, modify, or otherwise alter production data. If those privileges are present, the

permission exists; if not, it does not. This is more direct than reviewing configuration or implementation history.
Option B is not the best answer because reviewing how recent changes were implemented may indicate whether developers were involved in production changes, but it does not directly confirm whether they currently have permission to alter production data. It is indirect evidence.
Option C is also weaker than A. Access control system configuration may reveal how permissions are structured, but the clearest evidence is still the actual rights granted to the programmers or their roles.
Option D is incorrect because log settings show what may be recorded, not what access is authorized. Logs may help detect misuse, but they do not define whether permission exists.
Therefore, A is the best answer because reviewing granted access rights is the most direct and reliable way to determine whether programmers can alter production data.
References (Official ISACA):
* ISACA Journal, An Approach Toward Sarbanes-Oxley ITGC Risk Assessment - logical access and direct database access are central audit concerns.
* ISACA Journal, Auditing Amazon Web Services - audit focus includes how access is restricted and how administrative activity is segregated.
* ISACA, Selected COBIT 5 Processes for Essential Enterprise Security - access should be justified, authorized, logged, and monitored.

質問**: 36**
経営陣は、新たに導入された購買パッケージがどの程度業務要件を満たしているかを判断するため、導入後のレビューを要請しました。以下のうち、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. 実装方法論
C. 行処理の結果
D. テスト結果
正解**: C (**コメントを発表する**)**
A post-implementation review is a process of evaluating the outcome and benefits of a project or a system after it has been implemented. The main purpose of a post-implementation review is to determine to what extent the business requirements are being met by the new system. Therefore, the most likely aspect to be assessed is the results of line processing, which refers to the actual performance and functionality of the system in the operational environment.

質問**: 37**
IT運営委員会の主な責任は次のうちどれですか？
A. IT戦略統合の取り組みのレビューと支援

B. ITセキュリティ戦略の策定と評価
C. セキュリティをビジネス目標に統合するためのプロセスの実装
D. セキュアなシステム開発フレームワークの開発と実装
正解: **(**正解を表示します**)**
This means that the IT steering committee is responsible for ensuring that the IT strategy aligns with and supports the business strategy, vision, and goals of the organization. The IT steering committee is also responsible for overseeing and approving major IT initiatives, projects, and investments, and allocating resources and priorities accordingly12.
Developing and assessing the IT security strategy (B) is not the main responsibility of the IT steering committee, but rather a specific aspect of the IT strategy that may be delegated to a subcommittee or a dedicated security function. The IT steering committee may provide guidance and oversight for the IT security strategy, but it is not directly involved in developing and assessing it12.
Implementing processes to integrate security with business objectives is not the main responsibility of the IT steering committee, but rather an operational task that may be performed by the IT management and staff. The IT steering committee may monitor and evaluate the effectiveness of the security processes, but it is not directly involved in implementing them12.
Developing and implementing the secure system development framework (D) is not the main responsibility of the IT steering committee, but rather a technical task that may be performed by the IT developers and engineers. The IT steering committee may approve and endorse the secure system development framework, but it is not directly involved in developing and implementing it12.

質問: **38**
IS監査担当者が人工知能(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。このシステムでは、深刻な影響を及ぼす重大なエラーが複数発生しています。IS監査担当者は、エラーの原因を理解するために、次に次のうちどれを行うべきでしょうか？
A. システム所有者にインタビューする。
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ている意思決定ロジックをレビューします。
正解: **(**正解を表示します**)**

質問: **39**
共有プリンターで印刷された機密文書の漏洩を防ぐ方法として、次のうちどれが適切ですか？
A. パスワードを使用して、承認されたユーザーがプリンターにドキュメントを送信できるようにします。
B. 印刷物を作成するためにプリンターにキーコードの入力が必要

C. ユーザーのコンピュータとプリンタ間のデータストリームを暗号化します。
D. 印刷文書の分類レベルを示すヘッダーページを作成する
正解: **(**正解を表示します**)**
Requiring a key code to be entered on the printer to produce hard copy is a method to prevent disclosure of classified documents printed on a shared printer. This is because requiring a key code adds an extra layer of security and authentication to the printing process, ensuring that only authorized users can access and retrieve the printed documents. Requiring a key code also prevents unauthorized users from viewingor tampering with the documents while they are in the printer's queue or output tray1.
Using passwords to allow authorized users to send documents to the printer is not a sufficient method to prevent disclosure of classified documents printed on a shared printer. This is because passwords only protect the transmission of the documents from the user's computer to the printer, but they do not protect the documents once they are printed. Passwords can also be compromised or forgotten by users, making them vulnerable to unauthorized access or denial of service2.
Encrypting the data stream between the user's computer and the printer is not a sufficient method to prevent disclosure of classified documents printed on a shared printer. This is because encryption only protects the confidentiality and integrity of the documents while they are in transit, but they do not protect the documents once they are printed. Encryption can also introduce performance issues or compatibility problems with different printers or devices2.
Producing a header page with classification level for printed documents is not a method to prevent disclosure of classified documents printed on a shared printer. This is because producing a header page only informs the users about the sensitivity and handling of the documents, but it does not prevent unauthorized users from accessing or viewing them. Producing a header page can also waste paper and ink, as well asincrease the risk of misplacing or mixing up the documents

質問: **40**
情報システム監査担当者がITガバナンス監査を実施している際に、多くの取り組みが個々の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づきました。以下の推奨事項のうち、ITチームの成熟度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、翌年にフォローアップ監査を予定してください。
B. ITの優先順位付けと支出を監督するための学際的なIT運営委員会を設置する。
C. プロジェクト管理ツールですべてのIT関連の決定事項を文書化し、追跡します。
D. 正式な承認が得られ、文書化されるまで、現在進行中のすべてのITプロジェクトを中止してください。
正解: **B (**コメントを発表する**)**

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 measuredand 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

質問: **41**
IS監査マネージャーが、クラウドサービスプロバイダーの監査業務のための人員配置計画を作成しています。部門に新しく配属された監査担当者が以前このプロバイダーで勤務していたことを知った場合、マネージャーが最も懸念すべきことは何でしょうか？
A. 専門知識
B. リソースの可用性
C. 職業倫理
D. 独立
正解: **(**正解を表示します**)**

質問: **42**
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。
正解: **(**正解を表示します**)**
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?

質問: **43**
契約においてソースコードのエスクローを要求する主な目的は以下のとおりです。
A. ベンダー管理ポリシーを遵守する
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。
正解: **(正解を表示します)**
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 ReviewManual (Digital Version)1, Chapter 3, Section 3.2.2

質問: **44**
ある組織は、業務目的で個人情報を取得する提案を受けて、顧客向けWebアプリケーションのセキュリティ強化に取り組んでいます。この取り組みを実施する前に、以下のうちどれを最も重要視して確認すべきでしょうか？
A. 顧客への通知手順
B. 暗号化機能
C. 規制遵守要件
D. データ所有権の割り当て
正解: **C (コメントを発表する)**

質問: **45**
情報システム監査担当者は、セキュリティ侵害によって個人情報(PII)が漏洩した個人の数に基づいて罰則を課す新たな規制について知りました。顧客情報データベースの侵害に伴う組織の責任を軽減するために、最も適切な対策は何でしょうか？
A. データベースのセグメンテーション
B. データベース正規化
C. データベースの調和
D. データベース最適化
正解: **(正解を表示します)**
The best recommendation is database segmentation. If liability depends on the number of individuals whose PII is exposed, the organization should reduce the amount of data that could be compromised in any single breach event. Segmenting databases or separating sensitive data domains limits blast radius and can reduce the number of records exposed in a single incident. ISACA guidance supports isolating high-value assets and tightening internal controls as a way to reduce exposure and improve resilience.
Option A is correct because segmentation limits concentration risk. Instead of keeping all customer data in one broadly exposed logical store, segmentation helps confine access and reduce how many records a single compromise can reach. This directly supports limiting breach impact and, in this case, potential liability tied to the number of affected individuals. This conclusion is an inference from ISACA's risk-reduction principles around isolation, exposure control, and documenting exposure.
Option B is incorrect because database normalization improves data structure and reduces redundancy; it is not primarily a breach-liability reduction control.
Option C is incorrect because database harmonization is about consistency or integration across datasets, not limiting exposure in a breach.
Option D is incorrect because database optimization focuses on performance and efficiency, not on minimizing the number of PII records exposed in a security incident.
Therefore, A is the best answer because segmentation is the option that most directly reduces the scope of exposure in a breach and therefore helps limit liability based on affected individuals.
References (Official ISACA):
ISACA, Best Practices for Setting Up a Cybersecurity Operations Center - recommends prioritizing assets and isolating high-value asset networks.
ISACA Journal, Reporting on GDPR Compliance to the Board - emphasizes documenting exposure and relevant risk controls for privacy risk reporting.
ISACA Journal, Practical Data Security and Privacy for GDPR and CCPA - supports governance approaches to limiting privacy exposure. (Referenced conceptually from prior ISACA privacy guidance.)

質問: **46**

第三者が関与する共同開発活動において、組織の専有コードを最も適切に保護できるのは次のうちどれですか？
A. 作業範囲記述書(SOW)
B. 秘密保持契約(NDA)
C. サービスレベル契約 (SLA)
D. プライバシーに関する同意
正解: **(**正解を表示します**)**
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 and Implementation, Section 3.2: Project Management Practices.

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu　**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **47**
IS監査の過程で、経営陣はIS監査人が指摘した問題点について口頭で同意した。

しかし、報告書の草案を提示したところ、経営陣は調査結果に同意しませんでした。監査人は次に何をすべきでしょうか？
A. 経営陣の提案に従って調査結果を書き直してください。
B. これ以上の協議を中止し、最終報告書をそのまま発行する。
C. 調査結果の証拠を提示し、フォローアップ会議を要請する。
D. 直ちに監査委員会の委員長に報告してください。
正解: **(**正解を表示します**)**
The correct answer is C. Provide evidence for the finding and request a follow-up meeting. When management disagrees with an audit finding in the draft report, the auditor should support the finding with sufficient and appropriate evidence and discuss the matter with management. The purpose is to clarify facts, resolve misunderstandings, validate the evidence, and determine whether the finding should remain, be modified, or be removed.
Option A is incorrect because the auditor should not rewrite a finding simply because management disagrees.
Changes should be based on evidence. Option B is too rigid because issuing the report without further discussion may damage audit quality and stakeholder communication.
Option D may be appropriate only if the disagreement cannot be resolved or involves significant risk, but escalation to the audit committee is not the immediate next step.
ISACA's CISA Exam Content Outline includes audit evidence collection, audit reporting, communication of findings, and conducting audit follow-up under Domain 1. The auditor's conclusion should be evidence-based and properly communicated.
References: ISACA CISA Exam Content Outline, Domain 1; ISACA audit evidence and reporting concepts.

質問: **48**
IS監査担当者は、オペレーティングシステムのパラメータ変更が承認されたかどうかを判断するために、次のうちどれを最も確認する可能性が高いでしょうか？
A. 終了ルーチンのドキュメント
B. システム初期化ログ
C. 変更管理ログ
D. セキュリティシステムパラメータ
正解: **C (**コメントを発表する**)**
Operating system parameters are settings or values that affect the behavior or performance of the operating system1. Modifications to the operating system parameters may be necessary to improve the system functionality, security, or efficiency. However, such modifications may also introduce risks or errors that can affect the system stability, compatibility, or integrity. Therefore, modifications to the operating system parameters should be authorized and documented by the appropriate authority2.
A change control log is a record of all changes made to the system, including the date, time, description, reason, authorization, and impact of each change3. A change control log

can help the IS auditor to verify whether modifications to the operating system parameters were authorized by comparing the log entries with the actual system settings and the change approval documents4.

質問: **49**
電子商取引ウェブサイトのユーザー認証に使用されるサーバーのパフォーマンス低下を最も効果的に最小限に抑える方法はどれですか？
A. 1台のサーバーをプライマリ認証サーバーとして、2台目のサーバーをセカンダリ認証サーバーとして構成します。
B. 各認証サーバーを認証サーバーのクラスタに属するものとして構成します。
C. 各認証サーバーを設定し、そのRAIDの各ディスクがプライマリコントローラーに接続されていることを確認します。
D. 各認証サーバーを設定し、各サーバーのディスクがデュプレックスの一部を形成するようにします。
正解: **(**正解を表示します**)**
Configuring each authentication server as belonging to a cluster of authentication servers is the best way to minimize performance degradation of servers used to authenticate users of an e-commerce website. A cluster is a group of servers that work together to provide high availability, load balancing, and fault tolerance. If one server fails or becomes overloaded, another server in the cluster can take over its workload without disrupting the service. A single server as a primary authentication server and a second server as a secondary authentication server is not as effective as a cluster, because the secondary server is only used when the primary server fails, which means it is idle most of the time and does not improve performance. Configuring each authentication server and ensuring that each disk of its RAID is attached to the primary controller does not address the issue of performance degradation, but rather the issue of data redundancy and reliability. RAID (redundant array of independent disks) is a technology that combines multiple disks into a logical unit that can tolerate disk failures and improve data access speed. Configuring each authentication server and ensuring that the disks of each server form part of a duplex does not address the issue of performance degradation, but rather the issue of data backup and recovery. A duplex is a pair of disks that store identical copies of data, so that if one disk fails, the other disk can be used to restore the data. References: ISACA CISA Review Manual 27th Edition, page 310

質問: **50**
システム開発プロジェクトの課題管理プロセス中に発生する事象は次のうちどれですか？
A. 緊急時対応計画
B. 構成管理
C. ヘルプデスク管理
D. 影響評価

正解: **D (**コメントを発表する**)**
Impact assessment is an activity that occurs during the issues management process for a system development project. Issues management is a process of identifying, analyzing, resolving, and monitoring issues that may affect the project scope, schedule, budget, or quality. Impact assessment is a technique of evaluating the severity and priority of an issue, as well as its implications for the project objectives and deliverables. The other options are not activities that occur during the issues management process, but rather related to other processes such as contingency planning, configuration management, or help desk management. References:
CISA Review Manual (Digital Version), Chapter 4, Section 4.3.31
CISA Review Questions, Answers and Explanations Database, Question ID 217

質問: **51**
プロジェクト監査の過程で、情報システム監査担当者は、プロジェクト報告書が現在の進捗状況を正確に反映していないことに気づいた。
以下のうち、最も大きな影響をもたらすものはどれですか？
A. プロジェクトマネージャーを交代させる必要があります。
B. 取締役会に報告するプロジェクトは未完了となります。
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. このプロジェクトは品質保証(QA)レビューに耐えられません。
正解: **(**正解を表示します**)**
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 orad 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 predefined 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 and Responsibilities, Project Reporting Best Practices, Quality Assurance in Project Management

質問: **52**
コントロール自己評価(CSA)は、以下の目的で使用できます。
A. 資産の価値を決定します。
B. 基準値を設定します。
C. 戦略的な事業目標を評価する。
D. 監査を置き換えます。
正解: **B (**コメントを発表する**)**
Control self-assessment (CSA) is a process that allows business units to evaluate the effectiveness of internal controls. It is primarily used to establish baselines (Option B) for measuring control effectiveness and risk management.
ISACA CISA Reference: CSA is a recognized internal control mechanism that supports risk assessment and control improvement.
Risk Implication: If CSAs are not conducted properly, organizations may lack visibility into weak controls, increasing exposure to risks.
Alternative Choices:
Option A: CSA does not focus on asset valuation.
Option C: Strategic business goals are assessed separately through governance processes.
Option D: CSA complements, but does not replace, formal audits.

質問: **53**
組織のデバイス在庫を照合する担当者が以下のタスクを実行した場合、職務分掌(SoD)上の懸念が最も大きくなるのはどれでしょうか？
A. デバイスの発行を承認する
B. スペアパーツに使用される追跡装置
C. デバイスポリシーを作成中
D. 従業員へのデバイスの発行
正解: **(**正解を表示します**)**

質問: **54**
IS監査担当者は、以下のうちどれが最も高い機密レベルに分類されているかを確認すべきでしょうか？
A. サーバー室へのアクセス履歴
B. 緊急変更記録
C. ITセキュリティインシデント
D. 侵入テスト結果
正解: **(正解を表示します)**
The IS auditor should ensure that penetration test results are classified at the highest level of sensitivity, because they contain detailed information about the vulnerabilities and weaknesses of the IT systems and networks, as well as the methods and tools used by the testers to exploit them. Penetration test results can be used by malicious actors to launch cyberattacks or cause damage to the organization if they are disclosed or accessed without authorization. Therefore, they should be protected with the highest level of confidentiality, integrity and availability. The other options are not as sensitive as penetration test results, because they either do not reveal as muchinformation aboutthe IT security posture, or they are already known or reported by the organization. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.4

質問: **55**
IS監査人がリスク評価を実施する主な理由は次のうちどれですか？
A. 材料問題が発生する可能性が比較的高い領域を特定するのに役立ちます。
B. 是正措置計画の策定の基礎となる。
C. 不適切な管理行動の種類に対する認識を高める
D. 不正行為や不正確な行為に最も敏感な領域を特定するのに役立ちます。
正解: **A (コメントを発表する)**
The primary reason for an IS auditor to perform a risk assessment is to help identify areas with a relatively high probability of material problems. A risk assessment is a systematic process of evaluating the potential risks that may be involved in an activity or undertaking. It involves identifying the sources of risk, analyzing the likelihood and impact of the risk, and prioritizing the risks based on their significance. A risk assessment helps the IS auditor to focus on the areas that are most vulnerable to errors, fraud, or inefficiencies, and to design appropriate audit procedures to address those risks. A risk assessment also helps the IS auditor to allocate audit resources efficiently and effectively.
A risk assessment does not provide a basis for the formulation of corrective action plans, as this is a responsibility of management, not the IS auditor. A risk assessment does not increase awareness of the types of management actions that may be inappropriate, as this is a matter of professional ethicsand judgment. A risk assessment does not help to identify areas that are most sensitive to fraudulent or inaccurate practices, as this is a result of the risk assessment, not its purpose.

References:
ISACA, CISA Review Manual, 27th Edition, Chapter 1: The Process of Auditing Information Systems, Section 1.3: Risk Assessment in Planning1 Corporate Finance Institute, Audit Risk Model2

質問: **56**
ある組織が、月末業務プロセスをサポートする新しいシステムを導入しようとしています。業務停止時間を削減するために、以下の導入戦略のうちどれが最も効率的でしょうか？
A. ビッグバン
B. 段階的
C. カットオーバー
D. 並列
正解: **(**正解を表示します**)**
Minimizing business downtime is critical when implementing a new system that supports an essential process like month-end closing.
Option A (Incorrect):Thebig bang approachinvolves replacing the old system with the new system all at once.
This method carries ahigh riskbecause if issues arise, they may causesignificant downtimeand disruption.
Option B (Correct):Aphased approachgradually implements the system in stages, allowing users toadaptand minimizing the risk of complete failure. This strategy is ideal for critical systems that cannot afford extended downtime.
Option C (Incorrect):Thecutover approachis a variation of big bang, where the old system is shut down, and the new system is activated. This method isriskyfor month-end processes because errors can causebusiness delays.
Option D (Incorrect):Theparallel approachruns both old and new systems simultaneously to verify accuracy, but it isresource-intensiveand may not be practical for a high-volume month-end process.
Reference:ISACA CISA Review Manual -Domain 3: Information Systems Acquisition, Development, and Implementation- Covers system implementation strategies, risk management, and best practices.

質問: **57**
サイバー犯罪への対応プロセスを評価する際に、IS監査担当者が最も重視すべき事項は次のうちどれですか？
A. 法執行機関とのコミュニケーション
B. 規制当局への通知
C. 根本原因分析
D. 証拠収集
正解: **(**正解を表示します**)**

Evidence collection is the process of identifying, acquiring, preserving, and documenting digital evidence from various sources, such as computers, networks, mobile devices, or cloud services, that can be used to support the investigation and prosecution of cybercrimes. Evidence collection is an IS auditor's primary focus when evaluating the response process for cybercrimes, because it determines the quality and validity of the evidence that can be used to prove or disprove the facts of the case, identify the perpetrators, and recover the losses. Evidence collection should follow the standards and best practices for digital forensics, such as ISO
/IEC 270371, which provide guidelines for ensuring the integrity, authenticity, reliability, and admissibility of the evidence2.
The other possible options are:
A). Communication with law enforcement: This is the process of reporting, cooperating, and coordinating with law enforcement agencies that have the jurisdiction and authority to investigate and prosecute cybercrimes.
Communication with law enforcement is an important aspect of the response process for cybercrimes, but it is not an IS auditor's primary focus when evaluating it. Communication with law enforcement depends on the legal and regulatory requirements, the nature and severity of the incident, and the organizational policies and procedures. Communication with law enforcement should be done after evidence collection, to avoid compromising or contaminating the evidence3.
B). Notification to regulators: This is the process of informing and updating the relevant regulatory bodies or authorities that oversee or supervise the organization's activities or industry sector about the cybercrime incident. Notification to regulators is an important aspect of the response process for cybercrimes, but it is not an IS auditor's primary focus when evaluating it. Notification to regulators depends on the legal and regulatory requirements, the nature and impact of the incident, and the organizational policies and procedures. Notification to regulators should be doneafter evidence collection, to avoid disclosing sensitiveor confidential information4.
C). Root cause analysis: This is the process of identifying and analyzing the underlying factors or causes that led to or contributed to the cybercrime incident. Root cause analysis is an important aspect of the response process for cybercrimes, but it is not an IS auditor's primary focus when evaluating it. Root cause analysis helps to prevent or mitigate future incidents, improve security controls and processes, and learn from mistakes. Root cause analysis should be done after evidence collection, to avoid interfering with or affecting theinvestigation5.

質問**: 58**
IS監査担当者が、主要システムのキャパシティ管理がビジネス部門からの意見なしにIT部門によって行われていることを発見した場合、監査担当者の主な懸念事項は次のとおりである。
A. 機器の利用を最大限に活用できなかったこと

B. 企業の能力ニーズの予期せぬ増加。
C. データセンターのストレージ容量過剰のコスト
D. 将来の事業プロジェクト資金調達への影響。
正解: **(**正解を表示します**)**
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

質問: **59**
ある組織では、従業員が機密データを個人のモバイル端末に保存することを許可しています。紛失または盗難された端末からのデータ漏洩リスクを軽減するための最適な対策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る。
B. 重要なデータファイルをパスワードで保護します。
C. アクセス試行に複数回失敗した後に自動的にデータを消去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。
正解: **(**正解を表示します**)**
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-lockfunction are also good practices, but they may not be sufficient oreffective in preventing data leakage from lost or stolen devices. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.3

質問: **60**
次のアプローチのうち、データ分析を活用して新規アカウント作成プロセスのテストを促進するものはどれですか？
A. 無効な生年月日で新規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口座開設申請について、生年月日が無効でないかどうかを確認します。
D. 生年月日フィールドの要件に関する構成設定を評価します

正解: (正解を表示します)
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 and Examples1
Data Transformation: Definition and Examples2
Data Analysis: Definition and Examples3
Data Visualization: Definition and Examples
Functional Testing: Definition and Examples
Requirements Analysis: Definition and Examples
Configuration Testing: Definition and Examples

質問: **61**
リリース計画の主な役割は次のうちどれですか？
A. IT環境内のすべての構成項目を識別します。
B. 新しいリリースを本番環境に展開するためのタイムラインとスケジュールを提供します。
C. データベース統合の手順の概要を示します。
D. ITシステムに対する提案された変更や更新の影響を評価します。
正解: **(**正解を表示します**)**
The best answer is B. It provides a timeline and schedule for deploying new releases into production.
ISACA release and change guidance explains that successful deployment requires scrutiny over change and release, including scheduling, coordination among parties, and validation before implementation. That aligns directly with the role of a release plan: organizing when and how releases move into production.
Option A is more closely related to configuration management. Option C is too narrow because release plans cover much more than database integration. Option D is more closely associated with change evaluation and impact assessment before approval. The release plan's main function is the coordinated timeline and schedule for production rollout.
References (Official ISACA):
ISACA Journal, Implementing Emerging Technologies
ISACA Journal, Speeding Up Software Delivery With Effective Change Management

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu 「**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **62**

経理担当者による不正な電子資金振替を防止するための最適な推奨事項は次のうちどれですか？
A. 定期的なベンダーレビュー
B. デュアルコントロール
C. 独立した調整
D. 金額の再入力
E. インシデント対応のために外部のセキュリティインシデント対応専門家を起用する。
正解: **(**正解を表示します**)**
The best recommendation to prevent fraudulent electronic funds transfers by accounts payable employees is dual control. Dual control is a segregation of duties control that requires two or more individuals to perform or authorize a transaction or activity. Dual control can prevent fraudulent electronic funds transfers by requiring independent verification and approval of payment requests, amounts, and recipients by different accounts payable employees. The other options are not as effective as dual control in preventing fraudulent electronic funds transfers, as they do not involve independent checks or approvals. Periodic vendor reviews are detective controls that can help identify any irregularities or anomalies in vendor payments, but they do not prevent fraudulent electronic funds transfers from occurring. Independent reconciliation is a detective control that can help compare and confirm payment records with bank statements, but it does not prevent fraudulent electronic funds transfers from occurring. Re-keying of monetary amounts is an input control that can help detect any errors or discrepancies in payment amounts, but it does not prevent fraudulentelectronic funds transfers from occurring.
References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

質問: **63**
モバイル、ワイヤレス、およびモノのインターネット(IoT)デバイス向けにゼロトラスト戦略を実装する際に、最も重要な考慮事項は次のうちどれですか？
A. すべてのデバイスに最新のファームウェアアップデートが定期的に適用されるようにする
B. リソースへのアクセスを許可する前に、すべてのデバイスとユーザーの身元を検証します。
C. フィッシング攻撃を防ぐためのユーザー教育と意識向上に注力する
D. 転送中および保存中のデータに対する強力な暗号化プロトコルの実装
正解: **(**正解を表示します**)**
Zero Trustis based on the principle of " never trust, always verify, " makingidentity validationthe most critical aspect.
Option A (Incorrect):Firmware updatesare important for security but are onlyone partof aZero Trustapproach.
Option B (Correct):Device and user identity validationensures that onlyauthorizedentities can accesscritical resources, reducing the risk of unauthorized access.

Option C (Incorrect):User awarenessis important but does not enforce access control, which isfundamentalto Zero Trust.
Option D (Incorrect):Encryptionsecures data but does not controlwho can access resources, which is the primary focus of Zero Trust.
Reference:ISACA CISA Review Manual -Domain 5: Protection of Information Assets-CoversZero Trust security models and access control best practices.

質問: **64**
大量のリアルタイム処理システムにおいて、トランザクション処理を継続的に監視および分析するための最も効果的な手法は次のとおりです。
A. 統合試験施設(ITF)。
B. 並列シミュレーション。
C. トランザクションタグ付け。
D. 組み込み監査モジュール。
正解: **(**正解を表示します**)**
Transaction tagging is a technique by which transactions are marked with unique identifiers or headers and traced through the system using agents or sensors at each processing point1. Transaction tagging allows for continuous monitoring and analysis of transaction processing in a high-volume, real-time system by providing visibility into the performance, availability, and reliability of each transaction and its components1. Transaction tagging can also help to identify and isolate errors, bottlenecks, anomalies, and security issues in the system1.

質問: **65**
以下のうち、総当たり攻撃の成功確率を最も効果的に低減できるのはどれですか？
A. パスワードの最小文字数を要求
B. アカウントアクティビティのタイムアウトを設定する
C. アカウントロックアウトポリシーの設定
D. パスワード変更頻度の増加
正解: **C (**コメントを発表する**)**

質問: **66**
IS監査担当者の視点から見て、組織内で展開されているソフトウェアのインベントリが不完全な場合、以下のうちどれが最大のリスクとなるでしょうか？
A. 重要なサーバーで未使用のポートを閉じることができない
B. 組織内で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適用できません
D. 展開されたソフトウェアのコストを決定できない
正解: **(**正解を表示します**)**

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 configurations, 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

質問**: 67**
同時コード編集が行われる場合、頻繁なプログラムファイルの変更を最も効果的に管理できるのは次のうちどれですか？
A. 必須のアーキテクチャレビュー。
B. ソースコード構成のスキャン。
C. ソースコードのバージョン管理。
D. 変更管理自己評価(CSA)。
正解**: (**正解を表示します**)**
The correct answer is C. Source code version control.
When multiple developers make frequent and simultaneous code changes, the most effective control is source code version control. Version control allows the organization to track changes, manage branches, merge code, identify conflicts, restore prior versions, and maintain accountability for who changed what and when.
Option A is not the best answer because architecture reviews help ensure design alignment, but they do not manage simultaneous file edits. Option B is not the best answer because source code composition scanning identifies third-party/open-source component risks, licensing issues, or known vulnerabilities, but it does not control concurrent code changes. Option D is not correct because CSAs may help teams assess controls, but they do not technically manage code versions.
This question maps to Information Systems Acquisition, Development and Implementation, because ISACA's CISA Exam Content Outline includes system development methodologies, development controls, implementation testing, and change management-related practices.
References: ISACA CISA Exam Content Outline, Domain 3; ISACA Interactive Glossary, "Version control" and "Change control."

質問**: 68**
ウェブアプリケーションのセキュリティ脆弱性を標的としてデータセットへのアクセス権を取得する攻撃の種類はどれですか？
A. サービス拒否 (DoS)

B. SQLインジェクション
C. フィッシング攻撃
D. ルートキット
正解: **(**正解を表示します**)**
A SQL injection attack is a type of attack that targets security vulnerabilities in web applications to gain access to data sets. A SQL injection attack exploits a flaw in the web application code that allows an attacker to inject malicious SQL statements into the input fields or parameters of the web application. These SQL statements can then execute on the underlying database server and manipulate or retrieve sensitive data from the database. A SQL injection attack can result in data theft, data corruption, unauthorized access, denial of service or even complete takeover of the database server. A denial of service (DOS) attack is a type of attack that aims to disrupt the availability or functionality of a web application or a network service by overwhelming it with excessive requests or traffic. A phishing attack is a type of attack that uses deceptive emails or websites to trick users into revealing their personal or financial information or credentials. A rootkit is a type of malware that hides itself from detection and grants unauthorized access or control over a compromised system. References: IS Audit and Assurance Tools and Techniques, CISA Certification | Certified Information Systems Auditor | ISACA

質問: **69**
組織のオフィス間で機密データを転送する方法を監査するIS監査担当者にとって、以下のうちどれが最も懸念すべき事項でしょうか？
A. この方法は、公開鍵基盤(PKI)の使用のみに依存しています。
B. この方法は、デジタル署名の使用のみに依存しています。
C. この方法は、非対称暗号化アルゴリズムの使用のみに依存しています。
D. この方法は、128ビット暗号化の使用のみに依存しています。
正解: **(**正解を表示します**)**
The greatest concern to an IS auditor reviewing an organization's method to transport sensitive data between offices is that the method relies exclusively on the use of asymmetric encryption algorithms. Asymmetric encryption algorithms, also known as public key encryption, use two different keys for encryption and decryption: a public key that is shared with anyone who wants to communicate with the sender, and a private key that is kept secret by the sender. Asymmetric encryption algorithms are more secure than symmetric encryption algorithms, which use the same key for both encryption and decryption, but they are also slower and more computationally intensive. Therefore, relying exclusively on asymmetric encryption algorithms may not be efficient or practical for transporting large amounts of sensitive data between offices. A better method would be to use a combination of symmetric and asymmetric encryption algorithms, such as using asymmetric encryption to exchange a symmetric key and then using symmetric encryption to encrypt and decrypt the data.

The other options are not as concerning as option C. The method relying exclusively on the use of public key infrastructure (PKI) is not a concern, because PKI is a system that provides the services and mechanisms for creating, managing, distributing, using, storing, and revoking digital certificates that are based on asymmetric encryption algorithms. PKI enables secure and authenticated communication between parties who do not have a prior trust relationship. The method relying exclusively on the use of digital signatures is not a concern, because digital signatures are a way of verifying the authenticity and integrity of a message or document by using asymmetric encryption algorithms. Digital signatures ensure that the sender cannot deny sending the message or document, and that the receiver can detect any tampering or alteration of the message or document. The method relying exclusively on the use of 128-bit encryption is not a concern, because 128-bit encryption is a level of encryption that uses a 128-bit key to encrypt and decrypt data. 128-bit encryption is considered to be strong enough to resist brute-force attacks by modern computers. References: Asymmetric vs Symmetric Encryption: What are differences?, Public Key Infrastructure (PKI), Digital Signature, What is
128-bit Encryption?

質問**: 70**
以下のうち、内部監査組織が報告プロセスの独立性と透明性を支援するように構成されていることを示すものはどれですか？
A. 監査人は、業務上の義務または活動を実行する責任があります。
B. 内部監査マネージャーは、上級管理職に機能的に報告します。
C. 内部監査マネージャーは監査委員会に報告する権限を持っています。
D. 監査人は、内部統制システムの評価と運用に責任を負います。
正解**: C (**コメントを発表する**)**
The internal audit manager should have a reporting line to the audit committee, which is an independent body that oversees the internal audit function and ensures its objectivity and accountability. Reporting functionally to a senior management official may compromise the independence and clarity of the internal audit reporting process, as senior management may have a vested interest in the audit results or influence the audit scope and priorities. *References: According to the ISACA IT Audit and Assurance Standards, Guidelines and Tools and Techniques for IS Audit and Assurance Professionals, section 1002 Independence, "The chief audit executive (CAE)should report functionally to the board or its equivalent (e.g., audit committee) and administratively to executive management." 1

質問**: 71**
ある組織が、メール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メールを送信することで、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。意識向上トレーニングの効果を最もよく示す指標は次のうちどれですか？
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. メール送信者の詳細を知るためにリンクをクリックしたユーザー数
C. メールをビジネスユニットマネージャーに転送しているユーザーの数
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数
正解**: D (**コメントを発表する**)**
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

質問**: 72**
IS監査人が、一連のクレジットカード取引における不正行為を検出するためのデータ分析手法としてベンフォードの法則を使用する計画をレビューする際に、検証すべき最も重要な事項は次のうちどれですか？
A. トランザクションは倍精度整数形式です。
B. 取引金額は制限なくランダムに選択されます。
C. トランザクション分析は、標準偏差内のトランザクションに限定されます。
D. 取引はすべて同じ通貨で行われています。
正解**: (**正解を表示します**)**
Benford ' s Law analyzes numerical data to detect anomalies based on the frequency distribution of leading digits. For it to be effective, the dataset must follow specific criteria, including consistency in measurement units. If transactions are in different currencies, the leading digits can vary due to currency conversion rates, invalidating the analysis.
Double Integer Format (Option A):Benford's Law applies to any set of numerical data, not specifically double integers.
Random Selection of Transactions (Option B):The data set must represent the entire population, not a random selection.
Limiting Analysis to Standard Deviations (Option C):This is irrelevant to the application of Benford ' s Law.
Reference:ISACA CISA Review Manual, Job Practice Area 2: Information Systems Audit and Assurance.

質問**: 73**
POS(販売時点情報管理)システムにおけるデビットカードまたはクレジットカードデータのスキミングを防止するための最適な対策は、次のうちどれですか？
A. 暗号化
B. ICチップとPINコード

C. ハッシュ化
D. 生体認証
正解: **B (**コメントを発表する**)**

質問: **74**
内部監査の品質保証(QA)および継続的改善プロセスをレビューする際に、以下のうちどれが最も大きな懸念事項となるでしょうか？
A. 改善の機会は一元的に追跡されていません。
B. 監査機能は、独立した定期的な外部レビューの対象ではありません。
C. 一部の監査の評価段階では、実証テストは実施されません。
D. 四半期報告書は監査委員会には配布されません。
正解: **B (**コメントを発表する**)**
The best answer is B.
A quality assurance and improvement program is meant to evaluate whether the audit function is performing effectively and independently. ISACA's candidate guide explicitly includes evaluating audit processes as part of QA and improvement programs, and ISACA peer-review guidance states that a peer review process assessing internal audit is essential to ensure it is appropriately carrying out its role. The absence of independent periodic external review is therefore the most serious concern because it weakens objective assessment of audit quality itself.
Option A is a weakness, but tracking improvement opportunities centrally is secondary to having independent validation that the function meets expected quality standards. Option C is not the best answer because substantive testing during an assessment phase may vary by engagement design. Option D matters for governance communication, but it is still less central to QA than the lack of external independent review.
References (Official ISACA):
ISACA, Certification Exam Candidate Guide.
ISACA Journal, A Standardized Approach for Peer Review of Internal Audit.

質問: **75**
外部監査において、情報システム監査担当者は、組織内でシステムの重要度分類に一貫性がないことに気づきました。システムの重要度を判断するための主たる要素として、次のうちどれを推奨すべきでしょうか？
A. リカバリポイント目標(RPO)
B. 最大許容ダウンタイム (MAD)
C. 平均復旧時間 (MTTR)
D. 主要業績評価指標(KPI)
正解: **(**正解を表示します**)**
The primary factor to determine system criticality is the maximum allowable downtime (MAD), which is the maximum period of time that a system can be unavailable before

causing significant damage or risk to the organization. TheMAD reflects the business impact and the recovery requirements of the system, and it can be used to prioritize the systems and allocate the resources for disaster recovery planning. The other options are not as important as the MAD, and they may vary depending on the system characteristics and the recovery strategy. The recovery point objective (RPO) is the maximum amount of data loss that is acceptable for a system. The mean time to restore (MTTR) is the average time required to restore a system after a failure. The key performance indicators (KPIs) are metrics that measure the performance and effectiveness of a system. References: CISA Review Manual (Digital Version) 1, page 468-469.

質問: **76**
優先度の高いアクティビティに十分なシステムリソースが確保されるようにするための最も効果的な方法は、次のうちどれですか？
A. システム仮想化
B. ジョブスケジューリング
C. ゼロトラスト
D. コード最適化
正解: **B (**コメントを発表する**)**
Job scheduling ensures that system resources are allocated efficiently by prioritizing high-priority tasks during peak periods. It prevents resource contention by scheduling less critical jobs at off-peak times or when resources are underutilized. This method is the most direct and effective way to ensure adequate resources for essential activities.
System Virtualization (Option A):While useful for optimizing resource utilization, it does not prioritize activities dynamically.
Zero Trust (Option C):This is a security framework and does not address resource allocation.
Code Optimization (Option D):This improves performance but is not directly related to resource scheduling.
Reference:ISACA CISA Review Manual, Job Practice Area 3: Information Systems Operations and Business Resilience.

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu ↥**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **77**
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
正解: **(**正解を表示します**)**
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

質問: **78**
ある組織が最近、VoIP(Voice-over IP)通信システムを導入しました。IS監査担当者が最も重視すべき事項は次のうちどれでしょうか？
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. 音声通信とデータ通信の統合不足
D. パケットの落下による音声品質の低下
正解: **(**正解を表示します**)**
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

質問: **79**
IS監査担当者がファイアウォールルールを評価する際に、最初に考慮すべき事項は次のうちどれですか？

A. 組織のセキュリティポリシー
B. リモートノードの数
C. ファイアウォールのデフォルト設定
D. ファイアウォールの物理的な位置
正解: **(**正解を表示します**)**
This should be the first thing that an IS auditor considers when evaluating firewall rules, because it defines the objectives, standards, and guidelines for securing the organization's network and information assets. The firewall rules should be aligned with the organization's security policy, and reflect the level of risk and protection required for each type of network traffic, system, or data. The IS auditor should compare the firewall rules with the security policy, and identify any discrepancies, gaps, or conflicts that could compromise the security or performance of the network.
The other options are not as important as the organization's security policy when evaluating firewall rules:
The number of remote nodes. This is a factor that may affect the complexity and scalability of the firewall rules, but it is not a primary consideration for the IS auditor. Remote nodes are devices or systems that connect to the network from outside locations, such as teleworkers, mobile users, or branch offices. The IS auditor should ensure that the firewall rules provide adequate security and access control for remote nodes, but this depends on the organization's security policy and business needs.
The firewalls' default settings. These are the predefined configurations that come with the firewall devices or software, and that determine how they handle network traffic by default. The IS auditor should review the firewalls' default settings, and verify that they are appropriate and secure for the organization's network environment. However, the firewalls' default settings may not match the organization's security policy or specific requirements, and may need to be customized or overridden by firewall rules.
The physical location of the firewalls. This is a factor that may affect the placement and design of the firewall rules, but it is not a critical consideration for the IS auditor. The physical location of the firewalls refers to where they are installed or deployed in relation to the network topology, such as at the network perimeter, between network segments, or on individual hosts. The IS auditor should ensure that the firewall rules are consistent and coordinated across different locations, but this depends on the organization's security policy and network architecture.

質問: **80**
クラウドサービスプロバイダーを利用して顧客データを処理している組織にとって、最も重要なプライバシーに関する考慮事項は次のうちどれですか？
A. データプライバシーは、組織に適用される規制に従って管理されなければなりません。
B. 顧客に通知することなく、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。

C. データプライバシーは、業界標準およびベストプラクティスに従って監視されなければなりません。
D. 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。
正解: **(**正解を表示します**)**

質問: **81**
ある組織では、自動化された継続的インテグレーション／継続的デプロイメント（CI/CD）ツールを使用して、本番環境への変更のデプロイを行っています。このような状況において、情報システム監査人が最も懸念する事項は次のどれでしょうか？
A. リリースは週に 1 回スケジュールされます。
B. 実装後のレビューは四半期ごとに実施されます。
C. テストケースが不正確である可能性があります。
D. 機能要件はユーザーによって頻繁に変更されます。
正解: **(**正解を表示します**)**
The greatest concern in a CI/CD environment is the accuracy of automated testing. Since code is deployed rapidly and often without manual intervention, weak or inaccurate test cases can allow vulnerabilities and defects to be pushed directly into production. Release frequency (A) and changing user requirements (D) are expected characteristics of agile/DevOps models and can be managed with governance. Delayed post-implementation reviews (B) may reduce oversight but do not directly undermine the core pipeline integrity.
ISACA's DevOps guidance emphasizes that automated testing and validation of requirements must be thorough and reliable to ensure continuous deployment does not compromise quality or security.
References (ISACA): COBIT Focus Area for DevOps; BAI06 Managed IT Changes.

質問: **82**
ファイルサーバーに必要なデータ保護レベルを判断するための最適な情報源は次のうちどれですか？
A. データ分類ポリシーと手順
B. 類似ファイルサーバーのアクセス権限
C. 過去のデータ侵害事件報告
D. 利用規定およびプライバシーに関する声明
正解: **(**正解を表示します**)**
The best source of information to determine the required level of data protection on a file server is the data classification policy and procedures, which define the criteria and methods for classifying data according to its sensitivity, value, and criticality, and specify the appropriate security measures and controls for each data category. Data classification policy and procedures help to ensure that data is protected in proportion to its importance

and risk exposure. Access rights of similar file servers, previous data breach incident reports,and acceptable use policy and privacy statements are not sufficient or reliable sources of information to determine the required level of data protection on a file server, as they do not provide clear and consistent guidance on how to classify and protectdata.
References: CISA Review Manual (Digital Version), Chapter 5: Protection of Information Assets, Section 5.1: Information Asset Security Framework

質問: **83**
IT ポートフォリオ管理の戦略を決定するのに最も役立つのは次のどれですか?
A. ライフサイクル費用便益分析
B. IT ロードマップ
C. IT メトリクス ダッシュボード
D. 能力成熟度モデル
正解: **(正解を表示します)**

質問: **84**
ユーザーから、新しくリリースされた企業資源計画(ERP)システムの動作が遅すぎるとの苦情が寄せられています。品質保証(QA)フェーズで実施された以下のテストのうち、どれがこの問題を特定できたでしょうか？
A. ストレス
B. 並列
C. 回帰
D. インターフェース
正解: **(正解を表示します)**
Astress testevaluates system performance under extreme conditions, such as high user loads, to determine how the system behaves under peak traffic or resource exhaustion.
Stress Testing (Correct Answer - A)
Identifies performance bottlenecks in software applications.
Helps ensure the ERP system can handle expected workloads.
Example:Simulating thousands of concurrent users accessing the ERP system to test response times and server load capacity.
Parallel Testing (Incorrect - B)
Compares a new system with an old one but does not test system performance under load.
Regression Testing (Incorrect - C)
Tests whether recent code changes have affected existing functionality but does not focus on performance.
Interface Testing (Incorrect - D)
Checks interactions between system components but does not measure performance.
References:
ISACA CISA Review Manual

COBIT 2019: Performance and Capacity Planning
NIST 800-37 (Risk Management Framework)

質問: **85**
外部の情報システム監査人が大手銀行の継続的モニタリングシステムをレビューし、いくつかの潜在的な問題点に気づきました。モニタリングシステムの信頼性に関して、最も懸念されるのはどれですか？
A. システムの結果は上級管理職によってレビューされません。
B. アラートしきい値は定期的に更新されます。
C. 監視しきい値は変更管理の対象ではありません。
D. 監視システムはサードパーティによって構成されました。
正解: **(正解を表示します)**
Monitoring systems rely heavily on thresholds to detect anomalies or incidents. If thresholds can be changed without proper change management controls, the entire system's reliability is compromised because unauthorized or improper changes could either suppress critical alerts or generate excessive false positives.
While senior management review (A) is important for governance, it does not directly affect the accuracy of monitoring results. Periodic threshold updates (B) are actually good practice as long as they are controlled.
Third-party configuration (D) can be acceptable if properly governed. ISACA's COBIT BAI06 (Managed IT Changes) stresses that all changes to production systems-including monitoring thresholds-must follow formal change control processes to maintain integrity and reliability.
References (ISACA): COBIT 2019, BAI06 Managed IT Changes.

質問: **86**
組織のプライバシープログラムの確立を支援する上で、内部監査が果たすべき適切な役割は次のうちどれでしょうか？
A. 新たな規制によって生じるリスクの分析
B. 個人データの利用状況を監視するための手順の開発
C. 組織内におけるプライバシー関連の役割の定義
D. 個人データを保護するための制御の設計
正解: **(正解を表示します)**
An appropriate role of internal audit in helping to establish an organization's privacy program is analyzing risks posed by new regulations. A privacy program is a set of policies, procedures, and controls that aim to protect the personal data of individuals from unauthorized or unlawful collection, use, disclosure, or disposal.
A privacy program should comply with the applicable laws and regulations that govern the privacy rights and obligations of individuals and organizations, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA). New

regulations may introduce new requirements or changes that affect the organization's privacy program and expose it to potential compliance risks or penalties. Therefore, internal audit can help to establish an organization's privacy program by analyzing the risks posed by new regulations and providingassurance, advice, or recommendations on how to address them1. The other options are less appropriate or incorrect because:
B). Developing procedures to monitor the use of personal data is not an appropriate role of internal audit in helping to establish an organization's privacy program, as it is more of a management or operational role.
Internal audit should not be involved in designing or implementing the organization's privacy program, as it would compromise its independence and objectivity. Internal audit should provide assurance on the effectiveness and efficiency of the organization's privacy program, but not create or execute it2.
C). Defining roles within the organization related to privacy is not an appropriate role of internal audit in helping to establish an organization's privacy program, as it is more of a governance or strategic role. Internal audit should not be involved in setting or approving the organization's privacy strategy, objectives, or policies, as it would compromise its independence and objectivity. Internal audit should provide assurance on the alignment and compliance ofthe organization's privacy program with its strategy, objectives, and policies, but not define or approve them2.
D). Designing controls to protect personal data is not an appropriate role of internal audit in helping to establish an organization's privacy program, as it is more of a management or operational role. Internal audit should not be involved in designing or implementing the organization's privacy program, as it would compromise its independence and objectivity. Internal audit should provide assurance on the adequacy and effectiveness of the organization's privacy program, but not design or implement it2. References: ISACA Introduces New Audit Programs for Business Continuity/Disaster ..., Best Practices for Privacy Audits - ISACA, ISACA Produces New Audit and Assurance Programs for Data Privacy and ...

質問**: 87**
バッチ処理監視の主な目的は次のどれですか?
A. バッチの失敗によって発生する可能性のあるインシデントを防ぐため
B. バッチ処理でエラーイベントをログに記録する
C. セキュリティ基準に準拠するため
D. バッチ処理レポートを要約する
正解**: (**正解を表示します**)**

質問**: 88**
IS監査担当者は、リソースの制約により、いくつかの重要なパッチが適時に適用されていないことを発見しました。この状況において、組織にとって最大のリスクは次のうちどれでしょうか？

A. システムによっては互換性がない場合があります。
B. システムがユーザーの要件を満たさない可能性があります。
C. システムはベンダーによるサポート対象外となる場合があります。
D. 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。
正解: **D** (コメントを発表する)

質問: **89**
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ていたところ、重要なサーバーへの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。アラートの内容を確認し、正確性を確保した後、次に取るべき行動は何ですか？
A. インシデント対応計画を実行します。
B. 影響を受けるシステムを隔離します。
C. 実施したすべての手順を文書レポートに記録してください。
D. 根本原因分析を実行します。
正解: (正解を表示します)

質問: **90**
IT関連フレームワークの導入を成功させる上で、最も効果的なのは次のうちどれでしょうか？
A. 枠組み活動を支援 ·監督するための委員会の設置
B. IT関連のポリシーと手順を文書化する
C. 枠組み内で適切なビジネス代表者を関与させる
D. 業界のベストプラクティスにフレームワークを合わせる
正解: (正解を表示します)

質問: **91**
従業員が携帯端末を紛失し、機密性の高い企業データが漏洩しました。次のうち、データ漏洩を最も効果的に防ぐ方法はどれでしょうか？
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発動
D. モバイルデバイスユーザー向け意識向上トレーニング
正解: (正解を表示します)
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

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu　**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **92**
ある組織がすべてのインフラストラクチャをクラウドに移行しました。災害発生時に組織が業務を継続できる能力に関して、情報システム監査担当者が最も懸念するのは次のうちどれでしょうか？
A. 移行後に災害復旧計画(DRP)のテストが実施されたという証拠はありません。
B. クラウドサービスプロバイダー上で冗長サービスが構成されているのは、業務上重要なサーバーのみです。
C. 以前のインフラは、災害発生時の事業運営をサポートするために維持されていませんでした。
D. 移行後、段階的な復旧プロセスが災害復旧計画 (DRP) で更新されませんでした。
正解: **(**正解を表示します**)**
After migrating infrastructure to the cloud, it ' s imperative to test the disaster recovery plan (DRP) to ensure its effectiveness in the new environment. Without evidence of DRP testing post-migration, the organization cannot be certain that it can recover and continue operations during a disaster. While updating the DRP and configuring redundancy are essential steps, their effectiveness can only be validated through rigorous testing. Retaining previous infrastructure is less relevant if the cloud environment is properly configured and tested for disaster recovery.
References:
ISACA CISA Review Manual, 28th Edition, Chapter 4: Information Systems Operations and Business Resilience.

質問: **93**
新しいIT運用パフォーマンス監視システムの導入を監査する際に、IS監査担当者が最も重視すべき事項は次のうちどれでしょうか？

A. ベースラインが確立されているかどうかを検証する
B. 運用強化の一環として多要素認証(MFA)が導入されているかどうかを確認します
C. メンテナンスマニュアルの年次レビュープロセスが存在するかどうかを判断する
D. すべての変更が実施されたかどうかを確認する
正解: **(**正解を表示します**)**

質問: **94**
組織のセキュリティポリシーに準拠してファイアウォールが構成されていることを示す、最も適切な監査証拠となるのは、次のうちどれですか？
A. 構成変更がどのように実行されるかを分析する
B. ログファイルを分析しています
C. ルールベースの確認
D. 侵入テストの実施
正解: **(**正解を表示します**)**
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 testingare useful audit techniques, but they do not provide direct evidence of the firewall configuration compliance. References: CISA Review Manual (Digital Version)1, page 383.

質問: **95**
アプリケーションプログラミングインターフェース(API)統合の実装に伴う盗聴リスクを軽減するために、IS監査担当者が最も推奨する対策は次のうちどれですか？
A. 拡張マークアップ言語 (XML) ファイルを暗号化します。
B. トランスポート層セキュリティ(TLS)を実装します。
C. シンプルオブジェクトアクセスプロトコル (SOAP) を実装します。
D. APIエンドポイントをマスクします。
正解: **(**正解を表示します**)**
The best recommendation to mitigate the risk of eavesdropping associated with an API integration implementation is to implement Transport Layer Security (TLS). TLS is a cryptographic protocol that provides secure communication over a network by encrypting the data in transit and authenticating the parties involved. TLS can prevent unauthorized parties from intercepting, modifying or tampering with the data exchanged between the API endpoints. Encrypting the XML file, implementing SOAP, and masking the API endpoints are not sufficient to mitigate the risk of eavesdropping, as they do not provide end-to-end encryption or authentication for the API communication. References: IS Auditand

Assurance Tools and Techniques, CISA Certification | Certified Information Systems Auditor | ISACA

質問: **96**
永続的に重要な電子情報が、長期にわたってアクセス可能な状態を維持することを最も確実に保証するのは、次のうちどれでしょうか？
A. 古いハードウェアの予防保守を実施する
B. 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を取得する
C. 定期的にデータを最新技術に移行する
D. アーカイブされたデータを定期的にバックアップする
正解: **C** (コメントを発表する)

質問: **97**
以下の制御のうち、データベース管理者(DBA)が実行するデータ抽出クエリが監視されることを保証するのに役立つものはどれですか？
A. データベースアクセスログの保存
B. 定期的なアクセスレビューの実施
C. DBAアクティビティへのアクセスを制限する
D. DBAの活動ログを確認する
正解: (正解を表示します)

質問: **98**
大規模アプリケーション開発プロジェクトにおける統制の評価において、IS監査担当者の時間を最も効果的に活用する方法は、以下の項目をレビューおよび評価することである。
A. アプリケーションのテストケース。
B. 受け入れテスト。
C. 費用便益分析。
D. プロジェクト計画。
正解: **A** (コメントを発表する)
Reviewing and evaluating application test cases is the most effective use of an IS auditor's time during the evaluation of controls over a major application development project. Application test cases are designed to verify that the application meets the functional and non-functional requirements and specifications. They also help to identify and correct any errors, defects, or vulnerabilities in the application before it is deployed. By reviewing and evaluating the test cases, the IS auditor can assess the quality, reliability, security, and performance of the application and provide recommendations for improvement.

質問: **99**
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準備する際、IS監査担当者にとって最適なアプローチは次のうちどれですか？

A. 投資収益率(ROI)のために戦略的プロジェクトをレビューする
B. 組織の成熟度を測るために、他の部署からフィードバックを募る
C. 経営幹部と面談し、事業目標を理解する
D. 組織の主要業績評価指標(KPI)を確認する
正解**: (**正解を表示します**)**
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"

質問**: 100**
重要なITプロジェクトの導入後レビューを実施する際、IS監査担当者が最も重点的に取り組むべき事項は次のうちどれでしょうか？
A. プロジェクト運営委員会に企業代表が含まれていることを確認してください。
B. プロジェクトの目標が期待どおりに達成されたかどうかを判断する。
C. プロジェクトが予定通りかつ予算内で完了したかどうかを判断する。
D. 主要関係者がプロジェクト完了を承認したことを確認する。
正解**: (**正解を表示します**)**
The correct answer is B. Determine if project goals were met as expected.
The primary purpose of a post-implementation review is to determine whether the project achieved its intended objectives, delivered the expected business value, met requirements, and produced the expected benefits. For a critical IT project, the most important audit focus is not only whether the project was delivered on time or within budget, but whether it actually achieved what the organization expected from it.
ISACA's CISA Exam Content Outline specifically includes Post-implementation Review under Domain 3 and states that CISA tasks include conducting post-implementation reviews to determine whether project deliverables, controls, and requirements are met.
Option A is useful but not the primary focus. Business representation on the steering committee supports good governance, but it does not prove that the project achieved its objectives.
Option C is also important, but on-time and on-budget delivery does not necessarily mean project success. A project can be delivered on time and within budget but still fail to meet business requirements.
Option D is evidence of formal project closure, but stakeholder signoff alone does not provide enough assurance that the project goals and expected benefits were achieved.

ISACA also notes that benefit realization is measured after implementation and that a post-implementation review is usually recommended to quantify actual benefits from a program. References: ISACA CISA Exam Content Outline, Domain 3; ISACA guidance on post-implementation review and benefit realization.

質問: **101**
新しいウェブサーバーをサポートするためのハードウェアを調達する組織の実現可能性調査において、以下のうちどれを省略することが最も懸念されるでしょうか？
A. 買収資金調達の代替案
B. 潜在的なベンダーの財務安定性
C. 潜在的なベンダーの評判
D. 入手可能な製品の費用対効果分析
正解: **(**正解を表示します**)**
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

質問: **102**
国際機関がグローバルなデータプライバシーポリシーを展開しようとする場合、IS監査担当者が最も懸念すべき事項は次のうちどれでしょうか？
A. 要求が不合理になる可能性がある。
B. このポリシーは、既存のアプリケーション要件と矛盾する可能性があります。
C. 地域の規制は、この方針と矛盾する可能性があります。
D. 現地の経営陣は、この方針を受け入れない可能性があります。
正解: **(**正解を表示します**)**
The greatest concern for an IS auditor when an international organization intends to roll out a global data privacy policy is that local regulations may contradict the policy. Data privacy regulations vary across different countries and regions, and they may impose different or conflicting requirements on how personal data can be collected, processed, stored, transferred, and disclosed. The organization should ensure that its global data privacy policy complies with the applicable local regulations in each jurisdiction where it operates, or risk facing legal sanctions or reputational damage. Requirements may become unreasonable, but this is not a major concern for an IS auditor, as it is a business decision that should be based on a cost-benefit analysis. The policy may conflict with existing application requirements, but this is not a serious concern for an IS auditor, as it can be resolved by modifying or updating the applications to align with the policy. Local

management may not accept the policy, but this is not a critical concern for an IS auditor, as it can be mitigated by providing adequate training and awareness on the policy and its benefits. References:
CISA Review Manual, 27th Edition, pages 406-4071
CISA Review Questions, Answers and ExplanationsDatabase, Question ID: 2592

質問: **103**
新しいアプリケーションシステムの導入中にデータ変換と移行をレビューする監査担当者にとって、次のうちどれが最も懸念すべき事項でしょうか？
A. 変更管理プロセスが正式に文書化されていませんでした
B. 旧システムおよびデータのバックアップはオンラインでは利用できません
C. 変換中に不正なデータ変更が発生しました。
D. データ変換は手動プロセスを使用して実行されました
正解: **C (**コメントを発表する**)**
The finding that should be of greatest concern to an IS auditor reviewing data conversion and migration during the implementation of a new application system is that unauthorized data modificationsoccurred during conversion. Data conversion and migration is a process that involves transferring data from one system to another, ensuring its accuracy, completeness, integrity, and usability. Unauthorized data modifications during conversion can result in data loss, corruption, inconsistency, or duplication, which can affect the functionality, performance, reliability, and security of the new system. Unauthorized data modifications can also have serious business implications, such as affecting decision making, reporting, compliance, customer service, and revenue. The IS auditor should verify that adequate controls are in place to prevent, detect, and correct unauthorized data modifications during conversion, such as access control, data validation, reconciliation, audit trail, and backup and recovery. The other findings (A, B and D) are less concerning, as they can be mitigated by documenting the change management process, restoring the backups of the old system and data from offline storage, or automating the data conversion process. References: CISA Review Manual (Digital Version), Chapter 3: Information Systems Acquisition, Development and Implementation, Section 3.4:
System Implementation

質問: **104**
従業員の立ち入り制限区域へのアクセスを制限するためにスワイプカードを使用する場合、どのような追加的な制御を導入する必要がありますか？
A. 制限区域へのアクセスには、全従業員の物理的なサインインが必要です。
B. 追加のPINパッドの実装
C. 管理部門によるアクセスプロファイルの定期的な見直し
D. 閉回路テレビ(CCTV)の設置
正解: **(**正解を表示します**)**

Periodic review of access profiles by management is an additional control that is required when using swipe cards to limit employee access to restricted areas. Swipe cards are a type of physical access control that use magnetic stripes or radio frequency identification (RFID) to store and transmit information about the cardholder's identity and access rights. Swipe cards can help to prevent unauthorized entry, protect sensitive assets and data, and monitor access activity. However, swipe cards alone are not enough to ensure effective access control. They need to be complemented by other controls, such as:
Periodic review of access profiles by management: This is a type of logical access control that involves verifying that the access rights assigned to each cardholder are appropriate, necessary, and consistent with the organization's policies and procedures. Periodic review of access profiles can help to detect and correct any errors, inconsistencies, or violations in the access control system, such as outdated, excessive, or redundant access rights, segregation of duties conflicts, or unauthorized changes. Periodic review of access profiles can also help to ensure compliance with internal and external audit requirements and regulations.
Implementation of additional PIN pads: This is a type of multi-factor authentication (MFA) that requires the cardholder to enter a personal identification number (PIN) in addition to swiping their card. MFA can enhance the security of the access control system by adding another layer of verificationand reducing the risk of lost, stolen, or cloned cards being used by unauthorized persons.
Installation of closed-circuit television (CCTV): This is a type of surveillance system that uses cameras and monitors to record and display the images of the people and activities in the restricted areas. CCTV can deter potential intruders, provide evidence of any security incidents or breaches, and enable real-time monitoring and response by security personnel.
The other options are not as effective or relevant as periodic review of access profiles by management for an additional control when using swipe cards. Physical sign-in of all employees for access to restricted areas is a redundant and inefficient control that can be easily bypassed or manipulated. It also does not provide any assurance or verification of the identity or access rights of the cardholders. 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. 236
ISACA, ITAF: A Professional Practices Framework for IS Audit/Assurance, 3rd Edition, 2014, p. 88 Data Analytics for Auditing Access Control

質問**: 105**
重要なITインフラストラクチャに対する脆弱性スキャンを実施する際に、最も重要な考慮事項は次のうちどれですか？

A. スキャンはピーク時以外の時間帯に行われます。
B. スキャンに続いて侵入テストが行われます。
C. スキャンは費用対効果が高いでしょう。
D. スキャンによってシステムのパフォーマンスが低下することはありません。
正解: **(**正解を表示します**)**
The scanning will not degrade system performance. This is the most important consideration when establishing vulnerability scanning on critical IT infrastructure, because any degradation of system performance could affect the availability, reliability, and functionality of the IT services that depend on the infrastructure. Scanning during non-peak hours (A) could reduce the impact of scanning on system performance, but it does not guarantee that the scanning will not cause any degradation. Scanning followed by penetration testing (B) could provide more in-depth information about the vulnerabilities and their exploitability, but it does not address the potential impact of scanning on system performance. Scanning cost- effectiveness is a relevant factor for choosing a scanning service or tool, but it is not as important as ensuring that the scanning will not compromise the system performance.
Reference: CISA Vulnerability Scanning, Description.

質問: **106**
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) を介して通信します。
B. 許可されたユーザーによる不正なアクティビティをブロックします。
C. 外部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。
正解: **(**正解を表示します**)**
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

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジン

を手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu 1605問、３０%ディスカウント、特別な割引コード: JPNshiken」

質問: **107**
データ保持ポリシーを導入する最も適切な理由は次のうちどれですか？
A. 災害復旧手順の復旧目標時点(RPO)を設定する
B. 情報の保管および保護に関連する責任を制限するため
C. 組織内でのデータ処理に関する業務目標を文書化する
D. データ保護に関する責任と所有権をIT部門外に割り当てる
正解: **B** (コメントを発表する)
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 and More

質問: **108**
IS監査人が職務分掌が実施されていることを検証する最良の方法は、以下の手順を実行することです。
A. 人事ファイルの確認。
B. 文書化された職務記述書の分析。
C. 組織図のレビュー。
D. 職務内容の説明。
正解: (正解を表示します)

Awalk-through of job functionsprovides direct evidence thatseparation of duties (SoD)is implemented effectively. It involves observing employees as they perform tasks to confirm that no single person has excessive privileges.
Walk-through of Job Functions (Correct Answer - D)
Confirms that duties are appropriately divided in real-world operations.
Helps verify whether security policies and controls are enforced.
Example:An auditor observes that the same person cannot create and approve financial transactions.
Review of Personnel Files (Incorrect - A)
Personnel files contain job details but do not confirm how duties are performed.
Analysis of Documented Job Descriptions (Incorrect - B)
Job descriptions may be outdated or inaccurate.
Review of Organizational Chart (Incorrect - C)
Shows reporting relationships but does not confirm SoD implementation.
References:
ISACA CISA Review Manual
COBIT 2019: Risk Management and Governance
ISO 27001: Segregation of Duties Control

質問**: 109**
以下のうち、IT戦略が組織の目標や目的に合致していることを最もよく示しているのはどれですか？
A. IT戦略はすべてのビジネス関係者に伝達されます
B. 組織戦略は最高情報責任者(CIO)に伝えられます。
C. ビジネス関係者がIT戦略の承認に関与します。
D. 最高情報責任者(CIO)は組織戦略の承認に関与している。
正解**: C (**コメントを発表する**)**
Business stakeholders being involved in approving the IT strategy best demonstrates that IT strategy is aligned with organizational goals and objectives. IT strategy is a plan that defines how IT resources and capabilities will support and enable the achievement of business goals and objectives. Business stakeholders are the individuals or groups who have an interest or influence in the organization's activities and outcomes.
By involving business stakeholders in approving the IT strategy, the organization can ensure that the IT strategy reflects and supports the business needs, expectations, and priorities. The other options do not necessarily indicate that IT strategy is aligned with organizational goals and objectives, as they do not involve the participation or feedback of business stakeholders. References: CISAReview Manual, 27th Edition, page
97

質問**: 110**

業務に必要なメールが、従業員の個人端末に保存されている。
IS監査担当者にとって、次のうちどれが最も適切な推奨事項でしょうか？
A. 従業員に個人端末でのパスワードの使用を義務付ける
B. 従業員が会社のメールを個人端末に保存することを禁止する
C. 個人用デバイスにウイルス対策ソフトがインストールされていることを確認してください。
D. 個人用デバイスにメールコンテナ化ソリューションを実装する
正解: **(**正解を表示します**)**
Implementing an email containerization solution on personal devices is the best recommendation for an IS auditor, because it allows the organization to separate and secure the email data from the rest of the device data. Email containerization creates a virtual environment that encrypts andisolates the email data, preventing unauthorized access, leakage, or loss of sensitive information12. Requiring passwords or antivirus protection on personal devices may not be sufficient or enforceable, while prohibiting employees from storing companyemail onpersonal devices may not be feasible or practical. References: 1: CISA Review Manual (DigitalVersion), Chapter 5, Section 5.4.3 2: CISA Online Review Course, Module 5, Lesson 4

質問: **111**
以下の技術のうち、広範囲にわたるネットワーク攻撃のリスクを最も効果的に軽減できるのはどれですか？
A. 構成評価
B. セグメンテーション
C. 非武装地帯(DMZ)
D. 暗号化
正解: **B (**コメントを発表する**)**

質問: **112**
プログラムの変更が実装された際にソースコードが再コンパイルされない場合、ソースコードとオブジェクトの同期を確保するための補償制御として適切なのは次のうちどれですか？
A. オブジェクトコードと実行可能コードの比較
B. コンパイル日の監査証跡のレビュー
C. ソースコードとオブジェクトコードの日付スタンプの比較
D. 実行可能コード内の開発者コメントのレビュー
正解: **(**正解を表示します**)**
Source code synchronization is the process of ensuring that the source code and the object code (the compiled version of the source code) are consistent and up-to-date1. When program changes are implemented, the source code should be recompiled to generate a new object code that reflects the changes. However, if the source code is not

recompiled, there is a risk that the object code may be outdated or incorrect. A compensating control is a measure that reduces the risk of an existing control weakness or deficiency2. A compensating control for source code synchronization is to compare the date stamping of the source and object code. Date stamping is a method of recording the date and time when a file is created or modified3. By comparing the date stamping of the source and object code, one can verify if they are synchronized or not. If the date stamping of the source code is newer than the object code, it means that the source code has been changed but not recompiled. If the date stamping of the object code is newer than the source code, it means that the object code has been compiled from a different source code. If the date stamping of both files are identical, it means that they are synchronized.

質問: **113**
アプリケーションやITシステムによって支えられている組織のビジネスプロセスを評価する際に、IS監査担当者が最も役立つのは、次のうちどれですか？
A. 構成管理データベース(CMDB)
B. エンタープライズアーキテクチャ(EA)
C. ITポートフォリオ管理
D. ITサービス管理
正解: **(正解を表示します)**
The most helpful thing for an IS auditor to review when evaluating an organization's business processes that are supported by applications and IT systems is the enterprise architecture (EA). EA is the practice of designing a business with a holistic view, considering all of its parts and how they interact. EA defines the overall goals, the strategies that support those goals, and the tactics that are needed to execute those strategies.
EA also outlines the ways various components of IT projects interact with one another and with the business processes. By reviewing the EA, an IS auditor can gain a comprehensive understanding of how the organization aligns its IT efforts with its overall mission, business strategy, and priorities. An IS auditor can also assess the effectiveness, efficiency, agility, and continuity of complex business operations.
The other options are not as helpful as option B. A configuration management database (CMDB) is a database that stores and manages information about the components that make up an IT system. A CMDB tracks individual configuration items (CIs), such as hardware, software, or data assets, and their attributes, dependencies, and changes over time. A CMDB can help an IS auditor to monitor the performance, availability, and configuration of IT assets, but it does not provide a holistic view of how they support the business processes. IT portfolio management is the practice of managing IT investments, projects, and activities as a portfolio. IT portfolio management aims to optimize the value, risk, and cost of IT initiatives and align them with the business objectives. IT portfolio management can help an IS auditor to evaluate the return on IT investments and the alignment of IT projects with the business strategy, but it does not provide a detailed view

of how they support the business processes. IT service management (ITSM) is the practice of planning, implementing, managing, and optimizing IT services to meet the needs of end users and customers.
ITSM focuses on delivering IT as a service using standardized processes and best practices. ITSM can help an IS auditor to review the quality, efficiency, and effectiveness of IT service delivery and support, but it does not provide a comprehensive view of how they support the business processes. References: What is enterprise architecture (EA)? - RingCentral, What is a configuration management database (CMDB)? - Red Hat, IT Portfolio Management Strategies | Smartsheet, What is IT service management (ITSM)? | IBM

質問: **114**
ベンダーがサポートするソフトウェアが常に最新の状態に保たれていることを最も確実に保証するのは、次のうちどれですか？
A. ソフトウェア資産管理
B. リリースおよびパッチ管理
C. ライセンス契約およびエスクロー
D. バージョン管理
正解: **B** (コメントを発表する)

質問: **115**
アプリケーションデータベースからデータウェアハウスへデータが転送されています。抽出プロセスで一部のフィールドが取得されなかったため、データウェアハウスに転送されませんでした。この状況に関連する最大のリスクは次のうちどれですか？
A. アプリケーション内でトランザクションエラーが発生する可能性があります。
B. 経営陣への報告が遅れる可能性があります。
C. 倉庫に転送されたデータは正確ではない可能性があります。
D. 経営判断は不完全なデータに基づいている可能性があります。
正解: **D** (コメントを発表する)

質問: **116**
IS監査担当者が、製造工場における産業用IoT(IoT)インフラストラクチャの実装に関連する統制のレビューを準備しています。次のうち、組織にとって最大のセキュリティリスクとなる脆弱性はどれでしょうか？
A. 盗難防止のため、Lo I デバイス周辺の物理的なセキュリティ対策が不十分です。
B. IoTデバイス内でのオープンソースソフトウェアコンポーネントの使用
C. コードアップグレードのためのIoTデバイスファームウェアストレージ容量の制約
D. 無線ネットワーク接続を使用していないIoTデバイス
正解: (正解を表示します)

The use of open-source software components in IoT devices presents the greatest security risk due to potential vulnerabilities that may exist within the software. These vulnerabilities can be exploited if patches are not applied promptly, and the organization might not have direct control over the software ' s maintenance and security updates. This risk is amplified in critical manufacturing environments where compromised IoT devices can lead to operational disruptions.
Physical Security (Option A):While important, theft of IoT devices generally poses less risk compared to a system-wide compromise due to software vulnerabilities.
Firmware Storage Constraints (Option C):While a limitation, this is a secondary concern compared to exploitable software.
Devices Not Using Wireless Connectivity (Option D):Wired devices are generally more secure, reducing this as a significant concern.
Reference:ISACA CISA Review Manual, Job Practice Area 4: Protection of Information Assets.

質問**: 117**
セキュリティインシデント発生後に実施された事後レビューの結果をIS監査人が検証する最も重要な理由は次のうちどれですか？
A. 継続的改善活動の有効性を評価する
B. インシデント対応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、事件を再分析する。
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
正解**: (**正解を表示します**)**
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.

質問**: 118**
プライバシー通知の主な目的は次のうちどれですか？
A. 個人情報の不正使用に関するユーザーからの訴訟から組織を保護するため
B. 個人情報の利用と保護に関する組織の責任を確立するため
C. 個人情報を第三者機関に販売するための承認を得るため
D. 組織のプライバシー管理がユーザーの地域のプライバシー法に準拠していることを確認するため

正解: (正解を表示します)
The best answer is B. To establish the organization's accountability for the use and protection of personal information.
ISACA privacy guidance emphasizes accountability as a core privacy principle and describes privacy notices as documents that explain how personal information is collected, used, shared, retained, and protected. A privacy notice is fundamentally about transparency and accountability to data subjects regarding the organization's handling of personal information.
Option A is incorrect because a privacy notice is not primarily a liability shield. Option C is incorrect because a privacy notice may disclose sharing practices, but it is not primarily to obtain blanket approval for sale of personal information. Option D is also incorrect because compliance of controls is a broader privacy governance objective; the notice itself is mainly for transparent disclosure and accountability.
References (Official ISACA):
ISACA, Privacy Notice.
ISACA Privacy Resource Center.
ISACA Journal, Creating a Compliant and Accountable Data Culture.
ISACA, Using ISACA Privacy Principles for GDPR Compliance.

質問: **119**
組織がセキュリティ情報およびイベント管理(SIEM)システムを導入する際に、どのような種類の制御が確立されていると言えるでしょうか？
A. 予防的
B. 探偵
C. 指令
D. 修正
正解: (正解を表示します)

質問: **120**
データ分類プログラムを実装する際に、以下のうち最も重要なものはどれですか？
A. データ分類レベルの理解
B. データ所有権の形式化
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
正解: (正解を表示します)
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 Howto Implement It

質問**: 121**
IS監査担当者が組織のプライバシーポリシーをレビューする際に、最も重要な検討事項は次のうちどれですか？
A. 規制当局から個人データを収集する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. 組織が個人データを保護するために選択した暗号化メカニズム
正解**: (**正解を表示します**)**
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

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu 「**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **122**
ビジネスアプリケーションのアウトソーシングを検討している組織は、まず最初に以下の点を確認する必要があります。
A. サービスレベル要件を定義します。
B. 脆弱性評価を実行します。
C. 費用対効果分析を実施する。
D. 提案依頼書 (RFP) を発行する。
正解: **(正解を表示します)**
An organization considering the outsourcing of a business application should first conduct a cost-benefit analysis to evaluate the feasibility, viability and desirability of the outsourcing decision. A cost-benefit analysis should compare the costs and benefits of outsourcing versus keeping the application in-house, taking into account factors such as financial, operational, strategic, legal, regulatory, security and quality aspects. A cost-benefit analysis should also identify the risks and opportunities associated with outsourcing, and provide a basis for defining the service level requirements, performing a vulnerability assessment, and issuing a request for proposal (RFP) in the subsequent stages of the outsourcing process. References: Info Technology and Systems Resources | COBIT, Risk, Governance ... - ISACA, CISACertification | Certified Information Systems Auditor | ISACA

質問: **123**
ある通信会社が最近、従業員3名からなる新たな不正対策部門を設立し、人工知能(AI)モジュールを使用した不正検出システムを導入しました。このシステムを監査する情報システム監査担当者にとって、以下のうちどれが最も懸念されるでしょうか？
A. 非常に多くの真の陰性例
B. 偽陰性の数がごくわずか
C. 真陽性の数が少数
D. 多数の偽陽性
正解: **(正解を表示します)**

質問: **124**

ITインターフェース制御のレビューの結果、組織には受信システムに転送されないレコードを特定して修正するプロセスがないことが判明しました。IS監査担当者の最も適切な推奨事項は次のうちどれですか？
A. システム間のデータの自動照合を実行するソフトウェアを実装します。
B. データファイルの自動暗号化、復号化、および電子署名を有効にします。
C. コーダーにシステム間のデータの手動照合を行わせる。D
D. システム間のデータ転送を可能な限り自動化する。
正解: **(**正解を表示します**)**

質問: **125**
以下の制御のうち、システム構成を通じて実装するのが最も適切なものはどれですか？
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のアクセス権限は、適切性を確認するため180日ごとに見直されます。
C. 主要レポートの財務データは、完全性と正確性を確保するためにソースシステムまで遡って追跡されます。
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。
正解: **(**正解を表示します**)**
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 ofunauthorized or malicious use of their accounts12.
References1: Configuration and Change Management - CISA2: What is IT Governance? - Definition from Techopedia

質問: **126**
セキュリティ指標ダッシュボードを導入することで解決できる経営上の懸念事項は、次のうちどれですか？
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の比較
C. セキュリティに割り当てられた総時間数
D. 偽陽性の総数
正解: **(**正解を表示します**)**
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

質問**: 127**
インターネット経由でデータを転送する際には、以下のどのプロトコルを使用すべきでしょうか？
A. ユーザーデータグラムプロトコル (UDP)
B. ハイパーテキスト転送プロトコル (HTTP)
C. セキュアファイル転送プロトコル (SFTP)
D. リモートデスクトッププロトコル (RDP)
正解**: (**正解を表示します**)**
SFTP (Secure File Transfer Protocol)is the most secure option for transferring data over the internet, as it encrypts both commands and data, ensuring confidentiality and integrity.
SFTP (Correct Answer - C)
Uses SSH (Secure Shell) for encryption.
Provides authentication and encryption for secure data transfers.
Example:A company uses SFTP to securely transmit payroll files to a third-party processor.
UDP (Incorrect - A)
Faster but lacks encryption and data integrity checks.
HTTP (Incorrect - B)
Transfers data in plaintext and is vulnerable to interception.
RDP (Incorrect - D)
Used for remote desktop access, not secure file transfers.
References:
ISACA CISA Review Manual
NIST 800-52 (Guidelines for Transport Layer Security)

質問**: 128**
IS監査担当者は、事業主が本番データにアクセスできるWebページを作成することで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。監査担当者の次のステップは次のとおりであるべきです。
A. 上級管理職にエスカレーションする。
B. ウェブページを閉じます。

C. 十分なアクセス制御が存在するかどうかを判断します。
D. 生産データの感度を評価する。
正解: **(**正解を表示します**)**

質問: **129**
ある組織は、ITポリシーの策定において、ボトムアップ型アプローチからトップダウン型アプローチへと移行しました。これにより、以下の結果が期待されます。
A. 組織全体でより高い一貫性。
B. 既存の運用方針の統合。
C. より包括的なリスク評価計画。
D. ベストプラクティスへのより高い遵守。
正解: **A (**コメントを発表する**)**
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 orconflict among different policies. References: ISACA Frameworks: Blueprints for Success, IT Governance and Process Maturity

質問: **130**
ITリソースへ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. 出来高分析(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
正解: **A (**コメントを発表する**)**
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 performanceand 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 and Management (EVA/EVM) - Definition and Formulae1 Return on Investment (ROI) Formula2 What Is a Gantt Chart?3 Critical Path Method for Project Management

質問**: 131**
データ仮想化が利用されている環境において、以下のうちどれが最適な災害復旧ソリューションとなるでしょうか？
A. オンサイトのディスクベースバックアップシステム
B. テープベースのバックアップシステム
C. 仮想テープライブラリ
D. 独立ディスク冗長アレイ (RAID)
正解**: (**正解を表示します**)**
A virtual tape library (VTL) is a disk-based backup system that emulates a tape library. It provides faster backup and recovery than traditional tape systems, and it can be integrated with data deduplication and replication technologies to enhance disaster recovery. A VTL can also be replicated to an offsite location for additional protection. A VTL is the best disaster recovery solution for an environment where data virtualization is used, because it can handle large volumes of data, support multiple backup applications, and provide consistent performance.
Onsite disk-based backup systems (A) are not the best disaster recovery solution, because they are vulnerable to the same risks as the primary data center, such as fire, flood, power outage, or sabotage. Tape-based backup systems (B) are not the best disaster recovery

solution, because they are slow, prone to errors, and require manual intervention.
Redundant array of independent disks (RAID) (D) is not a backup system, but a storage technology that improves performance and fault tolerance by distributing data across multiple disks. RAID does not protect against data corruption, human error, or malicious attacks.
References:
Virtualization Disaster Recovery Overview: Definitions and Guides
Disaster Recovery Virtualization - VMware
What is Virtual Disaster Recovery? - Definition from Techopedia
How Does Virtualization Help With A Disaster Recovery Plan

質問**: 132**
組織が正式な情報セキュリティ監査を実施する主な理由は次のうちどれですか？
A. 情報セキュリティ戦略をビジネス目標に整合させる。
B. 重要な情報セキュリティ上の脆弱性を特定する。
C. 情報セキュリティソフトウェアのライセンス費用を削減するため。
D. 情報セキュリティチームの生産性を監視する。
正解**: (**正解を表示します**)**
The correct answer is B. To identify material information security vulnerabilities.
The primary purpose of a formal information security audit is to independently evaluate whether security controls are adequate and effective, and to identify material vulnerabilities, weaknesses, or risks that could affect the confidentiality, integrity, and availability of information assets. ISACA states that audit objectives often center on substantiating the existence of internal controls to minimize business risk, and ISACA's cybersecurity audit guidance describes reviewing gathered data to identify potential security vulnerabilities or risk and documenting findings and recommendations.
Option A is important, but it is more directly related to information security governance and strategy than the primary purpose of a formal audit. Option C is not correct because reducing software licensing cost is a cost- management activity, not the main objective of an information security audit. Option D is also incorrect because monitoring security team productivity is a management function, not the primary purpose of an independent audit.
This question maps mainly to Information Systems Auditing Process because it concerns why an audit is conducted: to provide independent assurance, identify material issues, and support risk-based recommendations.
References: ISACA CISA Exam Content Outline, Domain 1; ISACA Interactive Glossary, "Audit objective,"
"Audit evidence," and "Auditor's opinion"; ISACA article, Six Benefits of a Cybersecurity Audit.

質問**: 133**

新しいIT導入がエンタープライズアーキテクチャ(EA)の原則と要件に合致するようにするための最良の方法は、次のうちどれですか？
A. EAの一部としてセキュリティビューを文書化する
B. EAを定義する際には、利害関係者の懸念事項を考慮する
C. IT導入後の必須レビューを実施する
D. 変更諮問委員会の一環としてEAレビューを実施する
正解: **D** (コメントを発表する)
The best way to help ensure new IT implementations align with enterprise architecture (EA) principles and requirements is to conduct EA reviews as part of the change advisory board (CAB). A CAB is a committee that evaluates and authorizes changes to IT services, such as new IT implementations. By conducting EA reviews as part of the CAB process, the organization can ensure that the proposed changes are consistent with the EA vision, goals, standards, and guidelines. This can help avoid potential conflicts, risks, or inefficiencies that may arise from misaligned IT implementations. Additionally, EA reviews can help identify opportunities for improvement, optimization, or innovation in the IT services.
The other options are not the best ways to help ensure new IT implementations align with EA principles and requirements. Documenting the security view as part of the EA is important, but it does not guarantee that new IT implementations will follow the security requirements or best practices. Considering stakeholder concerns when defining the EA is also essential, but it does not ensure that new IT implementations will meet the stakeholder expectations or needs. Performing mandatory post-implementation reviews of IT implementations is a good practice, but it does not prevent potential issues or problems that may arise from misaligned IT implementations.
References:
5: Change Advisory Board Best Practices: 15+ Industry Leaders Weigh In
6: What Does the Change Advisory Board (CAB) Do?
7: How do I set up an effective change advisory board? - ServiceNow
8: ITIL Change Management - The Role of the Change Advisory Board

質問: **134**
ある小規模組織は、IT部門の人員を削減し、多数の重要な責任を最上級ITエンジニアの役割に統合することでコスト削減を図りました。この状況における主要なリスクは次のうちどれでしょうか？
A. 役割の統合は、リソースの最適化不足につながります。
B. 役割の統合により、権限が限定される。
C. 責任が統合されているため、適切な職務分担ができません。
D. 責任の統合は後継者育成計画を弱体化させる。
正解: (正解を表示します)

The correct answer is C. The consolidated responsibilities do not allow for appropriate separation of duties.
The primary risk is that too many critical responsibilities are concentrated in one individual. This creates a segregation/separation of duties issue, because one person may be able to initiate, approve, implement, and monitor critical IT activities without independent review. In IT, this could allow unauthorized changes, inappropriate access, fraud, errors, or malicious actions to occur without timely detection.
ISACA defines segregation/separation of duties as a basic internal control that prevents or detects errors and irregularities by assigning incompatible responsibilities to different individuals. ISACA also notes that SoD helps ensure no single person is in a position to introduce fraudulent or malicious code without detection.
Option A is not the best answer because resource optimization may be affected, but the major control risk is excessive authority and incompatible duties. Option B is incorrect because the issue is not limited authority; the concern is too much combined authority. Option D is a valid secondary concern because succession planning may be weakened when knowledge is concentrated in one person, but CISA questions usually prioritize the control risk of inadequate separation of duties over staffing continuity concerns.
This maps mainly to Governance and Management of IT because the issue relates to organizational structure, IT governance, resource management, roles, responsibilities, and control ownership. ISACA's CISA Exam Content Outline includes organizational structure, IT governance, IT resource management, and determining whether ownership of IT risk, controls, and standards has been defined.
References: ISACA CISA Exam Content Outline, Domain 2; ISACA Interactive Glossary, "Segregation
/separation of duties."

質問**: 135**
プログラムの変更によって発生した新たなエラーを特定する最も効果的な方法は、次のうちどれですか？
A. 単体テスト。
B. インターフェーステスト。
C. 統合テスト。
D. 回帰テスト。
正解**: (**正解を表示します**)**
The correct answer is D. Regression testing.
Regression testing is specifically designed to determine whether program changes have unintentionally introduced new errors or caused previously working functions to fail. After a system change, regression testing retests affected and related functions to confirm that the modified application still works as expected.

ISACA's glossary defines regression analysis and testing as a software verification and validation task used to determine the extent of analysis and testing that must be repeated when changes are made to previously examined software products. It also defines regression testing as a technique used to retest earlier program abends or logical errors that occurred during the initial testing phase.
Option A is not the best answer because unit testing verifies individual program modules or components. It is useful, but it does not provide the same assurance that a change has not affected existing functionality elsewhere. Option B is not the best answer because interface testing focuses on data exchange and communication between systems or components. Option C is not the best answer because integration testing verifies that components work together, but regression testing is the specific method for detecting unintended effects of changes.
This question maps to Information Systems Acquisition, Development and Implementation because ISACA's CISA Exam Content Outline includes system development methodologies, system readiness, implementation testing, and controls throughout the system development life cycle.
References: ISACA CISA Exam Content Outline, Domain 3; ISACA Interactive Glossary, "Regression analysis and testing" and "Regression testing."

質問**: 136**
リスク評価プロセスにおいて、最初に特定すべき事項は次のうちどれですか？
A. 脅威に対する脆弱性
B. 既存のコントロール
C. 情報資産
D. 法的要件
正解**: C (**コメントを発表する**)**
The risk assessment process involves identifying the information assets that are at risk, analyzing the threats and vulnerabilities that could affect them, evaluating the impact and likelihood of a risk event, and determining the appropriate controls to mitigate the risk. The first step is to identify the information assets, as they are the objects of protection and the basis for the rest of the process. Without knowing what assets are at risk, it is not possible to assess their value, exposure, or protection level. References: ISACA Frameworks: Blueprints for Success

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジン

を手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu 1605問、３０%ディスカウント、特別な割引コード: JPNshiken」

質問: **137**
IS監査担当者は、内部統制自己評価(CSA)プログラムのサポートを提供するよう依頼されました。以下のうち、このプログラムにおける監査担当者の役割範囲を最も適切に表しているのはどれですか？
A. 監査人は詳細な監査手続きを実施する必要があります。
B. 監査人はプログラムの促進者として行動すべきである。
C. 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。
D. 監査人はプロセスの生産性向上に注力すべきである
正解: **(**正解を表示します**)**

質問: **138**
以下のうち、アウトソーシングされたプロバイダー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どれですか？
A. 社内業績基準は企業戦略と一致している。
B. ベンダーは、そのパフォーマンスを示すために過去のデータを提供します。
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ています。
D. サービスレベル契約(SLA)の不遵守に対して適切な措置が講じられています。
正解: **D (**コメントを発表する**)**

質問: **139**
IS監査人は、経営陣が組織にとって不適切なレベルの残存リスクを受け入れていると考えています。監査人が取るべき最も適切な行動は次のうちどれですか？
A. 経営陣がリスクを受け入れる決定を下したことを取締役会に通知する報告書を提出する。
B. IS監査管理部門および経営陣とこの件について話し合う。
C. 監査報告書にリスクを受け入れるという経営陣の対応を記載し、それ以上の措置は取らない。
D. 監査報告書にリスクを所見として記載するが、経営陣のリスク受容については記載しない。
正解: **(**正解を表示します**)**
The correct answer is B. Discuss the matter with IS audit management and executive management.
Residual risk is the risk remaining after management has implemented a risk response. Risk acceptance must be made within the organization's risk appetite and risk tolerance. ISACA defines risk acceptance as a decision to accept risk according to the risk appetite and tolerance set by senior management, where the enterprise can assume the risk and absorb any losses.

If the IS auditor believes management accepted a risk level that is not appropriate, the auditor should not ignore the issue or simply document it without further discussion. The appropriate first step is to discuss the matter with IS audit management and executive management. This gives the organization an opportunity to reassess the decision, confirm whether the risk is within appetite, and determine whether additional treatment is required.
Option A may become appropriate later if executive management continues to accept a risk that exceeds risk appetite. ISACA guidance on follow-up activities states that when accepted risk is greater than the enterprise' s risk appetite, it should be discussed with senior management and brought to the attention of the audit committee or board if necessary.
Option C is incorrect because taking no further action would be inappropriate when the auditor believes the accepted residual risk is excessive. Option D is also incorrect because the audit report should fairly represent management's response, including risk acceptance, rather than omitting it.
This question maps to Information Systems Auditing Process because it concerns audit judgment, communication of audit findings, escalation, and reporting.
References: ISACA CISA Exam Content Outline, Domain 1; ISACA Interactive Glossary, "Residual risk,"
"Risk acceptance," and "Risk appetite"; ISACA guidance on audit follow-up activities.

質問**: 140**
監査の過程で、IS監査担当者は、多くの場合、システムから過剰な権限が削除されていないことを発見した。
監査人が最も推奨する内容は次のうちどれですか？
A. システム管理者は、割り当てられた権限の一貫性を確保する必要があります。
B. ITセキュリティは、過剰なシステム権限を定期的に取り消すべきです。
C. 人事部は、退職した従業員のアクセス権限を削除する必要があります。
D. ライン管理者はアクセス権限を定期的に見直し、変更を要求する必要があります。
正解**: D (**コメントを発表する**)**
The best recommendation for the auditor to make is D. Line management should regularly review and request modification of access rights. Access rights are the permissions and privileges granted to users to access, view, modify, or delete data or resources on a system or network1. Excessive rights are access rights that are not necessary or appropriate for a user's role or function, and may pose a risk of unauthorized or inappropriate use of data or resources2. Therefore, it is important to ensure that access rights are alignedwith the principle of least privilege, which means that users should only have the minimum level of access required to perform their duties2.
Line management is responsible for overseeing and supervising the activities and performance of their staff, and ensuring that they comply with the organization's policies

and standards3. Therefore, line management should regularly review and request modification of access rights for their staff, as they are in the best position to:
Understand the roles and functions of their staff, and determine the appropriate level of access rights needed for them to perform their duties effectively and efficiently.
Monitor and evaluate the usage and behavior of their staff, and identify any changes or anomalies that may indicate excessive or inappropriate access rights.
Communicate and collaborate with IT security or system administrators, who are responsible for granting, revoking, or modifying access rights, and request any necessary adjustments or corrections.

質問: **141**
組織の運用ログ管理をレビューするIS監査担当者にとって、以下のうちどれが最も懸念すべき事項でしょうか？
A. ログファイルのサイズは年々増加しています。
B. 重大なイベントは、変更不可能なログファイルに記録されます。
C. アプリケーションが複数のログファイルにイベントを記録しています。
D. すべてのログでデータ形式が標準化されていません。
正解: **D (**コメントを発表する**)**

質問: **142**
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次のうちどれですか？
A. ソースコード内に詳細情報を埋め込みます。
B. ファイル命名規則を標準化する。
C. 自動バージョン管理を利用する。
D. 変更登録簿に詳細を文書化する。
正解: **(**正解を表示します**)**
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.

質問: **143**
オペレーティングシステム監査中にベースラインイメージを取得する主な目的は次のうちどれですか？
A. 異常な実行プロセスを特定する
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へのアクセスを識別するため

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確認する
正解: **(**正解を表示します**)**
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]

質問: **144**
どのデータ損失防止 (DLP) 展開モデルで、組織の境界またはゲートウェイでデータ検査とポリシー適用が実行されますか?
A. ネットワークベースのDLP
B. クラウドベースのDLP
C. ハイブリッドDLP
D. エンドポイントベースのDLP
正解: **(**正解を表示します**)**

質問: **145**

IS監査の問題点を経営陣に伝える際に、最も重視すべき点は次のうちどれですか？
A. 問題を解決するための詳細なソリューション
B. 組織が問題によってさらされるリスク
C. その後の監査フォローアップの性質、範囲、およびタイミング
D. 問題がどのように発見され、誰が責任を負うのか
正解: **B** (コメントを発表する)

質問: **146**
情報システム投資に関する事業計画書は、以下の期間まで審査のために公開されるべきである。
A. 情報システムへの投資は終了しました。
B. 情報システムが耐用年数を過ぎました。
C. 正式な投資決定が承認されました。
D. メリットは完全に実現されました。
正解: **D** (コメントを発表する)
The business case for an information system investment is a document that provides the rationale and justification for the investment, based on the expected costs, benefits, risks, and impacts of the project12. The business case should be available for review until the benefits have been fully realized, because it serves as a baseline for measuring the actual performance and outcomes of the project against the planned ones34. This helps to evaluate the success and value of the investment, and to identify any gaps or issues that need to be addressed5.
References
1: The Business Case for Security - CISA
2: Beyond the Business Case: New Approaches to IT Investment
3: #HowTo: Build a Business Case for Cybersecurity Investment
4: ISACA CISA Certified Information Systems Auditor Exam ... - PUPUWEB
5: The Business Case for Security | CISA

質問: **147**
ある組織は、電子メールのセキュリティを確保するために公開鍵基盤(PKI)を使用しています。電子メールメッセージが送信中に改ざんされたかどうかを判断する最も効率的な方法は次のうちどれでしょうか？
A. メッセージは対称アルゴリズムを使用して暗号化されています。
B. メッセージはトランスポート層セキュリティ (TLS) プロトコルを使用して送信されます。
C. メッセージは、メッセージの暗号化されたハッシュ値とともに送信されます。
D. メッセージは送信者の秘密鍵を使用して暗号化されています。
正解: (正解を表示します)

This method is known as creating a digital signature of the message. It ensures the integrity of the message by verifying that it has not been tampered with in transit. The process involves hashing the message and encrypting the hash value with the sender's private key. Any changes to the message will result in a different hash value1. This method is used in DomainKeys Identified Mail (DKIM), which verifies an email's domain and helps show that the email has not been tampered with in transit2.
References:
Understanding Digital Signatures | CISA
Using DomainKeys Identified Mail (DKIM) in your organisation

質問**: 148**
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。
正解**: (**正解を表示します**)**
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

質問: **149**
特権アクセスの使用状況を監視するために、手動レビューを行う代わりに自動セキュリティログ監視ツールを使用する主な利点は次のうちどれですか？
A. 不審な活動を検出する可能性が高まる
B. ログファイルの保存と管理の容易さ
C. レビューの自動化に伴うコスト削減
D. 監査目的でのログ取得の容易さ
正解: **(**正解を表示します**)**

質問: **150**
IS監査担当者は、経費精算システムにおける不正行為を防止するプロセスをレビューするよう指示されました。このレビューにおいて、以下のステークホルダーのうち、最も重要な関与者はどれでしょうか？
A. 情報セキュリティマネージャー
B. 品質保証(QA)マネージャー
C. 事業部門責任者
D. ビジネスプロセスオーナー
正解: **D (**コメントを発表する**)**
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, aswell 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 performanceof 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

質問**: 151**
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ため
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を遵守するため
D. 業界のベストプラクティスに従う
正解**: (**正解を表示します**)**
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 and Why Is It Important? - RiskOptics
Data Classification Policy: Definition, Examples, and 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

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジン

を手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu 1605問、３０%ディスカウント、特別な割引コード: JPNshiken」

質問: **152**
ある組織は、複数のモジュールで構成される新しいITソリューションを導入する準備を整えています。最後のモジュールは、処理されたデータをデータベースに更新します。IS監査担当者にとって、以下のどの調査結果が最も懸念すべきでしょうか？
A. データ辞書がありません
B. 脆弱な暗号化の使用
C. 入力検証の欠如
D. 正式な変更承認プロセスが存在しない
正解: **(**正解を表示します**)**

質問: **153**
組織が顧客データを使用してAIアルゴリズムを訓練するかどうかを決定する際に、最も重要な規制上の考慮事項は次のうちどれですか？
A. トレーニングプロセス中のAIアルゴリズムの精度に関するドキュメント
B. データコンピューティングリソースの倫理的かつ最適な利用
C. データの収集およびデータ主体の同意の取得
D. AIアルゴリズムのパフォーマンスを継続的に監視します。
正解: **(**正解を表示します**)**
Data collection and obtaining consentis themost critical regulatory requirementwhen using customer data for AI training, especially under laws likeGDPR, CCPA, and ISO 27701.
Collection of Data and Obtaining Consent (Correct Answer - C)
Ensures compliance withprivacy lawsthat require explicit customer consent.
Example:UnderGDPR, companies mustinform usershow their data will be used and allow them toopt out.
AI Algorithm Accuracy (Incorrect - A)
Important formodel performancebutnot a primary legal concern.
Ethical Use of Computing Resources (Incorrect - B)
Ethical considerations are valuable butnot a regulatory priority.
Continuous Monitoring of AI (Incorrect - D)
Ensuresperformance, butregulatory compliance focuses on data privacy.
References:
ISACA CISA Review Manual
GDPR and CCPA Compliance Guidelines
ISO 27701 (Privacy Information Management System)

質問: **154**

継続的デプロイメントプログラムの一環としてのセキュアなコードレビューは、どのタイプの制御に該当しますか？
A. 探偵
B. 論理
C. 予防的
D. 修正
正解: **C** (コメントを発表する)
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

質問: **155**
セキュリティ意識向上トレーニングを最も効果的にするには、管理者は次の点をトレーニングで徹底する必要があります。
A. 特定のグループに合わせて調整されます。
B. 毎年発生します。
C. IT 担当者によって実施されます。
D. IT 環境のあらゆる側面をカバーします。
正解: (正解を表示します)

質問: **156**
災害復旧計画(DRP)には、以下の手順を含める必要があります。
A. リスクの評価と定量化。
B. 災害対策コンサルタントとの契約交渉。
C. アプリケーション制御要件の特定。
D. 代替品の入手。

正解: **D** (コメントを発表する)
A disaster recovery plan (DRP) is a set of detailed, documented guidelines that outline a business' critical assets and explain how the organization will respond to unplanned incidents. Unplanned incidents or disasters typically include cyberattacks, system failures, power outages, natural disasters, equipment failures, or infrastructure damage1. A DRP aims to minimize the impact of a disaster on the business continuity, data integrity, and service delivery of the organization. A DRP also helps the organization recover from a disaster as quickly and efficiently as possible.
A DRP should include steps for obtaining replacement supplies, as this is an essential part of restoring the normal operation of the organization after a disaster. Replacement supplies may include hardware, software, data, network components, office equipment, or other resources that are needed to resume the business functions and processes that were disrupted by the disaster. Obtaining replacement supplies may involve contacting vendors, suppliers, or partners; activating backup or alternative systems; or purchasing or renting new equipment. A DRP should identify the sources, locations, and costs of the replacement supplies, as well as the procedures and responsibilities for acquiring and installing them.
The other three options are not steps that a DRP should include, as they are either part of the pre-disaster planning process or not directly related to the disaster recovery objectives. Assessing and quantifying risk is a step that should be done before creating a DRP, as it helps identify the potential threats and vulnerabilities that could affect the organization and determine the likelihood and impact of each scenario2. Negotiating contracts with disaster planning consultants is also a pre-disaster activity that may help the organization design, implement, test, and maintain a DRP with external expertise and guidance3. Identifying application control requirements is not a step in a DRP, but rather a part of the application development and maintenance process that ensures the quality, security, and reliability of the software applications used by the organization.
Therefore, obtaining replacement supplies is the correct answer.
References:
What is a DisasterRecovery Plan? + Complete Checklist
Risk Assessment- ISACA
Disaster Recovery Planning - ISACA
[Application Controls - ISACA]

質問: **157**
IS監査担当者が、組織のユーザープロビジョニングプロセスで特定された問題点についてフォローアップ監査を実施しています。改善策をテストする際に、サンプリング対象として最も適切な母集団は次のうちどれですか？
A. 問題が最初に特定された後にプロビジョニングされたすべてのユーザー
B. 管理者が監査問題を解決した後、すべてのユーザーがプロビジョニングされました
C. 最終監査レポート発行後にプロビジョニングされたすべてのユーザー

D. 管理部門が提供するユーザープロビジョニングプロセスに従ったすべてのユーザー
正解: **(**正解を表示します**)**
The most appropriate population to sample from when testing for remediation of findings identified in an organization's user provisioning process is all users provisioned after the final audit report was issued. This is because the final audit report is the official document that communicates the audit findings, recommendations, and action plans to the management and other stakeholders. It also establishes a baseline for measuring the progress and effectiveness of the remediation efforts. Therefore, sampling from the users provisioned after the final audit report was issued would provide the most relevant and reliable evidence of whether the audit issues have been resolved or not.
The other options are not as appropriate as option C, as they may not reflect the actual status of the remediation efforts. All users provisioned after the finding was originally identified may include users who were provisioned before the final audit report was issued, which may not capture the full impact of the remediation actions. All users provisioned after management resolved the audit issue may not be accurate, as management's resolution may not be verified or validated by an independent party. All users who have followed user provisioning processes provided by management may not be representative, as there may be exceptions or deviations from the processes that could affect the remediation results.
References:
6: What Is User Provisioning? Definition, Process and Best Practices - Spiceworks
7: What Is User Provisioning? All You Need to Know in One Place - G2
8: What is User Account Provisioning? - Tools4ever
9: What Is Provisioning and Deprovisioning? | Okta

質問: **158**
ある組織は、すべての部門で遵守される成熟したリスク管理手法を確立しています。監査チームがこのリスク管理の成熟度を活用する最も効果的な方法は何でしょうか？
A. 経営陣に代わってリスク対応を実施する
B. 監査計画目的でリスクレジスターを統合する
C. リスクに関して経営陣に保証を提供する
D. 監査リスクの特定と評価に関するワークショップの促進
正解: **(**正解を表示します**)**
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 CertifiedInformation Systems Auditor - Question0551

質問: **159**
IS監査担当者が特定の仕入先の買掛金取引のサンプルを分析し、平均取引額の5倍の金額を持つ取引を1件特定しました。監査担当者は次に次のうちどれを行うべきでしょうか？
A. 差異を直ちに監査委員会に報告する
B. 監査対象者に対し、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. サンプル母集団からトランザクションを除外する
正解: **(**正解を表示します**)**
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 itmay affect the validity and reliability of the audit results. References: CISA Review Manual (Digital Version), [ISACA Auditing Standards]

質問: **160**
IS監査担当者は、ネットワーク脆弱性評価において、以下のうちどれを期待すべきでしょうか？
A. 設定ミスとアップデートの欠落
B. 悪意のあるソフトウェアとスパイウェア
C. ゼロデイ脆弱性
D. セキュリティ設計上の欠陥
正解: **A (**コメントを発表する**)**
A network vulnerability assessment is a process of identifying and evaluating the weaknesses and exposures in a network that could be exploited by attackers to compromise the confidentiality, integrity, or availability of the network or its resources. A network vulnerability assessment typically involves scanning the network devices, such as routers, switches, firewalls, servers, and workstations, using automated tools that compare the device configurations, software versions, and patch levels against a database of known vulnerabilities. A network vulnerability assessment can also include manual testing and verification of the network architecture, design, policies, and procedures. One of the main objectives of a network vulnerability assessment is to detect and report any

misconfiguration and missing updates in the network devices that could pose a security risk1.
Misconfiguration refers to any deviation from the recommended or best practice settings for the network devices, such as weak passwords, open ports, unnecessary services, default accounts, or incorrect permissions. Missing updates refer toany outdated or unsupported software or firmware that has not been patched with the latest security fixes or enhancements from the vendors2. Misconfiguration and missing updates are common sources of network vulnerabilities that can be exploited by attackers to gain unauthorized access, executemalicious code, causedenial of service, or escalate privileges on the network devices3.
Therefore, an IS auditor should expect to see misconfiguration and missing updates in a network vulnerability assessment. The other options are less relevant or incorrect because:
B). Malicious software and spyware are not usually detected by a network vulnerability assessment, as they are more related to the content and behavior of the network traffic rather than the configuration and patch level of the network devices. Malicious software and spyware are programs that infect or monitor the network devices or their users for malicious purposes, such as stealing data, displaying ads, or performing remote commands. Malicious software and spyware can be detected by other security tools, such as antivirus software, firewalls, or intrusion detection systems4.
C). Zero-day vulnerabilities are not usually detected by a network vulnerability assessment, as they are unknown or undisclosed vulnerabilities that have not been reported or patched by the vendors or the security community. Zero-day vulnerabilities are rare and difficult to discover, as they require advanced techniques and skills to exploit them. Zero-day vulnerabilities can be detected by other security tools, such as intrusion prevention systems, anomaly detection systems, or artificial intelligence systems5.
D). Security design flaws are not usually detected by a network vulnerability assessment, as they are more related to the logic and functionality of the network rather than the configuration and patch level of the network devices. Security design flaws are errors or weaknesses in the network architecture, design, policies, or procedures that could compromise the security objectives of the network. Securitydesign flaws can be detected by other security methods, such as security reviews, audits, or assessments6. References: Network VulnerabilityAssessment - ISACA, Network Vulnerability Scanning - NIST, Network Vulnerabilities - SANS, Malware - ISACA, Zero-Day Attacks - ISACA, Security Design Principles - NIST

質問**: 161**
企業ITのガバナンスを実施する際に、IS監査を関与させることの最も重要な利点は次のうちどれですか？
A. エンタープライズITガバナンスフレームワークに関連する役割の特定
B. リスク対応と残存リスクの監視に関する意思決定
C. 法的、規制的、および契約上の要件が満たされていることを検証する

D. ITプロセスの改善を促進するために、独立した客観的なフィードバックを提供する
正解: **(**正解を表示します**)**
The most important benefit of involving IS audit when implementing governance of enterprise IT is providing independent and objective feedback to facilitate improvement of IT processes.Governance of enterprise IT is the process of ensuring that IT supports the organization's strategy, goals, and objectives in an effective, efficient, ethical, and compliant manner. IS audit can provide value to governance of enterprise IT by assessing the alignment of IT with business needs, evaluating the performance and value delivery of IT, identifying risks and issues related to IT, recommending corrective actions and best practices, and monitoring the implementation and effectiveness of IT governance activities. IS audit can also provide assurance that IT governance processes are designed and operating in accordance with relevant standards, frameworks, laws, regulations, and contractual obligations. Identifying relevant roles for an enterprise IT governance framework is a benefit of involving IS audit when implementing governance of enterprise IT, but not the most important one. IS audit can help define and clarify the roles and responsibilities of various stakeholders involved in IT governance, such as board members, senior management, business units, IT function, external parties, etc. IS audit can also help ensure that these roles are aligned with the organization's strategy, goals, and objectives, and that they have adequate authority, accountability, communication, and reporting mechanisms. However, this benefit is more related to the design phase of IT governance implementation than to the ongoing monitoring and improvement phase. Making decisions regarding risk response and monitoring of residual risk is a benefit of involving IS audit when implementing governance of enterprise IT, but not the most important one. IS audit can help identify and assess the risks associated with IT activities and processes, such as strategic risks, operational risks, compliance risks, security risks, etc. IS audit can also help evaluate the effectiveness of risk management practices and controls implemented by management to mitigate or reduce these risks. However, this benefit is more related to the assurance function of IS audit than to its advisory function. Verifying that legal, regulatory, and contractual requirements are being met is a benefit of involving IS audit when implementing governance of enterprise IT, but not the most important one. IS audit can help verify that IT activities and processes comply with applicable laws, regulations, and contractual obligations, such as data protection laws, privacy laws, cybersecurity laws, industry standards, service level agreements, etc. IS audit can also help identify and report any instances of noncompliance or violations that could result in legal or reputational consequences for the organization. However, this benefit is more related to the assurance function of IS audit than to its advisory function.
References: ISACA CISA Review Manual 27th Edition, page 283

質問: **162**
公開鍵基盤(PKI)環境において、否認防止はどのようにサポートされるのでしょうか？
A. ユーザーが受信したデータを復号するために秘密鍵を使用することによって

B. 認証局(CA)が発行した証明書を使用することによって
C. 送信メッセージに楕円曲線暗号を使用することにより
D. エンタープライズキー管理システムの使用を通じて
正解: **B** (コメントを発表する)

質問: **163**
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. 導入後レビューを実施する-
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。
正解: (正解を表示します)
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 and Systems Resources | COBIT, Risk, Governance ... - ISACA, IT Governance and Process Maturity

質問: **164**
IS監査担当者が、ローカルデータベースサーバーで2週間ごとにバックアップを実行しているものの、データバックアップと復元手順を規定する正式なポリシーを持たない組織を監査しています。以下の所見のうち、組織にとって最も大きなリスクとなるのはどれでしょうか？
A. データバックアップポリシーの欠如
B. オフサイトデータバックアップの欠如
C. データバックアップ頻度が不十分です
D. 定期的なデータ復元テストの欠如
正解: (正解を表示します)

質問: **165**
エンドユーザーコンピューティング(EUC)において、財務報告にスプレッドシートを利用することに伴う最大のリスクは次のうちどれですか？
A. 規制違反の増加
B. 処理の整合性の欠如
C. 運用上のインシデントの増加

D. パスワード保護の欠如
正解: **(**正解を表示します**)**

質問: **166**
仮想サーバーファームの潜在的なソフトウェア脆弱性に関する監査を実施する際、IS監査担当者は、以下の観察事項のうちどれを最大の危険とみなすでしょうか？
A. ゲストOS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台の仮想サーバー上で様々なゲストオペレーティングシステムが動作する。
D. アンチウイルス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。
正解: **(**正解を表示します**)**
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

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu　**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **167**
グローバル企業のポリシーでは、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。IS監査担当者が、このポリシーへの継続的な準拠を示す最良の証拠として提示できるのは、次のうちどれでしょうか？
A. 侵入テストの結果
B. 経営陣による証明

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
正解**: C (**コメントを発表する**)**
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

質問**: 168**
機密データを含む外部公開システムが、ユーザーが読み取り専用権限または管理者権限のいずれか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権限を持っています。この状況に関連する最大のリスクは次のうちどれですか？
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. ユーザーは不正な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。
正解: **(**正解を表示します**)**
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

質問: **169**
ITポートフォリオ管理が組織戦略と整合していることを示す最良の証拠は、次のうちどれですか？
A. ITプロジェクトの優先順位付けの承認を含むIT運営委員会の議事録
B. ITプロジェクトの提案とマイルストーンに対するプロジェクトスポンサーの承認
C. プロジェクトスポンサーがプロジェクト開始から終了まで全てのプロジェクト文書を承認
D. 年間IT予算の承認を含む財務委員会の議事録
正解: **(**正解を表示します**)**

質問: **170**
スプレッドシートを使用してプロジェクトのコスト見積もりを計算します。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。システムにデータが正確に入力されることを保証するための最適な管理方法はどれですか？
A. プロジェクト別合計金額の調整
B. 有効性チェック、文字データの入力を防止します
C. 各コストタイプの妥当性チェック
D. 入力後にプロジェクト詳細の裏面を表示する
正解: **(**正解を表示します**)**
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)

質問: **171**
IS監査リソースの利用を最適化する上で、最も役立つ監査手法はどれですか？
A. アジャイル監査
B. 継続監査
C. 監査業務のアウトソーシング
D. リスクベース監査
正解: **(**正解を表示します**)**
Risk-based auditing is an audit approach that focuses on the analysis and management of risk within an organization. Risk-based auditing helps identify and prioritize the areas or processes that pose the highest risk to the organization's objectives and allocate audit resources accordingly. Risk-based auditing also helps provide assurance and advisory services related to the organization's risk management processes and controls.
By using risk-based auditing, internal auditors can optimize the use of their audit resources and add value to the organization.
Agile auditing, continuous auditing, and outsourced auditing are not audit approaches that are most helpful in optimizing the use of IS audit resources. Agile auditing is a flexible and iterative audit methodology that adapts to changing circumstances and stakeholder needs. Continuous auditing is a method of performing audit activities on a real-time or near-real-time basis using automated tools and techniques. Outsourced auditing is a practice of contracting external auditors to perform some or all of the internal audit functions. These audit methods may have some advantages or disadvantages depending on the context and objectives of the audit, but they do not necessarily optimize the use of IS audit resources.

質問: **172**
IS監査担当者がさまざまなアプリケーションやデバイスからのアクセス制御リストを組み合わせて比較するのに最も適した方法はどれですか？
A. 統合試験施設(ITF)
B. スナップショット
C. データ分析
D. 監査フック
正解: **(**正解を表示します**)**
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

質問**: 173**
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、指標が以下の条件を満たすことです。
A. 業界標準に準拠する。
B. は理解しやすいです。
C. 実用的なデータを提供する。
D. すべての事業部門に適用されます。
正解**: (**正解を表示します**)**

質問**: 174**
ある組織は、大量の取引が発生する複雑なシステムにおいて、ベンダーへの支払いが重複していることを懸念しています。情報システム監査人がベンダーへの支払いの重複の有無を判断する上で、次のうちどれが最も役立つでしょうか？
A. コンピュータ支援技術
B. 層化抽出法
C. 統計的サンプリング
D. プロセスウォークスルー
正解**: (**正解を表示します**)**

A computer-assisted technique is the most helpful method for an IS auditor to determine whether duplicate vendor payments exist on a complex system with a high volume of transactions. A computer-assisted technique is a tool or procedure that can be used to perform audit tests or procedures on data stored in electronic form. Examples of computer-assisted techniques include data analysis software, query tools, scripting languages, and specialized audit software. A computer-assisted techniquecan help an IS auditor to identify and extract duplicate payments from a large data set, perform calculations and comparisons, and generate reports and summaries. A computer-assisted technique can also provide more accuracy, efficiency, and coverage than manual methods.
Stratified sampling, statistical sampling, and process walk-through are not as helpful as a computer-assisted technique for this purpose. Stratified sampling is a sampling method that divides the population into subgroups based on certain characteristics and selects samples from each subgroup. Statistical sampling is a sampling method that uses probability theory to determine the sample size and selection criteria. Process walk-through is a review technique that involves following a transaction or process from start to finish and observing the inputs, outputs, controls, and documentation. These methods may be useful for other audit objectives, but they are not as effective as a computer-assisted technique for detecting duplicate payments in a complex and high-volume system.
References: ISACA Frameworks: Blueprints for Success, [ISACA Glossary of Terms]

質問**: 175**
組織のリスク許容度とリスク耐性に関して、最も有用な情報を提供するのは次のうちどれですか？
A. ギャップ分析
B. 監査報告書
C. リスクプロファイル
D. リスク登録簿
正解**: (**正解を表示します**)**
The most useful information regarding an organization's risk appetite and tolerance is provided by its risk profile, as this is a document that summarizes the key risks that the organization faces, the potential impacts and likelihoods of those risks, and the acceptable levels of risk exposure for different objectives and activities.
A gap analysis is a tool that compares the current state and the desired state of a process or a system, and identifies the gaps that need to be addressed. Audit reports are documents that present the findings, conclusions, and recommendations of an audit engagement. A risk register is a tool that records and tracks the identified risks, their causes, their consequences,and their mitigation actions. References: CISA Review Manual (Digital Version), Chapter 2: Governance and Management of IT, Section 2.1: IT Governance

質問**: 176**

モバイルデバイスを使用する際に、ネットワークの整合性を維持するための最も効果的な方法はどれですか？
A. ネットワークアクセス制御を実装します。
B. 送信ファイアウォールルールを実装します。
C. ネットワークレビューを実行します。
D. アクセス制御リストを確認します。
正解: **(正解を表示します)**
The most effective way to maintain network integrity when using mobile devices is to implement network access control. Network access control is a security control that regulates and restricts access to network resources based on predefined policies and criteria, such as device type, identity, location, or security posture.
Network access control can help maintain network integrity when using mobile devices by preventing unauthorized or compromised devices from accessing or affecting network systems or data. The other options are not as effective as network access control in maintaining network integrity when using mobile devices, as they do not address all aspects of network access or security. Implementing outbound firewall rules is a security control that filters and blocks network traffic based on source, destination, protocol, or port, but it does not regulate or restrict network access based on device characteristics or conditions. Performing network reviews is a monitoring activity that evaluates and reports on the performance, availability, or security of network resources, but it does not regulate or restrict network access based on device characteristics or conditions. Reviewing access control lists is a verification activity that validates and confirms the access rights and privileges of network users or devices, but it does not regulate or restrict network access based on device characteristics or conditions. References: CISA Review Manual (Digital Version), Chapter 5, Section
5.2.2

質問: **177**
ある組織は、重要なサーバーの日常的なバックアップの代わりに、仮想マシン(VM)のレプリケーションを実施している。
復旧手順の妥当性を評価する際に、検証すべき最も重要な項目は次のうちどれですか？
A. レプリケーションサーバーは外部に設置されています。
B. VMレプリケーションの定期テストが完了しました。
C. VMの負荷分散が設定されています。
D. VMバックアップ管理者のインターネットアクセスは制限されています。
正解: **(正解を表示します)**
The most important validation point is whether the VM replication process is periodically tested to confirm that recovery will actually work. ISACA guidance on backup and recovery states that when using new backup methodologies or technologies, management should

test the data afterward to ensure the process is reliably recording all required data, and auditors should ensure periodic health checks are performed.
Option B is correct because recovery adequacy is not proven by the mere existence of replication. ISACA specifically warns that replication alone can increase risk, since corruption can be replicated as well, and it emphasizes validating the reliability of the backup or replication process through testing and health checks.
Option A is important for resilience, but offsite location alone does not prove recoverability. A replica that is never tested may still fail when needed.
Option C is not the most important factor for evaluating recovery procedures. Load balancing supports performance and availability, but it is not the key evidence that replicated systems can be recovered successfully.
Option D is a useful security precaution. ISACA does note that VM backup administrators should not have Internet access to reduce ransomware exposure, but that is a security-hardening issue, not the primary validation of recovery adequacy.
Therefore, B is the best answer because periodic testing is the most important way to validate that VM replication will support actual recovery.
References (Official ISACA):
ISACA Journal, IS Audit Basics: Backup and Recovery - replication can increase risk if corruption is copied; auditors should ensure backup/recovery processes are tested and health checks are performed.
ISACA Journal, A Five-Layer View of Data Center Systems Security - disaster recovery design should consider criticality and RPO/RTO.

質問: **178**
ある組織は、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る。IS監査担当者の視点からすると、テーブルは以下に基づいて分類されるべきである。
A. テーブルにアクセスできるエンドユーザーの数。
B. 各テーブルの具体的な機能内容。
C. テーブルの更新頻度。
D. テーブル内の列名の説明。
正解: **(**正解を表示します**)**

質問: **179**
セキュリティ分類の異なるデータを含むサーバー上で、最小権限の原則を徹底するための最適な方法は次のうちどれですか？
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を遵守するためのユーザーからの正式な同意を得る
C. データ所有者によって決定され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します。

正解: **C** (コメントを発表する)
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 rightsand 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 and Explanations Database

質問: **180**
盗難または紛失したノートパソコン上の機密情報への不正アクセスを防ぐための、以下の対策のうちどれが最も効果的ですか？
A. リモートワイプ機能
B. ディスク暗号化
C. ユーザー認識
D. パスワードで保護されたファイル
正解: (正解を表示します)
Thebest protectionfor a stolen laptop isfull disk encryption, which prevents unauthorized accesseven if the device is lost.
Option A (Incorrect):Remote wipe capabilitiesare useful, but theyrequire an internet connectionto function, which is not always available when a device is stolen.
Option B (Correct):Full disk encryption (FDE)ensures that data remainsunreadablewithout the correct decryption key,even if the hard drive is removed.
Option C (Incorrect):User awarenessis helpful, but itdoes not physically securedata on a lost device.
Option D (Incorrect):Password-protected filescan be bypassed by copying them to another system, making them an inadequate security measure.
Reference:ISACA CISA Review Manual -Domain 5: Protection of Information Assets-Coversencryption, data security, and endpoint protection.

質問: **181**
フォローアップ監査中に、リスクの低い複雑なセキュリティ脆弱性が合意された期間内に解決されていないことが判明しました。IT部門は、脆弱性が特定されたシステムは交換中で、2か月後には完全に機能するようになると述べています。次のうち、最善の対応策はどれですか？

A. 発見事項が新しいシステム内で対処されることを示す文書を要求する
B. 上級管理職とこの問題について話し合うための会議を予定する。
C. 脆弱性が悪用されたかどうかを判断するために、臨時の監査を実施する。
D. 新システム導入前にこの問題を解決することを推奨します。
正解: **(**正解を表示します**)**
Requiring documentation that the finding will be addressed within the new system is the best course of action for a follow-up audit. An IS auditor should obtain evidence that the complex security vulnerability of low risk will be resolved in the new system and that there is a reasonable timeline for its implementation. The other options are not appropriate courses of action, as they may be too costly, time-consuming, or impractical for a low-risk finding. References:
CISA Review Manual (Digital Version), Chapter 2, Section 2.5.31
CISA Review Questions, Answersand Explanations Database, Question ID 209

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu ¶**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **182**
ある組織は、ロボティック・プロセス・オートメーション(RPA)技術を使用して、さまざまなソースからデータを抽出し、既存の財務アプリケーションに入力するソフトウェアボットを開発しました。IS監査人がソフトウェアボットのジョブスケジューリングと生産プロセスの自動化をレビューする際に、最も懸念すべき事項は次のうちどれでしょうか？
A. 軽微な上書きはビジネスによって承認されていません
B. ソフトウェアボットはトレーニングデータから学習することができなかった
C. ソフトウェアボットは、マウストラッキングを含むすべてのユーザー操作を記録するようにプログラムされていました。
D. パフォーマンス向上のため、スクリプトに無許可の変更が加えられました。
正解: **D (**コメントを発表する**)**
Unauthorized modifications to scripts (D) pose the greatest risk because they can lead to unintended processing errors, security vulnerabilities, or fraudulent activities. Change management controls should be in place to prevent unauthorized script changes.
Other options:
Minor overrides not authorized (A) is a concern but does not pose as much risk as unauthorized script changes.
Bots incapable of learning (B) is a limitation but not a security risk.

Recording user interactions (C) raises privacy concerns but is not as critical as unauthorized script modifications.
Reference: ISACA CISA Review Manual, Information Systems Operations and Business Resilience

質問: **183**
IS監査人が、組織のロボティック・プロセス・オートメーション(RPA > 定型業務を自動化する)導入計画をレビューする際に確認すべき最も重要な事項は次のうちどれですか？
A. エンドツーエンドのプロセスが理解され、文書化されています。
B. 対象となるビジネスプロセスについて、役割と責任が定義されています。
C. RPAを使用している同業他社とのベンチマーク調査が完了しました。
D. 適格なベンダーに対して提案依頼書(RFP)が発行されました。
正解: **A** (コメントを発表する)
The most important thing for an IS auditor to confirm when reviewing an organization's plans to implement robotic process automation (RPA) to automate routine business tasks is that the end-to-end process is understood and documented. This is because RPA involves the use of software robots or digital workers to mimic human actions and execute predefined rules and workflows. Therefore, it is essential that the IS auditor verifies that the organization has a clear and accurate understanding of the current state of the process, the desired state of the process, the inputs and outputs, the exceptions and errors, the roles and responsibilities, and the performance measures12. Without a properdocumentation of the end-to-end process, the organizationmay face challenges in designing, developing, testing, deploying, and monitoring the RPA solution3. References: 1: CISA ReviewManual (Digital Version), Chapter 4: Information Systems Operations and Business Resilience, Section 4.2: IT Service Delivery and Support, page 211 2:CISA Online Review Course, Module 4: Information Systems Operations and Business Resilience, Lesson 4.2: IT Service Delivery and Support 3: ISACA Journal Volume 5, 2019, Article: Robotic Process Automation: Benefits, Risks and Controls

質問: **184**
以下のアプローチのうち、品質保証(QA)機能の実装において最も大きな懸念事項となるのはどれでしょうか？
A. 変更を導入する開発者が、最もよく知っているため、作業をレビューします。
B. 変更内容に不慣れな同じ開発チームの同僚開発者がレビューを行います。
C. 組織内の別の開発チームの開発者が提出された変更をレビューします。
D. 開発グループ外の、開発役割を持たないレビュー担当者が変更内容をレビューします。
正解: **A** (コメントを発表する)
A strongQA functionrequires anindependentreview of changes toavoid biasandensure objectivity.

Option A (Correct):Ifdevelopers review their own changes, there is ahigh risk of biasand overlooking issues, making this the greatest concern. This violatesseparation of dutiesandbest practices for quality assurance.
Option B (Incorrect):Peer reviews within the same teamreduce risksincefresh eyesreview the changes, though it is not as strong as an external review.
Option C (Incorrect):Havingdevelopers from a separate teamreview the code providesbetter objectivityand reduces risks associated withself-review.
Option D (Incorrect):Whilenon-developers may lack technical expertise, their review ensuresindependence, making it a stronger control than self-review.
Reference:ISACA CISA Review Manual -Domain 3: Information Systems Acquisition, Development, and Implementation- Coversquality assurance, code reviews, and segregation of duties.

質問**: 185**
組織の事業影響分析(BIA)をレビューする情報システム監査担当者にとって、以下のうちどれが最も懸念すべき事項でしょうか？
A. BIAの完了前にリスク評価は実施されませんでした。
B. システムの重要度情報はITマネージャーからのみ提供されました。
C. 対面インタビューではなく、アンケートを用いて情報を収集した。
D. BIAは経営陣によって承認されていません。
正解**: B (**コメントを発表する**)**
The business impact analysis (BIA) is a critical component of an organization ' s business continuity planning (BCP) process. The most concerning issue is when system criticality information is provided only by the IT manager (Option B). This presents a risk of bias or incomplete analysis, as business units must also provide input to ensure a comprehensive assessment.
ISACA CISA Reference: According to ISACA's BCP and DRP guidelines, BIA should involve input from multiple business functions, including finance, operations, and risk management, rather than relying solely on IT.
Risk Implication: Without broader business input, the criticality of systems may be misclassified, leading to incorrect recovery priorities and potential business disruption.
Alternative Choices:
Option A: While a risk assessment is important, a BIA can still be completed without it and later validated.
Option C: The use of questionnaires is a valid method if responses are verified.
Option D: Lack of executive sign-off is concerning but does not directly impact the accuracy of system criticality assessment.

質問**: 186**

インターネットセキュリティの調査により、ユーザーがインターネットサービスプロバイダ(ISP)に個別のユーザーアカウントを持ち、これらのアカウントを使用して業務データをダウンロードしていることが明らかになった。組織は、社内ネットワークのみが使用されるようにしたいと考えている。組織はまず、以下のことを行うべきである。
A. プロキシサーバーを使用して、アクセスすべきでないインターネットサイトをフィルタリングします。
B. インターネットアクセスのログを手動で記録します。
C. リモートアクセス活動を監視します。
D. セキュリティポリシーにインターネットの使用に関する記述を含める。
正解**: (**正解を表示します**)**
The first step that the organization should take to ensure that only the corporate network is used for downloading business data is to include a statement in its security policy about Internet use. A security policy is a document that defines the rules, expectations, and overall approach that an organization uses to maintain the confidentiality, integrity, and availability of its data1. A security policy should clearly state the acceptable and unacceptable use of Internet resources, such as personalaccounts with ISPs, and the consequences of violating the policy. A security policy also helps to guide the implementation of technical controls, such as proxy servers, firewalls, or monitoring tools, that can enforce the policy and prevent or detect unauthorized Internet access.
The other options are not the first step that the organization should take, but rather subsequent or complementary steps that depend on the security policy. Using a proxy server to filter out Internet sites that should not be accessed is a technical control that can help implement the security policy, but it does not address the root cause of why users are using personal accounts with ISPs. Keeping a manual log of Internet access is a monitoring technique that can help audit the compliance with the security policy, but it does not prevent or deter users from using personal accounts with ISPs. Monitoring remote access activities is another monitoring technique that can help detect unauthorized Internet access, but it does not specify what constitutes unauthorized access or how to respond to it.
References:
ISACA CISA Review Manual 27th Edition (2019), page 247
What is a Security Policy? Definition, Elements, and Examples - Varonis1

質問**: 187**
デジタル証拠が元の形式のままであり、改ざんされていないことを証明するのに最も役立つのは、次のうちどれですか？
A. デジタルメディアのイメージング。
B. 書き込み保護メディア。
C. ハッシュ値。
D. 保管管理記録。

正解: **C** (コメントを発表する)
The correct answer is C. Hash values.
Hash values are the best way to establish that digital evidence remains unchanged. A hash is a fixed value mathematically generated from data. If even a small change is made to the evidence, the hash value changes.
Therefore, comparing the hash value calculated when evidence was collected with the hash value calculated later helps prove whether the evidence is still in its original form.
ISACA's glossary defines hashing as a cryptographic process that converts input data into a fixed-length hash value, ensuring data integrity and authentication. This directly supports the use of hash values to verify that digital evidence has not been altered.
Option A is not the best answer because imaging creates a forensic copy of the media, but the image still needs to be validated using hash values. Option B helps prevent accidental or intentional modification during examination, but it does not by itself prove the evidence is unchanged. Option D is important because chain of custody documents who handled evidence, when, and how it was protected. However, chain of custody is a procedural control; hash values provide the stronger technical proof of integrity. ISACA defines chain of custody as the evidence-handling process needed to maintain evidence validity and integrity, including documentation of who had access to the evidence and when.
This question maps mainly to Information Systems Auditing Process because it concerns audit evidence reliability, digital evidence handling, and support for audit conclusions.
ISACA's CISA Exam Content Outline includes audit evidence collection techniques and reporting under Domain 1.
References: ISACA CISA Exam Content Outline, Domain 1; ISACA Interactive Glossary, "Hashing" and
"Chain of custody."

質問: **188**
仮想化環境のアーキテクチャの一部として、ベアメタルまたはネイティブの仮想化では、ハイパーバイザは以下なしで実行されます。
A. ホストオペレーティングシステム。
B. ゲストオペレーティングシステム。
C. ゲストオペレーティングシステム上のアプリケーション。
D. ホストオペレーティングシステム上のアプリケーション。
正解: (正解を表示します)
In a bare metal or native virtualization, the hypervisor runs without a host operating system. A hypervisor, also known as a virtual machine monitor or VMM, is a type of virtualization software that supports the creation and management of virtual machines (VMs) by separating a computer's software from its hardware. A bare metal hypervisor, also called a Type I or Native hypervisor, is virtualization software that runs onhost machine hardware directly, without requiring an underlying operating system12. This

means that the bare metal hypervisor is the host or the operating system (OS) of the hardware1.
A guest operating system is an operating system that runs inside a virtual machine, on top of the hypervisor. A bare metal hypervisor can run multiple guest operating systems simultaneously, each with its own applications and resources. A guest operating system is not required for a bare metal hypervisor to run, but it is necessary for running applications on the virtual machine13.
Applications are software programs that perform specific tasks or functions for users. Applications can run on either the host operating system or the guest operating system, depending on the type of virtualization. In a bare metal virtualization, applications can run on the guest operating system, but not on the host operating system, since there is no host operating system. However, applications are not essential for a bare metal hypervisor to run, as they are only used by the users of the virtual machines

質問**: 189**
ある組織では、従業員が業務に個人のモバイル端末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適切に維持できる方法は次のうちどれでしょうか？
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. デバイス上で作業環境と個人スペースを分離する
C. ユーザーがアプリケーションを追加することを禁止する
D. 勤務時間中の私的目的でのデバイス使用の制限
正解**: (**正解を表示します**)**
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 and 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 yourapps and data4 9 Ways to Improve Mobile Security and Privacy in the Age of Remote Work5

質問: **190**
システム移行時のダウンタイムを最も効果的に最小限に抑える方法はどれですか？
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
正解: **D (**コメントを発表する**)**
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. Thisreduces 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

質問: **191**
給与計算アプリケーションに関する監査結果を受けて、経営陣は新たな自動化された統制を導入しました。IS監査人がこの新しい統制の有効性を評価する際に、最も役立つのは次のうちどれでしょうか？
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. 承認済みプロジェクト範囲文書
D. 卓上演習の結果のレビュー
正解: **(**正解を表示します**)**
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)

質問: **192**
組織の品質管理(QC)プロセスを管理する能力にとって、次のうちどれが最も大きなリスクとなるでしょうか？
A. 職務分掌の欠如
B. 専用の品質管理機能の欠如

C. 方針と手順の欠如
D. 正式な研修および証明の欠如
正解**: (**正解を表示します**)**
The greatest risk to an organization's ability to manage QC processes is the lack of policies and procedures that define the QC objectives, standards, methods, roles, and responsibilities. Without policies and procedures, the QC processes may be inconsistent, ineffective, inefficient, or noncompliant with the relevant regulations and best practices. Policies and procedures provide the foundation and guidance for the QC processes and help to ensure their quality, reliability, and accountability.
References
ISACA CISA Review Manual, 27th Edition, page 253
Quality Control - an overview | ScienceDirect Topics
Quality Control: Meaning, Importance, Definition and Objectives

質問**: 193**
コンピュータシステムの障害発生直前の状態に取引や記録を復元するために、適切なカットオフが設定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ロールバックする
C. システムコンソールログを電子形式で保持する
D. すべての送電線で双方向同期機能を確保する
正解**: (**正解を表示します**)**
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 and Explanations Database

質問**: 194**
管理合計を使用することで、以下のリスクが軽減されます。
A. 間違ったレコードに投稿しています。
B. 処理が完了していません。

C. バックアップが不適切です。
D. 不適切な認証。
正解: **(**正解を表示します**)**
Control totals are a method of verifying the accuracy and completeness of data processing by comparing the totals of key fields in input and output records1. Control totals can be used to reduce the risk of incomplete processing, which is the failure to process all the data or transactions that are expected or required2.
Incomplete processing can result in data loss, inconsistency, or incompleteness, which can affect the quality and reliability of the information system and its outputs. Incomplete processing can be caused by various factors, such as:
Hardware or software failures that interrupt the processing or transmission of data2 Human errors or omissions that skip or miss some data or transactions2 Malicious attacks or unauthorized access that delete or modify some data or transactions2 Environmental hazards or disasters that damage or destroy some data or transactions2 Control totals can help detect and prevent incomplete processing by:
Providing a benchmark or reference point to compare the input and output data or transactions1 Identifying any discrepancies or deviations from the expected or required totals1 Alerting the users or operators to investigate and resolve the causes of incomplete processing1 Ensuring that all the data or transactions are properly transmitted, converted, and processed1 The other options are not as relevant as control totals for reducing the risk of incomplete processing. Posting to the wrong record is the error of assigning or transferring data or transactions to an incorrect account, file, or record3. Improper backup is the failure to create, store, or restore copies of data or transactions in case of loss, corruption, or damage4. Improper authorization is the lack of proper permission or approval to access, modify, or process data or transactions. Control totals may not be able to prevent or detect these errors or failures, as they are not related to the completeness of data processing. Therefore, option B is the correct answer.
References:
control totals - Barrons Dictionary - AllBusiness.com
What is control total amount? - Sage Advice US
Posting Error Definition
Backup Definition
[Authorization Definition]

質問: **195**
次のうち、受動的な攻撃方法の例はどれですか？
A. キーストロークログ
B. 便乗
C. 盗聴
D. フィッシング
正解: **(**正解を表示します**)**

Comprehensive and Detailed in-Depth Explanation:
A passive attack involves monitoring or listening without altering data or system operations. Eavesdropping is a classic example, where attackers intercept data without affecting the transmission.
Keystroke logging (Option A) and phishing (Option D) are active attacks. Piggybacking (Option B) involves unauthorized access and is also active.
ISACA CISA Reference: Domain 5 - Protection of Information Assets

質問: **196**
情報セキュリティプログラムの成功にとって、次のうちどれが最も重要ですか？
A. 経営陣の情報セキュリティへの取り組み
B. 情報セキュリティに対するユーザーの責任
C. 情報セキュリティとIT目標の整合性
D. ビジネスと情報セキュリティの統合
正解: **A** (コメントを発表する)
The most critical factor for the success of an information security program is management's commitment to information security. Management's commitment to information security means that the senior management supports, sponsors, funds, monitors and enforces the information security program within the organization. Management's commitment to information security also demonstrates leadership, sets the tone and culture, and establishes the strategic direction and objectives for information security. User accountability for information security, alignment of information security with IT objectives, and integration of business and information security are also important factors for the success of an information security program, but they are not as critical as management's commitment to information security, as they depend on or derive from it.
References: Info Technology and Systems Resources | COBIT, Risk, Governance ... - ISACA, IT Governance and Process Maturity

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu 「**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **197**
組織内の以下の役割のうち、どの役割からの支援が情報セキュリティガバナンスに最も大きな影響力を持つか？
A. 最高情報セキュリティ責任者(CISO)
B. 情報セキュリティ運営委員会

C. 取締役会
D. 最高情報責任者(CIO)
正解**: (**正解を表示します**)**
Information security governance is the subset of enterprise governance that provides strategic direction, ensures that objectives are achieved, manages risk appropriately, uses organizational resources responsibly, and monitors the success or failure of the enterprise security program. Information security governance is essential for ensuring that an organization's information assets are protected from internal and external threats, and that the organization complies with relevant laws and standards.
Demonstrated support from which of the following roles in an organization has the most influence over information security governance? The answer is C, the board of directors. The board of directors is the highest governing body of an organization, responsible for overseeing its strategic direction, performance, and accountability. The board of directors sets the tone at the top for information security governance by:
Establishing a clear vision, mission, and values for information security Approving and reviewing information security policies and standards Allocating sufficient resources and budget for information security Appointing and empowering a chief information security officer (CISO) or equivalent role Holding management accountable for information security performance and compliance Communicating and promoting information security awareness and culture The board of directors has the most influence over information security governance because it has the ultimate authority and responsibility for ensuring that information security is aligned with the organization's business objectives, risks, and stakeholder expectations.
References:
10: What is Information Security Governance? - RiskOptics - Reciprocity
11: Information Security Governance and Risk Management | Moss Adams
12: ISO/IEC 27014:2020 - Information security, cybersecurity and privacy ...

質問**: 198**
IS監査担当者が、外部委託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れだけ効果的に実行しているかを示す最適な指標は次のうちどれですか？
A. チケットの平均年齢
B. 顧客満足度評価
C. 処理された通話数
D. 通話記録のレビュー
正解**: B (**コメントを発表する**)**

質問**: 199**
IS監査担当者が、ファイアウォールが旧式でベンダーによるサポートも受けられないことを発見しました。監査担当者が次に取るべき行動は次のうちどれでしょうか？

A. 緩和策を報告してください。
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ことのリスクを判断します。
正解: **D** (コメントを発表する)
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.

質問: **200**
IS監査担当者が、非常に大規模なeコマースプラットフォームの監査を実施しています。監査担当者がWebアプリケーションのセキュリティ上の欠陥を特定するのに最も適した手法は次のうちどれですか？
A. コードレビュー。
B. 脆弱性スキャン。
C. 論理セキュリティテスト。
D. 侵入テスト。
正解: (正解を表示します)
The correct answer is B. Vulnerability scanning.
For a very large e-commerce platform, vulnerability scanning is the best technique among the options because it provides automated, broad coverage for identifying security weaknesses across web applications, servers, interfaces, and related components. ISACA defines vulnerability scanning as an automated process used to proactively identify security weaknesses in a network or individual system. ISACA's CISA Exam Content Outline also includes threat and vulnerability management and the use of technical security testing to identify potential vulnerabilities.
Option A, code review, can be very useful for identifying insecure coding practices and logic flaws, but it is usually more time-consuming and less practical as the primary technique for a very large e-commerce environment. It may also require access to source code and specialized development expertise.
Option C, logical security testing, focuses mainly on access rights, authentication, authorization, and logical access controls. It is important, but it is narrower than vulnerability scanning for identifying web application security flaws.

Option D, penetration testing, is valuable because it attempts to exploit vulnerabilities in a controlled manner.
ISACA defines penetration testing as a live test of security defenses by mimicking real-life attackers.
However, penetration testing is usually more targeted and is often used to validate exploitability of vulnerabilities. For broad identification of web application flaws in a very large platform, vulnerability scanning is the stronger answer.
This question maps mainly to Protection of Information Assets because the CISA Exam Content Outline includes security testing tools and techniques, security monitoring, threat and vulnerability management, and protection of information assets under Domain 5.
References: ISACA CISA Exam Content Outline, Domain 5; ISACA Interactive Glossary, "Vulnerability scanning," "Vulnerability management," and "Penetration testing."

質問**: 201**
監査で指摘された事項は、まず被監査者に伝えるべきです。
A. レポートを作成する際。
B. 現地調査中。
C. 現地調査の終了時。
D. 監査報告書内
正解**: B (**コメントを発表する**)**
Audit observations are the findings and recommendations that result from an audit engagement. Audit observations should be first communicated with the auditee during fieldwork, which is the stage of the audit process where the auditor collects and analyzes evidence to evaluate the audit objectives1. Communicating audit observations during fieldwork has several benefits, such as2:
It allows the auditor to verify the accuracy and completeness of the observations, and to obtain additional information or clarification from the auditee if needed.
It enables the auditor to discuss the root causes, impacts, and risks of the observations, and to solicit the auditee's input on possible corrective actions and implementation timelines.
It helps to build rapport and trust between the auditor and the auditee, and to avoid surprises or disagreements at the end of the audit.
It facilitates timely resolution of audit observations, and reduces the risk of audit delays or disputes.
Therefore, option B is the correct answer.
Option A is not correct because communicating audit observations when drafting the report is too late, as it may lead to misunderstandings, conflicts, or revisions that could have been avoided if the observations were communicated earlier. Option C is not correct because communicating audit observations at the end of fieldwork is also not ideal, as it may not leave enough time for the auditor and the auditee to discuss and agree on the

observations and recommendations. Option D is not correct because communicating audit observations within the audit report is the final step of the audit process, not the first.
References:
Audit Process Overview1
Communicating Internal Audit Findings: Best Practices for Success2

質問: **202**
データ損失防止(DLP)ツールを導入する上で、最も重要な前提条件は次のうちどれですか？
A. ユーザーに、社内共有ドライブではなく、セキュリティ保護されたフォルダにファイルを保存することを義務付ける
B. データ転送ログをレビューして、データフローの履歴パターンを特定する。
C. DLPポリシーを策定し、ユーザーによる署名付き承認を要求する
D. 既存データの所在を特定し、データ分類マトリックスを確立する
正解: **D (**コメントを発表する**)**
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.

質問: **203**
以下の事業継続活動のうち、重要な機能の復旧を最優先事項としているのはどれですか？
A. 事業継続計画(BCP)のテスト
B. 事業影響分析(BIA)
C. 災害復旧計画(DRP)のテスト
D. リスク評価
正解: **(**正解を表示します**)**
A business impact analysis (BIA) is a process that identifies and evaluates the potential effects or consequences of disruptions or disasters on an organization's critical business functions or processes. A BIA can help prioritize the recovery of critical functions by assessing their importance and urgency for the organization's operations, objectives, and stakeholders, and determining their recovery time objectives (RTOs), which are the maximum acceptable time for restoring a functionafter a disruption. A business continuity

plan (BCP) testing is a process that verifies and validates the effectiveness and readiness of a BCP, which is a document that outlines the strategies and procedures for ensuring the continuity of critical business functions in the event of a disruption or disaster. A BCP testing does not prioritize the recovery of critical functions, but rather evaluates how well they are recovered according to the BCP. A disaster recovery plan (DRP) testing is a process that verifies and validates the effectiveness and readiness of a DRP, which is a document that outlines the technical and operational steps for restoring the IT systems and infrastructure that support critical business functions in the event of a disruption or disaster. A DRP testing does not prioritize the recovery of critical functions, but rather evaluates how well they are supported by the IT systems and infrastructure according to the DRP. A risk assessment is a process that identifies and analyzes the potential threats and vulnerabilities that could affect an organization's critical business functions or processes. A risk assessment does not prioritize the recovery of critical functions, but rather estimates their likelihood and impact of being disrupted by various risk scenarios.

質問**: 204**
IS監査プロジェクトを開始する前に、上級監査責任者が必ず実施しなければならない事項は次のうちどれですか？
A. 監査範囲の承認。
B. 計画立案の現場見学に参加する。
C. 監査計画文書を確認する。
D. 被監査企業の経営陣と面談する。
正解**: (**正解を表示します**)**
The best answer is C. Review audit planning documents.
Before an audit project starts, senior audit leadership must ensure the engagement has been adequately planned. Reviewing planning documents is the control point that lets leadership confirm the objective, scope, risk focus, resourcing, timing, and methodology are appropriate before fieldwork begins. This is the broadest and most essential oversight activity among the choices.
Option A can be part of governance in some audit functions, but direct scope signoff is narrower than review of the full planning package. Option B and D may occur depending on the audit approach, but they are not mandatory leadership actions in every case. The most defensible answer is leadership review of the planning documents because it establishes readiness and oversight before the project begins.
References (Official ISACA):
ISACA, CISA Exam Content Outline - audit planning and execution are structured and risk-based.
ISACA, Now Is the Time for IT Auditors to Perform Advisory Pre-Implementation Reviews - emphasizes engaging leadership and planning around risk and control deficiencies.

ISACA, An Appropriate Approach for Program and Project Management - supports structured planning and oversight before execution.

質問: **205**
組織がビジネス戦略をサポートするために新しい IT システムを取得する場合、内部情報システム監査人の主な機能はどれですか?
A. 重大なITエラーと不正行為の特定
B. リスクとコントロールギャップの緩和の実施
C. システム開発ライフサイクル（SDLC）管理の評価
D. ITリスクとコントロールの評価
正解: **(**正解を表示します**)**

質問: **206**
ITガバナンスは以下によって推進されるべきである：
A. 事業部門の取り組み。
B. バランススコアカード。
C. 方針と基準。
D. 組織戦略。
正解: **D (**コメントを発表する**)**
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.

質問: **207**
アプリケーションが個々のエンドユーザーアカウントを使用して基盤となるデータベースにアクセスする場合、以下のうち最も重大なリスクはどれですか？
A. データベースへの接続が複数回行われ、処理が遅くなります。
B. ユーザーアカウントは、解約後もアクティブなままになる場合があります。
C. ユーザーがアプリケーションの制御を回避できる可能性があります。
D. アプリケーションが完全な監査証跡を記録できない可能性があります。
正解: **C (**コメントを発表する**)**
The most significant risk when an application uses individual end-user accounts to access the underlying database is that users may be able to circumvent application controls. Application controls are the policies, procedures, and mechanisms that ensure the accuracy, completeness, validity, and authorization of transactions and data within an application. Application controls can include input validation, output verification, processing logic, reconciliation, exception handling, and audit trails. Application controls can help prevent or detect errors, fraud, or unauthorized access or modification of data.

However, if an application uses individual end-user accounts to access the underlying database, it means that the users have direct access to the database without going through the application layer. This can expose the database to potential risks such as:
Users may be able to bypass the application controls and manipulate the data in the database directly using SQL commands or other tools. For example, users may be able to change their own or others' salaries, grades, or balances without proper authorization or validation.
Users may be able to access or disclose sensitive or confidential data that they are not supposed to see or share. For example, users may be able to view other users' personal information, passwords, or credit card numbers.
Users may be able to introduce errors or inconsistencies in the data by entering invalid or incorrect data or by deleting or modifying existing data. For example, users may be able to create duplicate records, break referential integrity, or cause data loss or corruption.
Users may be able to compromise the security and performance of the database by creating unauthorized objects, granting excessive privileges, executing malicious code, or consuming excessive resources. For example, users may be able to create backdoors, viruses, or denial-of-service attacks.
Therefore, using individual end-user accounts to access the underlying database can pose a serious threat to the integrity, confidentiality, availability, and reliability of the data and the application.
The other options are not as significant as option C. Multiple connects to the database are used and slow the process is a performance issue that can affect the efficiency and responsiveness of the application and the database, but it does not necessarily compromise the data quality or security. User accounts may remain active after a termination is a security issue that can increase the risk of unauthorized access or misuse of data by former employees or others who have access to their credentials, but it can be mitigated by implementing proper account management and monitoring processes.
Application may not capture a complete audit trail is a compliance issue that can affect the accountability and traceability of transactions and data within the application and the database, but it does not directly affect the data accuracy or protection.
References:
Should application users be database users? - Stack Overflow1
An Approach Toward Sarbanes-Oxley ITGC Risk Assessment - ISACA2
ISACA CISA Certified Information Systems Auditor Exam ... - PUPUWEB3
Why inactive accounts are a security risk | Stratosphere4

質問**: 208**
ソフトウェア開発ライフサイクルのどの段階で、アプリケーション制御に関する議論を開始するのが最適でしょうか？
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確定しました

C. テストシナリオが設計され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
正解: **(**正解を表示します**)**
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 and Explanations Database - 12 Month Subscription2 What Is Application Control? | McAfee3 What Is Application Lifecycle Management? | Red Hat4

質問: **209**
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示す最も適切な兆候は次のうちどれですか？
A. 文書化されていない運用手順
B. 職務分担の欠如
C. ユーザーリクエストのバックログが過剰です
D. 主要業績評価指標(KPI)の欠如
正解: **C (**コメントを発表する**)**
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

質問: **210**
コンピュータフォレンジック監査が最も重要となるのは、次のうちどの状況でしょうか？
A. IT環境における管理体制の不備
B. トランザクションデータの不一致
C. サーバーパッチが不足しています
D. サーバーへのハッキングによるデータ損失
正解: **(**正解を表示します**)**

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, orsystem 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

質問: **211**
情報セキュリティ管理システムの主な目的は次のうちどれですか？
A. 情報セキュリティインシデントの根本原因を特定し、排除する
B. 情報セキュリティインシデントの監視に使用されるレポートの効果を高めるため
C. 情報セキュリティポリシーと手順を最新の状態に保つ
D. 情報セキュリティインシデントの発生頻度と影響を軽減する
正解: **(**正解を表示します**)**
The main purpose of an information security management system (ISMS) is to reduce the frequency and impact of information security incidents. An ISMS is a systematic approach to managing information security risks, policies, procedures, and controls within an organization. An ISMS aims to ensure the confidentiality, integrity, and availability of information assets, as well as to comply with relevant laws and regulations. The other options are not the main purpose of an ISMS, but rather some of its possible benefits or components. References:
CISA Review Manual (Digital Version), Chapter 7, Section 7.11
CISA Review Questions, Answers and Explanations Database, Question ID 205

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu 「**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **212**
内部サーバーへのアクセス不能を引き起こし、通常の業務運営を阻害するような事態が発生した場合、最初に行うべきことは次のうちどれですか？
A. サーバーに対する攻撃者のさらなる行動を防ぐため、すべての電源ケーブルを直ちに抜いてください。

B. 影響を受けるサーバー上のすべてのキーディレクトリとファイルをコピーし、コピーのハッシュ値を生成します。
C. 影響を受けるサーバーのビットレベルのコピーを作成し、コピーのハッシュ値を計算します。
D. サーバーの日付、時刻、場所、および最後に使用した人物を記録してください。
正解: **C** (コメントを発表する)

質問: **213**
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
正解: (正解を表示します)
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.

質問: **214**
IS監査担当者が組織のインシデント管理プロセスと手順をレビューしています。監査担当者が最も懸念すべき事項は次のうちどれでしょうか?
A. インシデント検出が効果的でない
B. インシデントの分類が不適切
C. インシデントの優先順位付けが効果的でない
D. インシデント後の検証が効果的でない
正解: (正解を表示します)

質問: **215**
アプリケーションインターフェースのエラーを迅速に特定するための最適なテスト方法はどれですか？
A. 統合テスト
B. 回帰テスト
C. 自動テスト
D. ユーザー受け入れテスト (UAT)
正解: **(正解を表示します)**
The best testing approach to facilitate rapid identification of application interface errors is automated testing.
Automated testing is the use of software tools or scripts to execute predefined test cases, compare expected and actual outcomes, and report any discrepancies. Automated testing can help to speed up the testing process, increase test coverage, reduce human errors, and improve test accuracy and consistency. Automated testing can also help to detect interface errors that may occur due to incompatible data formats, communication protocols, or system configurations. References:
CISA Review Manual (Digital Version), Chapter 3, Section 3.3.11
CISA OnlineReview Course, Domain 2, Module 2, Lesson 1

質問: **216**
適切に分離されたIT環境において、ネットワーク管理者の権限から制限すべき項目は次のうちどれですか？
A. アプリケーションの既存の構成を変更する
B. ネットワークポートの強化
C. 送信プロトコルが正しく機能していることを確認する
D. ネットワークトラフィックの監視
正解: **A (コメントを発表する)**

質問: **217**
以下のパラメータのうち、サービス中断を経験した組織のリスク閾値を反映しているのはどれですか？
A. 最大許容停電時間 (MTO)
B. リカバリポイント目標(RPO)
C. サービス提供目標 (SDO)
D. 許容中断ウィンドウ(AIW)
正解: **(正解を表示します)**
Maximum Tolerable Outage (MTO) (A) defines the longest time an organization can tolerate an IT service being unavailable before significant business impact occurs. It determines business continuity planning and disaster recovery strategies.
Other options:

RPO (B) defines acceptable data loss but does not determine the total outage limit.
SDO (C) is related to service agreements but does not set the risk threshold.
AIW (D) is similar to MTO but is not as commonly used in disaster recovery planning.
Reference: ISACA CISA Review Manual, Information Systems Operations and Business Resilience

質問: **218**
次のうち、デジタル署名を最も適切に説明しているのはどれですか？
A. それは受信機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. これは、それを使用する送信者固有のものです。
正解: **(**正解を表示します**)**
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 and 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

質問**: 219**
監査証拠の有用性を判断する際に、最も重要な考慮事項は次のうちどれですか？
A. 収集された証拠の性質
B. 証拠のタイミング
C. IS監査担当者の能力
D. レビューの全体的な目的
正解**: D (**コメントを発表する**)**

質問**: 220**
組織が設備利用率のしきい値を設定し、しきい値を超えた場合を監視します。この活動によって最も適切にサポートされるのは次のうちどれですか？
A. 誠実さ
B. 利用可能性
C. 機密保持
D. 否認防止
正解**: (**正解を表示します**)**
Monitoringcapacity utilizationsupportsavailabilityby ensuring thatresources remain functional and do not exceed operational limits.
Option A (Incorrect):Integrityensures that data isaccurate and unaltered, but monitoring capacity thresholds primarily relates tosystem availability.
Option B (Correct):Availabilityensures that systems remainaccessible and functional, and monitoring capacity utilization helpsprevent downtimeandservice disruptions.
Option C (Incorrect):Confidentialityensures that data isprotected from unauthorized access, which is unrelated to capacity monitoring.
Option D (Incorrect):Nonrepudiationensures that actions can betraced to specific individuals, but it does not relate tocapacity monitoring.

Reference:ISACA CISA Review Manual -Domain 4: Information Systems Operations and Business Resilience- Coverscapacity planning and monitoring for system availability.

質問: **221**
以下のうち、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. すべてのプロジェクトにIT要件を組み込んだアクションプラン
B. 管理策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. 企業戦略を支援するIT戦略計画
正解: **(**正解を表示します**)**

質問: **222**
IT関連の顧客サービスプロジェクトをレビューするIS監査担当者にとって、以下のうちどれが最も懸念されるでしょうか？
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用語で表現されます。
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. この組織は、提案されたサービスを最初に提供する組織となるでしょう。
正解: **(**正解を表示します**)**

質問: **223**
以下のITサービス管理活動のうち、ネットワーク遅延が繰り返し発生する根本原因の特定に最も役立つ可能性が高いのはどれですか？
A. 変更管理
B. 問題管理
C. インシデント管理
D. 構成管理
正解: **(**正解を表示します**)**
Problem management is an IT service management activity that is most likely to help with identifying the root cause of repeated instances of network latency. Problem management involves analyzing incidents that affect IT services and finding solutions to prevent them from recurring or minimize their impact. Change management is an IT service management activity that involves controlling and documenting any modifications to IT services or infrastructure. Incident management is an IT service management activity that involves restoring normal service operation as quickly as possible after an incident has occurred.
Configuration management is an IT service management activity that involves identifying and maintaining records of IT assets and their relationships. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 334

質問: **224**
ストレージメディアが限られている場合、以下のバックアップ方式のうちどれが最適な選択肢でしょうか？
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
正解: **(**正解を表示します**)**
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

質問: **225**
外部監査では、過去の同様の内部監査では例外が報告されていなかったにもかかわらず、ユーザー解約プロセスにおいて繰り返し例外が指摘されています。IS監査担当者が今後内部監査プロセスを改善するために取るべき最善の行動は次のうちどれでしょうか？
A. コントロール自己評価(CSA)の結果を確認します。
B. 内部監査のサンプリング方法論を見直してください。
C. ユーザー解約プロセスの変更点を確認してください。
D. 今後のすべての監査にユーザー終了プロセスを含める。
正解: **B (**コメントを発表する**)**

質問: **226**
従業員による不適切な行為のリスクを軽減するために、最も効果的な対策は次のうちどれですか？
A. ユーザーアクティビティの監視
B. 二段階認証
C. ネットワークセグメンテーション
D. アクセス再認証
正解: **A (**コメントを発表する**)**
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
Whatis 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

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu **1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **227**
ある組織が機密データを含むシステムを廃棄するため、ハードディスクからすべてのファイルを削除しました。
IS監査担当者は、以下の理由から懸念すべきである。
A. 削除されたデータは簡単に復元できません。
B. ファイルを論理的に削除しても、ファイルの物理データは上書きされません。
C. ファイルのバックアップコピーも削除されませんでした。
D. 個別にすべてのファイルを削除するよりも、ハードディスクをフォーマットする方が効率的です。
正解: **(**正解を表示します**)**
An IS auditor should be concerned because deleting the files logically does not overwrite the files' physical data. Deleting a file from a hard disk only removes the reference or pointer to the file from the file system, but does not erase the actual data stored on the disk sectors. The deleted data can still be recovered using special tools or techniques until it is overwritten by new data. This poses a risk of data leakage, theft, or misuse if the hard disk falls into the wrong hands. To securely dispose of a system containing sensitive data, the hard disk should be wiped or sanitized using methods that overwrite or destroy the physical data beyond recovery. References:
CISA Review Manual (Digital Version)
CISA Questions, Answers and Explanations Database

質問: **228**
プロジェクトチームは、既存の業務アプリケーションの代替となるものを開発するために、アジャイル開発手法に切り替えることを決定しました。IS監査担当者は、保護監査の有効性を確保するために、まず次のうちどれを行うべきでしょうか？
A. アジャイルプロセスを従来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. 採用される具体的なアジャイル手法を理解する。
D. ビジネスプロセスオーナーにインタビューを行い、ビジネス要件のリストを作成する
正解: **C** (コメントを発表する)
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 and Explanations Database, Question ID 211

質問: **229**
災害復旧計画(DRP)のテストを行うための以下の手順のうち、最も効果的なものはどれですか？
A. 復旧時間と復旧ポイント目標の見直し
B. 文書化されたバックアップおよびリカバリ手順を確認する
C. 四半期ごとの机上演習の実施
D. オフサイトのデータバックアップを使用してセカンダリサイトでテストを実施
正解: (正解を表示します)

質問: **230**
データベースのセキュリティを確認する情報システム監査人は、データベース管理者(DBA) が次のような場合、最も懸念すべきです。
A. アクセス ロールを承認します。
B. 回復手順を実行します。
C. データベースのロックを解決します。
D. データベースのパフォーマンスを評価します。
正解: (正解を表示します)

質問: **231**
ソフトウェア開発におけるウォーターフォール型ライフサイクルモデルは、次のうち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. このプロジェクトは時間的な制約を受けています。
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、新しい技術が活用されます。

正解: **A (**コメントを発表する**)**
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.

質問: **232**
内部監査部門が最近、品質保証(QA)プログラムを確立しました。QAプログラムの要件として含めるべき最も重要な活動は次のうちどれですか？
A. 長期的な内部監査リソース計画
B. 監査活動の継続的なモニタリング
C. 事業部門からのユーザー満足度レポートの分析
D. 内部監査スタッフからのフィードバック
正解: **(**正解を表示します**)**
Ongoing monitoring of the audit activities is the most important activity to include as part of the quality assurance (QA) program requirements for an internal audit department. An IS auditor should perform regular reviews and evaluations of the audit processes, methods, standards, and outcomes to ensure that they comply with the QA program objectives and criteria. This will help to maintain and improve the quality and consistency of the audit services and deliverables. The other options are less important activities to include as part

of the QA program requirements, as they may involve long-term resource planning, user satisfaction reports, or feedback from internal audit staff. References:
CISA Review Manual (Digital Version), Chapter 2, Section2.61
CISA Review Questions, Answers and Explanations Database, Question ID 224

質問: **233**
組織内の内在リスクについて、最も包括的な情報を提供するのは次のうちどれですか？
A. リスク評価。
B. リスクベースの監査結果。
C. ピアベンチマーク。
D. 事業影響分析(BIA)
正解: **(**正解を表示します**)**
The correct answer is A. Risk assessments.
Risk assessments provide the most comprehensive information about inherent risk because they identify and evaluate risks before considering the effect of controls. Inherent risk is the level of risk that exists naturally in a process, system, or activity before controls are applied.
Option B is not the best answer because risk-based audit findings usually reflect specific issues found during audits. They may not cover all inherent risks across the organization.
Option C is not the best answer because peer benchmarking compares the organization with others, but it does not provide a complete view of the organization's own inherent risk.
Option D is not the best answer because a BIA focuses on the impact of disruptions to business processes and resources. It is valuable for resilience planning, but it is not as comprehensive as enterprise or IT risk assessments for inherent risk.
ISACA's glossary defines risk assessment as a process used to identify and evaluate risk and its potential effects. ISACA's CISA Exam Content Outline also includes risk management, risk assessment, and IT risk reporting under Governance and Management of IT.
References: ISACA CISA Exam Content Outline, Domain 2; ISACA Interactive Glossary, "Risk assessment" and "Inherent risk."

質問: **234**
情報資産分類の主な利点は以下のとおりです。
A. 資産の損失を防ぎます。
B. 組織目標の整合に役立ちます。
C. 予算編成の精度向上に役立ちます。
D. リスク管理の意思決定を可能にする。
正解: **(**正解を表示します**)**
The primary benefit of information asset classification is that it enables risk management decisions.

Information asset classification helps to identify the value, sensitivity and criticality of information assets, and to determine the appropriate level of protection and controls required for them. This facilitates risk assessment and risk treatment processes, and ensures that information assets are aligned with business objectives and regulatory requirements. Preventing loss of assets, helping to align organizational objectives or facilitating budgeting accuracy are secondary benefits of information asset classification, but not the main purpose. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 300

質問: **235**
仮想化環境の利用に関連する最大のリスクは次のうちどれですか？
A. オペレーティングシステムの変更機能が制限される場合があります。
B. ゲストに割り当てる処理能力が不足している可能性があります。
C. セッションハイジャックの可能性が高まる可能性があります。
D. ホストはシステム内の潜在的な単一障害点となる可能性があります。
正解: **D (**コメントを発表する**)**

質問: **236**
侵入テストサイクルのどの段階で、テスターは特定された脆弱性を利用してターゲットシステムへのアクセスを試みますか？
A. 漏出
B. 悪用
C. 偵察
D. スキャン中
正解: **B (**コメントを発表する**)**
Exploitationis the phase where testersleverage identified vulnerabilitiestogain unauthorized accessto systems.
Exploitation (Correct Answer - B)
Attackers use techniques such as SQL injection, buffer overflow, or privilege escalation.
Example:A tester exploits a weak password to gain admin access.
Exfiltration (Incorrect - A)
The process of stealing dataaftergaining access.
Reconnaissance (Incorrect - C)
The initial stage where attackers gather information about the target.
Scanning (Incorrect - D)
Involves identifying open ports and services but does not involve actual attacks.
References:
ISACA CISA Review Manual
NIST 800-115 (Technical Guide to Security Testing)

質問: **237**
以下のうち、事業継続計画(BCP)と災害復旧計画(DRP)の主な違いを明確に示しているのはどれですか？
A. 年間の試験要件
B. システム復旧に重点を置く
C. プラン有効化までの期間
D. 上級管理職の関与
正解: **C (**コメントを発表する**)**
The primary difference between a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP) lies in their timeframe for activation and overall scope.
BCP (Business Continuity Plan):
Focuses on ensuring that critical business processes continue operating during and after a disruption.
It includes strategies for maintaining operations (e.g., alternative work locations, manual procedures, supplier dependencies).
Activated immediately when a disruption occurs to keep the business running.
DRP (Disaster Recovery Plan):
Primarily focuses on the recovery of IT systems and infrastructure after a disruption.
It includes steps for restoring data, servers, and applications to bring IT operations back to normal.
Activated after the disaster event to restore normal IT operations.
The timeframe for activation is the key difference because:
BCP is implemented immediately to ensure business continuity.
DRP is implemented after the disaster to restore IT operations.
A). The annual testing requirements # Both BCP and DRP require regular testing, so this is not the key differentiator.
B). The focus on system recovery # Only DRP focuses on system recovery, but the BCP covers more than just IT. The key difference is still the timeframe.
D). The involvement of senior management # Senior management is involved in both plans, so this is not the primary distinction.
References:ISACA CISA Review Manual, 28th Edition, Chapter 4: Information Systems Operations and Business Resilience

質問: **238**
IS監査担当者が、複数の地域にデバイスとシステムを持つ組織のログ管理システムを評価しています。監査担当者が検証すべき最も重要な項目は次のうちどれですか？
A. ログファイルは同時に更新されます。
B. ログファイルは複数の場所で確認されます。
C. ログファイルは暗号化され、デジタル署名されています。
D. サーバーのログファイルが同期されました。

正解: **C** (コメントを発表する)

質問: **239**
アプリケーションの設計に深く関わったIS監査担当者が、そのアプリケーションのレビューを依頼された。監査担当者は以下のことを行うべきである。
A. 利益相反を避けるため、割り当てを拒否する。
B. アプリケーションの知識を使用して監査を実施する。
C. 監査管理部門に以前の関与を通知する。
D. 監査の範囲を変更します。
正解: **C** (コメントを発表する)
The IS auditor should inform audit management of the earlier involvement in designing the application. This is to ensure that there is no conflict of interest or bias that may affect the objectivity or independence of the audit. Audit management can then decide whether to assign a different auditor or to proceed with the same auditor with appropriate safeguards. The other options are not appropriate for the IS auditor to do in this situation. Refusing the assignment to avoid conflict of interest is an extreme measure that may not be necessary or feasible, especially if there are no other qualified auditors available. Using the knowledge of the application to carry out the audit is risky, as it may lead to overlooking or ignoring potential issues or errors in the application. Modifying the scope of the audit is not advisable, as it may compromise the quality or completeness of the audit. References: CISA Review Manual (Digital Version), Chapter 2, Section 2.1

質問: **240**
オープンソースベースのソリューションを使用する最大の利点は、以下の点です。
A. 明確に定義されたサポートレベルを持つ。
B. 簡単に実装できます。
C. ベンダーへの依存度を減らす。
D. より優れたセキュリティ機能を提供する。
正解: (正解を表示します)
Open-source solutions provide flexibility and reduce vendor lock-in, allowing organizations to modify, enhance, and support software independently.
Option A (Incorrect):Open-source software often lacksformalizedsupport levels compared to proprietary solutions, which provide structured SLAs (Service Level Agreements).
Option B (Incorrect):While some open-source solutions are user-friendly, implementation complexity depends on the software and required customization.
Option C (Correct):A key benefit of open-source solutions is thefreedom from vendor dependence.
Organizations can customize the software, hire independent developers, or switch providers without being locked into a specific vendor ' s ecosystem.

Option D (Incorrect):Security in open-source software depends on the community and organization managing the solution. Some open-source tools have excellent security, while others may require additional hardening.
Reference:ISACA CISA Review Manual -Domain 4: Information Systems Operations and Business Resilience- Covers software licensing, vendor dependency, and support considerations.

質問: **241**
組織が市場で入手可能な製品からソフトウェアを購入することを決定したときに、実装を成功させるために最も重要なのは次のどれですか。
A. 要件定義
B. 実装後のレビュー
C. サポートおよびメンテナンス契約
D. ソフトウェアエスクロー
正解: **(**正解を表示します**)**
Defining clear, comprehensive, and testable requirements is critical before selecting and implementing a software product. Without well-documented requirements, the risk of choosing a solution that does not align with business needs increases significantly. A support contract (C) is important for long-term use, and escrow (D) may protect against vendor insolvency, but neither ensures that the product fits the organization's objectives. A post-implementation review (B) only evaluates success after implementation, which may be too late to correct fundamental misalignment. ISACA's COBIT framework (BAI03 and BAI05) stresses the importance of requirements gathering as the foundation for effective solution acquisition and development.
References (ISACA): COBIT 2019, BAI03 Managed Solutions Identification and Build; BAI05 Managed Organizational Change.

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu 「**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **242**
支払い取引データが適切なユーザーのみにアクセス可能であることを保証するための最良の方法は、次のうちどれですか？
A. 二要素認証の実装

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
正解: **(**正解を表示します**)**
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 orpurpose 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.

質問: **243**
IS監査担当者が、複数のアプリケーションの処理を単一の大型サーバーに統合するという決定をレビューしています。この決定による最も重要な影響は次のうちどれですか？
A. オペレーティングシステムのライセンス料の値上げ
B. サーバー障害の影響を受けたアプリケーションがさらに増加
C. 簡素化された資産管理
D. 脆弱性スキャンを必要とするアプリケーションサーバーの減少
正解: **(**正解を表示します**)**
Consolidating multiple applications on asingle serverincreases the risk that aserver outagewillimpact multiple applicationssimultaneously.
More Applications Affected by Outage (Correct Answer - B)
Asingle point of failurecoulddisrupt multiple services.
Example:If aconsolidated server crashes, all hosted applications gooffline.
Higher OS License Fees (Incorrect - A)
License feesmay increase, butdowntime risk is a greater concern.
Simplified Asset Management (Incorrect - C)

True, butdoes not outweigh the availability risk.
Fewer Vulnerability Scans (Incorrect - D)
Reducing the number of serversdoes not reduce security risks.
References:
ISACA CISA Review Manual
NIST 800-160 (System Security Engineering)

質問: **244**
可用性が最優先事項である環境において、IS監査担当者がパッチ管理手順をレビューする際に、最も重視すべき点は何でしょうか？
A. 展開前の包括的なテスト
B. 展開前の有効性認証
C. すべてのサーバーへのデプロイ自動化
D. 導入チームの技術スキル
正解: **(**正解を表示します**)**

質問: **245**
インターネットトラフィックを不正なウェブサイトにリダイレクトする攻撃を軽減するための最適な対策は、次のうちどれですか？
A. 定期的にユーザーセキュリティ意識向上トレーニングを実施する。
B. 強力なウェブブラウザのセキュリティ制御を適用します。
C. ドメインネームシステム(DNS)サーバーのセキュリティ強化を実行します。
D. Webアプリケーションファイアウォール(WAF)を実装します。
正解: **(**正解を表示します**)**
The best answer is C.
ISACA's glossary defines DNS poisoning as a cyberattack that alters DNS records to redirect users to fraudulent websites. Since the attack mechanism is DNS manipulation, the strongest control among the choices is DNS server security hardening. That directly addresses the infrastructure being targeted.
Option A can reduce user susceptibility but does not directly prevent redirection attacks. Option B can help at the endpoint, but it does not address poisoned or compromised DNS infrastructure as directly as DNS hardening. Option D is designed mainly to protect web applications from HTTP-layer attacks, not to stop DNS-based traffic redirection.
References (Official ISACA):
ISACA Glossary, Domain name system (DNS) poisoning.

質問: **246**
組織の情報セキュリティ管理をレビューする際に、最も重要な発見事項は何ですか？
A. 専任の警備員はいません
B. 情報セキュリティ管理システムの公式な管理者は存在しません

C. 脅威と脆弱性を特定するための定期的な評価は実施されていない。
D. 従業員の意識向上トレーニングおよび教育プログラムはありません。
正解: **(**正解を表示します**)**
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.

質問: **247**
ITリスク評価を実施する際に、最初に行うべき手順は次のうちどれですか？
A. 潜在的な脅威を特定します。
B. 脆弱性を評価する。
C. 保護対象となる資産を特定します。
D. 実施されている管理策を評価する。
正解: **(**正解を表示します**)**
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 and Management of IT, Section 2.3: IT Risk Management

質問: **248**
情報システム監査人が週次ユーザーアクセスレビューの運用効率を監査しています。サンプルとして抽出した5件の週次レビューのうち、1件に署名または日付が記入されていませんでした。この観察結果を指摘事項として記録する主な理由は何ですか？
A. レビューは正確ではない可能性があります。
B. レビューに適切な内容が含まれていない可能性があります。
C. レビューは業界標準に準拠していない可能性があります。

D. レビューが実行されていない可能性があります。
正解: **(**正解を表示します**)**
Evidence of a control's performance must be verifiable. A missing signature or date means there is no confirmation that the review was actually performed. This undermines the completeness and reliability of the control. Accuracy (A) and content (B) relate to quality but do not address the missing attestation. Industry standards (C) may be relevant, but the auditor's main concern is that the absence of sign-off creates doubt about whether the control occurred at all. ISACA audit guidance highlights that sufficient and appropriate evidence is required to support the conclusion that a control is operating as designed. References (ISACA): ISACA Standards - Evidence Collection; ISACA ITAF Guidelines.

質問: **249**
侵入検知システム(IDS)の機能性をレビューする際、情報セキュリティ監査担当者が最も懸念すべき点は以下のとおりです。
A. システムによってブロックされた正当なパケットが増加しました
B. 実際の攻撃は確認されていません
C. 検出されたイベントが増加しました
D. 偽陽性が報告されています
正解: **(**正解を表示します**)**
The main purpose of an IDS is to detect and report malicious or suspicious activity on a network or a host. If an IDS fails to identify actual attacks, it means that the IDS is not functioning properly or effectively, and it exposes the organization to serious security risks and potential damage. This is the most concerning scenario for an IS auditor, as it indicates a major deficiency in the IDS performance and configuration. ReferencesWhat is an intrusion detection system (IDS)?What is Intrusion Detection Systems (IDS)?How does it Work?When reviewing an intrusion detection system (IDS), an IS auditor ...Intrusion Detection Systems (IDS)-An Overview with a Generalized ...An overview of issues in testing intrusion detection systems - NISTA Review of Intrusion Detection Systems and Their ...

質問: **250**
災害復旧戦略を策定する際に、最も重要な考慮事項は次のうちどれですか？
A. 確認応答までの平均時間
B. 平均復旧時間(MTTR)
C. 最大許容ダウンタイム(MTD)
D. 最大故障間隔(MTBF)
正解: **(**正解を表示します**)**

質問: **251**

情報システム監査人が、複数の地域にオフィスを持つ組織の災害復旧計画（DRP）をレビューしています。監査人が主に注力すべき項目は次のうちどれですか？
A. 復旧ポイント目標（RPO）の監視
B. プロセスとシステムの依存関係
C. 災害復旧訓練
D. データのバックアップとストレージの変更
正解: **(正解を表示します)**
Comprehensive and Detailed Explanation:
For organizations with multiple regional offices, the primary audit focus should be on processes and system dependencies. Dependencies determine recovery sequencing, resource prioritization, and interconnectivity between systems across regions.
* RPO monitoring (A): Important but a subset of overall recovery planning.
* Training (C): Necessary but not the first priority when evaluating plan adequacy.
* Data backup/storage (D): Technical component but less comprehensive than analyzing dependencies.
# ISACA Reference: CISA Review Manual 27th Edition, Domain 2, section on disaster recovery planning and interdependencies.

質問: **252**
年次監査計画プロセスの一環として、以下のうちどれを必ず完了する必要がありますか？
A. 事業継続性分析
B. 業界ベンチマーク
C. リスク評価
D. リスク管理マトリックス
正解: **(正解を表示します)**
A risk assessment must be completed as part of annual audit planning. ISACA's ITAF-based guidance states that the IS audit and assurance function shall use an appropriate risk assessment approach and supporting methodology to develop the overall IS audit plan and determine priorities for effective allocation of audit resources.
Option C is correct because audit planning is fundamentally risk-based under ISACA guidance. Annual planning requires identifying and prioritizing risk areas so the audit plan focuses on the areas of greatest significance. ISACA also notes that, before creating the annual audit plan, the organizationwide risk register should be reviewed thoroughly to prioritize risk areas.
Option A may inform audit planning in some organizations, but it is not a universal required planning step.
Option B can be useful, but it is optional and supplementary, not mandatory.
Option D is typically developed at the engagement level for specific audits rather than as a mandatory organizationwide annual planning deliverable.
Therefore, C is the best answer because risk assessment is the required foundation of the annual audit plan under ISACA guidance.

References (Official ISACA):
* ISACA Journal, Developing the IT Audit Plan Using COBIT 2019 - ITAF requires an appropriate risk assessment approach to develop the overall IS audit plan.
* ISACA Journal, Auditing and Digital Transformation Are at a Crossroads - before creating the annual audit plan, the organizationwide risk register should be reviewed thoroughly.
* ISACA, Certification Exam Candidate Guide - includes evaluation of audit processes and quality programs, supporting structured audit planning.

質問: **253**
自宅勤務やオフィス勤務と比較して、場所を選ばずに働くシナリオにおいて、IS監査担当者が最も懸念すべき事項は次のうちどれでしょうか？
A. 標的型フィッシング攻撃に対する脆弱性
B. 安全でない設定の無線ネットワークの使用
C. 公共の場所における不十分な物理的セキュリティ対策
D. 脆弱なパスワードと認証方法の使用
正解: **(**正解を表示します**)**

質問: **254**
情報システム監査担当者は、業務上重要なアプリケーションに現在、耐障害性が全く備わっていないことを指摘した。
この状況において、最も懸念される点は次のうちどれですか？
A. サービスの低下
B. 損傷に対する許容範囲が限られている
C. 平均故障間隔(MTBF)の低下
D. 単一障害点
正解: **(**正解を表示します**)**
The greatest concern with this situation is that a business-critical application does not currently have any level of fault tolerance and thus has a single point of failure. A single point of failure is a component or element of a system that, if it fails, will cause the entire system to stop functioning. Fault tolerance is the ability of a system to continue operating without interruption or degradation in the event of a failure of one or more of its components or elements. Fault tolerance can be achieved by using techniques such as redundancy, replication, backup, or failover. A business-critical application should have a high level of fault tolerance to ensure its availability, reliability, and continuity. References:
CISA Review Manual (Digital Version), Chapter 5, Section 5.51
CISA Online Review Course,Domain 3, Module 3, Lesson 22

質問: **255**
以下のうち、効果的なIT投資管理を示す最良の指標はどれですか？
A. IT投資は、システム開発ライフサイクル(SDLC)に従って実施および監視されます。

B. IT投資は特定のビジネス目標に紐づけられています
C. IT投資を必要とする各事業について、主要業績評価指標(KPI)が定義されます。
D. IT投資予算は業界ベンチマークを大幅に下回っている。
正解: **(正解を表示します)**
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 systemsand 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.

質問: **256**
IS監査担当者は、注文処理システムのトランザクション処理時間がメジャーリリース後に大幅に増加したことに気づきました。IS監査担当者は、次のうちどれを最初に確認すべきでしょうか？
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
正解: **(正解を表示します)**
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 systemperforms 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 (DigitalVersion), Chapter 3, Section 3.3

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu　**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **257**
効果的なデータ分類プロセスによる最大のメリットは次のうちどれですか？
A. データは機密性に応じて保護されます
B. データに対する適切な所有権が割り当てられています
C. データ保持期間は明確に定義されています
D. データ管理者が特定されました。
正解: **A** (コメントを発表する)

質問: **258**
許可されたアクセス権限の意図しない悪用を軽減するための最も効果的な対策は、次のうちどれですか？
A. 利用規定の年次承認
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
正解: (正解を表示します)

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.

質問**: 259**
企業資源計画(ERP)システムの導入中に、IS監査人がユーザー受け入れテスト(UAT)の結果をレビューしています。監査人が最も重視すべき事項は次のうちどれでしょうか？
A. すべてのエラーがエンドユーザーに伝達されたことを確認してください。
B. ビジネスプロセスのオーナーが結果を承認したかどうかを確認する。
C. システム統合テストが実施されたことを確認します。
D. アプリケーションインターフェースが十分にテストされているかどうかを判断します。
正解**: (**正解を表示します**)**
The correct answer is B. Determine if the business process owner has signed off on the results.
User acceptance testing confirms whether the system meets business requirements and is acceptable for use by the business. For an ERP implementation, business process owners are responsible for validating whether the system supports required business processes, controls, workflows, reports, and transaction processing.
Their signoff is the key evidence that the business accepts the system.
Option A is not the best answer because communicating errors is useful, but it does not prove the system was accepted by the business. Option C is not the best answer because system integration testing is normally performed before or alongside UAT, but UAT focuses on business acceptance. Option D is important in an ERP environment, but interface testing is a technical/system testing concern, not the primary focus of UAT review.
This maps to Information Systems Acquisition, Development and Implementation, because ISACA's CISA Exam Content Outline includes implementation testing, system readiness, requirements validation, and post- implementation activities in Domain 3.
References: ISACA CISA Exam Content Outline, Domain 3; ISACA system implementation and testing control concepts.

質問**: 260**

停電時に許可されていない人物の侵入を防ぎたいデータセンターは、外部アクセスドアを確保する必要があります。
A. 物理キーのバックアップを用意してください。
B. フェイルセーフモードで動作します。
C. フェイルセキュアモードで動作します。
D. 警報が発せられ、監視されます。
正解: **(**正解を表示します**)**
The best answer is C. Operate in fail-secure mode.
If the goal is to prevent unauthorized entry during a power outage, the doors should remain locked when power fails. That is exactly what fail-secure operation is intended to do.
Alarming and monitoring may detect an issue, but they do not themselves prevent entry.
Physical key backup may help authorized access, but it does not address the primary requirement of staying secure during loss of power.
So the strongest answer is fail-secure, because it directly preserves physical access control during an outage.
References (Official ISACA):
* ISACA physical security and access-control terminology resources support layered protection of facilities.

質問: **261**
分散処理環境において、効果的な検出制御を構成するのは次のうちどれですか？
A. 特権アカウントの使用ログが確認されます。
B. ユーザーは電子メールシステムを介して追加のアクセスをリクエストする必要があります。
C. システム全体に対して災害復旧計画 (DRP) が策定されています。
D. パスワードを3回間違えると、ユーザーIDは停止されます。
正解: **(**正解を表示します**)**

質問: **262**
データセンターのIS監査中に、プログラマーが運用プログラムに対して緊急修正を行うことが許可されていることが判明しました。IS監査担当者が行うべき主な推奨事項は次のうちどれでしょうか？
A. プログラマーは、アプリケーション所有者から口頭での同意を得た後にのみ、緊急修正を実装することを許可されるべきである。
B. 変更が事後承認およびテストの対象となるように、バイパスユーザーID手順を導入する必要があります。
C. 緊急時のプログラム変更は、運用システムに適用する前に、プログラム移行およびテスト手順に従う必要があります。
正解: **C (**コメントを発表する**)**

質問: **263**
構成管理システムの主な目的は以下のとおりです。
A. ソフトウェアのアップデートを追跡します。
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. 変更承認を標準化する。
正解: **B (**コメントを発表する**)**
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 and Benefits - ServerWatch

質問: **264**
次のうち、新しいIS監査担当者がIT全体のパフォーマンスを評価する上で最も有用な情報を提供するものはどれですか？
A. IT価値分析
B. 過去の監査報告書
C. ITバランススコアカード
D. 脆弱性評価レポート
正解: **(**正解を表示します**)**
An IT balanced scorecard (BSC) is a performance metric that is used to identify, improve, and control the various functions and outcomes of an IT department or organization. An IT BSC is based on the concept of the balanced scorecard, which was introduced by Robert Kaplan and David Norton in 1992 as a strategic management system that translates the vision and strategy of an organization into measurable objectives and actions. An IT BSC adapts the balanced scorecard framework to the specific needs and goals of the IT function, aligning it with the business strategy and value proposition.

An IT BSC typically consists of four perspectives that help managers plan, implement, and evaluate the IT performance: customer, internal process, learning and growth, and financial. Each perspective defines a set of objectives, measures, targets, and initiatives that reflect the IT contribution to the organization's success. For example, the customer perspective may measure the satisfaction and retention of internal and external customers who use IT services or products; the internal process perspective may measure the efficiency and effectiveness of IT processes such as development, delivery, support, or security; the learning and growth perspective may measure the skills, knowledge, innovation, and culture of the IT staff; and the financial perspective may measure the costs, benefits, and return on investment of IT projects or assets.
An IT BSC provides a new IS auditor with the most useful information to evaluate overall IT performance because it:
Provides a comprehensive and balanced view of the IT function from multiple angles and stakeholders Links the IT objectives and activities to the business strategy and value creation Enables a clear communication and alignment of expectations and priorities among IT managers, staff, customers, and other stakeholders Facilitates a continuous monitoring and improvement of IT performance based on data-driven feedback and analysis Supports a holistic and integrated approach to IT governance, risk management, and compliance Therefore, an IT BSC is a valuable tool for a new IS auditor to assess how well the IT function is fulfilling its mission and delivering value to the organization.
References:
The IT Balanced Scorecard (BSC) Explained - BMC Software
What Is a Balanced Scorecard (BSC), How Is it Used in Business?
Lost in the Woods: COBIT 2019 and the IT Balanced Scorecard - ISACA

質問**: 265**
電力需要の予期せぬ増加が発生しやすい地域において、システムを最も効果的に保護できるのは次のうちどれでしょうか？
A. 電圧レギュレータ
B. 回路遮断器
C. 代替電源ライン
D. ジェネレーター
正解**: A (**コメントを発表する**)**

質問**: 266**
コンピューター室に火災警報システムが設置されました。火災警報制御盤の最も効果的な設置場所は、
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室
B. サーバーコンピュータに最も近いコンピュータ室
C. システム管理者室
D. 建物の警備員が使用するブース

正解: **D** (コメントを発表する)
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

質問: **267**
IT戦略とビジネス戦略の整合性を測定するのに最適な指標は次のうちどれですか？
A. 計画されたITプロジェクトの範囲に対するステークホルダーの満足度
B. IT関連リスクを含む企業リスク評価の割合
C. IT関連の役割に満足している統計データの割合
D. ビジネスプロセス能力成熟度評価の頻度
正解: **B** (コメントを発表する)
The best metric to measure the alignment of IT and business strategy is the percentage of enterprise risk assessments that include IT-related risk. This metric indicates how well the organization identifies and manages the IT risks that could affect its strategic objectives and performance. A high percentage of enterprise risk assessments that include IT-related risk shows that the organization considers IT as an integral part of its business strategy and aligns its IT resources and capabilities with its business needs and goals
. References: : CISA Review Manual (Digital Version), Chapter 2: Governance and Management of IT, Section 2.2: IT Strategy, page 67 : CISA Online Review Course, Module 2: Governance and Management of IT, Lesson 2.2: IT Strategy

質問: **268**

情報資産の機密性を保護する際に最も効果的な管理方法は以下のとおりです。
A. 規制要件に関する職員の意識向上研修
B. 二要素認証メカニズムの利用
C. 必要最小限のアクセス制御理念の徹底
D. すべてのユーザーに対する読み取り専用アクセスの設定
正解: **(**正解を表示します**)**

質問: **269**
データ損失防止(DLP)ツールの導入前レビューを実施するIS監査担当者にとって、次のうちどれが最も大きな懸念事項となるでしょうか？
A. この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. 暗号化キーは中央で管理されていません。
正解: **(**正解を表示します**)**
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.

質問: **270**
IS監査担当者が、現在も日常的に使用されているソフトウェアシステムが何年も前の旧バージョンで、サポートが終了していることを発見しました。被監査企業は、ソフトウェアが最新バージョンで稼働するまでに6か月かかると述べています。サポート対象外バージョンのソフトウェアを使用することに伴う差し迫ったリスクを軽減するための最善の方法は次のうちどれですか？
A. ソフトウェアシステムの旧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アクセス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. 古い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。

正解: **D** (コメントを発表する)
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 7of 7: Mitigating Risks of Unsupported Operating Systems) Upgrade, Retire, or Replace Unsupported Software (Part 4 of 7: Mitigating Risks of Unsupported Operating Systems)

質問: **271**
IS監査担当者が組織の内部統制の適切性を検証しており、規制の回避の可能性を懸念しています。次のうち、最も適切なサンプリング方法はどれですか？
A. 変数サンプリング
B. ランダムサンプリング
C. クラスターサンプリング
D. 属性サンプリング
正解: **D** (コメントを発表する)
The best sampling method to use for verifying the adequacy of an organization's internal controls and being concerned about potential circumvention of regulations is B. Random sampling. Random sampling is a method of selecting a sample from a population in which each item has an equal and independent chance of being selected1. Random sampling reduces the risk of bias or manipulation in the sample selection, and ensures that the sample is representative of the population. Random sampling can be used for both attribute and variable sampling, which are two types of audit sampling that test for the occurrence rate or the monetary value of errors, respectively2.

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu 1**605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **272**
IS監査担当者は、社内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。監査担当者は、まずどのフェーズの要件を調査すべきでしょうか？
A. 設定フェーズ
B. ユーザー研修フェーズ
C. 品質保証(QA)フェーズ
D. 開発段階
正解: **(**正解を表示します**)**
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 existinginfrastructure 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

質問: **273**
監査プロジェクトの締め切り日が近づいており、監査マネージャーは監査の完了率が60%に過ぎないことを確認しました。監査マネージャーはまず、次のうちどれを行うべきでしょうか？
A. 遅延が発生した箇所を特定する
B. 監査を補完するために追加のリソースを割り当てる
C. 監査委員会にエスカレーションする
D. 監査期限を延長する
正解: **(**正解を表示します**)**
The first thing that the audit manager should do when faced with a situation where only 60% of the audit has been completed and the due date is approaching is to determine where delays have occurred. This can help the audit manager to identify and analyze the root causes of the delays, such as unexpected issues, scope changes, resource constraints, communication problems, etc., and evaluate their impact on the audit objectives, scope, quality, and timeline. Based on this analysis, the audit manager can then decide on the best course of action to address the delays and complete the audit successfully. Assigning additional resources to supplement the audit is a possible option forresolving delays in an audit project, but it is not the first thing that the audit manager should do, as it may not be feasible or effective depending on the availability, cost, and suitability of the additional resources. Escalating to the audit committee is a possible option for communicating delays in an audit project and seeking guidance or support from senior management, but it is not the first thing that the audit manager should do, as it may not be necessary or appropriate depending on the severity and urgency of the delays. Extending the audit deadline is a possible option for accommodating delays in an audit project and ensuring sufficient time for completing the audit tasks and activities, but it is not the first thing that the audit manager should do, as it may not be possible or desirable depending on the contractual obligations, stakeholder expectations, and regulatory requirements.

質問: **274**
データ分類プロセスを実施する際に、データ所有者が負う最も重要な責任は次のうちどれですか？
A. データに対する緊急変更のレビュー
B. アプリケーションコードの変更を承認する
C. 適切なユーザーアクセスレベルの決定
D. データベーステーブルに対するアクセスルールの実装
正解: **(**正解を表示します**)**

The most important responsibility of data owners when implementing a data classification process is determining appropriate user access levels (option C). This is because:
Data owners are the persons or entities that have the authority and responsibility for the business processes and functions that collect, use, store, and dispose of data1.
Data owners are 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.
Data owners are 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.
Data owners 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.
Determining appropriate user access levels is the most important responsibility of data owners when implementing a data classification process, as it ensures that only authorized and legitimate users can access sensitive or important data. This provides confidentiality, integrity, availability, and accountability of data345.
Reviewing emergency changes to data (option A), authorizing application code changes (option B), and implementing access rules over database tables (option D) are not the most important responsibilities of data owners when implementing a data classification process. These are more related to the operational aspects of data management, which are usually delegated to other roles, such as the DBA or the IT staff. The data owner should oversee and approve these activities, but not perform them directly1.

質問**: 275**
情報システム監査担当者が、組織構造の変更に伴う業務プロセスへの重大な影響を踏まえ、組織の事業継続計画(BCP)をレビューしています。監査担当者が最も懸念すべき事項は次のうちどれでしょうか？
A. 主要なビジネスプロセスのエンドユーザーは、ビジネス影響分析(BIA)に参加しませんでした。
B. 再編以降、BCPのコピーは新しい事業部門のエンドユーザーに配布されていません。
C. BCPのテスト計画は過去2年間完了していません
正解**: (**正解を表示します**)**

A test plan for the BCP is essential to ensure that the plan is effective, updated and aligned with the current business needs and objectives. A change in organizational structure with significant impact to business processes may require a revision of the BCP and a new test plan to validate its adequacy. The lack of a test plan for the BCP for two years indicates a high risk of failure in the event ofa disaster or disruption.
Therefore, this should be the auditor's greatest concern among the given options.
References:
ISACA, IT Control Objectives for Sarbanes-Oxley, 4th Edition, section 5.3.21 ISACA, CISA Review Manual, 27th Edition, chapter 5, section 5.42

質問: **276**
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導入する最も重要な理由は次のうちどれですか？
A. 参照用に古いバージョンが利用可能であることを保証するため
B. アプリケーションの最新の承認済み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. 承認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ため
正解: **(**正解を表示します**)**
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.

質問: **277**
最適なリスク管理戦略を実施した場合、以下のうちどれが最も削減される可能性が高いでしょうか？
A. サンプリングリスク
B. 残存リスク
C. 固有のリスク
D. 検出リスク
正解: **(**正解を表示します**)**
The best answer is B. Residual risk.
ISACA defines residual risk as the amount of risk remaining after controls and mitigation efforts are put in place. Because risk management strategies are implemented to mitigate risk, the type of risk most directly reduced is residual risk. Inherent risk exists before controls are applied, so it is not the risk category most directly reduced by control implementation. Sampling risk and detection risk are audit risks, not the primary target of enterprise risk treatment strategies.
Option C is incorrect because inherent risk is the baseline level of risk absent controls.
Option A and D relate to audit methodology and audit assurance rather than enterprise risk

treatment outcomes. ISACA's risk guidance consistently describes controls and mitigation efforts as mechanisms to reduce remaining exposure to an acceptable level, which is residual risk.
References (Official ISACA):
ISACA Journal, Quantifying the Qualitative Technology Risk Assessment.
ISACA Journal, Risk Assessment and Analysis Methods.
ISACA Journal, From Measurement to Management.

質問: **278**
以下の技術のうち、デバイス間のデータ伝送における最大通信距離が最も短いのはどれですか？
A. Wi-Fi
B. Bluetooth
C. 長期進化 (LTE)
D. 近距離無線通信(NFC)
正解: **(**正解を表示します**)**
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 and300 meters outdoors2. Bluetooth can reach up to 800 feet with Bluetooth5.0 specification3. Long-term evolution (LTE) canreach 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

質問: **279**
電子媒体に保存されている機密データを破壊する最も効果的な方法はどれですか？
A. 消磁
B. ランダムな文字の上書き
C. 物理的破壊
D. 低レベルの書式設定
正解: **C (**コメントを発表する**)**
The most effective method of destroying sensitive data stored on electronic media is physical destruction, which involves breaking, shredding, melting, or incinerating the media to make it unreadable and unrecoverable. Degaussing, random character overwrite, and

low-level formatting are methods of sanitizing or erasing data from electronic media, but they do not guarantee complete destruction of data and may leave some traces that can be recovered by advanced techniques. Therefore, physical destruction is the most secure and reliable method of data disposal for sensitive data. References: CISA Review Manual (Digital Version), Chapter 5: Protection of Information Assets, Section 5.4: Data Disposal

質問: **280**
外部監査会社が、システム導入プロジェクトの妥当性確認および検証レビューを実施するために雇われた。IS監査人は、回帰テストがプロジェクト計画に含まれておらず、システム導入チームによって実施されていないことを指摘した。チームによると、実施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あるとのことだ。監査人は次にどのような行動をとるべきだろうか？
A. 実施されている並行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およびストレステストの実施を推奨します。
C. 並列テストで十分であり、回帰テストは不要であると結論付ける
D. システム実装チームによる回帰テストの実施を推奨します
正解: **(**正解を表示します**)**
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)

質問: **281**
組織のプライバシーポリシーの妥当性を評価するための基準として、情報システム監査人が使用する情報源として最適なのは次のうちどれですか？
A. 過去のプライバシー侵害とその根本原因
B. 世界的に認められたプライバシーのベストプラクティス
C. 地域のプライバシー基準と規制
D. 類似組織のベンチマーク調査
正解: **(**正解を表示します**)**
The best source of information for an IS auditor to use as a baseline to assess the adequacy of an organization' s privacy policy is the local privacy standards and regulations. Privacy standards and regulations are legal requirements that specify how personal data should be collected, processed, stored, shared, and disposed of by organizations. By using local privacy standards and regulations as a baseline, the IS auditor can ensure that the organization's privacy policy complies with the applicable laws and protects the rights and interests of data subjects. Historical privacy breaches and related root causes, globally accepted privacy best practices, and benchmark studies of similar organizations are useful sources of information for improving an organization's

privacy policy, but they are not as authoritative and relevant as local privacy standards and regulations. References: CISAReview Manual (Digital Version): Chapter 2 - Governance and Management of Information Technology

質問: **282**
IT キャパシティ管理プロセスを実装することによる主な利点は次のどれですか?
A. インフラストラクチャが現在のパフォーマンス要件を満たしていることを確認する
B. 新しいソフトウェアアプリケーションの迅速な導入を可能にする
C. 重大なセキュリティ上の懸念の解決を支援する
D. ITサービスの導入にかかるコストと時間を削減
正解: **(正解を表示します)**
Comprehensive and Detailed Explanation:
The primary purpose of IT capacity management is to ensure that IT infrastructure can meet current and future performance requirements in a cost-effective manner.
Option A is correct because it directly relates to capacity management goals.
Option B (rapid deployment) relates more to change management.
Option C (security concerns) is outside the scope of capacity management.
Option D (reducing cost/time) may be a secondary benefit but not the primary objective.
ISACA Reference: CISA Review Manual 27th Edition, Domain 2, section on capacity management and IT service performance.

質問: **283**
組織のデジタルトランスフォーメーションプログラムを監督するために設立された運営委員会は、次のうちどの活動に関与する可能性が最も高いでしょうか？
A. インターフェースコントロールの設計。
B. 要件の文書化。
C. エスカレーションされたプロジェクトの問題のレビュー。
D. プロジェクト進捗報告書の作成。
正解: **(正解を表示します)**
The correct answer is C. Reviewing escalated project issues.
A steering committee provides governance, oversight, prioritization, funding direction, issue escalation, and decision-making support for major initiatives. In a digital transformation program, the steering committee is most likely to review escalated project issues, resolve conflicts, approve major decisions, and ensure the program remains aligned with business objectives.
ISACA guidance on digital transformation governance highlights the importance of project governance frameworks, steering committees, and escalation paths. ISACA also describes executive steering committees as bodies that guide strategy, approve funding, make formal risk decisions, and support clear escalation paths and decision-making protocols.

Option A is not correct because designing interface controls is a technical/system design responsibility.
Option B is usually performed by business analysts, process owners, and project teams.
Option D is usually prepared by the project manager or program manager, although the steering committee may review the status reports.
This question maps to Governance and Management of IT, because steering committees are part of IT governance, strategic oversight, resource allocation, and project/program governance.
References: ISACA CISA Exam Content Outline, Domain 2; ISACA guidance on project governance, steering committees, and escalation paths.

質問: **284**
IT戦略文書をレビューするIS監査担当者にとって、以下のうちどれが最も懸念されるでしょうか？
A. 前年度のIT戦略目標は達成されませんでした。
B. 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。
C. 新規事業の財務見積もりは文書内で開示されています。
D. 戦略的なIT目標は、最新の市場動向のみに基づいて策定されます。
正解: **D (**コメントを発表する**)**
AnIT strategymust bealigned with business objectives, not solely based onmarket trends.
Strategic IT Goals Derived Solely from Market Trends (Correct Answer - D) IT strategy should supportorganizational goals, not justfollow industry trends.
Example:A company investing inAIjust because it'strendy, without considering business needs.
Previous Year's IT Goals Not Achieved (Incorrect - A)
A concern, butdoes not indicate a fundamental strategy flaw.
Target Architecture Defined at a Technical Level (Incorrect - B)
Technical details are important for implementation.
Financial Estimates Included (Incorrect - C)
Cost transparency is agood practice.
References:
ISACA CISA Review Manual
COBIT 2019 (IT Governance)

質問: **285**
IS監査人がIoTデバイスへの不正アクセスを防止するために推奨する最適な方法は次のうちどれですか？
A. IoTデバイスは、デバイスシステムアカウントの使用状況を監視する必要があります。
B. IoT デバイスはアクセス試行をログに記録し、アラートを発するべきである。
C. IoTデバイスは識別と認証を必要とするべきである。

D. IoT デバイスはホスト ネットワークからのみアクセス可能である必要があります。
正解: **(**正解を表示します**)**

質問: **286**
次のうち、探偵のコントロールとなるものはどれですか？
A. データ入力に対するプログラムによる編集チェック
B. バックアップ手順
C. パスカードを使用して物理的な施設にアクセスする
D. ハッシュ合計の検証
正解: **(**正解を表示します**)**
Verification of hash totals is a detective control. A detective control is a control that aims to identify and report errors or irregularities that have already occurred. Verification of hash totals is a technique that compares the hash values of data before and after transmission or processing to detect any changes or corruption. The other options are examples of other types of controls, such as programmed edit checks (preventive), backup procedures (recovery), and use of pass cards (preventive). References: CISA Review Manual, 27th Edition, page 223

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu 1**605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **287**
IS監査担当者は、ある組織がコスト効率の良い方法で必要に応じて新しいサーバーを追加できないことを発見しました。監査担当者の最も適切な推奨事項は次のうちどれですか？
A. 既存システムの容量を増強する。
B. ハードウェアを最新技術にアップグレードする。
C. IT部門の臨時契約社員を雇用する。
D. 仮想環境を構築します。
正解: **(**正解を表示します**)**
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

質問**: 288**
ビジネスとITの連携において、最も大きな課題となるのは次のうちどれですか？
A. 最高情報責任者(CIO)が取締役会に関与していないこと
B. 新規事業プロジェクトを実行するためのIT予算が不足している
C. ビジネス戦略策定における情報セキュリティの関与不足
D. 最高情報責任者(CIO)が議長を務めるIT運営委員会
正解**: A (**コメントを発表する**)**
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 theycanbe addressed by other means such as collaboration, negotiation, or escalation.
References: CISA Review Manual (Digital Version)1, Chapter 1, Section 1.2.1

質問**: 289**
ユーザーから、新しくリリースされた企業資源計画(ERP)システムの動作が遅すぎるとの苦情が寄せられています。品質保証(QA)フェーズで実施された以下のテストのうち、どれがこの問題を特定できたでしょうか？
A. ストレス
B. 回帰
C. インターフェース

D. 統合
正解: **A** (コメントを発表する)
Stress testing is a type of performance testing that evaluates how a system behaves under extreme load conditions, such as high user traffic, large data volumes, or limited resources. It is useful for identifying potential bottlenecks, errors, or failures that may affect the system's functionality or availability. Stress testing during the quality assurance (QA) phase would have identified the concern of users complaining that a newly released ERP system is functioning too slowly. The other options are not as relevant for this concern, as they relate to different aspects of testing, such as regression testing (verifying that existing functionality is not affected by new changes), interface testing (verifying that the system interacts correctly with other systems or components), or integration testing (verifying that the system works as a whole after combining different modules or units). References: CISA Review Manual (Digital Version), Domain 5: Protection of Information Assets, Section 5.4 Testing Techniques1

質問: **290**
年次監査サイクルにおいて、組織のIT部門の監査で多くの問題点が指摘されました。次回の監査を計画する際に、最も重要な考慮事項は次のうちどれでしょうか？
A. すべての指摘事項が是正されるまで、審査を延期する
B. 不十分な領域にレビューを限定する
C. すべての推奨事項が実施されたことを確認します
D. すべての勧告の状況を追跡調査する
正解: **D** (コメントを発表する)
The most important consideration when planning the next audit after many findings is to follow up on the status of all recommendations, as this will ensure that the audit findings are addressed in a timely and effective manner, and that the root causes of the issues are resolved12. Following up on the status of all recommendations will also help to assess the progress and performance of the IT department, and to identify any new or emerging risks or challenges34.
References
1: What to consider when resolving internal audit findings3 2: A brief guide to follow up4 3: Guidance on auditing planning for Internal Audit2 4: Corrective Action Plan (CAP): How to Manage Audit Findings1

質問: **291**
監査結果に関連するフォローアップ活動の適切な期間を設定する際に、最も重要な決定要因は次のうちどれですか？
A. IS監査リソースの可用性
B. 管理回答に含まれる是正措置の日付
C. 事業活動のピーク期間

D. 監査で特定された業務プロセスの複雑性
正解: **(**正解を表示します**)**
The most important determining factor when establishing appropriate timeframes for follow-up activities related to audit findings is the remediation dates included in management responses. The IS auditor should ensure that the follow-up activities are aligned with the agreed-upon action plans and deadlines that management has committed to in response to the audit findings. The follow-up activities should verify that management has implemented the corrective actions effectively and in a timely manner, and that the audit findings have been resolved or mitigated.
The other options are less important factors for establishing timeframes for follow-up activities:
Availability of IS audit resources. This is a practical factor that may affect the scheduling and execution of follow-up activities, but it should not override the priority and urgency of verifying management's corrective actions.
Peak activity periods for the business. This is a factor that may affect the availability and cooperation of auditees during follow-up activities, but it should not delay or postpone the verification of management's corrective actions beyond reasonable limits.
Complexity of business processes identified in the audit. This is a factor that may affect the scope and depth of follow-up activities, but it should not affect the timeframe for verifying management's corrective actions.

質問: **292**
コンプライアンス監査の計画段階で、情報システム監査担当者は、銀行のコンプライアンス要件一覧に、データリスク管理に関する最近の規制変更が含まれていないことを発見しました。監査担当者はまず何をすべきでしょうか？
A. 経営陣に、規制変更がなぜ含まれていないのかを尋ねてください。
B. 法務部門と潜在的な規制上の問題について話し合う
C. 不足している規制更新を最高情報責任者(CIO)に報告してください。
D. 最近の規制変更を監査範囲から除外する。
正解: **(**正解を表示します**)**
Asking management why the regulatory changes have not been included is the first thing that an IS auditor should do during the planning stage of a compliance audit. An IS auditor should inquire about the reasons for not updating the inventory of compliance requirements with recent regulatory changes related to managing data risk. This will help the IS auditor to understand whether there is a gap in awareness, communication, or implementation of compliance obligations within the organization. The other options are not the first things that an IS auditor should do, but rather possible subsequent actions that may depend on management's response. References:
CISA Review Manual (Digital Version), Chapter 2, Section 2.31
CISA Review Questions, Answers and Explanations Database, Question ID 214

質問: **293**
IS監査担当者は、組織の事業継続計画(BCP)が事業戦略と整合しているかどうかを確認したいと考えています。以下のうち、レビューするのに最も役立つのはどれでしょうか？
A. 災害復旧計画(DRP)のテスト結果
B. 事業影響分析(BIA)
C. 企業リスク管理方針
D. 主要業績評価指標(KPI)
正解: **(正解を表示します)**
To ensure that theBCP aligns with business strategy, aBusiness Impact Analysis (BIA)is the most valuable resource.
Option A (Incorrect):DRP testing resultsshow how wellsystems recover, but they do notestablish strategic alignmentwith business priorities.
Option B (Correct):ABIA identifies critical processes, financial impact, and business priorities, ensuring that theBCP is alignedwith strategic goals.
Option C (Incorrect):Thecorporate risk management policyis broader and does not focus onbusiness continuity priorities.
Option D (Incorrect):KPIs measure performance, but they do notdefine business continuity needs.
Reference:ISACA CISA Review Manual -Domain 4: Information Systems Operations and Business Resilience- CoversBCP, BIA, and business continuity alignment.

質問: **294**
IS監査担当者は、ある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、その組織が最近生産工場を閉鎖したことを知りました。監査担当者にとって最適な行動は次のうちどれでしょうか？
A. 事業影響分析(BIA)が組織の構造と状況に合致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、それらがBCPにどのように影響するかを判断します。
C. 回復時間目標 (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する。
正解: **(正解を表示します)**
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

質問: **295**

ある銀行が利息計算用のコンピュータプログラムに軽微な変更を加えた。利息計算が正しいかどうかを判断する上で、以下のどの手法が最も強力な証拠となるだろうか？
A. ソースコードレビュー
B. 監査ソフトウェアを使用した並列シミュレーション
C. 結果サンプルの手動検証
D. 品質保証(QA)テスト結果のレビュー
正解: **B** (コメントを発表する)
Parallel simulation involves running the same data through two systems and comparing the results1. In this case, the bank's data would be processed using both the modified interest calculation program and an audit software. The results from both systems would then be compared to check for discrepancies1. This technique provides strong evidence of the correctness of interest calculations as it directly tests the program's output against a known and trusted output1. While source code review23, manual verification of a sample of results4567, and review of QA test results8910 can also provide valuable insights, they do not offer the same level of direct, comparative evidence as parallel simulation1.
References:
Parallel simulation in IT testing - Universal CPA Review
5 code review best practices - Work Life by Atlassian
How to Make Good Code Reviews Better - Stack Overflow
Guidelines for the validation and verification of quantitative and qualitative test methods - Mathematics LibreTexts Method Validation and Verification - University of Utah Sample Procedure for Method Validation - NIST Method validation and verification - CFS Good Practices for Quality Assurance Reviewers: Assessing Evidence of Supervisory Review - IGNET How do quality assurance engineers test calculations? - Software Quality Assurance and Testing Stack Exchange Quality Assurance/Quality Control (QA/QC) Plan and Procedures - UNFCCC

質問: **296**
退会会議で、IS監査担当者はバックアップサイクルについて強調します。
オペレーターエラーにより見落とされているものがあり、これらの例外は
管理されていません。次のうちどれがベストな方法ですか？
経営陣が関連リスクを理解するのに役立つか？
A. 災害復旧への影響について説明します。
B. リソース要件への影響について説明します。
C. インシデント管理への影響について説明します。
D. バックアップのスケジュールへの影響について説明します。
正解: **A** (コメントを発表する)
The best way to help management understand the associated risk of missing backup cycles due to operator error and lack of exception management is to explain the impact to disaster recovery. Disaster recovery is the process of restoring normal operations and

functions after a disruptive event, such as a natural disaster, a cyberattack, or a hardware failure. Backup cycles are essential for disaster recovery, because they ensure that the organization has copies of its critical data and systems that can be restored in case of data loss or corruption. If backup cycles are missed due to operator error, and these exceptions are not managed, the organization may not have the latest or complete backups available for disaster recovery, which can result in prolonged downtime, reduced productivity, lost revenue, reputational damage, and legal or regulatory penalties. The other options are not as effective as explaining the impact to disaster recovery, because they either do not address the risk of data loss or corruption, or they focus on operational or technical aspects rather than business outcomes. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.1

質問**: 297**
従業員所有のモバイルデバイスにプッシュ配信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、最も優れたST方式を提供するのは次のうちどれですか？
A. リモートデータ消去機能の有効化
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します
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化
正解**: (**正解を表示します**)**
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

質問**: 298**
セキュリティ意識向上トレーニングに含めるべき最も重要な項目は次のうちどれですか？
A. さまざまな種類の不審な活動への対応方法
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
正解**: (**正解を表示します**)**
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 AwarenessTraining | KnowBe4, SecurityAwareness Training Course (ISC) | Coursera

質問**: 299**
展開プログラムの一環として安全なコードレビューを実施する場合、どのような種類の制御が実装されていますか?
A. 探偵
B. 修正
C. 監視
D. 抑止力
正解**: (**正解を表示します**)**
Comprehensive and Detailed Explanation:
Secure code reviews identify security flaws or vulnerabilities in code before deployment. This makes them detective controls, since they help find issues but do not directly prevent or correct them.
* Option A: Correct - they detect flaws.
* Option B: Corrective controls are applied after issues are detected.
* Option C: Monitoring is ongoing observation, not review-based.
* Option D: Deterrent controls discourage actions (e.g., policies, warnings), not detect issues.

ISACA Reference: CISA Review Manual 27th Edition, Domain 3, section on software development controls and code review practices.

質問: **300**
小規模組織のデータ分類プロセスと手順を監査していた際、情報システム監査担当者は、データがしばしば誤ったレベルで分類されていることに気づきました。この状況を改善するために、組織にとって最も効果的な方法は何でしょうか？
A. コンテンツに基づいて文書を自動的に分類します。
B. ITセキュリティ担当者がデータ所有者向けに的を絞ったトレーニングを実施する。
C. データ分類ポリシーを企業ウェブポータルに公開する。
D. 情報分類ポリシーに関する啓発プレゼンテーションやセミナーを実施する。
正解: **(**正解を表示します**)**
This is the most effective way for the organization to improve its data classification processes and procedures, because data owners are the ones who are responsible for assigning the appropriate level of classification to the data they create, collect, or manage. Data owners should be aware of the data classification policy, the criteria for each level of classification, and the implications of misclassification. IT security staff can provide tailored training for data owners based on their roles, functions, and types of data they handle.
The other options are not as effective as having IT security staff conduct targeted training for data owners:
Use automatic document classification based on content. This is a possible option, but it may not be feasible or accurate for a small organization. Automatic document classification is a process that uses artificial intelligence or machine learning to analyze the content of a document and assign a class label based on predefined rules or models. However, this process may require a lot of resources, expertise, and maintenance, and it may not capture all the nuances and context of the data. The IS auditor should also verify the reliability and validity of the automatic document classification system.
Publish the data classification policy on the corporate web portal. This is a good practice, but it is not enough to improve the data classification situation. Publishing the data classification policy on the corporate web portal can increase the visibility and accessibility of the policy, but it does not ensure that data owners will read, understand, and follow it. The IS auditor should also monitor and enforce the compliance with the policy.
Conduct awareness presentations and seminars for information classification policies. This is a useful measure, but it is not the most effective one. Conducting awareness presentations and seminars can raise the general awareness and knowledge of information classification policies among all employees, but it may not address the specific needs and challenges of data owners. The IS auditor should also provide more in-depth and practical training for data owners.

質問: **301**

クラウド プロバイダーの変更管理プロセスが効果的であることを示す最良の証拠は次のどれですか。
A. ベンダーとの定期的な変更管理会議の議事録
B. ベンダーの CEO および CIO からの書面による保証
C. ベンダーが提供する第三者レビューの結果
D. ベンダーが提供する変更管理ポリシーのコピー
正解: **(**正解を表示します**)**
The results of a third-party review provided by the vendor would provide the best evidence that a cloud provider's change management process is effective, because it would be an independent and objective assessment of the vendor's compliance with best practices and standards for managing changes in the cloud environment. A third-party review would also include testing of the vendor's change management controls and procedures, and provide recommendations for improvement if needed.
Minutes from regular change management meetings with the vendor would not provide sufficient evidence, because they would only reflect the vendor's self-reported information and may not capture all the changes that occurred or their impact on the cloud services.
Written assurances from the vendor's CEO and CIO would also not provide sufficient evidence, because they would be based on the vendor's own opinion and may not be verified by external sources. A copy of change management policies provided by the vendor would not provide sufficient evidence, because it would only show the vendor's intended approach to change management, but not how it is implemented or monitored in practice.
References:
ISACA Cloud Computing Audit Program, Section 4.5: Change Management
Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives, Section 4.3:
Change Management

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu **1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **302**
次のうち、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しているのはどれですか？
A. インシデント解決時間の短縮
B. IT管理部門によるレビュー対象インシデント数の増加

C. ヘルプデスクへの電話件数の減少
D. 報告された重大インシデント数の増加
正解**: A (**コメントを発表する**)**
Decreased time for incident resolution is the best indicator that an incident management process is effective.
Incident management is a process that aims to restore normal service operation as quickly as possible after an incident, which is an unplanned interruption or reduction in quality of an IT service. Decreased time for incident resolution means that the incident management process is able to identify, analyze, respond to, and resolve incidents efficiently and effectively. The other indicatorsdo not necessarily reflect the effectiveness of the incident management process, as they may depend on other factors such as the nature, frequency, and severity of incidents. References: CISA Review Manual, 27th Edition, page 372

質問**: 303**
レガシーシステムを置き換える新しいアプリケーションシステムへの移行データの正確性と完全性を検証する場合、IS監査担当者がレビューするのが最も効果的です。
A. データ分析結果。
B. 監査証跡
C. 受容と持続的な結果
D. ロールバック計画
正解**: (**正解を表示します**)**
When verifying the accuracy and completeness of migrated data for a new application system replacing a legacy system, it is most effective for an IS auditor to review data analytics findings. Data analytics is a technique that uses software tools and statistical methods to analyze large volumes of data and identify patterns, anomalies, errors or inconsistencies. Data analytics can help to compare the source and target data sets, validate the data quality and integrity, and detect any data loss or corruption during the migration process. The other options are not as effective, because audit trails only record the actions performed on the data, acceptance testingresults only verify the functionality of the new system, and rollback plans only provide contingency measures in case of migration failure. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.6

質問**: 304**
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際、最初に行うべき手順は次のうちどれですか？
A. データインベントリと分類の作業を実施します。
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

正解: **A** (コメントを発表する)

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 and 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 and 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 and Examples
How to Create Effective Data Loss Prevention Policies

質問: **305**
ファイル転送後のデータ整合性を最も確実に保証できるのは、次のうちどれですか？
A. チェックデジット
B. 貨幣単位のサンプリング
C. ハッシュ値
D. 妥当性チェック
正解: **(正解を表示します)**
The best assurance of data integrity after file transfers is hash values. Hash values are unique strings that are generated by applying a mathematical function to the data. Hash values can be used to verify that the data has not been altered or corrupted during the transfer, as any change in the data would result in a different hash value. By comparing the hash values of the source and destination files, one can confirm that the data is identical and intact.
The other options are not as effective as hash values for ensuring data integrity after file transfers. Check digits are digits added to a number to detect errors in data entry or transmission, but they are not reliable for detecting intentional or complex modifications of the data. Monetary unit sampling is a statistical sampling technique used for auditing financial statements, but it is not applicable for verifying data integrity after file transfers. Reasonableness check is a validation method that checks whether the data falls within an expected range or format, but it does not guarantee that the data is accurate or consistent with the source.
References:
5: On Windows, how to check that data is unchanged after copying? - Super User
6: Data integrity | Cloud Storage Transfer Service Documentation | Google Cloud
7: Checking File Integrity - HECC Knowledge Base
8: How to setup File Transfer Integrity Checks - Progress.com

質問: **306**
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うちどれですか？
A. 割り当てられた分類に従って情報資産を保護する
B. 資産が割り当てられた分類に従って保護されていることを検証します
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を定義する
正解: **(正解を表示します)**
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 and Explanations Database, Question ID 206

質問: **307**
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、組織を攻撃から保護するために、IS監査担当者が最も推奨する対策は次のうちどれですか？
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) を設置します。
D. 安全なプロトコルを実装します。
正解: **(**正解を表示します**)**
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 anorganization 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 asecuretunnel 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

質問: **308**
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対策を講じる必要があるでしょうか？
A. 必要不可欠な外部サービスのみを許可すべきです。
B. ファイアウォールは非武装地帯 (DMZ) に設置する必要があります。
C. すべての外部通信はファイアウォールを経由する必要があります。
D. 外部情報用のフィルタを定義する必要があります。
正解: **(**正解を表示します**)**

質問: **309**
インシデント管理監査中に、IS監査担当者は監査期間中に類似したインシデントが複数記録されていることを発見しました。監査担当者が取るべき最も重要な行動は次のうちどれですか？
A. 調査結果を文書化し、経営陣に報告する。
B. 根本原因分析が実施さ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に対して対応が行われたかどうかを検証します。
正解: **B (**コメントを発表する**)**
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.

質問: **310**
探偵管理体制の継続的な悪化によって生じる最も大きな影響は、次のうちどれですか？
A. 丸太の保管スペースに対する需要の増加
B. セキュリティログにおける偽陰性の増加
C. 根本原因分析の有効性の低下
D. 全体的な回復時間の短縮

正解: **B** (コメントを発表する)

質問: **311**
鑑識捜査の一環としてデジタル証拠を保護する上で、以下の技術のうちどれが最も役立ちますか？
A. ハードウェアベースのメディア書き込みブロッカー
B. データ暗号化
C. 差分バックアップ
D. ソースメディアのサニタイズ
正解: (正解を表示します)
A hardware-based media write blocker (Option A) ensures that forensic investigators can acquire digital evidence without altering the original data, maintaining its integrity for legal proceedings.
ISACA CISA Reference: Digital forensics best practices emphasize write-blocking devices to prevent contamination of evidence.
Risk Implication: Without a write blocker, evidence may be tampered with, compromising its admissibility in court.

質問: **312**
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重要な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ための最善の方法はどれですか？
A. スキル評価を実施して、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、監査を進めます。
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起用する。
正解: (正解を表示します)
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

質問: **313**

組織が最近導入したBYOD(Bring Your Own Device)戦略に伴うセキュリティリスクに対処するために、最も効果的な方法は次のうちどれでしょうか？
A. モバイルデバイス追跡プログラム
B. モバイル端末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
正解: **(**正解を表示します**)**
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. Amobile device awareness program can also help the organization to comply with relevant regulations and standards that governdata 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

質問: **314**
情報システム監査担当者は、組織の分散環境において複数のサーバー障害が発生していることを知る。
将来的にサーバー障害が発生した場合の影響を最小限に抑えるための最適な推奨事項は次のうちどれですか？
A. 冗長な経路
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
正解: **B** (コメントを発表する)
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, failoverpower, 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.

質問: **315**
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引き起こされるデータ品質の問題を防止するための最善の方法は何ですか？
A. 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するためのデータ品質アラートを設定します。
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への変更を含める)
D. 2つのシステム間の抽出/転送/ロード(ETL)プロセスにおける変更へのアクセスを制限する
正解: **C** (コメントを発表する)
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 and Explanations Database, Question ID 226

質問**: 316**
IS監査担当者が、監査指摘事項を是正するための合意された経営陣の対応に対するフォローアップ活動を計画する際に、最も重視すべき事項は次のうちどれでしょうか？
A. 修復作業による業務中断
B. IT予算の制約
C. 責任あるIT担当者の確保
D. 元の研究結果のリスク評価
正解**: D (**コメントを発表する**)**
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

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジン

を手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu 1605問、３０%ディスカウント、特別な割引コード: JPNshiken」

質問: **317**
プロジェクトの期待される利益が達成されたかどうかを評価する際に、情報システム監査人が確認することが最も重要です。
A. ビジネスケース。
B. プロジェクトのスケジュール。
C. 提案された機能強化。
D. 品質保証 (QA) の結果。
正解: **(正解を表示します)**
The business case defines the project's expected benefits, success criteria, and performance metrics.
Reviewing the business case allows the auditor to assess whether the benefits identified at initiation have been realized post-implementation. The schedule (B) only tracks timeliness, not value. Proposed enhancements (C) address future improvements, not whether benefits have been delivered. QA results (D) reflect product quality but not business value. ISACA emphasizes that value delivery and benefits realization are key elements of enterprise governance of IT, aligning with COBIT's EDM02 (Ensure Benefits Delivery).
References (ISACA): COBIT 2019, EDM02 Ensure Benefits Delivery.

質問: **318**
組織のラップトップ コンピューター上のデータを保護するための最良の方法は次のうちどれですか。
A. 無効なUSBポート
B. フルディスク暗号化
C. 多要素認証（MFA）
D. パスキーフレーズ
正解: **(正解を表示します)**
Comprehensive and Detailed Explanation:
The greatest risk to laptop computers is data exposure in case of theft or loss. The most effective safeguard is full disk encryption, which ensures that even if the device is stolen, data remains unreadable without the encryption key.
* Disabled USB ports (A): Prevents some forms of data exfiltration but does not protect stored data.
* MFA (C): Protects user authentication but not the data if the disk is removed.
* Passkey phrases (D): Improves authentication strength but is weaker than encryption for data protection.
# ISACA Reference: CISA Review Manual 27th Edition, Domain 5 (Protection of Information Assets), section on endpoint security and encryption controls.

質問: **319**
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うちどれでしょうか？
A. サービス監査員の報告書
B. パフォーマンス指標
C. ベンダーへの抜き打ち訪問
D. ベンダーとのインタビュー
正解: **(正解を表示します)**
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 formonitoring the service levels. References: CISA Review Manual(Digital Version), Chapter 2: Governanceand Management of IT, Section 2.4: IT Service Delivery and Support

質問: **320**
組織のパッチ管理プログラムを評価するIS監査担当者にとって、以下のうちどれが最も懸念すべき事項でしょうか？
A. 中リスクおよび低リスクの脆弱性に対するパッチは省略されています。
B. 不足しているパッチを特定するためにネットワークをスキャンするプロセスがありません。
C. パッチは複数のデプロイメントサーバーからデプロイされます。
D. パッチが適用されていないサーバーを隔離するプロセスは存在しません。
正解: **(正解を表示します)**

質問: **321**
サービスベンダーが顧客の要求する管理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、次のうちどれでしょうか？
A. 合意された基準を用いて定期的に現地調査を実施する。
B. ベンダーとのサービスレベル契約(SLA)を定期的に見直してください。
C. ベンダーのITシステムに対する予告なしの脆弱性評価を実施する。
D. ベンダーの管理自己評価(CSA)の証拠を入手する。
正解: **(正解を表示します)**
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

質問: **322**
監査報告書を提出した後、監査マネージャーは監査中に証拠が見落とされていたことを発見しました。この証拠は、手続き上の統制が失敗した可能性があり、監査の結論と矛盾する可能性があることを示しています。この見落としによって最も影響を受けるリスクは次のうちどれですか？
A. 固有の
B. 運用中
C. 監査
D. 財務
正解: **C (**コメントを発表する**)**
The risk that is most affected by this oversight is audit risk. Audit risk is the risk that the auditor may express an inappropriate opinion or conclusion based on the audit evidence obtained. Audit risk consists of inherent risk, control risk, and detection risk. Inherent risk is the risk that material errors or frauds exist in the audited area before considering the effectiveness of internal controls. Control risk is the risk that the internal controls fail to prevent or detect material errors or frauds. Detection risk is the risk that the auditor fails to identify material errors or frauds using the audit procedures performed. In this case, the auditor has overlooked evidence that could contradict a conclusion of the audit, which increases the detection risk and consequently the audit risk. References:
CISA Review Manual (DigitalVersion), Chapter 2, Section 2.31
CISA Online Review Course, Domain 1, Module 1, Lesson 32

質問: **323**
組織がサードパーティ製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、次のうちどれですか？

A. 第三者が要件を満たすために十分なリソースを割り当てることを保証する。
B. 内部監査機能内で分析を活用する
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
正解: **(**正解を表示します**)**
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.

質問: **324**
組織のインシデント対応チームの有効性を向上させるために、最も効果的な方法はどれですか？
A. 定期的なテストを実施し、得られた教訓を取り入れる
B. 平均解決時間の増加と主要業績評価指標(KPI)指標の公開
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入りの確認を求める。
D. すべてのチームメンバーが情報システム技術を理解していることを確認する
正解: **A (**コメントを発表する**)**
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.

質問: **325**
個人データの保持期間および破棄条件は、によって決定されるべきです。
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。
正解: **(正解を表示します)**
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.

質問: **326**
次のうち、ソーシャルエンジニアリング攻撃の手法はどれですか？
A. 許可されていない人物が、許可された人物の後についてセキュリティドアを通ってセキュリティ施設への不正アクセスを試みる。
B. 従業員が電話で質問に答えることで、機密のIPアドレスとパスワードを漏洩するように誘導される。

C. ハッカーがスキャンツールを使用してオフィスビル内を歩き回り、無線ネットワークを探してアクセス権を取得しようとしている。
D. 侵入者がネットワークを流れる機密情報を盗聴・収集し、第三者に販売します。
正解: **(**正解を表示します**)**
An employee is induced to reveal confidential IP addresses and passwords by answering questions over the phone. This is a social engineering attack method that exploits the trust or curiosity of the employee to obtain sensitive information that can be used to access or compromise the network. According to the web search results, social engineering is a technique that uses psychological manipulationto trick users into making security mistakes or giving away sensitive information1. Phishing, whaling, baiting, and pretexting are some of the common forms of social engineering attacks2. Social engineering attacks are often more effective and profitable than purely technical attacks, as they rely on human error rather than system vulnerabilities

質問: **327**
対象領域が適切に特定された後、IS監査担当者がサンプリング対象を選択する際の次のステップは何ですか？
A. サンプリング対象の母集団を定義します。
B. サンプルサイズを計算します。
C. サンプルを採取します。
D. サンプリング方法を決定します。
正解: **A (**コメントを発表する**)**

質問: **328**
ITプロジェクトのどのフェーズで、ベネフィット実現分析を実施するのが最も適切ですか？
A. 導入後レビュー段階
B. ユーザー受け入れテスト (UAT) フェーズ
C. 最終実装段階
D. 設計レビュー段階
正解: **(**正解を表示します**)**

質問: **329**
IS監査担当者は、組織が質の高いセキュリティポリシーを持っていると結論付けました。次に確認すべき最も重要な事項は次のうちどれですか？ポリシーは次の条件を満たす必要があります。
A. 全従業員に十分に理解されている。
B. 業界標準に基づいています。
C. プロセスオーナーによって開発されました。
D. 頻繁に更新されます。

正解: **A** (コメントを発表する)
The most important thing to determine next after concluding that an organization has a quality security policy is whether the policy is well understood by all employees. A security policy is a document that defines the objectives, scope, roles, responsibilities, and rules for information security within an organization. A quality security policy is one that is clear, concise, consistent, comprehensive, and aligned with business goals and requirements. However, a quality security policy is useless if it is not well understood by all employees who are expected to comply with it.Therefore, the IS auditor should assess the level of awareness and understanding of the security policy among employees and identify any gaps or issues that need to be addressed. The other options are not as important as ensuring that the security policy is well understood by all employees, as they do not directly affect the implementation and effectiveness of the security policy. References: CISA Review Manual, 27th Edition, page 317

質問: **330**
以下のうち、監査機能が基準および倫理規定を遵守していることを経営陣および取締役会に最も適切に示すものはどれですか？
A. 監査スタッフへのインタビュー
B. 品質管理レビュー
C. コントロール自己評価(CSA)
D. 是正措置計画
正解: (正解を表示します)
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. Thesereviews assess the efficiency and effectiveness of the audit function, ensure compliance with audit standards and ethics, and identify areasfor 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

質問: **331**
IS監査担当者は、取引不正の発生源が、休暇中のeビジネス担当者のデスクトップシステムであることを突き止めました。監査担当者が調査の成功を確実にするための最善の方法は次のうちどれですか？
A. 攻撃されたシステムのイメージを作成し、メモリをファイルにダンプしてレビューします。
B. 攻撃を受けたシステムを直ちに封鎖し、調査が完了するまで全てのアクセスを遮断してください。

C. 攻撃を受けたシステムを再起動し、ログファイルとファイルのタイムスタンプを速やかに確認してください。
D. ビジネススタッフにインタビューし、最近のシステム活動の詳細を提供するよう依頼します。
正解: **A** (コメントを発表する)
The best way to ensure a successful investigation is to preserve digital evidence immediately, including both a forensic image of the system and volatile memory capture where feasible. ISACA defines digital forensics as identifying, preserving, analyzing, and presenting digital evidence in a legally acceptable manner. That makes evidence preservation the first priority.
Option A is correct because creating a system image preserves the state of the disk, while capturing memory preserves volatile information that may be lost if the system is altered, powered off, or rebooted. ISACA's glossary notes that memory dumps allow analysis of memory contents at the time of failure, which supports preserving volatile evidence for forensic review.
Option B is not the best answer. Isolating the system may help preserve evidence, but by itself it does not collect the volatile and nonvolatile evidence needed for a strong investigation. Evidence preservation is stronger when the system is forensically imaged and memory is captured.
Option C is incorrect because rebooting can destroy volatile evidence and alter timestamps or system state, which can undermine a forensic investigation. That runs directly counter to digital forensics principles centered on preservation.
Option D may be useful later, but interviews are secondary to preserving digital evidence. Human recollection cannot substitute for properly preserved forensic artifacts.
Therefore, A is the best answer because it preserves the most complete and reliable digital evidence for investigation.
References (Official ISACA):
* ISACA, Overview of Digital Forensics - digital forensics is the process of identifying, preserving, analyzing and presenting digital evidence.
* ISACA Glossary, Digital forensics.
* ISACA Glossary, Memory dump.

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu 「**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **332**
運用ログ管理の主な利点は次のどれですか?
A. 予測分析によりユーザーエクスペリエンスが向上します。
B. ネットワーク データをリアルタイムで監視することでセキュリティが向上します。
C. パフォーマンスの問題を識別するためにデータを整理します。
D. 統合ストレージを使用したデータ集約をサポートします。
正解: **B** (コメントを発表する)
Operational log management primarily enhances security by enabling real-time monitoring and detection of anomalies within network data. Logs provide valuable information for identifying threats, investigating incidents, and ensuring compliance with security policies.
* Predictive Analysis for User Experience (Option A):While logs may support analytics, this is not the primary benefit.
* Performance Issue Identification (Option C):Logs can help identify performance issues, but the focus of operational log management is security.
* Data Aggregation Using Unified Storage (Option D):This supports management but is secondary to the security benefits.
Reference:ISACA CISA Review Manual, Job Practice Area 3: Information Systems Operations and Business Resilience.

質問: **333**
年次内部監査計画の策定に携わるIS監査担当者は、最高情報責任者(CIO)が、前年度の多数の勧告事項に対応するためにより多くの時間が必要であるとして、来年度のIS監査は実施しないよう要請したことを知った。監査担当者は、次のうちどれを最初に行うべきだろうか?
A. 監査計画について話し合うため、監査管理部門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. 来年度の計画からIS監査を除外する
D. クラン内のIS監査の数を増やす
正解: **A** (コメントを発表する)
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

質問: **334**
情報システム監査担当者がハードディスクの使用率レポートをレビューしたところ、使用率が常に95%を超えていることがわかった。
IS監査担当者にとって、以下のうちどれが最も懸念すべき事項でしょうか？
A. データセキュリティ
B. サービス拒否(DoS)攻撃
C. 利用可能性
D. 一貫性
正解: **(正解を表示します)**

質問: **335**
再利用するストレージメディアから機密情報を削除するのに最適な方法は次のうちどれですか？
A. クロスカットシュレッディング。
B. 複数回の上書き。
C. 再分割。
D. 再フォーマット中。
正解: **(正解を表示します)**
The correct answer is B. Multiple overwriting.
When storage media will be reused, the goal is to remove sensitive data while keeping the media physically usable. Multiple overwriting writes new patterns of data over existing data so the previous sensitive information is no longer practically recoverable. ISACA describes overwriting as placing an additional layer of information over existing material, with the purpose of protecting the information while not damaging the hard drive itself.
Option A is not correct because cross-cut shredding physically destroys the media. It may be appropriate when media will be disposed of, but not when the storage device must be reused. Option C is not correct because repartitioning changes the disk structure but does not securely erase the underlying data. Option D is not correct because reformatting may remove file system references but often does not securely eliminate recoverable data.
A useful CISA exam point is this:
For reuse, choose logical sanitization such as overwriting.
For disposal, choose physical destruction, degaussing, or shredding depending on the media type and sensitivity.
ISACA notes that common digital data destruction methods include overwriting, degaussing, and physical destruction. Since degaussing and physical destruction generally make media unsuitable for normal reuse, overwriting is the best answer in this question.
References: ISACA CISA Exam Content Outline, Domain 5; ISACA article on data destruction methods.

質問: **336**

IT災害復旧目標時間(RTO)は、以下の点に基づいて設定する必要があります。
A. 許容される最大データ損失。
B. 停電の性質
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。
正解: **(**正解を表示します**)**
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.

質問: **337**
エンタープライズアーキテクチャ(EA)ガバナンスの主な目的は次のうちどれですか？
A. 新しいプロセスとテクノロジーが既存のプロセスと調和するようにする
B. EAが新たな技術動向に適応できるようにするため
C. EAが現地の法律および規制に準拠していることを確認する
D. 新しい取り組みが許容できる投資収益率(ROI)を生み出すことを保証する
正解: **A (**コメントを発表する**)**
Enterprise architecture (EA) governance ensures that IT and business alignment is maintained and that new processes and technologies integrate well with existing structures.
Option A (Correct):The primary purpose of EA governance is to ensure that new technologies, processes, and systems align and harmonize with existing architecture to maintain operational efficiency and consistency.
Option B (Incorrect):While adaptability to emerging technology trends is important, EA governance focuses more on structure, consistency, and compliance rather than just adaptability.
Option C (Incorrect):Compliance with regulations is crucial, but it is just one component of governance. EA governance has a broader scope, including strategic alignment and process integration.
Option D (Incorrect):Ensuring ROI is an important financial consideration, but it is not themainobjective of EA governance.
Reference:ISACA CISA Review Manual -Domain 1: Information Systems Auditing Process- Covers governance, risk management, and ensuring alignment of EA with business objectives.

質問: **338**

以下のうち、自己評価によるコントロール(CSA)の主な目的はどれですか？
A. 一部の管理監視責任を機能領域に移管する
B. 従業員の参加を通じて結束力のあるチームを作る
C. 監査評価プロセスを改善するため
D. 特定の機能に関連する制御コストを削減する
正解: **(**正解を表示します**)**

質問: **339**
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の監督を一時的に任されました。監査部門に戻った後、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。監査部門でITプロジェクト管理の経験を持つのは、この監査マネージャーだけです。最善の対応策は何でしょうか？
A. ITプロジェクト管理の経験がないにもかかわらず、別の監査マネージャーに業務を移管する。
B. 監査を独立した資格のある専門家に委託する。
C. 他に適切な経験を持つ人がいないため、監査を管理してください。
D. 上級IS監査担当者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施する。
正解: **B (**コメントを発表する**)**
Outsourcing the audit to independent and qualified resources is the best course of action for the IS audit manager who was temporarily tasked with supervising a project manager assigned to the organization's payroll application upgrade. This is because the IS audit manager has a potential conflict of interest and a threat to objectivity and independence, which are essential principles and standards for IS auditors.
According to the ISACA Code of Professional Ethics, IS auditors should maintain objectivity and independence in their professional judgment and avoid any situations that may impair or be presumed to impair their objectivity or independence1. Objectivity is the mental attitude of an IS auditor that allows them to perform their work honestly, impartially, and with integrity, while independence is the freedom from conditions that threaten the ability of an IS auditor to carry out their work in an unbiased manner2.
The IS audit manager who was involved in supervising the payroll application upgrade project may have a self-review threat, which is the risk that an IS auditor will not appropriately evaluate the results of a previous judgment made or service performed by them or their subordinates3. The IS audit manager may also have a familiarity threat, which is the risk that an IS auditor will be influenced by a close relationship with someone involved in the project or by their own personal interests4. These threats may compromise the IS audit manager's objectivity and independence and affect the quality and credibility of the audit.

Therefore, the IS audit manager should disclose their involvement in the project to their senior management and the audit committee and decline to perform or manage the audit. The IS audit manager should also recommend outsourcing the audit to independent and qualified resources who have no connection or interest in the project and who have the necessary skills and experience to conduct a reliable and effective audit.
The other options are not the best course of action for the IS audit manager.
Transferring the assignment to a different audit manager despite lack of IT project management experience is not the best course of action because it may result in a low-quality audit that does not meet the expectations and standards of the stakeholders. IT project management experience is essential for auditing an IT project, as it requires knowledge of project management methodologies, tools, techniques, risks, and best practices. An audit manager who lacks IT project management experience may not be able to plan, execute, report, and follow up on the audit effectively and efficiently.
Managing the audit since there is no one else with the appropriate experience is not the best course of action because it violates the ethical principles and standards of objectivity and independence for IS auditors.
Managing the audit would create a conflict of interest and a threat to objectivity and independence for the IS audit manager, as they would be reviewing their own work or that of their subordinate. Managing the audit would also undermine the credibility and reliability of the audit results and recommendations, as they may be biased or influenced by personal or professional relationships or interests.
Having a senior IS auditor manage the project with the IS audit manager performing final review is not the best course of action because it still involves the IS audit manager in the audit process, which poses a conflict of interest and a threat to objectivity and independence. Performing final review would require the IS audit manager to evaluate and approve the work done by the senior IS auditor, which may be affected by their previous involvement in or knowledge of the project. Performing final review would also expose theIS audit manager to undue pressure or influence from management or other stakeholders who may have expectations or preferences regarding the audit outcome.

質問**: 340**
内部統制自己評価(CSA)におけるIS監査人の主な役割は次のうちどれですか？
A. ワークショップの進行役を務める。
B. プロセスの文書化。
C. 管理上の弱点を特定する。
D. 内部統制の監視。
正解**: (**正解を表示します**)**
The correct answer is A. Facilitating workshops.
In a control self-assessment, the responsibility for assessing controls belongs mainly to management and staff of the business unit, not to the IS auditor. The auditor's primary role

is normally to act as a facilitator, helping participants understand the CSA process, discuss risks and controls, and document results in a structured way.
ISACA defines control self-assessment as an assessment of controls made by the staff of the unit or units involved, and ISACA's glossary notes that the assessment may be under the guidance of a facilitator, such as an auditor or risk manager.
Option B is not the best answer because documenting processes may occur during CSA, but it is not the auditor's primary role. Option C is not the best answer because identifying control weaknesses should primarily come from the process owners and participants; the auditor facilitates and may challenge or validate, but should not take ownership of management's self-assessment. Option D is not correct because monitoring internal controls is a management responsibility, not the primary role of the IS auditor in CSA.
This question maps to Information Systems Auditing Process because it concerns audit techniques, auditor independence, and the auditor's role in assurance-related activities.
ISACA's CISA Exam Content Outline identifies Domain 1 as the Information Systems Auditing Process domain.
References: ISACA CISA Exam Content Outline, Domain 1; ISACA Interactive Glossary, "Control self- assessment"; ISACA Journal, IS Audit Basics: Doing More With Less.

質問**: 341**
データ保持ポリシーを導入する最も適切な理由は次のうちどれですか？
A. 情報の保管および保護に関連する責任を制限するため
B. 組織内でのデータ処理に関する業務目標を文書化する
C. IT部門外にデータ保護の責任と所有権を割り当てる
D. (トースターリカバリ手順の)リカバリポイント検出(RPO)を確立する
正解**: A (**コメントを発表する**)**
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 document that defines how long data should be kept by an organization and how they should be disposed of when they are no longer needed. A data retention policy should comply with the applicable laws and regulations that govern the data retention requirements and obligations of organizations, such as tax laws, privacy laws, or industry standards4. Implementing a data retention policy can help to limit the liability associated with storing and protecting information by reducing the amount of data that need to be stored and secured, minimizing the risk of data breaches or leaks, ensuringcompliance with legal or contractual obligations, and avoiding potential fines or penalties for non- compliance5. The other options are less relevant or incorrect because:
B). Documenting business objectives for processing data within the organization is not a reason to implement a data retention policy, as it is more related to data governance than data retention. Data governance refers to the policies, procedures, and controls that define how data are collected, used, managed, and shared within an organization. Data

governance helps to ensure that data are aligned with business objectives and support decision making6.
C). Assigning responsibility and ownership for data protection outside IT is not a reason to implement a data retention policy, as it is more related to data accountability than data retention. Data accountability refers to the identification and assignment of roles and responsibilities for data protection among different stakeholders within an organization. Data accountability helps to ensure that data are handled appropriately and securely by authorized parties7.
D). Establishing a recovery point objective (RPO) for disaster recovery procedures is not a reason to implement a data retention policy, as it is more related to data backup than data retention. Data backup refers to the process of creating copies of data that can be restored in case of data loss or corruption. Data backup helps to ensure that data are available and recoverable in case of disaster8. RPO is a measure of the maximum amount of data that canbe lost or acceptable in case of disaster9. References: Data Retention Policy - ISACA, Data Retention - ISACA, Data Governance - ISACA, Data Accountability - ISACA, Data Backup - ISACA, Recovery Point Objective - ISACA

質問**: 342**
ベンダーがシステムセキュリティ要件を遵守していることを確認するための最良の方法は、次のうちどれですか？
A. ベンダーのセキュリティコンプライアンスに関する過去の監査をレビューします。
B. ベンダーのスタッフにセキュリティ研修を義務付ける。
C. ベンダー契約にコンプライアンス条項を必須とする。
D. ベンダーから報告された過去のインシデントを確認します。
正解**: C (**コメントを発表する**)**

質問**: 343**
IS監査担当者が、アプリケーションのシステムログに記録されたアクセスのサンプルを分析しています。監査担当者は、例外が1つでも見つかった場合、徹底的な調査を開始する予定です。どのサンプリング方法が適切でしょうか？
A. 発見サンプリング
B. 判断サンプリング
C. 変数サンプリング
D. 層化抽出法
正解**: (**正解を表示します**)**
Discovery sampling is an appropriate sampling method for an IS auditor who intends to launch an intensive investigation if one exception is found. Discovery sampling is a type of attribute sampling that determines the sample size based on an acceptable risk of not finding at least one occurrence of an attribute when a given rate of occurrence exists in a population. Discovery sampling can be used by an IS auditor who wants to detect fraud or

errors that have a low probability but high impacton an audit objective. The other options are not appropriate sampling methods for this purpose, as they may involve judgmental sampling, variable sampling, or stratified sampling. References:
CISA Review Manual (Digital Version), Chapter 2, Section 2.31
CISA ReviewQuestions, Answers and Explanations Database, Question ID 230

質問: **344**
アジャイル監査手法を採用する最大のメリットは次のうちどれですか？
A. 主要なリスクに対処する能力の向上
B. クライアントとのやり取りの頻度が低い
C. 文書作成要件の軽減
D. 年間コスト削減額
正解: **A (コメントを発表する)**

質問: **345**
企業資源計画(ERP)システムの監査中に、IS監査担当者は、アプリケーションパッチが本番環境に適用されていることを発見しました。IS監査担当者にとって最も重要なことは、以下の担当者からの承認を確認することです。
A. 情報資産の所有者。
B. 情報セキュリティ責任者。
C. システム管理者。
D. プロジェクトマネージャー。
正解: **(正解を表示します)**

質問: **346**
変更管理プロセスを評価するIS監査担当者は、変更ログからサンプルを選択する必要があります。監査担当者が変更ログが完全であることを確認するための最善の方法は何ですか？
A. 変更管理担当者に完全性についてインタビューする。
B. ログから項目を取得し、システムまで遡って追跡します。
C. 完全性に関する経営陣の証明を取得する。
D. システムからの最後の変更を取得し、ログまで遡って追跡します。
正解: **(正解を表示します)**
The answer D is correct because the best way for the auditor to confirm the change log is complete is to take the last change from the system and trace it back to the log. A change log is a record of all the changes that have been made to a system, such as software updates, bug fixes, configuration modifications, etc. A change log should contain information such as the date and time of the change, the description and purpose of the change, the person or service who made the change, and the approval status of the

change. A complete change log helps to ensure that the system is secure, reliable, and compliant with the relevant standards and regulations.
An IS auditor evaluating the change management process must select a sample from the change log to verify that the changes are properly authorized, documented, tested, and implemented. However, before selecting a sample, the auditor must ensure that the change log is complete and accurate, meaning that it contains all the changes that have been made to the system and that there are no missing, duplicated, or falsified entries. To do this, the auditor can use a technique called backward tracing, which involves taking the last change from the system and tracing it back to the log. This way, the auditor can check if the change is recorded in the log with all the relevant details and if there are any gaps or inconsistencies in the log. If the last change from the system is not found in the log or does not match with the log entry, it indicates that the change log is incomplete or inaccurate.
The other options are not as good as option D. Interviewing change management personnel about completeness (option A) is not a reliable way to confirm the change log is complete because it relies on subjective opinions and self-reported information, which may not be truthful or accurate. Taking an item from the log and tracing it back to the system (option B) is a technique called forward tracing, which can be used to verify that a specific change in the log has been implemented in the system. However, this technique does not confirm that all changes in the system are recorded in the log. Obtaining management attestation of completeness (option C) is not a sufficient way to confirm the change log is complete because it does not provide any evidence or verification of completeness. Management attestation may also be biased or influenced by conflicts of interest.
References:
IS Audit Basics: Auditing Data Privacy
Audit Logging: What It Is and How It Works | Datadog
Change Management for SOC: Risks, Controls, Audits, Guidance
Turn auditing on or off | Microsoft Learn
#118 | ITGC- System Change (Audit) Log Review - A2Q2

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu ↥**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **347**
設計段階にあるプロジェクトが組織目標を達成できるかどうかを判断する際、ビジネスケースと比較するのに最適な基準は何でしょうか？
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
正解: **(**正解を表示します**)**
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 asrequirements analysisfor comparing against the business case. References: CISA Review Manual (Digital Version), Chapter 4, Section 4.2.1

質問: **348**
フォローアップ監査の過程で、IS監査担当者は、最初の監査以降、主要な経営陣の一部が交代しており、現在の経営陣が以前に承認した勧告の一部を実施しないことを決定したことを知りました。監査担当者にとって最善の行動は何でしょうか？
A. 監査委員会の委員長に通知してください。
B. 監査マネージャーに通知してください。
C. コントロールを再テストします。
D. 監査結果をクローズします。
正解: **(**正解を表示します**)**
The auditor's best course of action in this situation is to notify the audit manager. The audit manager is responsible for overseeing the audit follow-up process and ensuring that audit issues are resolved in a timely and satisfactory manner. The audit manager can then decide whether to escalate the matter to higher authorities, such as the chair of the audit committee, or to accept management's decision and close the audit finding. The other options are not appropriate for the auditor to do without consulting with the audit manager first. Notifying the chair of the audit committee is a drastic step that may undermine the relationship between the auditor and management, and it should be done only after exhausting other means of resolving the issue.
Retesting the control is not necessary, as management has already decided not to implement therecommendations. Closing the audit finding is premature, as management's decision may not be aligned with the audit objectives or risk appetite. References: CISA Review Manual (Digital Version), Chapter 2, Section 2.4

質問: **349**

クレジットカードデータが関与するサイバー攻撃のフォレンジック調査において、以下のうちどれを最も確実にすることが重要ですか？
A. 適切なカードセキュリティ機能が有効になっています。
B. 同社の決済プラットフォームがブロックされています。
C. 適切な保管管理記録が維持されています。
D. 決済カード部門の全スタッフにインタビューを実施します。
正解: **(**正解を表示します**)**
In forensic investigations,maintaining a proper chain of custodyiscriticalto ensuring that evidence is admissible in court and has not been altered.
Option A (Incorrect):Activatingsecurity features(e.g., encryption or tokenization) is apreventive measurebut does not aid in investigating the attack.
Option B (Incorrect):Blocking payment platforms may be necessary fordamage control, but it does not ensure a properinvestigation.
Option C (Correct):Thechain of custodyensures thatevidence remains intact, can betraced, and islegally validfor prosecution. This is the most critical aspect of forensic investigations.
Option D (Incorrect):Interviewing staff may provide insights, but without properevidence handling, the investigation's integrity is at risk.
Reference:ISACA CISA Review Manual -Domain 5: Protection of Information Assets-Coversforensic investigations, evidence handling, and legal compliance.

質問: **350**
属性サンプリングは、以下の推定に最適です。
A. 承認された手順への準拠度
B. 母集団における総誤差量。
C. 人口の真の金銭的価値。
D. 平均からの標準偏差。
正解: **(**正解を表示します**)**

質問: **351**
デジタル署名によって最も防げる可能性が高いのは、次のうちどれでしょうか？
A. 否認
B. 不正な変更
C. 汚職
D. 開示
正解: **(**正解を表示します**)**
A digital signature is a cryptographic technique that uses the sender's private key to generate a unique code for a message or document. The receiver can use the sender's public key to verify the authenticity and integrity of the message or document. A digital signature can prevent unauthorized change, as any modification to the message or document will invalidate the signature and alert the receiver of tampering.

References
What is a digital signature?
Digital Signature - an overview | ScienceDirect Topics
ISACA CISA Review Manual, 27th Edition, page 253

質問: **352**
従来の人的資源(HR)システムからクラウドベースのシステムへのデータ移行に伴う最大のセキュリティリスクは、次のうちどれですか？
A. 送信元システムとターゲットシステムからのデータが傍受される可能性があります。
B. ソースシステムとターゲットシステムのデータは、データ形式が異なる場合があります。
C. 保存期間を過ぎた記録は、新しいシステムに移行できない場合があります。
D. システムのパフォーマンスは移行によって影響を受ける可能性があります
正解: **A (**コメントを発表する**)**
The greatest security risk associated with data migration from a legacy human resources (HR) system to a cloud-based system is data from the source and target system may be intercepted. Data interception is an attack that occurs when an unauthorized entity or individual captures or accesses data that are being transmitted or stored on an information system or network. Data interception can compromise the confidentiality and integrity of data, and cause harm or damage to data owners or users. Data migration from a legacy HR system to a cloud-based system involves transferring data from one system or location to another system or location over a network connection. This poses a high risk of data interception, as data may be exposed or vulnerable during transit or storage on unsecured or untrusted networks or systems. Data from the source and target system may have different data formats is a possible challenge associated with data migration from a legacy HR system to a cloud-based system, but it is not a security risk. Data formats are specifications that define how data are structured or encoded on an information system or network. Data formats may vary depending on different systems or platforms. Data migration may require converting data from one format to another format to ensure compatibility and interoperability between systems. Records past their retention period may not be migrated to the new system is a possible outcome associated with data migration from a legacy HR system to a cloud-based system, but it is not a security risk. Retention period is a duration that defines how long data should be kept or stored on an information system or network before being deleted or destroyed. Retention period may depend on various factors such as legal requirements, business needs, storage capacity, etc. Data migration may involve deleting or destroying data that are past their retention period to reduce the volume or complexity of data to be transferred or to comply with regulations or policies. System performance may be impacted by the migration is a possible impact associated with data migration from a legacy HR system to a cloud-based system, but it is not a security risk. System performance is a measure of how well an

information system or network functions or operates, such as speed, reliability, availability, etc. System performance may be affected by data migration, as data migration mayconsume significant resources or bandwidth, cause interruptions or delays, or introduce errors or inconsistencies.

質問: **353**
大規模な集団の中で、類似した行動や特徴を持つグループを特定しようとする場合、以下の分析方法のうちどれが最も有用でしょうか？
A. 偏差検出
B. クラスターサンプリング
C. ランダムサンプリング
D. 分類
正解: **D (**コメントを発表する**)**
The most useful analytical method when trying to identify groups with similar behavior or characteristics in a large population is classification. Classification is a technique that assigns data points to predefined categories or classes based on their features or attributes. Classification can help to discover patterns, trends, and relationships among the data and reveal the similarities or differences among the groups. Classification can also help to support decision making, prediction, or recommendation based on the data analysis. References:
CISA ReviewManual (Digital Version), Chapter 3, Section 3.4.21
CISA Online Review Course, Domain 2, Module 3, Lesson 12

質問: **354**
IS監査担当者が、組織の財務業務アプリケーションの論理アクセス制御をレビューしています。監査担当者にとって最も懸念すべき所見は次のうちどれですか？
A. ユーザーは定期的にパスワードを変更する必要はありません
B. 管理者はアプリケーションユーザーのアクティビティログを確認しません
C. ユーザーアカウントはユーザー間で共有されます
D. パスワードの長さは8文字に設定されています
正解: **(**正解を表示します**)**
The finding that should be of greatest concern to the IS auditor is that user accounts are shared between users.
User accounts are unique identifiers that grant access to an organization's financial business application based on the roles and responsibilities of the users. User accounts should be individualized and personalized to ensure accountability, traceability, and auditability of user actions and transactions. User accounts should not be shared between users, because this can compromise the confidentiality, integrity, and availability of the financial data and systems, and can enable unauthorized or fraudulent activities. If user accounts are shared between users, the IS auditor may not be able to determine who performed what action or transaction, or whether the user had the appropriate

authorization or approval. The other findings are also concerning, but not as much as user account sharing, because they either affect the password strength or frequency rather than the useridentity, or they relate to monitoring rather than controlling user access.
References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.2

質問: **355**
資産管理監査のフォローアップを実施している際、IS監査担当者は、組織の在庫に記録されていないIT機器の支払い済み請求書を発見しました。監査担当者が取るべき最善の行動は次のうちどれですか？
A. 請求書はフォローアップに含まれていないため無視してください。
B. 監査部門と運用部門の両方に不一致について警告する。
C. 将来の監査の範囲に含めるために、証拠をメモしておいてください。
D. 資産管理担当者にデバイスの所在を尋ねてください。
正解: **(**正解を表示します**)**

質問: **356**
組織がデータ消去を自動化する最も重要な理由は次のうちどれですか？
A. プライバシー侵害からの保護
B. 保管コスト削減
C. 災害復旧計画
D. ランサムウェア対策
正解: **(**正解を表示します**)**

質問: **357**
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どれですか？
A. 検査結果の偽陽性数が少ない
B. ネットワーク帯域幅がより効率的に利用されます
C. カスタム開発されたアプリケーションは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、多数の資産を対象とすることができます。
正解: **(**正解を表示します**)**
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

質問**: 358**
退職面談の際、経営陣は監査報告書の草案に記載されている事実の一部に異議を唱え、報告書から削除するよう求めました。監査人が取るべき最善の行動は次のうちどれでしょうか？
A. 上級管理職の異議に基づいて評価を修正する。
B. 問題を監査管理部門にエスカレーションしてください。
C. 監査報告書の草案を変更せずに最終決定する。
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
正解**: (**正解を表示します**)**
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 and Explanations Database, question ID 3338

質問**: 359**
IS 監査人がジョブ スケジューリング ソフトウェアをレビューし、処理時間の遅延、予期しないジョブの中断、および順序どおりにジョブが実行されない例に気づきました。これらの例の原因を特定するために、監査人が最初に調査する必要があるのは次のうちどれですか。

A. ジョブスケジュール
B. 例外ログ
C. システムスケジュール
D. 変更ログ
正解: **(**正解を表示します**)**

質問: **360**
IS監査のプロセスと実践の継続的な改善を促進するための最良の方法は、次のうちどれですか？
A. 外部監査人および規制当局を招き、IS監査機能の定期的な評価を実施する。
B. IS監査成果物に対する厳格な管理レビューと承認を実施する。
C. IS監査の方針、手順、および指示マニュアルを頻繁に確認する。
D. IS監査機能内に品質保証(QA)を確立し、組み込む。
正解: **(**正解を表示します**)**
The best way to foster continuous improvement of IS audit processes and practices is to establish and embed quality assurance (QA) within the IS audit function, as this will ensure that the IS audit activities are aligned with the standards, expectations, and objectives of the organization and the stakeholders12. QA involves periodic internal and external assessments, benchmarking, feedback, and root cause analysis to identify and address gaps, issues, and opportunities for improvement34.
References
1: The Basics and Principles of Continuous Improvement4 2: ISO 9001 Auditing Practices Group Guidance on5 3: INSIGHTS TO QUALITY3 4: Continuous Auditing: Coordinating Continuous Auditing and Monitoring to Provide Continuous Assurance2

質問: **361**
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
正解: **(**正解を表示します**)**
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.

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu 「**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **362**
次のうち、ソーシャルエンジニアリング攻撃の手法はどれですか？
A. 従業員が電話で質問に答えることで、機密のIPアドレスとパスワードを漏洩するように誘導される。
B. ハッカーがスキャンツールを使用してオフィスビル内を歩き回り、無線ネットワークを探してアクセス権を得ようとしています。
C. 侵入者がネットワークを流れる機密情報を盗聴・収集し、第三者に販売する。
D. 許可されていない人物が、許可された人物の後についてセキュリティドアを通ってセキュリティ施設に侵入しようとする。
正解: **(**正解を表示します**)**
Social engineering is a technique that exploits human weaknesses, such as trust, curiosity, or greed, to obtain information or access from a target. An employee is induced to reveal confidential IP addresses and passwords by answering questions over the phone is an example of a social engineering attack method, as it involves manipulating the employee into divulging sensitive information that can be used to compromise the network or system. A hacker walks around an office building using scanning tools to search for a wireless network to gain access, an intruder eavesdrops and collects sensitive information flowing through the network and sells it to third parties, and an unauthorized person attempts to gain access to secure premises by following an authorized person through a secure door are not examples of social engineering attack methods, as they do not involve human interaction or deception. References: [ISACA CISA Review Manual 27th Edition], page 361.

質問: **363**
データセンターの脅威評価をレビューするIS監査担当者が最も懸念するのは、次のような場合です。
A. 特定された喉の中には、発生する可能性が低いものもあります。

B. 識別された喉はすべて外部エンティティに関連しています。
C. 演習は現地管理によって完了しました。
D. 近隣組織の活動が含まれています。
正解: **(正解を表示します)**
An IS auditor reviewing the threat assessment for a data center would be most concerned if the exercise was completed by local management, because this could introduce bias, conflict of interest, or lack of expertise in the assessment process. A threat assessment is a systematic method of identifying and evaluating the potential threats that could affect the availability, integrity, or confidentiality of the data center and its assets. A threat assessmentshould be conducted by an independent and qualified team that has the necessary skills, knowledge, and experience to perform a comprehensive and objective analysis of the data center's environment, vulnerabilities, and risks1.
The other options are not as concerning as option C for an IS auditor reviewing the threat assessment for a data center. Option A, some of the identified threats are unlikely to occur, is not a problem as long as the likelihood and impact of each threat are properly estimated and prioritized. A threat assessment should consider all possible scenarios, even if they have a low probability of occurrence, to ensure that the data center is prepared for any eventuality2. Option B, all identified threats relate to external entities, is not a flaw as long as the assessment also considers internal threats, such as human errors, malicious insiders, or equipment failures. External threats are often more visible and severe than internal threats, butthey are not the only source of risk for a data center3. Option D, neighboring organizations' operations have been included, is not a mistake as long as the assessment also focuses on the data center's own operations. Neighboring organizations' operations may have an impact on the data center's security and availability, especially if they share physical or network infrastructure or resources. A threat assessmentshould take into account the interdependencies and interactions between the data center and its external environment4.
References:
ISACA, CISA Review Manual, 27th Edition, 2019
ISACA, CISA Review Questions, Answers and Explanations Database - 12 Month Subscription Data Center Threats and Vulnerabilities1 Datacenter threat, vulnerability, and risk assessment2 Data Centre Risk Assessment3

質問: **364**
ある組織は、収益性を向上させるために、複数の事業体に分割するという戦略的決定を下した。
しかし、ITインフラストラクチャは両組織間で共有されたままです。IS監査が年次計画の一環としてIT環境内の主要なリスク領域を確実に網羅するために、次のうちどれが最も役立つでしょうか？
A. 各事業体に対するリスクベースのIS監査の頻度を増やす

B. 各事業体の業務プロセスを考慮したリスクベースの計画を策定する
C. 新たに導入されたITポリシーと手順の監査を実施する
D. 分割後に導入されたIT変更に焦点を当てるため、IS監査計画を改訂する
正解: **B** (コメントを発表する)
Developing a risk-based plan considering each entity's business processes would best help to ensure that IS audit still covers key risk areas within the IT environment as part of its annual plan. A risk-based plan is a plan that prioritizes the audit activities based on the level of risk associated with each area or process. A risk- based plan can help to allocate the audit resources more efficiently and effectively, and provide more assurance and value to the stakeholders1.
By considering each entity's business processes, the IS audit can identify and assess the specific risks and controls that affect the IT environment of each entity, and tailor the audit objectives, scope,and procedures accordingly. This can help to address the unique needs and expectations of eachentity, and ensure that the IS audit covers the key risk areas that are relevant and significant to each entity's operations, performance, and compliance2.
The other options are not as effective as developing a risk-based plan considering each entity's business processes in ensuring that IS audit still covers key risk areas within the IT environment as part of its annual plan. Option A, increasing the frequency of risk-based IS audits for each business entity, is not a feasible or efficient solution, as it may increase the audit costs and workload, and create duplication or overlap of audit efforts. Option C, conducting an audit of newly introduced IT policies and procedures, is a limited and narrow approach, as it may not cover all the aspects or dimensions of the IT environment that may have changed or been affected by the split. Option D, revising IS audit plans to focus on IT changes introduced after the split, is a reactive and short-term approach, as it may not reflect the current or future state of the IT environment or the business objectives of each entity.
References:
ISACA, CISA Review Manual, 27th Edition, 2019
ISACA, CISA Review Questions, Answers and Explanations Database - 12 Month Subscription Risk-Based Audit Planning: A Guide for Internal Audit1 Risk-Based Audit Approach: Definition and Example

質問: **365**
災害復旧計画プロセスの主な目的は次のとおりです。
A. データが完全に回復できることを確認します。
B. 運用の中断を最小限に抑えます。
C. インシデント対応時間を業界のベストプラクティスに合わせて調整します。
D. 規制要件に準拠します。
正解: (正解を表示します)

質問: **366**
IS監査人が監査フォローアップ活動を開始する前に、以下のうちどれが準備されてい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、実施予定日
C. リスクの観点からギャップと推奨事項が表示された治癒マップ
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
正解: **(正解を表示します)**
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.

質問: **367**
最近ランサムウェア攻撃を受けた組織の監査を実施するIS監査担当者にとって、以下のうちどれが最も懸念すべき事項でしょうか？

A. ウイルス対策ソフトウェアは適切にアップデートされていたにもかかわらず、攻撃を防ぐことができませんでした。
B. 最新のセキュリティパッチは実装前にテストされていません。
C. バックアップはローカルネットワーク内でのみ実行されました
D. 従業員はサイバーセキュリティの方針と手順に関する研修を受けていなかった。
正解: **(**正解を表示します**)**
The greatest concern to an IS auditor conducting an audit of an organization that recently experienced a ransomware attack is that backups were only performed within the local network. This means that the backups could have been encrypted or deleted by the ransomware, making it impossible to restore the data and systems without paying the ransom or losing the data. Backups are a critical part of the recovery process from a ransomware attack, and they should be performed frequently, securely, and off-site or in the cloud to ensure their availability and integrity.
The other options are not as concerning as option C, although they may also indicate some security weaknesses. Antivirus software was unable to prevent the attack even though it was properly updated, but this is not surprising given that ransomware variants are constantly evolving and antivirus software may not be able to detect them all. The most recent security patches were not tested prior to implementation, but this is a trade-off between security and availability that may be justified depending on the severity and urgency of the patches. Employees were not trained on cybersecurity policies and procedures, but this is a preventive measure that may not have prevented the attack if it was initiated by other means such as phishing or exploiting vulnerabilities.
References:
10: Infrastructure-as-a-Service Security Responsibilities - CloudTweaks
5: 3 steps to prevent and recover from ransomware | Microsoft Security Blog
7: How to Recover From a Ransomware Attack - eSecurityPlanet

質問: **368**
データセンターの監視カメラ(CCTV)に関連する以下の問題のうち、IS監査担当者が最も懸念すべき点はどれでしょうか？
A. CCTVの録画映像は定期的に確認されていません。
B. 休憩室には防犯カメラは設置されていません
C. CCTVの録画は1年後に削除されます。
D. CCTV映像は24時間365日録画されているわけではありません。
正解: **(**正解を表示します**)**
The most concerning issue associated with a data center's CCTV surveillance cameras is that the recordings are not regularly reviewed. This means that any unauthorized access, theft, vandalism, or other security incidents may go unnoticed and unreported. CCTV recordings are a valuable source of evidence and deterrence for data center security, and they should be monitored and audited periodically to ensure compliance with policies and

regulations. If the recordings are not reviewed, the data center may face legal, financial, or reputational risks in case of a security breach or an audit failure.
The other options are less concerning because they do not directly affect the security of the data center. CCTV cameras are not required to be installed in break rooms, as they are not critical areas for data protection.
CCTV records can be deleted after one year, as long as they comply with the data retention policy of the organization and the applicable laws. CCTV footage does not need to be recorded 24 x 7, as long as there is sufficient coverage of the data center during operational hours and when access is granted to authorized personnel. References:
ISACA Journal Article: Physical security of a data center1
Data Center Security: Checklist and Best Practices | Kisi2
Video Surveillance Best Practices | Taylored Systems

質問: **369**
組織が、オンサイト業務から完全リモート業務へと恒久的に移行する場合、既存の事業影響分析(BIA)はいつ見直すべきでしょうか？
A. 次回の定期レビュー時に
B. 移行後少なくとも1年経過
C. 新しい運用モデルが導入され次第
D. 移行に関する決定が発表され次第
正解: **(**正解を表示します**)**

質問: **370**
情報システムセキュリティ担当者のビジネスプロセスアプリケーションに関する主な責任は以下のとおりです。
A. 安全な緊急アクセスを許可する
B. 組織のセキュリティポリシーを承認する
C. アクセスルールがポリシーと一致することを確認する
D. 各ビジネスプロセスに対してロールベースのルールを作成する
正解: **(**正解を表示します**)**
Ensuring access rules agree with policies is an information systems security officer's primary responsibility for business process applications. An information systems security officer should verifythat the access controls implemented for the business process applications are consistent with the organization's security policy and objectives. The other options are not the primary responsibility of an information systems security officer, but rather the tasks of an application owner, a senior management, or a business analyst. References:
CISA Review Manual (Digital Version), Chapter 7, Section 7.3.11
CISA Review Questions, Answers and Explanations Database, Question ID 208

質問: **371**

コントロール自己評価(CSA)ファシリテーターの主な役割は以下のとおりです。
A. 背景情報を得るためにインタビューを実施する。
B. チームを内部統制に集中させる。
C. 内部統制の弱点に関する報告書。
D. 制御の弱点に対する解決策を提供する。
正解: **(**正解を表示します**)**
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 and Explanations Database - 12 Month Subscription, QID
1066693
PwC, Control Self Assessments4
Workiva, 4factors of an effective control self-assessment (CSA) program5

質問: **372**
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、以下の点を提供することです。
A. 間接費を配分するための基準。
B. 機器の交換費用。
C. 推定所有コスト。
D. 財源配分の基準。
正解: **(**正解を表示します**)**
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

質問: **373**
データセンターが利用できなくなるような災害が発生した場合、以下のタスクのうち、最初に実行すべきものはどれですか？
A. データ復旧を実行します。
B. 二次的な場所を手配する。
C. リスクを分析する。
D. コールツリーをアクティブ化します。
正解: **D** (コメントを発表する)
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

質問: **374**
IS監査担当者が、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た。監査担当者の主な懸念事項は次のとおりである。
A. 組織のリスクプロファイルによっては、違反報告書を保持しない場合があります。
B. 違反報告は適時に審査されない場合があります。
C. かなりの数の誤検出違反が報告される可能性があります。
D. 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場合があります。
正解: (正解を表示します)

質問: **375**
サードパーティシステムの導入案に関するビジネスケースをレビューする際、IS監査担当者が最も懸念すべき事項は次のうちどれでしょうか？
A. 継続的なメンテナンス費用がかからない
B. 研修教材の不足
C. パイロット実施計画の欠如
D. 詳細な作業分解構造の欠如
正解: **A** (コメントを発表する)

The IS auditor's greatest concern when reviewing a business case for a proposed implementation of a third- party system should be A. Lack of ongoing maintenance costs. This is because ongoing maintenance costs are an essential part of the total cost of ownership (TCO) of a third-party system, and they can have a significant impact on the return on investment (ROI) and the feasibility of the project. If the business case does not include ongoing maintenance costs, it may underestimate the true cost of the project and overestimate the benefits. This could lead to poor decision making and unrealistic expectations.
Lack of training materials (B), lack of plan for pilot implementation , and lack of detailed work breakdown structure (D) are also potential issues that could affect the quality and success of the project, but they are not as critical as lack of ongoing maintenance costs. Training materials can be developed or acquired later, pilot implementation can be planned during the project initiation or planning phase, and work breakdown structure can be refined as the project progresses. However, ongoing maintenance costs are difficult to change or estimate once the project is approved and implemented, and they can have long-term implications for the organization. Therefore, they should be included and analyzed in the business case.

質問: **376**
IS監査担当者が医療施設の物理セキュリティ監査を実施したところ、患者ケアエリアに監視カメラ(CCTV)システムが設置されていることが判明しました。以下のうち、最も懸念されるのはどれですか？
A. カメラは24時間365日監視されているわけではありません。
B. ISの記録が進行中であることを示す通知はありません。
C. ビデオ録画の保存期間は未定義です
D. 動画のバックアップはありません。
正解: **(**正解を表示します**)**
The greatest concern with finding closed-circuit television (CCTV) systems located in a patient care area is that there are no notices indicating recording is in progress. This is because CCTV systems in healthcare settings can pose a threat to the privacy and confidentiality of patients, staff, and visitors, especially in sensitive areas where personal or medical information may be exposed. According to the government's Surveillance camera code of practice1, CCTV operators must be as transparent as possible in the use of CCTV, and inform people that they are being recorded by using clear and visible signs. The signs should also provide contact details of the CCTV operator and the purpose of the surveillance. By providing notices, CCTV operators can comply with data protection law and respect the rights and expectations of individuals.
Option B is correct because the lack of notices indicating recording is in progress is a clear violation of the Surveillance camera code of practice1, which applies to local authorities and the police, and is encouraged to be adopted by other CCTV operators in England and

Wales. The code also applies to Scotland, along with the National Strategy for Public Space CCTV2. The code is intended to be used in conjunction with the guidance provided by the Information Commissioner's Office (ICO)3, which applies across the UK. The ICO states that CCTV operators must inform people that they are being recorded by using prominent signs at the entrance of the CCTV zone and reinforcing this with further signs inside the area.
Option A is incorrect because cameras not being monitored 24/7 is not the greatest concern, as it does not necessarily affect the privacy and confidentiality of individuals. CCTV systems may have different purposes and objectives, such as deterring or monitoring crime, enhancing security, or improving patient care.
Depending on the purpose, CCTV systems may not require constant monitoring, but rather periodic review or analysis. However, CCTV operators should still ensure that they have adequate security measures to protect the CCTV systems from unauthorized access or tampering.
Option C is incorrect because the retention period for video recordings being undefined is not the greatest concern, as it does not directly affect the privacy and confidentiality of individuals. However, CCTV operators should still define and document their retention policy, and ensure that they do not keep video recordings for longer than necessary, unless they are needed for a specific purpose or as evidence. The retention period should be based on a clear and justifiable rationale, and comply with data protection law and industry guidelines.
Option D is incorrect because there being no backups of the videos is not the greatest concern, as it does not affect the privacy and confidentiality of individuals. However, CCTV operators should still consider having backups of their videos, especially if they are needed for a specific purpose or as evidence. Backups can help to prevent data loss or corruption due to system failures, disasters, or malicious attacks. Backups should also be stored securely and encrypted to prevent unauthorized access or disclosure.

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu　**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **377**
IS監査担当者が、業務担当者が期末財務諸表作成に必要なスクリプトを実行し忘れていたことを発見しました。以下のうち、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する。

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部門に配置転換する。
正解: **B (**コメントを発表する**)**
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

質問: **378**
ITプロジェクトで完了した作業が予算コストと一致しているかどうかを判断する際に、最も適切なレビュー対象は次のうちどれですか？
A. 投資収益率(ROI)分析
B. 出来高分析(EVA)
C. 財務価値分析
D. 事業影響分析(BIA)
正解: **(**正解を表示します**)**
EVA is a project management technique that measures the performance of a project by comparing the actual work completed, the actual costs incurred, and the planned costs for the work scheduled. EVA can help determine if the project is on track, ahead of schedule, or behind schedule, and if the project is under budget, over budget, or on budget. EVA can also help forecast the final cost and schedule of the project based on the current performance.
References
ISACA CISA Review Manual, 27th Edition, page 255
18. Project Completion - Project Management - 2nd Edition
How to Measure Project Success | Smartsheet

質問: **379**
データセンターへの請負業者のアクセスを管理する最も効果的な方法は何ですか？
A. 訪問者が着用するバッジ識別
B. 訪問者の入館には付き添いが必要です
C. 訪問者の身分証明書の確認
D. 訪問者のアクセスに対する管理者の承認

正解: **(**正解を表示します**)**

質問: **380**
IS監査担当者が、知的財産および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策をレビューしています。監査担当者が最も懸念すべき点は次のうちどれでしょうか？
A. 知的財産権および特許を扱う部署には研修が提供されなかった。
B. コンテンツフィルタリングのログ記録と監視は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. この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。
正解: **(**正解を表示します**)**
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 anactivity 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.

質問: **381**
組織のセキュリティプログラムの有効性を測る上で最も重要な指標は、次のとおりです。
A. インシデントが重要な事業活動に及ぼす悪影響。
B. 報告された新たな脆弱性の数。
C. 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。
D. 競合他社が経験した重大なインシデントとの比較。
正解: **A** (コメントを発表する)

質問: **382**
経営陣は、監査勧告案を受けてリスクを受け入れることを決定しました。IS監査担当者は次にどのような行動を取るべきでしょうか？
A. 承認を監査委員会にエスカレーションする。
B. 来年の計画にフォローアップ監査が含まれていることを確認してください。
C. 承認を役員会にエスカレートする。
D. 監査報告書における文書管理の承認。
正解: **D** (コメントを発表する)

質問: **383**
情報システム監査担当者がVoIP(Voice-over IP)通信に関して考慮すべき最も重要な事項は次のうちどれですか？

A. サービスの継続性
B. ID管理
C. ネットワークの均一性
D. 否認防止
正解**: (**正解を表示します**)**
The most important issue for an IS auditor to consider with regard to Voice-over IP (VoIP) communications is the homogeneity of the network, because it affects the quality, security, and reliability of the VoIP service. Ahomogeneous network is one that uses a single protocol or standard for VoIP communication, such as Session Initiation Protocol (SIP) or H.32312. A homogeneous network can reduce thecomplexity, latency, and interoperability issues that may arise from using different or incompatible protocols or devices forVoIP communication12. Continuity of service, identity management, and nonrepudiation are also important issues for VoIP communications, but not as important as the homogeneity of the network. References: 1: CISA Review Manual (Digital Version), Chapter 4, Section 4.4.3 2: CISA Online Review Course, Module 4, Lesson 4

質問**: 384**
小規模事業部門が、内部統制自己評価(CSA)プログラムを導入し、内部監査機能を活用して内部統制を毎年テストしています。このアプローチの最も重要な利点は次のうちどれですか？
A. コンプライアンスコストが削減されます。
B. リスクがより早期に検出されます。
C. 経営者は、本来の役割に集中できるようになります。
D. ラインマネジメントは、制御例外を回避することに、より意欲的である。
正解**: (**正解を表示します**)**
The most significant benefit of implementing a control self-assessment (CSA) program and leveraging the internal audit function to test its internal controls annually is that risks are detected earlier. A CSA program is a process that enables business owners and managers to assess and improve their own internal controls on a regular basis, without relying on external auditors or consultants. A CSA program can help identify and mitigate risks, enhance performance, increase accountability, and foster a culture of control within the organization. By leveraging the internal audit function to test its internal controls annually, a small business unit can also obtain independent assurance and validation of its CSA results, as well as recommendations for improvement. This approach can help reduce compliance costs, as external audits may be less frequent or extensive. However, this is not the most significant benefit, as compliance costs are only one aspect of the total cost of risk. Business owners can also focus more on their core roles, as they can delegate some of their control responsibilities to their staff or teams through CSA. However, this is not the most significant benefit, as business owners still need to oversee and monitor their CSA activities and results, and ensure that they align with their strategic objectives and

priorities. Line management may also be more motivated to avoid control exceptions, as they are directly involved in assessing and improving their own controls through CSA. However, this is not the most significant benefit, as motivation alone may not be sufficient to ensure effective control design and operation. References: Info Technology and Systems Resources | COBIT, Risk, Governance ... - ISACA, IT Governance and Process Maturity

質問: **385**
IT監査組織における役割と責任を定義する文書として、次のうちどれが適切でしょうか？
A. 監査憲章
B. 年間監査計画
C. 婚約書
D. 監査範囲に関する書簡
正解: **A (**コメントを発表する**)**
Theaudit charteris a formal document that definesthe purpose, authority, and responsibilitiesof the internal audit function.
Audit Charter (Correct Answer - A)
Establishesroles, reporting structure, and independenceof the audit team.
Example:TheIS audit team's roleinrisk assessmentsis outlined in the charter.
Annual Audit Plan (Incorrect - B)
Outlinesaudit activitiesbutdoes not define roles and responsibilities.
Engagement Letter (Incorrect - C)
Used forspecific audits, not theentire audit function.
Audit Scope Letter (Incorrect - D)
Detailswhat is coveredin an audit but doesnot define responsibilities.
References:
ISACA CISA Review Manual
COBIT 2019 (Audit Governance)

質問: **386**
IS品質保証(OA)グループは以下の責任を負います。
A. プログラムの変更が確立された基準に準拠していることを確認する。
B. 偶発的なデータ漏洩からデータを保護するための手順を設計する。
C. システム処理から受け取った出力が完全であることを保証します。
D. コンピュータ処理タスクの実行を監視する。
正解: **(**正解を表示します**)**
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 dataagainst 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.

質問**: 387**
大規模金融機関に対する継続監査において、以下のうちどれが最適なプロセスでしょうか？
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. システム間で並列テストを実行する
D. ヘルプデスク指標のパフォーマンスを検証する
正解**: B (**コメントを発表する**)**
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

質問**: 388**
組織がITセキュリティ要件に影響を与える可能性のある新しい規制を認識した場合、IS監査担当者は以下のうちどれを最初に行うよう推奨すべきでしょうか？
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のあるシステムとIT関連プロセスを特定します。
C. セキュリティ意識向上とトレーニング内容にどのような影響があるかを評価する。
D. 既存のIT統制の設計と有効性をレビューする。
正解**: (**正解を表示します**)**
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 resourcesto 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 invalidfindings that may not capture the regulatory requirements or the organizational performance

質問: **389**
組織における新しいIT資産の安全な構成を確保するために、最初に行うべきことは次のうちどれですか？
A. 新しいIT資産を導入する前に、脆弱性を特定して修復する。
B. 強化基準を定義し、実装する。
C. 新しいIT資産のセキュリティ脆弱性をスキャンします。
D. 新しいIT資産を構成するためのセキュリティツールを購入する。
正解: **B (**コメントを発表する**)**
The first step in ensuring secure configuration of new IT assets is to establish the baseline configuration requirements those assets must meet. ISACA guidance supports the use of documented security configuration standards, secure baselines, and hardening requirements before deployment. Without predefined hardening standards, vulnerability scanning or remediation lacks a clear benchmark for what "secure" should look like.
Option B is correct because defining and implementing hardening standards establishes the secure baseline for systems, operating systems, applications, and devices. ISACA material notes that resources should adhere to a minimum-security baseline composed of standard security configurations, and secure configurations should be documented and maintained. This makes hardening standards the logical and control-oriented first step.
Option A is not first. Identifying and remediating vulnerabilities is important, but this activity should follow the establishment of hardening standards. Otherwise, there is no approved baseline against which to assess and remediate deviations. In CISA logic, standards come before testing against standards.
Option C is also not first for the same reason. Vulnerability scanning is an assessment technique, but organizations must first define the secure configuration baseline or hardening standard to know what they expect from the asset. Scanning should validate configuration and identify weaknesses after standards have been established.
Option D is clearly incorrect because purchasing tools is not the starting point of good control design. Tools may support implementation and verification, but governance requires that standards be defined first. In ISACA terms, sound control begins with policy, standards, and procedures, not with tool acquisition.

Therefore, the best answer is B because secure configuration starts with defining and applying hardening standards, which then enable scanning, validation, and remediation activities.
References (Official ISACA):
* ISACA-linked guidance, A Look at CIS Controls Version 7.1 - "Establish Secure Configurations" and maintain documented security configuration standards.
* ISACA, Best Practices for Auditable Security Controls - all resources should adhere to a minimum- security baseline of standard security configurations.
* ISACA, Can Hardening Reduce Cyberrisk? - highlights hardening systems and infrastructure to reduce risk.
* ISACA, Digital Businesses Need Tailored Security Solutions and Services - refers to minimum baseline hardening standards and guidelines.

質問: **390**
内部ネットワークセグメント間のファイアウォールは、以下の点によりセキュリティを向上させ、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します
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報告
D. 接続され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。
正解: **(**正解を表示します**)**
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 and Systems Resources | COBIT, Risk, Governance ... - ISACA, section "Book COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution | Digital | English"

質問: **391**
効果的な災害復旧計画(DRP)が策定されていることを最もよく示すのは、次のうちどれでしょうか？
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. 完全動作テスト
正解: **(**正解を表示します**)**
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 betested regularly and thoroughly to identify and resolve any issues or gaps that might hinder itsexecution2345. 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 toensure that the backup systems, data, anddocumentation 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 andperformance 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.
Amongthese methods, full interruption testing would best demonstrate that an effectiveDRP is in place, as it provides the most accurate and comprehensive evaluation ofthe 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 ofthe 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 normaloperations4. Therefore, it should be planned

carefullyand 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 atheoretical 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 toKnow - Enterprise Storage Forum 5: Disaster Recovery Testing Best Practices - MSP360 1: How to Test a Disaster Recovery Plan - Abacus

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu　**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **392**
導入前の評価において、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. 事業計画は利害関係者の要求を反映しています。
B. ビジネスケースは実績のある方法論に基づいています。
C. 事業計画は独立機関による品質審査に合格しました。
D. ビジネスケースでは、コスト配分に関する具体的な計画が示されています。
正解: **A** (コメントを発表する)
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]

質問: **393**
ドメインコントローラーの既知の脆弱性をハッカーが悪用したセキュリティ侵害を受けて、IS監査部門が統制評価を実施するよう依頼された。監査担当者の最善の行動は、以下の点を判断することである。
A. パッチが更新されました。
B. ログが監視されました。
C. ネットワークトラフィックが監視されていました。
D. ドメインコントローラは高可用性用に分類されました。
正解: **(**正解を表示します**)**
The auditor's best course of action after a security breach in which a hacker exploited a well-known vulnerability in the domain controller is to determine if the logs were monitored. Log monitoring is an essential control for detecting and responding to security incidents, especially when known vulnerabilities exist in the system. The auditor should assess if the logs were properly configured, collected, reviewed, analyzed, and acted upon by the responsible parties. Updating patches, monitoring network traffic, and classifying domain controllers for high availability are also important controls, but they are not directly related to the detection and response of the security breach. References:
CISA Review Manual (Digital Version), page 301
CISA Questions, Answers and Explanations Database, question ID 3340

質問: **394**

ソフトウェア開発プロジェクトが予定通り完了する見込みであることを示す最良の指標は、次のうちどれですか？
A. 技術仕様と開発要件が合意され、正式に記録されました。
B. ソフトウェア開発ライフサイクルの各フェーズについて、プロジェクト計画の期日が文書化されています。
C. 予定されているソフトウェアの稼働開始日は、エンドユーザーおよび関係者に事前に通知されています。
D. ユーザー受け入れテスト (UAT) 中に特定された問題は、当初の実装日より前に解決済みです。
正解: **(**正解を表示します**)**

質問: **395**
IT資産の廃棄プロセスをレビューする際に、IS監査担当者が最も懸念すべき事項は次のうちどれですか？
A. 資産の金銭的価値。
B. 廃棄証明書。
C. 新しい資産へのデータ移行。
D. 資産に保存されているデータ。
正解: **(**正解を表示します**)**
The correct answer is D. Data stored on the asset.
When reviewing IT asset disposal, the auditor's most important concern is whether sensitive, confidential, regulated, or business-critical data remains on the asset. Even if the hardware has little monetary value, the data stored on it may expose the organization to privacy breaches, regulatory penalties, intellectual property loss, reputational damage, or legal liability.
ISACA discusses secure disposal as an important control area and notes that data disposal protects personal data from exposure. ISACA also identifies disposal methods such as data anonymization, data deletion, crypto-shredding, degaussing, and destruction.
ISACA's CISA Exam Content Outline includes IT asset management under Domain 4 and data loss prevention, data encryption, and information asset security controls under Domain 5.
Option A is not the best answer because the monetary value of the hardware is usually less important than the sensitivity of the data. Option B is important, but a certificate of destruction is evidence of disposal; the auditor must first be concerned with whether the data was properly protected or removed. Option C may be relevant when replacing equipment, but the most significant disposal risk is residual data remaining on the retired asset.
A good CISA exam rule is: during asset disposal, focus first on data confidentiality and sanitization, not hardware value.

References: ISACA CISA Exam Content Outline, Domains 4 and 5; ISACA podcast/article page, Why (And How to) Dispose of Digital Data.

質問: **396**
組織がビジネス目標に合わせてITインフラストラクチャを標準化するために、最も効果的な方法はどれですか？
A. エンタープライズアーキテクチャ(EA)
B. 運用技術
C. データアーキテクチャ
D. ロボティック・プロセス・オートメーション(RPA)
正解: **(**正解を表示します**)**

質問: **397**
組織が、企業ネットワークへの不正なモノのインターネット (IoT) デバイスの接続を防止するための効果的な制御を備え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. 認証されたネットワークの脆弱性スキャン結果を確認する
B. 実装されたIoTデバイス構成の評価
C. ネットワークアクセス制御（NAC）構成の評価
D. IoTの認可に関するITポリシーの見直し
正解: **(**正解を表示します**)**
Comprehensive and Detailed Explanation:
The most effective way to prevent unauthorized IoT devices from connecting is through network access control (NAC), which enforces authentication and authorization before allowing a device onto the network.
* Vulnerability scans (A): Identify weaknesses but do not actively prevent device connections.
* Reviewing IoT configurations (B): Focuses on existing devices, not unauthorized ones.
* Policies (D): Provide guidance but do not enforce technical prevention.
# ISACA Reference: CISA Review Manual 27th Edition, Domain 5, section on network security and endpoint access control.

質問: **398**
ローカル通信ループへの冗長なインターネット接続の組み合わせを提供する復旧設備は、どのタイプの通信継続性の例ですか？
A. 音声復元
B. 代替ルート
C. 長距離ネットワークの多様性
D. ラストマイル回路保護
正解: **(**正解を表示します**)**

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. Byhavingmultiple Internet connections from different providers or technologies, such as cable, DSL, fiber, wireless, or satellite, the recoveryfacilities 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

質問: **399**
外部監査において、情報システム監査担当者は、組織内でシステムの重要度分類に一貫性がないことに気づきました。システムの重要度を判断するための主たる要素として、次のうちどれを推奨すべきでしょうか？
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)
正解: **(**正解を表示します**)**
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 onthe organization's operations, reputation, compliance, and finances. MAD can help to prioritize system recovery efforts, allocate resources, and establish recovery objectives.

質問: **400**
システム障害発生時の調査において、情報システム監査担当者は、ITサポートスタッフが権限レベルを超えた意思決定を行う立場に置かれていたことを指摘した。
今後このような事態を防ぐための最善策は、次のうちどれでしょうか？
A. エスカレーションプロトコルを導入する。
B. 能力マトリックスを作成する。
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。
正解: **A (**コメントを発表する**)**

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?

質問: **401**
あるスタートアップ企業がデータ損失防止(DLP)プログラムを開発しようとしている。最初のステップとして、以下のことを実装する必要がある。
A. データ暗号化
B. セキュリティ意識向上トレーニング
C. データ分類
D. アクセス制御
正解: **(**正解を表示します**)**

質問: **402**
IS監査担当者は、システム障害のビジネスへの影響を最も適切に評価するために、以下の方法を用いることができます。
A. システム生成ログを確認しています。
B. ユーザー満足度レベルの評価。
C. 機器保守ログの分析。
D. セキュリティ管理者にインタビューする。
正解: **(**正解を表示します**)**

質問: **403**
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. 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

B. 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
C. 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
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
正解: **(**正解を表示します**)**

質問: **404**
継続監査に最も適しているのは、次のうちどれですか？
A. 少額取引
B. リアルライム取引
C. 不規則な取引
D. 手動トランザクション
正解: **(**正解を表示します**)**
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 and Explanations Database, Question ID: 253

質問: **405**
IT管理に関する組織の標準とガイドラインの見直しにおいて、IS開発方法論に含めるべき項目は次のうちどれですか？
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
正解: **(**正解を表示します**)**
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 developinginformation 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

質問: **406**
ある組織は、消費者間取引を可能にするeコマースプラットフォームを提供しています。このプラットフォームは現在、ブロックチェーン技術を使用して、取引当事者が取引を否認できないようにしています。この技術が対処しているリスク要素を最もよく表しているのは、次のうちどれですか？
A. 否認防止
B. 機密保持
C. 誠実さ
D. 利用可能性
正解: **A** (コメントを発表する)

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu ↥**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **407**

IS監査人がデータ分析手法を用いる主な理由は、どのタイプの監査リスクを軽減するためですか？
A. テクノロジーリスク
B. 検出リスク
C. リスク管理
D. 固有のリスク
正解: **(**正解を表示します**)**
The primary reason for an IS auditor to use data analytics techniques is to reduce detection risk. Detection risk is the risk that an IS auditor will fail to detect material errors or irregularities in the information systems environment. By using data analytics techniques, such as data extraction, analysis, visualization, and reporting, an IS auditor can enhance the audit scope, coverage, efficiency, and effectiveness. Data analytics techniques can help an IS auditor to identify anomalies, patterns, trends, correlations, and outliers in large volumes of data that may indicate potential issues or risks. Technology risk, control risk, and inherent risk are types of audit risk that are not directly affected by the use of data analytics techniques by an IS auditor. References: [ISACA Journal Article: Data Analytics for Auditors]

質問: **408**
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導入計画段階で、最も重要な決定事項は次のうちどれですか？
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およびオフボーディングのプロセス
D. 管理者アクティビティをレビューするためのプロセス
正解: **A (**コメントを発表する**)**
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 thatgovern 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 uploadedto 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 communicationswith the acquisition of Cloud9 Technologies3 Cloud messaging and collaboration | Sumo Logic

質問: **409**
有効な数値部品番号を入力する際の、最も効果的な精度管理方法は次のうちどれですか？
A. ハッシュ合計
B. 説明のオンラインレビュー
C. 過去の注文パターンとの比較
D. 自己チェック数字
正解: **(**正解を表示します**)**
A self-checking digit is the most effective accuracy control for entry of a valid numeric part number. This method involves adding an extra digit at the end of every number which is calculated from the other digits. This digit is then used to check the accuracy of the entered number1. While hash totals, online review of description, and comparison to historical order pattern can be used as accuracy controls, they are not as effective as a self-checking digit.

質問: **410**
送信取引の完全性を確保するために最も効果的な管理策は次のうちどれですか？
A. 編集チェックを実行して、誤った、異常な、または無効な取引を特定します。
B. ヘッダーレコード内のトランザクションが連番になっていることを確認します。
C. 受信者IDの有効性を確認し、自動番号付きレポートを使用してください。
D. 送信されたメッセージ数のログを保持し、定期的に検証します。
正解: **(**正解を表示します**)**
To ensurecompleteness of outbound transactions, alog with periodic validationis thebest control.
Option A (Incorrect):Edit checkshelp withdata accuracy, not completeness.

Option B (Incorrect):Sequential numberingdetects missing transactions but does not verifyactual transmission.
Option C (Incorrect):Recipient ID validationis important foraccuracy, not for ensuring all transactions are sent.
Option D (Correct):Maintaining and validating transaction logsensures thatall outbound transactions are properly accounted for, making it the best completeness control.
Reference:ISACA CISA Review Manual -Domain 3: Information Systems Acquisition, Development, and Implementation- Coversdata integrity, completeness controls, and transaction logging.

質問: **411**
フォローアップ監査において、IS監査担当者は、最初の監査では問題とならなかった問題の証拠を確認しました。監査担当者にとって最適な対応策は次のうちどれでしょうか？
A. 証拠の検証を含めるようにフォローアップの範囲を拡大する。
B. フォローアップレポートでリスクを経営陣に報告してください。
C. 証拠を今後の監査の一部として含める。
D. フォローアップの範囲内の領域についてのみ報告してください。
正解: **(**正解を表示します**)**

質問: **412**
新規アプリケーションのビジネスケース開発において、IS監査担当者は主に以下の事項に関与すべきである。
A. システムテスト。
B. トランザクションの設計図。
C. ユーザー受け入れテスト (UAT)。
D. 実現可能性調査。
正解: **D (**コメントを発表する**)**
The best answer is D. Feasibility study.
ISACA guidance notes that, in projects, an auditor reviews the feasibility of projects based on resources, time, and other factors, and evaluates whether projects are aligned with the organization's strategic goals. That is exactly the stage where internal audit's advisory involvement is most appropriate during development of the business case.
Option A, B, and C occur later in the system development lifecycle and are more operational or project- delivery focused. The question is specifically about the development of a business case, and feasibility analysis is the phase most directly tied to whether the initiative is practical, justified, and aligned with business goals.
References (Official ISACA):
ISACA Journal, Innovation and the Auditor.
ISACA, An Appropriate Approach for Program and Project Management.

質問: **413**
IS監査担当者は、ITマネージャーがコスト削減のために最近SaaS(Software as a Service)プロバイダーとの契約を変更したことを発見しました。新しい契約では、インシデントの解決に要する時間が増加しています。監査担当者が最も懸念すべき事項は次のうちどれでしょうか？
A. 新しい契約はITセキュリティポリシーに準拠していません。
B. 代替のコスト削減方法は検討されなかった。
C. 業務プロセスへの影響は評価されていません。
D. 該当するサービスレベル契約(SLA)は変更されていません。
正解: **C (**コメントを発表する**)**
The correct answer is C. The impact on business processes has not been evaluated.
The auditor's greatest concern is not simply that the contract became cheaper or that incident resolution time increased. The key concern is whether management evaluated the business impact of the longer incident resolution time. A longer incident resolution period may affect system availability, customer service, operational processing, contractual commitments, regulatory obligations, or business continuity.
ISACA defines a service level agreement as an agreement between a service provider and customer that defines minimum performance targets for a service and how those targets will be measured. ISACA's CISA Exam Content Outline includes IT vendor management, IT service level management, problem and incident management, and evaluating whether IT service management practices align with organizational requirements.
Option A may be a concern if the new contract violates security policy, but the question does not state that it does. Option B is not the greatest concern because failing to consider alternative cost reductions is a management efficiency issue, not the primary audit risk.
Option D is a concern because the SLA should match the contract, but updating the SLA alone does not solve the more important issue: whether the changed incident response commitment is acceptable to the business.
In CISA terms, IT decisions should be evaluated based on business impact and alignment, not only cost savings. A cheaper SaaS contract may create unacceptable operational risk if slower incident resolution affects critical business processes.
References: ISACA CISA Exam Content Outline, Domains 2 and 4; ISACA Interactive Glossary, "Service level agreement."

質問: **414**
次のうち、仮想化に関連する懸念事項はどれですか？
A. データセンター内のサーバーの物理的な設置面積が縮小する可能性があります。
B. ホストのパフォーマンスの問題は、ゲストオペレーティングシステムに影響を与える可能性があります。
C. 処理能力は複数のオペレーティングシステム間で共有される場合があります。

D. 1台のホストに同じオペレーティングシステムの複数のバージョンが存在する場合があります。
正解: **(**正解を表示します**)**
A concern associated with virtualization is that performance issues with the host could impact the guest operating systems, which are the operating systems that run on virtual machines within the host. For example, if the host has insufficient memory, CPU, disk space, or network bandwidth, it could affect the performance and availability of the guest operating systems and the applications running on them. The physical footprint of servers could decrease within the datacenter, processingcapacity may be shared across multiple operating systems, and one host may have multiple versions of the same operating system are not concerns associated with virtualization, but rather benefits or features of virtualization that can help reduce costs, improve efficiency, and enhance flexibility.
References: CISA Review Manual (Digital Version), Chapter 4:
Information Systems Operations and Business Resilience, Section 4.2: IT Service Delivery and Support

質問: **415**
重要な業務プロセスを実行するライセンスソフトウェアの契約を審査する情報システム監査担当者にとって、最大の懸念事項は何ですか？
A. 契約には監査権条項が含まれていません。
B. 運用レベル合意(OLA)は交渉されなかった。
C. 複数のベンダーの納品物が約束の期日を過ぎました。
D. ソフトウェアのエスクローは交渉されませんでした。
正解: **(**正解を表示します**)**
The greatest concern for an IS auditor reviewing contracts for licensed software that executes a critical business process is that software escrow was not negotiated. Software escrow is an arrangement where a third- party holds a copy of the source code and documentation of a licensed software in a secure location. The software escrow agreement specifies the conditions under which the licensee can access the escrowed materials, such as in case of bankruptcy, termination, or breach of contract by the licensor. Software escrow is important for ensuring the continuity and availability of a critical business process that depends on a licensed software. Without software escrow, the licensee may face significant risks and challenges in maintaining, modifying, or recovering the software in case of any disruption or dispute with the licensor. References:
CISA Review Manual (Digital Version)
CISA Questions, Answers and Explanations Database

質問: **416**
プログラムの最新リリースを本番環境からロールバックする必要がある場合、コードの差分バージョンにおける対応する変更は次のようになります。

A. 問題の調査における今後の参考のために、本番環境に登録されました。
B. 本番環境で使用されているバージョンを反映したソースコードに適用されます。
C. 本番環境のバージョンを反映したソースコードから削除されました。
D. バージョンを本番環境に戻す際に再インストールされます。
正解**: (**正解を表示します**)**
When a program release needs to be backed out of production, the changes introduced by that release must be removed from the source code to ensure the system returns to its prior state. This approach ensures that the source code reflects the stable version without the problematic changes.
References
ISACA CISA Review Manual 27th Edition, Page 244-245 (Change Management)

質問**: 417**
ハッシュ化されたメッセージの完全性を確認するには、受信側は以下を使用する必要があります。
A. 送信者と同じハッシュアルゴリズムを使用してファイルのバイナリイメージを作成します。
B. 送信者とは異なるハッシュアルゴリズムを使用してファイルのバイナリイメージを作成します。
C. 送信者と同じハッシュアルゴリズムを使用して、ファイルの数値表現を作成します。
D. 送信者とは異なるハッシュアルゴリズムを使用して、ファイルの数値表現を作成します。
正解**: (**正解を表示します**)**
To confirm integrity for a hashed message, the receiver should use the same hashing algorithm as the sender' s to create a binary image of the file. A hashing algorithm is a mathematical function that transforms an input data into a fixed-length output value, called a hash or a digest. A hashing algorithm has two main properties:
it is one-way, meaning that it is easy to compute the hash from the input, but hard to recover the input from the hash; and it is collision-resistant, meaning that it is very unlikely to find two different inputs that produce the same hash. These properties make hashing algorithms useful for verifying the integrity of data, as any change in the input data will result in a different hash value. Therefore, to confirm integrity for a hashed message, the receiver should use the same hashing algorithm as the sender's to create a binary image of the file, which is a representation of the file in bits (0s and 1s). The receiver should then compare this binary image with the hash value sent by the sender. If they match, then the message has not been altered in transit.
If they do not match, then the message has been corrupted or tampered with.
References:
Ensuring Data Integrity with Hash Codes
Message Integrity

質問: **418**
組織の品質保証(QA)機能の以下の責任のうち、IS監査人が懸念すべきものはどれですか？
A. 開発プロセスにおいて基準が遵守されていることを確認する
B. テスト作業が観察結果を裏付けていることを確認する
C. 開発方法論の更新
D. 欠陥を修正するためのソリューションの実装
正解: **(正解を表示します)**
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.

質問: **419**
組織の最も機密性の高いデータにとって、最も大きなリスクとなる攻撃の種類はどれですか？
A. パスワード攻撃
B. 盗聴攻撃
C. 内部犯行
D. スピアフィッシング攻撃
正解: **C (コメントを発表する)**
An insider attack poses the greatest risk to an organization's most sensitive data. An insider attack is a type of cyberattack that is carried out by someone who has legitimate access to the organization's network, systems, or data, such as an employee, contractor, or business partner. An insider attack can be intentional or unintentional, malicious or negligent, and can have various motives, such as financial gain, revenge, espionage, sabotage, or curiosity.
An insider attack poses the greatest risk to an organization's most sensitive data because:
An insider has a high level of trust and privilege within the organization, which allows them to bypass security controls and access confidential or restricted data without raising suspicion or detection.
An insider has a deep knowledge of the organization's operations, processes, policies, and vulnerabilities, which enables them to exploit them effectively and cause maximum damage or disruption.
An insider can use various techniques and tools to conceal their identity and actions, such as encryption, steganography, deletion, or alteration of logs or evidence.
An insider can cause significant harm or loss to the organization in terms of data integrity, availability, confidentiality, reputation, compliance, and profitability.

According to the 2023 Cost of Insider Threats Global Report by Ponemon Institute and ObserveIT 1, the average annual cost of insider threats for organizations worldwide was $11.45 million in 2022, a 31% increase from 2018. The report also found that the average number of incidents per organization was 77 in 2022, a
47% increase from 2018. The report classified insider threats into three categories: careless or negligent employees or contractors, criminal or malicious insiders, and credential thieves. The report revealed that careless or negligent insiders were the most common and costly type of insider threat, accounting for 62% of all incidents and $4.58 million in costs.
The other options are not the greatest risk to an organization's most sensitive data, although they can still pose significant threats.
A password attack is a type of cyberattack that attempts to guess or crack a user's password to gain unauthorized access to their account or system. A password attack can use various methods, such as brute force, dictionary, rainbow table, phishing, keylogging, or social engineering. A password attack can compromise the security and privacy of the user's data and information. However, a password attack can be prevented or mitigated by using strong and unique passwords, changing passwords frequently, enabling multi- factor authentication (MFA), and avoiding clicking on suspicious links or attachments.
An eavesdropping attack is a type of cyberattack that intercepts or monitors the communication between two parties without their knowledge or consent. An eavesdropping attack can use various techniques, such as wiretapping, packet sniffing, man-in-the-middle (MITM), or side-channel. An eavesdropping attack can expose the content and metadata of the communication, such as messages, files, voice calls, emails, etc.
However, an eavesdropping attack can be prevented or mitigated by using encryption, authentication, digital signatures, VPNs (virtual private networks), or secure protocols.
A spear phishing attack is a type of phishing attack that targets a specific individual or group with personalized and convincing emails that appear to come from a trusted source. A spear phishing attack aims to trick the recipient into clicking on a malicious link or attachment that can infect their device with malware or steal their credentials or data. A spear phishing attack can compromise the security and privacy of the recipient's data and information. However, a spear phishing attack can be prevented or mitigated by verifying the sender's identity and email address, checking the email content for spelling and grammar errors, hovering over links before clicking on them (or not clicking at all), scanning attachments for viruses before opening them (or not opening at all), and reporting suspicious emails to IT security staff.

質問**: 420**
IS監査担当者がバックアップのパフォーマンスを評価している際に、システム管理者が予期せぬピーク使用時に手動でバックアップを開始していることに気づきました。監査担当者にとって最適な対応策は次のうちどれでしょうか？
A. 職務分担に関する文書を確認してください。

B. ロードバランサーの設定を確認します。
C. クラウドベースのバックアップの使用をお勧めします。
D. ログを調べて、バックアップがタイムリーに実行されたことを確認します。
正解: **(**正解を表示します**)**
A key aspect ofbackup managementis ensuring backups are performed on time and without manual intervention to avoid human error.
Option A (Incorrect):While separation of duties is important, the concern here is not aconflict of interestbut rather the reliability of backup execution.
Option B (Incorrect):Load balancer configuration relates tonetwork traffic management, which is not directly relevant to backup reliability.
Option C (Incorrect):Cloud-based backups can be a good option, but the immediate priority is toverify if backups are consistently executedbefore suggesting alternative solutions.
Option D (Correct):Reviewing backup logs provides concreteevidenceof whether backups are performed on schedule and if they weremisseddue to peak usage periods. If issues are found, automation or scheduling adjustments may be recommended.
Reference:ISACA CISA Review Manual -Domain 4: Information Systems Operations and Business Resilience- Covers backup procedures, performance monitoring, and audit approaches.

質問: **421**
IS監査担当者は、組織の新たなプライバシー法への対応をレビューする際に、まず何を評価すべきでしょうか？
A. 個人情報の収集を制限するための実施計画
B. 他国のプライバシー関連法規には、同様の要件が含まれている可能性がある。
C. 法令遵守を実現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
正解: **D (**コメントを発表する**)**
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 foran 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 Protection and Privacy Legislation Worldwide | UNCTAD, Data minimization - Wikipedia

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu　**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **422**
従業員が公共のソーシャルネットワーキングサイトを利用する際に、組織にとって最も大きなリスクとなるのは次のうちどれですか？
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
正解: **C** (コメントを発表する)

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

質問: **423**
組織のコンピューティングリソースの効率性を向上させるために、IS監査担当者が最も推奨する対策は次のうちどれですか？
A. ハードウェアのアップグレード
B. 中央処理装置(CPU)のオーバークロック
C. リアルタイムバックアップ
D. 仮想化
正解: **D** (コメントを発表する)

質問: **424**
IS監査担当者が、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。どの環境で、ソフトウェアのバージョンが本番環境と同じである可能性が最も高いでしょうか？
A. ステージング
B. テスト中
C. 統合
D. 開発
正解: **A** (コメントを発表する)
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.

質問: **425**
ある組織が買収を計画しており、対象企業のITガバナンスフレームワークを評価するためにIS監査人を雇いました。フレームワークの有効性を判断する上で、次のうちどれが最も役立つでしょうか？
A. IT能力と成熟度に関する販売評価レポート
B. 競合他社とのITパフォーマンスベンチマークレポート
C. 最近の第三者機関によるIS監査報告書
D. 現在および過去の内部IS監査報告書
正解: **C** (コメントを発表する)
Recent third-party IS audit reports would be most helpful in determining the effectiveness of the IT governance framework of the target company. IT governance is a framework that defines the roles, responsibilities, and processes for aligning IT strategy with business strategy. A third-party IS audit is an independent and objective examination of an organization's IT governance framework by an external auditor.
Recent third-party IS audit reports can provide reliable and unbiased evidence of the strengths, weaknesses, and maturity of the IT governance framework of the target company. The other options are not as helpful as recent third-party IS audit reports, as they may not be as comprehensive, accurate, or current as external audits. References: CISA Review Manual, 27th Edition, page 94

質問: **426**
IS監査担当者は、組織の設備投資と修繕 ･保守費用を比較分析するよう指示されました。この目的のためにデータ分析ツールを使用する最適な理由は次のうちどれですか？
A. データの信頼性を向上させます。
B. 監査人が取引の 100% を扱うことができるようになります。
C. エラー率を低減します。
D. 監査を実施するために必要なサンプルサイズを削減します。
正解: (正解を表示します)

質問: **427**
IS監査担当者が、ある企業の幹部が従業員に対し、業務目的でソーシャルネットワーキングサイトを利用することを奨励していることを発見しました。データ漏洩のリスクを軽減するために、以下の推奨事項のうちどれが最も効果的でしょうか？

A. 従業員による方針の承認および秘密保持契約(NDA)への署名を義務付ける
B. 機密データに対する強力なアクセス制御の確立
C. 従業員に対し、ソーシャルネットワーキングサイトの利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ク利用状況の監視
正解: **(**正解を表示します**)**
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.

質問: **428**
組織の最終的なリスク評価プロセスをレビューする際、IS監査人が許容リスクレベルと残存リスクを比較する主な理由は何でしょうか？
A. 経営陣にリスク許容度レベルについて助言する
B. 完了したリスク評価における漏れを特定する
C. さらなるリスク低減のための管理強化策を推奨する
D. 組織が対処しなければならない新たなリスクを特定する
正解: **(**正解を表示します**)**

質問: **429**
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うちどれですか？
A. 侵入テストの成功回数
B. 保護されたビジネスアプリケーションの割合
C. セキュリティインシデ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
正解: **(**正解を表示します**)**
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

質問: **430**
分散型で不変な台帳を作成するために、ブロックチェーン技術で主に使われるのは次のうちどれですか？
A. アプリケーションの強化
B. エッジコンピューティング
C. 人工知能 (AI)
D. 暗号化
正解: **(正解を表示します)**

質問: **431**
アジャイルソフトウェア開発プロジェクトのライフサイクル全体を通してセキュリティ要件が考慮されるようにするための、最適な管理策は次のうちどれですか？
A. セキュリティ管理要件を文書化し、内部監査の承認を得る
B. セキュリティに関する専門知識を提供できるプロジェクトチームメンバーを含む
C. 従来のウォーターフォール型ソフトウェア開発ライフサイクル(SDLC)手法に戻る
D. プロジェクトを本番環境にリリースする前に認証を受けることを義務付ける
正解: **(正解を表示します)**

質問: **432**
ITガバナンスレビューで得られた以下の所見のうち、最も懸念すべきものはどれですか？
A. IT予算は監視されていません
B. すべてのITサービスは第三者によって提供されます。
C. IT価値分析が完了していません。
D. ITは2つの異なるオペレーティングシステムをサポートしています。
正解: **(正解を表示します)**
IT value analysis has not been completed is a finding from an IT governance review that should be of greatest concern. IT value analysis is a process of measuring and demonstrating the contribution of IT to the organization's goals and objectives. An IS auditor should be concerned about the lack of IT value analysis, as it may indicate that the IT investments and resources are not aligned with the business needs and expectations, or that the IT performance and outcomes are not monitored and evaluated. The other options are less critical findings that may not have a significant impact on the IT governance.
References:

CISA Review Manual (Digital Version), Chapter 5, Section 5.11
CISA Review Questions, Answers and Explanations Database, Question ID 218

質問: **433**
オープンソース製品の使用を導入する際に、以下のうちどれを最も重視すべきでしょうか？
A. サポート
B. パフォーマンス
C. 機密保持
D. ユーザビリティ
正解: **(**正解を表示します**)**
Support should be given the greatest consideration when implementing the use of an open-source product, as open-source software may not have the same level of technical support, maintenance, and updates as proprietary software1. Open-source software users may have to rely on the community of developers and users, online forums, or third-party vendors for support, which may not be timely, reliable, or consistent2. Therefore, before implementing an open-source product, users should evaluate the availability and quality of support options, such as documentation, forums, mailing lists, bug trackers, chat channels, etc.3

質問: **434**
年次監査計画プロセスの一環として、以下のうちどれを必ず完了する必要がありますか？
A. 事業影響分析(BIA)
B. フィールドワーク
C. リスク評価
D. リスク管理マトリックス
正解: **C (**コメントを発表する**)**
Risk assessment is a mandatory part of the annual audit planning process, as it helps to identify and prioritize the areas that pose the highest risk to the organization's objectives and operations. Risk assessment involves analyzing the internal and external factors that affect the organization's risk profile, evaluating the likelihood and impact of potential events or scenarios, assessing the existing controls and mitigation strategies, and determining the residual risk level. Based on the risk assessment results, the IS auditor can allocate resources and schedule audits accordingly. A business impact analysis (BIA) is a process that identifies and evaluates the critical business functions and processes that could be disrupted by a disaster or incident, and estimates the potential impact on the organization's operations, reputation and finances. A BIA is not a mandatory part of the annual audit planning process, but it can be used as an input for risk assessment or as a subject for audit. Fieldwork is the phase of an audit where the IS auditor collects evidence to support the audit objectives and conclusions. Fieldwork is not part of the annual audit planning process, but it is part of each individual audit engagement. A risk control matrix is a tool

that maps the risks identified in a risk assessment to the controls that mitigate them. A risk control matrix is not a mandatory part of the annual audit planning process, but it can be used as an output of risk assessment or as a tool for audit testing. References: CISA Review Manual (Digital Version) 1, Chapter 1: Information Systems Auditing Process, Section 1.2: Audit Planning.

質問: **435**
経理部門は、機密性の高い財務取引を計算するためにスプレッドシートを使用しています。スプレッドシート内のデータのセキュリティを維持するために、次のうち最も重要な管理策はどれですか？
A. スプレッドシートと財務システムの間には調整プロセスがあります
B. スプレッドシートの別コピーが定期的にバックアップされます
C. スプレッドシートは、意図しない変更を防ぐためにロックされています。
D. スプレッドシートへのアクセスは、アクセスが必要な人にのみ許可されます。
正解: **(**正解を表示します**)**
Access to the spreadsheet is given only to those who require access is the most important control for maintaining the security of data in the spreadsheet. An IS auditor should ensure that the principle of least privilege is applied to limit the access to sensitive financial data and prevent unauthorized disclosure, modification, or deletion. The other options are less important controls that may enhance the accuracy, availability, or integrity of data in the spreadsheet, but not its security. References:
CISA Review Manual (Digital Version), Chapter 6, Section 6.31
CISA Review Questions, Answers and Explanations Database, Question ID 210

質問: **436**
ルーターなどのネットワーク機器が、別のIPアドレスとの通信時に、エラーメッセージや通信の成功 -失敗を示す運用情報を送信するために使用するネットワーク通信プロトコルは、次のうちどれですか？
A. 伝送制御プロトコル／インターネットプロトコル(TCP/IP)
B. インターネット制御メッセージプロトコル
C. ポイントツーポイントトンネリングプロトコル
D. 多目的トランザクションプロトコル
正解: **(**正解を表示します**)**

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジン

を手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu 1605問、３０%ディスカウント、特別な割引コード: JPNshiken」

質問: **437**
クライアントに対して内部および外部の侵入テストの実施を計画する場合、最初に実行する必要があるのは次のうちどれですか?
A. テストのタイミングを確立します。
B. マイルストーンを特定します。
C. テストレポートを決定します。
D. 関与のルールを確立します。
正解: **(正解を表示します)**
The rules of engagement define the scope, objectives, methodology, deliverables, and limitations of the penetration testing. They also specify the legal and ethical boundaries, communication channels, and escalation procedures. Establishing the rules of engagement is the first step when planning to conduct penetration testing for a client, as it ensures that both parties agree on the expectations and outcomes of the testing. The other options are important steps, but they should be done after the rules of engagement are established. References: CISA Review Manual (Digital Version) 1, page 381.

質問: **438**
チェックサムはどのタイプの制御に分類されますか？
A. 探偵制御
B. 予防的制御
C. 修正制御
D. 管理制御
正解: **(正解を表示します)**
A checksum is classified as a detective control. A checksum is a mathematical value that is calculated from a data set and used to verify the integrity of the data. A checksum can detect if the data has been altered or corrupted during transmission or storage. A checksum does not prevent or correct the data corruption, but it alerts the user or system of the problem. Therefore, it is a detective control. A preventive control is a control that prevents an error or incident from occurring. A corrective control is a control that restores normal operations after an error or incident has occurred. Anadministrative control is a controlthat involves policies, procedures, standards, guidelines, or organizational structures. References: CISA Review Manual (Digital Version)1, page 439.

質問: **439**
クラウドアクセスセキュリティブローカー(CASB)は、顧客組織に代わって、サービスとしてのソフトウェア(SaaS)のユーザーアクセスを管理します。サービスの監査を実施する際、IS監査担当者が確認すべき最も重要な事項は次のうちどれですか？

A. CASB はアクセス要求をサービスレコードとしてログに記録し、アクセスを許可した後にレビューします。
B. CASBは、顧客ポリシーへの準拠を確保するために、アクセス要求の定期的な監査を実施します。
C. CASB は、SaaS アプリケーションで使用されるフェデレーション ディレクトリ サービスへの安全なアクセスを管理します。
D. CASB は、アクセスを許可する前に、指定された顧客担当者からのアクセス要求を検証します。
正解: **(**正解を表示します**)**

質問: **440**
組織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ものは、次のうちどれですか？
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
正解: **(**正解を表示します**)**
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

質問: **441**
成熟したリスク管理プログラムを示す最も強力な指標は次のどれですか?
A. リスク評価の結果は、情報に基づいた意思決定に使用されます。
B. リスクのすべての属性はリスク所有者によって評価されます。
C. メトリクス ダッシュボードが上級管理職によって承認されました。
D. リスク レジスターは、リスク担当者によって定期的に更新されます。
正解: **(**正解を表示します**)**
A mature risk management program ensures that risk assessmentsdirectly influence decision-makingto align IT risks with business objectives.
Risk Assessment Results Used for Decision-Making (Correct Answer - A)
Demonstrates that risk management is embedded in business processes.
Enables proactive risk mitigation strategies.

Example:A company identifies a cybersecurity risk and delays the launch of a new cloud service until additional controls are in place.
Risk Owner Evaluating All Risk Attributes (Incorrect - B)
Important, but risk management is a shared responsibility.
Metrics Dashboard Approved by Management (Incorrect - C)
A useful tool, but does not indicate effective risk management.
Regular Updates to the Risk Register (Incorrect - D)
Keeping records updated is necessary but not a strong indicator of maturity.
References:
ISACA CISA Review Manual
COBIT 2019: Risk Governance
ISO 31000 (Risk Management Framework)

質問: **442**
データ損失防止(DLP)ツールを導入する上で、最も重要な成功要因は次のうちどれですか？
A. 不要な通信遮断を避けるため、ツールをモニターモードで実装します。
B. 機密データ移動を監視するためのポリシーとツールルールセットの定義と構成
C. 本番環境に移行する前に、テスト環境でツールをテストする
D. ツールの保守に関する責任を該当するデータ所有者および利害関係者に割り当てる
正解: **(正解を表示します)**
The success of a DLP implementation relies heavily on accurately defining and configuring the policies and rule sets. These configurations ensure that the DLP tool effectively monitors and controls the movement of sensitive data within the organization, thereby preventing data loss.
References
ISACA CISA Review Manual 27th Edition, Page 301-302 (Data Loss Prevention)

質問: **443**
変更管理に関して、IS監査人が最も深刻なリスクとみなすべき事項は次のうちどれですか？
A. 変更は承認後2週間で展開されます。
B. 変更管理を追跡するためのソフトウェアは使用されていません。
C. 変更は事業主によって承認されていません。
D. 変更の開発は費用対効果が高くありません。
正解: **C (コメントを発表する)**

質問: **444**
テクノロジーリソースのキャパシティ管理レビューを実施する主な理由は、以下の点を確実にするためです。

A. インフラとプロセスは現在および将来のビジネスニーズを満たすことができます。
B. 利用可能な容量は安全かつ法令遵守の方法で運用されます。
C. 技術リソースの取得は、現在の必要な能力に合致している。
D. 技術リソース容量要件が適切に定義されている。
正解: **A** (コメントを発表する)
The correct answer is A. infrastructure and processes can meet current and future business needs.
Capacity management is concerned with ensuring that IT resources are sufficient to support business operations, service levels, growth, and future demand. A capacity management review should determine whether infrastructure, applications, networks, storage, processing power, and related operational processes can support both current and expected business requirements.
Option B is not the best answer because security and compliance are important, but they are not the primary purpose of a capacity management review. Option C is too narrow because capacity management is not only about acquisitions; it also includes monitoring, forecasting, utilization analysis, performance trends, and planning. Option D is also too narrow because defining capacity requirements is only one part of the broader objective. The main objective is ensuring the organization can meet current and future business needs.
ISACA's CISA Exam Content Outline places Systems Availability and Capacity Management under Domain
4, Information Systems Operations and Business Resilience. It also includes evaluating whether IT operations and maintenance practices support organizational objectives.
A simple CISA way to remember this is: capacity management is not just about "more hardware." It is about ensuring IT capacity is aligned with business demand, service expectations, and future growth.
References: ISACA CISA Exam Content Outline, Domain 4.

質問: **445**
アウトソーシングされたプロバイダーサービスが適切に管理されていることを最も確実に保証するものは、次のうちどれですか？
A. 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ています。
B. サービスレベル契約(SLA)の不遵守に対して適切な措置が講じられています。
C. ベンダーは、そのパフォーマンスを示すために過去のデータを提供します。
D. 社内業績基準は企業戦略と一致している。
正解: (正解を表示します)
Adequate action taken for noncompliance with the service level agreement (SLA) provides the best evidence that outsourced provider services are being properly managed. This shows that the organization is monitoring the performance of the provider and enforcing the terms of the SLA.

The other options are not as convincing as evidence of proper management. Option A, the SLA includes penalties for non-performance, is a good practice but does not guarantee that the penalties are actually applied or that the performance is satisfactory. Option C, the vendor provides historical data to demonstrate its performance, is not reliable because the data may be biased or inaccurate. Option D, internal performance standards align with corporate strategy, is irrelevant to the question of outsourced provider management.
References:
ISACA, CISA Review Manual, 27th Edition, 2019, page 2821
ISACA, CISA Review Questions, Answers and Explanations Database - 12 Month Subscription, QID
1066692

質問**: 446**
予定されていたアップデートから1週間後に基幹システムが故障し、サービスに影響を与える停止が発生しました。この問題に対処する際に、インシデント管理において最も重要な点は次のうちどれでしょうか？
A. 障害の根本原因を分析し、同様の事態が再発しないようにする
B. システムを可能な限り迅速に運用状態に復旧する
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. 失敗した変更を以前の状態にロールバックします
正解**: (**正解を表示します**)**
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.

質問**: 447**
管理されたアプリケーション開発環境において、最も重要な職務分掌は、本番環境に変更を実装する担当者と、以下の担当者との間で行われるべきである。
A. アプリケーションプログラマー
B. システムプログラマー
C. コンピュータオペレーター
D. 品質保証(QA)担当者
正解**: (**正解を表示します**)**
In a controlled application development environment, the most important segregation of duties should be between the person who implements changes into the production environment and the application programmer. This segregation of duties ensures that no one person can create and deploy code without proper review, testing, and approval. This reduces the risk of errors, fraud, or malicious code being introduced into the production environment.
The other options are not as important as the segregation between the application programmer and the person who implements changes into production, but they are still relevant for achieving a secure and reliable application development environment. The segregation of duties between the person who implements changes into production and the systems programmer is important to prevent unauthorized or untested changes to system software or configuration. The segregation of duties between the person who implements changes into production and the computer operator is important to prevent unauthorized or uncontrolled access to production data or resources. The segregation of duties between the person who implements changes into production and the quality assurance (QA) personnel is important to ensure independent verification and validation of code quality and functionality.
References:
ISACA CISA Review Manual 27th Edition (2019), page 247
Segregation of Duties in an Agile Environment | AKF Partners3
Separation of Duties: How to Conform in a DevOps World4

質問: **448**
キャパシティ管理によって、組織は以下のことが可能になります。
A. 予測技術トレンド
B. ネットワーク通信リンクの容量を確立する
C. コンポーネントのアップグレードが必要な範囲を特定する
D. ビジネス取引量を決定する。
正解: **(正解を表示します)**
Capacity management is a process that ensures that the IT resources of an organization are sufficient to meet the current and future demands of the business. Capacity management enables organizations to identify the extent to which components need to be upgraded, by monitoring and analyzing the performance, utilization, and availability of the IT components, such as servers, networks, storage, applications, etc., and identifying any bottlenecks, gaps, or risks that may affect the service level agreements (SLAs) or quality of service (QoS). Capacity management also helps organizations to plan and optimize the use of IT resources, by forecasting the future demand and growth of the business, and aligning the IT capacity with the business needs and objectives. Forecasting technology trends is a possible outcome of capacity management, but it is not its main purpose. Establishing the capacity of network communication links is a part of capacity management, but it is not its main goal. Determining business transaction volumes is an input for capacity management, but it is not its main objective.

質問: **449**
法医学捜査中に収集された電子証拠が将来の法的手続きにおいて証拠として認められるために、以下のうち最も重要なものはどれですか？
A. 証拠へのアクセスを専門資格を持つ法医学捜査官に限定する
B. 法医学捜査全体を通して職員による証拠の取り扱いを記録する
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的調査を依頼する
正解: **(正解を表示します)**
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 and Explanations Database

質問: **450**
情報システム監査担当者が、ウェブベースの顧客サービスアプリケーション開発プロジェクトの進捗状況を評価している。
この評価に最も役立つのは、次のうちどれでしょうか？
A. バックログ消費レポート
B. クリティカルパス分析レポート
C. 開発者ステータスレポート
D. 変更管理ログ
正解: **A (**コメントを発表する**)**
A backlog consumption report is a report that shows the amount of work that has been completed and the amount of work that remains to be done in a project. It is a useful tool for measuring the progress and performance of a web-based customer service application development project, as it can indicate whether the project is on track, ahead or behind schedule, and how much effort is required to finish the project. A backlog consumption report can also help identify any issues or risks that may affect the project delivery. Critical path analysis reports, developer status reports and change management logs are also helpful for evaluating a project, but they are not as helpful as a backlog consumption report, as they do not provide a clear picture of the overall project status and completion rate. References:
[Backlog Consumption Report Definition]
Backlog Consumption Report | ISACA

質問: **451**
事業継続戦略に事業影響分析(BIA)を導入することの主な利点は次のうちどれですか？
A. 事業サービスの中断によって発生する可能性のある法的義務を特定します。
B. 発生する可能性のある災害のリスクレベルに関する最新情報を提供します。
C. 危機時に組織が果たすべき従業員の責任を明確にするものです。
D. システムとアプリケーションの復旧の優先順位付けに役立ちます
正解: **(**正解を表示します**)**
The primary purpose of a Business Impact Analysis (BIA) is to prioritize the restoration of systems and applications (D) based on their criticality to business operations. A BIA assesses the impact of disruptions, identifies critical processes, and determines recovery time objectives (RTOs) and recovery point objectives (RPOs).
Other options:
Identifying legal obligations (A) is an aspect of compliance but not the primary benefit of a BIA.
Providing updates on disaster risk levels (B) falls under risk management rather than BIA objectives.

Delineating employee responsibilities (C) is part of business continuity planning (BCP), not the BIA's main goal.
Reference: ISACA CISA Review Manual, Information Systems Operations and Business Resilience

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu 「**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **452**
IS監査担当者は、社内ユーザーがインターネットに接続されたWebブラウザ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担当者の最適な推奨事項は次のうちどれですか？
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機能を活用してください。
正解: **(**正解を表示します**)**
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, CISAReview Questions, Answers and ExplanationsDatabase - 12 Month Subscription2 What Is Cloud Security? | Google Cloud3
5 Cloud Application Security Best Practices | Snyk4

質問**: 453**
災害復旧計画(DRP)において、最も重要な定義事項は次のうちどれですか？
A. 事業継続計画(BCP)
B. バックアップデータ復元のテスト結果
C. 災害復旧シナリオと優先事項の包括的なリスト
D. 復旧チームメンバーの役割と責任
正解**: D (**コメントを発表する**)**
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

質問**: 454**
監査を計画する際、IS 監査人がサービス レベル管理に関するサードパーティ プロバイダーの外部監査レポートに依拠することは許容されます。
A. 範囲と方法論が監査要件を満たしている
B. サービス提供者は独立した認証および認定を受けています
C. サービスレベルが侵害されていないことを報告書が確認
D. レポートは過去12ヶ月以内に公開されました
正解**: (**正解を表示します**)**
It is acceptable for an IS auditor to rely on a third-party provider's external audit report on service level management when the scope and methodology meet audit requirements. This means that the external audit report covers the same objectives, criteria, standards and procedures that the IS auditor would use to assess the service level management. This way, the IS auditor can avoid duplication of work and reduce audit costs and efforts. The service provider's certification and accreditation, the report's confirmation of service

levels and the report's release date are not sufficient to justify reliance on the external audit report. References: CISA Review Manual (Digital Version) , Chapter 2, Section 2.3.3.

質問: **455**
ハードドライブのフォレンジックイメージを作成する際に、以下のうち最も重要なものはどれですか？
A. ハードドライブのコンテンツハッシュを生成しています
B. 業界をリードするフォレンジックソフトウェアツールの選択
C. ハードドライブのバックアップコピーを確保する
D. 画像処理中に独立した第三者の立ち会いを義務付ける
正解: **(**正解を表示します**)**

質問: **456**
IS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どのような場合でしょうか？
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収集時
C. 規制要件違反が確認された場合
D. 被監査者からの陳述を評価する際
正解: **(**正解を表示します**)**
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 forIS Audit and Assurance Professionals, section 12022

質問: **457**
サイバー攻撃を受けた組織が、影響を受けたユーザーのコンピュータのフォレンジック分析を実施しています。このプロセスをレビューする情報システム監査担当者にとって、以下のうちどれが最も懸念すべき事項でしょうか？
A. 各コンピュータからデータのコピーを取得するために、イメージング処理が使用されました。
B. 法務部は関与していません。

C. 保管管理の記録がありません。
D. 監査は情報の抽出時のみに関与した。
正解: **(**正解を表示します**)**
The chain of custody has not been documented is a finding that should be of greatest concern for an IS auditor reviewing a forensic analysis process of an organization that has suffered a cyber attack. The chain of custody is a record of who handled, accessed, or modified the evidence during a forensic investigation.
Documenting the chain of custody is essential to preserve the integrity, authenticity, and admissibility of the evidence in a court of law. The other options are less concerning findings that may not affect the validity or reliability of the forensic analysis process.
References:
CISAReview Manual (Digital Version), Chapter 7, Section 7.51
CISA Review Questions, Answers and Explanations Database, Question ID 220

質問: **458**
IS部門は、コスト対収益比率、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、BEST zedのアプリケーションとして使用されます。
A. リスクフレームワーク
B. バランススコアカード
C. バリューチェーン分析
D. コントロール自己評価(CSA)
正解: **(**正解を表示します**)**
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.

質問: **459**
多くの責任が共有されているIT組織において、不正なデータ変更を検出するための最適な制御策は次のうちどれですか？
A. ユーザーは定期的に責任を交代する必要があります
B. 職務分掌の衝突は定期的に見直される。
C. データ変更は別のグループによって独立してレビューされます。
D. データ変更は外部アプリケーションに記録されます
正解: **(**正解を表示します**)**

The best control for detecting unauthorized data changes in an IT organization where many responsibilities are shared is to have data changes independently reviewed by another group. This is because an independent review can provide an objective and unbiased verification of the data changes and ensure that they are authorized, accurate, and complete. An independent review can also help to detect any errors, fraud, or malicious activities that may have occurred during the data changes. An independent review can also provide assurance that the data integrity and security are maintained.
References:
CISA Review Manual (Digital Version), Chapter 4, Section 4.31
CISA Online Review Course, Domain 1, Module 4, Lesson 22

質問: **460**
ITシステムに対する侵入テストが完了し、結果が判明したら、次のステップは次のとおりであるべきです。
A. 脆弱性スキャンと再確認。
B. システムに加えられたすべての変更を分析しています。
C. 修復と再テスト。
D. 検査報告書の機密性を維持する。
正解: **C (**コメントを発表する**)**
The correct answer is C. Remediation and retesting.
ISACA guidance explains that penetration testing identifies exploitable weaknesses and provides guidance to address them. Once findings are identified, the next logical and control-appropriate step is to remediate the weaknesses and then retest to confirm they have been effectively resolved.
Option A is not the best next step because vulnerability scanning may supplement testing, but after a completed penetration test with findings, the priority is to fix what was found and verify closure.
Option B may be part of root cause work, but it is not the primary next step.
Option D is important from an information-handling perspective, but it does not address the control weaknesses identified by the test.
Therefore, the correct answer is C, because findings from a penetration test should drive remediation followed by retesting to validate that the identified weaknesses have been corrected.
References (Official ISACA):
* ISACA, The Future of Cybersecurity Assessments Is Here - VAPT identifies weaknesses and provides guidance to address them.
* ISACA, Taking a Risk-Based Approach to Pen Testing - findings should be evaluated and acted on according to business impact.
* ISACA, Smarter Testing Equals Safer Digital Experiences - findings should be assessed for exploitability and impact, supporting focused remediation.

質問: **461**
以下の環境機器のうち、データセンターの床タイル下に設置される可能性が最も高いのはどれですか？
A. 温度センサー
B. 湿度センサー
C. 水センサー
D. 空気圧センサー
正解: **(正解を表示します)**
Water sensors are devices that can detect the presence of water or moisture in a given area. They are often deployed below the floor tiles of a data center to monitor for any water leaks that may damage the equipment or cause electrical hazards. Water sensors can alert the data center staff or trigger an automatic response to prevent or mitigate the water leakage.
The other options are not likely to be deployed below the floor tiles of a data center. Temperature sensors and humidity sensors are usually deployed above the floor tiles to measure the ambient conditions of the data center and ensure optimal cooling and ventilation. Air pressure sensors are typically deployed at the air vents or ducts to monitor the airflow and pressure distribution in the data center.
References:
Data Center Environmental Monitoring
Water Detection in Data Centers

質問: **462**
組織の設計を評価するIS監査担当者にとって、次のうちどれが最も懸念されるでしょうか。のインシデント管理プロセスは？
A. サービス管理基準が遵守されていません。
B. インシデント解決までの予想時間は指定されていません。
C. 指標は上級管理職には報告されません。
D. 優先順位付け基準が定義されていません。
正解: **(正解を表示します)**
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

質問: **463**

組織の事業継続計画(BCP)をレビューする情報システム監査担当者にとって、以下のうちどれが最も懸念すべき事項でしょうか？
A. BCPの連絡先情報を更新する必要があります
B. BCP はバージョン管理されていません。
C. BCPは上級管理職によって承認されていません。
D. BCPは最初に発行されて以来、テストされていません。
正解: **D** (コメントを発表する)
The greatest concern for an IS auditor reviewing an organization's business continuity plan (BCP) is that the BCP has not been tested since it was first issued. A BCP is a document that describes how an organization will continue its critical business functions in the event of a disruption or disaster. A BCP should include information such as roles and responsibilities, recovery strategies, resources,procedures, communication plans, and backup arrangements3. Testing the BCP is a vital step in ensuring its validity, effectiveness, and readiness. Testing the BCP involves simulating various scenarios and executing the BCP to verify whether it meets its objectives and requirements. Testing the BCP can also help to identify and correct any gaps, errors, or weaknesses in the BCP before they become issues during a real incident4. Therefore, an IS auditor should be concerned if the BCP has not been tested since it was first issued, as it may indicate that the BCP is outdated, inaccurate, incomplete, or ineffective. The other options are less concerning or incorrect because:
A). The BCP's contact information needs to be updated is not a great concern for an IS auditor reviewing an organization's BCP, as it is a minor issue that can be easily fixed. Contact information refers to the names, phone numbers, email addresses, or other details of the people involved in the BCP execution or communication. Contact information needs to be updated regularly to reflect any changes in personnel or roles. While having outdated contact information may cause some delays or confusion during a BCP activation, it does not affect the overall validity or effectiveness of the BCP.
B). The BCP is not version controlled is not a great concern for an IS auditor reviewing an organization's BCP, as it is a moderate issue that can be improved. Version control refers to the process of tracking and managing changes made to the BCP over time. Version control helps to ensure that only authorized changes are made to the BCP and that there is a clear record of who made what changes when and why. Version control also helps to avoid conflicts or inconsistencies among different versions of the BCP. While having no version control may cause some difficulties or risks in maintaining and updating the BCP, it does not affect the overall validity or effectiveness of the BCP.
C). The BCP has not been approved by senior management is not a great concern for an IS auditor reviewing an organization's BCP, as it is a high-level issue that can be resolved. Approval by senior management refers to the formal endorsement and support of the BCP by the top executives or leaders of the organization.
Approval by senior management helps to ensure that the BCP is aligned with the organization's strategy, objectives, and priorities, and that it has sufficient resources and

authority to be implemented. Approval by senior management also helps to increase the awareness and commitment of the organization's stakeholders to the BCP. While having no approval by senior management may affect the credibilityand acceptance of the BCP, it does not affect the overall validity or effectiveness of the BCP. References: Working Toward a Managed, Mature Business Continuity Plan - ISACA, ISACA Introduces New Audit Programs for Business Continuity/Disaster ..., Disaster Recovery and Business Continuity Preparedness for Cloud-based ...

質問: **464**
IS監査担当者が、データベースに管理者が任意のテーブルを直接変更できるオプションがあることを発見しました。このオプションはソフトウェアのバグを解消するために必要ですが、めったに使用されません。テーブルへの変更は自動的にログに記録されます。IS監査担当者が最初に行うべきことは次のうちどれでしょうか？
A. データベースを直接変更するオプションを直ちに削除することを推奨します。
B. データベースの変更には2人が関与することをシステムに推奨します。
C. テーブルの変更ログがバックアップされているかどうかを判断します。
D. 監査証跡が保護され、レビューされているかどうかを判断します。
正解: **(正解を表示します)**
The IS auditor's first action after discovering an option in a database that allows the administrator to directly modify any table should be to determine whether the audit trail is secured and reviewed. This is because direct modification of database tables can pose a significant risk to data integrity, security, and accountability. An audit trail is a record of all changes made to database tables, including who made them, when they were made, and what was changed. An audit trail can help to detect unauthorized or erroneous changes, provide evidence for investigations or audits, and support data recovery or restoration. The IS auditor should assess whether the audit trail is protected from tampering or deletion, and whether it is regularly reviewed for anomalies or exceptions.

質問: **465**
IS監査担当者は、IT部門と事業部門の間でアプリケーションサーバーの可用性について意見の相違があることに気づいた。IS監査担当者は、問題を理解するために、まず次のうちどれを調査すべきか？
A. サービスレベルの正確な定義とその測定方法
B. アプリケーションサーバー上のアラートおよび測定プロセス
C. 実質的なテストの一環としてのサーバーの実際の可用性
D. 定期的なパフォーマンス報告ドキュメント
正解: **(正解を表示します)**
The exact definition of the service levels and their measurement is the first thing that the IS auditor should review in order to understand the problem of different opinions on the availability of their application servers.

Service levels are the agreed-upon standards or targets for delivering IT services, such as availability, reliability, performance, and security. Service level measurement is the process of collecting, analyzing, and reporting data related to the achievement of service levels. By reviewing the exact definition of the service levels and their measurement, the IS auditor can identify any gaps, inconsistencies, or ambiguities that may cause confusion or disagreement among IT and the business. The other options are not as important as reviewing the exact definition of the service levels and their measurement, as they do not address the root cause of the problem. References: CISA Review Manual, 27th Edition,page 372

質問: **466**
IS監査担当者が、リモートワークを行うユーザーのパスワードリセット方法について調査しています。この作業に必要な詳細な手順を理解するために、どのような種類の文書を要求すべきでしょうか？
A. ガイドライン
B. 規格
C. ポリシー
D. 手順
正解: **(**正解を表示します**)**

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu 「**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **467**
組織のセキュリティポリシーに準拠してファイアウォールが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うちどれですか？
A. パラメータ設定の確認
B. システムログを確認中
C. ファイアウォール管理者へのインタビュー
D. 実際の手順を確認する
正解: **(**正解を表示します**)**
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 possibleaudit 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.

質問**: 468**
フォローアップを計画する際、IS監査担当者は、最近の組織変更により以前に特定されたリスクが解消されたため、アクションプランの実施は不要になったと運用管理部門から通知を受けました。監査担当者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非現実的になったと報告する。
B. 経営陣の主張を受け入れ、リスクは対処済みであると報告する。
C. 変更によって対処が必要な新たなリスクが生じたかどうかを判断する。
D. 変更内容を確認し、リスクが対処されているかどうかを判断します。
正解**: B (**コメントを発表する**)**
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)

質問**: 469**

ある金融機関は、取引先の1社が複数の海外にサーバーを拡張するクラウドソリューションを利用していることを知りました。この金融機関にとって、以下のうちどれが最も懸念すべき事項でしょうか？

A. 現行制度におけるデータ処理のアウトソーシングは、規制に違反する可能性があります。

B. 分散サーバーの展開により、データの整合性が損なわれる可能性があります。

C. データが海外のサーバーに保存されると、データ分類が無効になる可能性があります。

D. 銀行とビジネスパートナー間のデータ所有権が不明確になる可能性があります。

正解: **(**正解を表示します**)**

The greatest concern is regulatory noncompliance arising from cross-border data processing and storage.

ISACA guidance on cloud data sovereignty states that when data is stored across multiple jurisdictions, organizations must navigate complex legal and regulatory challenges, including conflicting national laws and cross-border transfer restrictions. This is especially important for financial organizations, which often operate under stricter regulatory obligations regarding customer data, outsourcing, and location of processing.

Option A is correct because the key risk in extending cloud servers into several foreign countries is that the outsourced processing arrangement may violate applicable regulations or create conflicts among data protection, financial-sector, and jurisdictional requirements. ISACA notes that data sovereignty means data is governed by the laws of the country where it is stored, and that organizations must ensure compliance when cloud data spans borders.

Option B is not the greatest concern. Distributed server deployment can introduce integrity challenges, but ISACA's cross-border cloud guidance emphasizes the legal and governance burden far more directly than integrity degradation as the primary risk.

Option C is incorrect because data classification does not become invalid merely because data is stored overseas. Classification remains an internal governance concept, although handling requirements may change depending on jurisdiction. ISACA specifically recommends maintaining strong data classification systems alongside legal and compliance review for cross-border cloud use.

Option D is also not the greatest concern. Data ownership and responsibility should be clarified contractually, but ISACA identifies legal compliance and jurisdictional conflicts as the dominant governance risk in cross- border cloud environments.

Therefore, A is the best answer because regulatory exposure from cross-border outsourced processing is the most significant concern in this scenario.

References (Official ISACA):

ISACA, Cloud Data Sovereignty: Governance and Risk Implications of Cross-Border Cloud Storage.

ISACA Journal, Data Owners' Responsibilities When Migrating to the Cloud.

ISACA Journal, Addressing the Challenges of IT Audits by Supreme Audit Institutions.

質問: **470**
フォローアップ監査の結果、一部の経営改善計画が開始されていないことが判明した場合、IS監査担当者はまず何をすべきでしょうか？
A. 特定されたリスクが依然として有効であるかどうかを確認します。
B. 監査委員会に報告書を提出する。
C. 計画が完了していないことを経営陣に報告する。
D. 調査結果を確認するために、追加のアクションプランレビューを依頼します。
正解: **A** (コメントを発表する)
The first thing that an IS auditor should do when a follow-up audit reveals some management action plans have not been initiated is to escalate the lack of plan completion to executive management. This is because the failure to implement the agreed management action plans may indicate that the management is not taking the audit findings and recommendations seriously, or that they are accepting too much risk by not addressing the identified issues. Escalating the lack of plan completion to executive management can help to raise awareness and accountability, as well as to seek support and intervention to ensure that the management action plans are executed in a timely and effective manner12.
Confirming whether the identified risks are still valid is not the first thing to do, although it may be a useful step to reassess the current situation and the potential impact of not implementing the management action plans. However,confirming the validity of the risks does not address the root causeof why the management action plans have not been initiated, nor does it provide any assurance or remediation for the unresolved issues34.
Providing a report to the audit committee is not the first thing to do, although it may be a necessary step to communicate and document the results of the follow-up audit. However, providing a report to the audit committee does not guarantee that the management action plans will be initiated, nor does it resolve any conflicts or challenges that may prevent the management from implementing them34.
Requesting an additional action plan review to confirm the findings is not the first thing to do, although it may be a prudent step to verify and validate the accuracy and completeness of the follow-up audit. However, requesting an additional review may delay or defer the implementation of the management action plans, as well as consume more internalaudit resources and time

質問: **471**
アプリケーションが仕様どおりに動作していることを確認するための最良の方法は、次のうちどれですか？
A. 単体テスト
B. パイロットテスト
C. システムテスト

D. 統合テスト
正解: **(**正解を表示します**)**
Integration testing is the best way to ensure that an application is performing according to its specifications, because it tests the interaction and compatibility of different modules or components of the application. Unit testing, pilot testing and system testing are also important, but they do not cover the whole functionality and integration of the application as well as integration testing does. References: CISA Review Manual (Digital Version)1, Chapter 4, Section 4.2.3

質問: **472**
分散型データベースアーキテクチャが集中型アーキテクチャに比べて持つ主な利点は、次のうちどれですか？
A. サービス拒否(DoS)攻撃のリスクと影響が軽減されます。
B. 公共ネットワークを介してデータをリアルタイムでより簡単に同期できます。
C. 分散環境で実行されるトランザクションは、より一貫性があります。
D. 統一されたセキュリティポリシーをより簡単に適用できます。
正解: **(**正解を表示します**)**
The primary advantage of a decentralized database architecture over a centralized one is that it reduces the concentration of risk in a single location or single service point. Because data and processing are distributed, the effect of a single outage or denial of service event is generally reduced compared with a centralized architecture, where one core point of failure can disrupt the whole environment.
Option A is therefore the best answer. Decentralization improves resilience by avoiding total dependency on one central database or service node. In audit and risk terms, this lowers the impact of certain availability attacks or failures by distributing exposure.
Option B is incorrect because real-time synchronization over public networks is usually more difficult, not easier, in decentralized environments. Distributed synchronization introduces latency, consistency, and network management challenges.
Option C is incorrect because transaction consistency is generally harder to maintain in decentralized systems.
Distributed databases often trade some degree of simplicity or immediacy of consistency for resilience, scalability, or local autonomy.
Option D is incorrect because uniform security policy enforcement is usually easier in centralized architectures, where governance and administration can be applied from a single control point.
So the correct answer is A, because the main architectural benefit of decentralization in this context is reduced single-point failure risk and reduced impact from centralized service disruption.
References (Official ISACA):
* ISACA Glossary - control and architecture terminology reference.

* ISACA COBIT resources - governance and resilience principles support reducing concentration risk through architectural design choices.

質問: **473**
ネットワークの脆弱性に関する外部評価において、最も重要な検証事項は何ですか？
A. セキュリティ情報イベント管理 (SIEM) ルールの更新
B. ネットワークセキュリティポリシーの定期的な見直し
C. ネットワーク資産インベントリの完全性
D. 侵入検知システム(IDS)の設置場所
正解: **(正解を表示します)**
An external assessment of network vulnerability is a process of identifying and evaluating the weaknesses and risks that affect the security and availability of a network froman outsider's perspective. The most important factor to verify during this process is the completeness of network asset inventory, which is a list of all the devices, systems, and software that are connected to or part of the network. A complete and accurate network asset inventory can help identify the scope and boundaries of the network, the potential attack vectors and entry points, the critical assets and dependencies, and the existing security controls and gaps. Without a complete network asset inventory, an external assessment of network vulnerability may miss some important assets or vulnerabilities, leading to inaccurate or incomplete results and recommendations.
References:
1 explains what is an external vulnerability scan and why it is important to have a complete network asset inventory.
2 provides a guide on how to conduct a full network vulnerability assessment and emphasizes the importance of knowing the network assets.
3 compares internal and external vulnerability scanning and highlights the need for a comprehensive network asset inventory for both types.

質問: **474**
BYOD(Bring Your Own Device)プログラムの導入に関する監査の計画段階において、最も重要な情報源となるのは次のうちどれでしょうか？
A. 過去の監査結果
B. リスク評価の結果
C. 企業ネットワークに接続する個人用デバイスの一覧
D. BYODの許容ユーザーに関する記述を含むポリシー
正解: **(正解を表示します)**
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 objectivesof 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.

質問**: 475**
情報システム監査担当者が、レポートシステムの読み取り専用ユーザーに対する定期的なレビューが実施されていないことを発見した。
IS監査担当者が次に取るべき行動は次のうちどれでしょうか？
A. エンドユーザーのリストを確認し、承認の必要性を評価します。
B. この管理プロセスの弱点を上級管理職に報告してください。
C. この免除に対する経営陣の承認を確認してください
D. この免除についてIT部門から口頭での確認を得てください。
正解**: B (**コメントを発表する**)**
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 and Explanations Database3, Question ID: QAE_CISA_710.

質問: **476**
IS監査担当者が、重要システムのバックアップが事業継続計画(BCP)で定められた復旧目標時点(RPO)に従って実施されていないことを発見しました。監査担当者は次に何をすべきでしょうか？
A. 監査範囲を拡大します。
B. 即時バックアップの実行を要求します。
C. 根本原因を特定します。
D. 観察結果を報告書に含める。
正解: **(正解を表示します)**

質問: **477**
以下の検査のうち、医療機関が患者データを適切に取り扱っていることを最も確実に保証できるのはどれですか？
A. 最近の監査結果に基づく行動計画の遵守状況
B. 現地の法律および規制の遵守
C. 業界標準およびベストプラクティスへの準拠
D. 組織の方針および手順の遵守
正解: **B (コメントを発表する)**
The best test to provide assurance that a health care organization is handling patient data appropriately is compliance with local laws and regulations, as these are the primary sources of authority and obligation for data protection and privacy. Compliance with action plans, industry standards, or organizational policies and procedures are also important, but they may not cover all the legal requirements or reflect the currentbest practices for handling patient data. References: CISA Review Manual (Digital Version), Chapter 2, Section
2.3

質問: **478**

現行の規制では、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。この規制への準拠を促進するために、IS監査担当者が推奨する最善策は次のうちどれでしょうか？
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)を確立する。
B. インシデント対応のために外部のセキュリティインシデント対応専門家を起用する。
C. 侵入検知システム (IDS) のアラート機能を強化します。
D. 要件をインシデント管理対応計画に含める。
正解: **(**正解を表示します**)**
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.

質問: **479**
システムの復元力におけるフォールト トレランスの概念を最もよく説明しているのは次のうちどれですか。
A. 障害発生時に冗長システムへの切り替えが可能になります。

B. ダウンタイムを最小限に抑え、継続的な運用を保証します。
C. 障害が発生してもシステムが動作を継続できるようにします。
D. 過負荷を防ぐために、複数のサーバーにワークロードを分散します。
正解: **C** (コメントを発表する)
Comprehensive and Detailed Explanation:
Fault tolerance refers to the ability of a system to continue functioning despite the occurrence of faults or hardware failures.
* Option A: Describes failover, not fault tolerance.
* Option B: Is a benefit but not the exact definition.
* Option D: Refers to load balancing, not fault tolerance.
# ISACA Reference: CISA Review Manual 27th Edition, Domain 2, section on system availability, resilience, and fault tolerance.

質問: **480**
ビジネスインパクト分析(B1A)を実施する上で、最も有用な情報を提供するのは次のうちどれですか？
A. 関連するビジネスプロセスのインベントリ
B. 企業調達に関する方針
C. アプリケーション構成のドキュメント
D. 事業再開計画の取り組みの結果
正解: (正解を表示します)
A business impact analysis (BIA) is a process that identifies and evaluates the potential effects of disruptions to critical business operations as a result of a disaster, accident or emergency. A BIA should include an inventory of relevant business processes that support the organization's strategic objectives and are essential for its continuity. The inventory should also identify the dependencies, interdependencies, recovery priorities and time frames for each business process. Policies for business procurement, documentation of application configurations and results of business resumption planning efforts are not as useful as an inventory of relevant business processes for performing a BIA. References:
Business Impact Analysis (BIA) Definition
Business Impact Analysis (BIA) | ISACA

質問: **481**
情報漏洩が発生した場合、顧客に個人情報が漏洩した可能性があることを通知するまでの最大期間を判断するための最適な情報源は何ですか？
A. 業界規制
B. 業界標準
C. インシデント対応計画
D. 情報セキュリティポリシー
正解: **A** (コメントを発表する)

Following a breach, the maximum amount of time before customers must be notified that their personal information may have been compromised depends on the industry regulations that apply to the organization.
Different industries and jurisdictions may have different legal and regulatory requirements for breach notification, such as the General Data Protection Regulation (GDPR) in the European Union, the Health Insurance Portability and Accountability Act (HIPAA) in the United States, or the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada. Industry standards, incident response plans, and information security policies are not as authoritative as industry regulations in determining the breach notification time frame. References: CISA Review Manual (Digital Version), [ISACA Privacy Principles and Program Management Guide]

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu　**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **482**
特権アクセスの使用を監視するために、手動レビューではなく自動セキュリティ ログ監視ツールを使用する主な利点は次のどれですか。
A. 疑わしい活動を検出する可能性が高まります
B. レビューの自動化に伴うコストの削減
C. インシデント対応時間の改善
D. ログを確認するための手作業の労力を削減
正解: **(正解を表示します)**
Automated monitoring tools increase the likelihood of detecting suspicious activity (Option A) by continuously analyzing security logs for anomalies.
ISACA CISA Reference: Security Information and Event Management (SIEM) solutions are recommended for privileged access monitoring.

質問: **483**
ジョブ スケジューリングは、次の点でシステムの可用性と信頼性に影響を与えます。
A. システムのダウンタイムを削減します。
B. 柔軟性とスケーラビリティを確保します。
C. リソース使用率を最適化します。
D. システムの複雑さを軽減します。
正解: **(正解を表示します)**

Job scheduling is a core operational control that ensures workloads are executed in an orderly and efficient manner, balancing demands across processing resources. Its primary benefit is optimization of system resources-CPU, memory, I/O, and network bandwidth-leading to improved throughput and consistent service levels. While scheduling may indirectly reduce downtime (A) or support scalability (B), its direct impact is ensuring resources are allocated efficiently. Decreasing complexity (D) is not the key purpose of scheduling. ISACA's DSS01 (Managed Operations) recognizes workload and job scheduling as crucial practices for sustaining reliable, high-performance IT services. References (ISACA): COBIT 2019, DSS01 Managed Operations.

質問: **484**
ある組織は、磁気テープへの夜間バッチ処理バックアップを、第2のデータセンターへのリアルタイムレプリケーションに置き換える計画を立てています。この変更に伴う最大のリスクは次のうちどれですか？
A. バージョン管理の問題
B. システムパフォーマンスの低下
C. サイバーセキュリティ攻撃からの復旧能力の欠如
D. IT投資コストの増加
正解: **(**正解を表示します**)**
Real-time replication to a second data center means that any changes made to the primary data center are immediately copied to the secondary data center. This can improve data availability and performance, but also introduces the risk of propagating malicious or erroneous changes to the backup data center. If a cybersecurity attack compromises the primary data center, it may also affect the secondary data center, making it difficult or impossible to recover from the attack using the replicated data. Therefore, option C is the greatest risk associated with this change.
Option A is not correct because version control issues are more likely to occur with batch processing backup, which may create inconsistencies between different versions of the data. Option B is not correct because real- time replication may reduce system performance at the primary data center, but it may also improve system performance at the secondary data center by reducing latency and network traffic. Option D is not correct because although real-time replication may increase IT investment cost, this is not a risk but a trade-off that the organization has to consider.
References:
Data Replication: The Basics, Risks, and Best Practices1
Best Practices for Data Replication Between Data Centers2
The Good, Bad, and Ugly of Data Replication3

質問: **485**
システム開発プロジェクトは、継続的な人員不足のため遅延が発生しています。実装時のシステム品質を最も確実に保証できる戦略は次のうちどれでしょうか？

A. すべての開発スタッフに残業手当とボーナスを導入する。
B. 生産性を向上させるために、新しいシステム開発ツールを活用する。
C. システム開発を加速するためにISスタッフを採用する。
D. 当初の目標期日にはコア機能のみを提供する。
正解: **(正解を表示します)**
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.

質問: **486**
ある組織が、外部の業界標準への準拠を示すために、テクノロジーポリシーフレームワークを近代化しています。IS監査人がその結果を検証する上で、次のうちどれが最も役立つでしょうか？
A. 組織が承認したポリシー例外のリスト
B. 組織の管理体制に対する関連規格のマッピング
C. 同業他社との比較による内部標準のベンチマーク
D. 大手外部コンサルティング会社からの政策提言
正解: **(正解を表示します)**

質問: **487**
次のうち、変革管理の有効性を示す最も適切な指標はどれですか？
A. 設定変更とレコード更新の間の時間差
B. システムソフトウェアの変更回数
C. ドキュメント資料の変更と更新の間に時間差が生じる。
D. 変更によって発生したインシデントの数
正解: **D (コメントを発表する)**
Change management is the process of planning, implementing, monitoring, and evaluating changes to an organization's information systems and related components. Change management aims to ensure that changes are aligned with the business objectives, minimize risks and disruptions, and maximize benefits and value.

One of the key aspects of change management is measuring its effectiveness, which means assessing whether the changes have achieved the desired outcomes and met the expectations of the stakeholders. There are various indicators that can be used to measure change management effectiveness, such as time, cost, quality, scope, satisfaction, and performance.

Among the four options given, the most appropriate indicator of change management effectiveness is the number of incidents resulting from changes. An incident is an unplanned event or interruption that affects the normal operation or service delivery of an information system. Incidents can be caused by various factors, such as errors, defects, failures, malfunctions, or malicious attacks. Incidents can have negative impacts on the organization, such as loss of data, productivity, reputation, or revenue.

The number of incidents resulting from changes is a direct measure of how well the changes have been planned, implemented, monitored, and evaluated. A high number of incidents indicates that the changes have not been properly tested, verified, communicated, or controlled. A low number of incidents indicates that the changes have been executed smoothly and successfully. Therefore, the number of incidents resulting from changes reflects the quality and effectiveness of the change management process.

The other three options are not as appropriate indicators of change management effectiveness as the number of incidents resulting from changes. The time lag between changes to the configuration and the update of records is a measure of how timely and accurate the configuration management process is. Configuration management is a subset of change management that focuses on identifying, documenting, and controlling the configuration items (CIs) that make up an information system. The time lag between changes and updates of documentation materials is a measure of how well the documentation process is aligned with the change management process. Documentation is an important aspect of change management that provides information and guidance to the stakeholders involved in or affected by the changes. The number of system software changes is a measure of how frequently and extensively the system software is modified or updated. System software changes are a type of change that affects the operating system, middleware, or utilities that support an information system.

While these three indicators are relevant and useful for measuring certain aspects of change management, they do not directly measure the outcomes or impacts of the changes on the organization. They are more related to the inputs or activities of change management than to its outputs or results. Therefore, they are not as appropriate indicators of change management effectiveness as the number of incidents resulting from changes.

References:

Metrics for Measuring Change Management - Prosci
How to Measure Change Management Effectiveness: Metrics, Tools and Processes
Metrics for Measuring Change Management 2023 - Zendesk

質問: **488**
次のうち、買掛金管理システムにおける予防的統制の例はどれですか？
A. このシステムは、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を許可します。
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. このシステムは、スタッフが請求書の合計と比較するために使用する日々の支払い概要レポートを作成します。
D. 方針と手順は、買掛金部門のすべてのメンバーに明確に伝達されています。
正解: **(正解を表示します)**
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

質問: **489**
ある組織がリモートワーク体制に移行しようとしています。その準備として、IT部門はリモートアクセスインフラストラクチャとシステムのストレステストとキャパシティテストを実施しています。どのような制御が実装されていますか？
A. 指令
B. 探偵
C. 予防的
D. 補償
正解: **(正解を表示します)**
An organization is shifting to a remote workforce. In preparation, the IT department is performing stress and capacity testing of remote access infrastructure and systems. This type of control is being implemented to direct or guide actions to achieve a desired outcome. Therefore, it is a directive control. Directive controls are proactive controls that seek to prevent undesirable events from occurring. They include policies, standards, procedures, guidelines, training, and testing. Detective controls are reactive controls that seek to identify undesirable events that have already occurred. They include monitoring, logging, auditing, and reporting.
Preventive controls are proactive controls that seek to avoid undesirable events from occurring. They include authentication, encryption, firewalls, and antivirus software. Compensating controls are alternative controls that provide a similar level of protection as the primary controls when the primary controls are not feasible or cost-effective. They

include segregation of duties, manual reviews, and backup systems. References: CISA Review Manual (Digital Version), [ISACA Glossary of Terms]

質問: **490**
ITスタッフ育成計画をIT戦略と整合させるために、まず最初に行うべきことはどれですか？
A. ITスタッフの職務記述書を見直して整合性を確認する
B. ITスタッフ全員を対象とした四半期ごとの研修を実施する。
C. 主要なビジネスプロセスをサポートするために必要なITスキルセットを特定する
D. 戦略目標とITスタッフの業績目標を含める
正解: **(**正解を表示します**)**
Identifying required IT skill sets that support key business processes is the first step to enable the alignment of IT staff development plans with IT strategy. An IT strategy is a plan that defines how IT will support the organization's goals and objectives. Identifying required IT skill sets means determining the knowledge, abilities, and competencies that IT staff need to perform their roles and responsibilities effectively and efficiently. This can help to align IT staff development plans with IT strategy, as well as to identify and address any skill gaps or needs within the IT workforce. The other options are not the first steps to enable alignment, but rather possible subsequent actions that may depend on the required IT skill sets. References:
CISA Review Manual (Digital Version), Chapter 5, Section 5.11
CISA Review Questions, Answers and ExplanationsDatabase, Question ID 229

質問: **491**
IT戦略の修正の効果を示す最良の証拠となるのは、次のうちどれでしょうか？
A. IT戦略委員会の会議議事録
B. IT活動と企業目標の同期
C. IT 戦略委員会の委員長
D. 事業部門満足度調査結果
正解: **(**正解を表示します**)**
The best evidence of an IT strategy correction's effectiveness is the synchronization of IT activities with corporate objectives. The IT strategy correction is a process of reviewing and adjusting the IT strategy to ensure that it aligns with and supports the corporate strategy and objectives. The synchronization of IT activities with corporate objectives means that the IT activities are consistent with and contribute to the achievement of the corporate goals and vision. The IS auditor can measure and evaluate the IT strategy correction's effectiveness by comparing the IT activities with the corporate objectives, and assessing whether they are aligned, integrated, and coordinated. The other options are not as good evidence of an IT strategy correction's effectiveness, because they either do not reflect the alignment of IT and business, or they are inputs or outputs of the IT strategycorrection

process rather than outcomes or results. References: CISA Review Manual (Digital Version)1, Chapter 1, Section 1.2.1

質問: **492**
乾式消火システムを湿式システムよりも使用する主な利点は、乾式システムでは次の点が挙げられます。
A. 炎を抑えるのに効果的です。
B. 抑制剤の放出を中止するための時間を延長します。
C. 漏出のリスクが低い。
D. 乾燥化学抑制剤のみを散布します。
正解: **(正解を表示します)**
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

質問: **493**
インシデント管理の主な目的は次のどれですか?
A. 重要度に基づいてサービスを復旧する
B. 個々のインシデントを経営陣に報告する
C. インシデントの根本原因の特定
D. インシデントの原因となったプログラムの修復
正解: **(正解を表示します)**
Comprehensive and Detailed Explanation:
The primary objective of incident management is to restore IT services as quickly as possible based on business criticality, minimizing business disruption.
Root cause analysis (C) is more aligned with problem management, not incident management.
Reporting incidents (B) is important but not the primary objective.
Repairing programs (D) is a corrective activity, not the central goal.
ISACA Reference: CISA Review Manual 27th Edition, Domain 2 (IT Operations and Business Resilience), section on ITIL incident management process.

質問: **494**

アプリケーションテストを自動化する主なメリットは以下のとおりです。
A. テストの一貫性を提供します。
B. より柔軟性を提供します。
C. すべての手動テストプロセスを置き換えます。
D. コードレビューにかかる時間を短縮します。
正解: **(**正解を表示します**)**
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 and Explanations Database - 12 Month Subscription

質問: **495**
新しいシステムの導入中に、IS監査担当者は、特定の自動計算が規制要件に準拠しているかどうかを評価する必要があります。この保証を得るための最良の方法は次のうちどれですか？
A. 承認文書を確認する
B. 計算に関連するソースコードを確認する
C. 監査ソフトウェアを使用して計算を再実行する
D. ユーザー受け入れテスト(UAT)の結果を検査する
正解: **(**正解を表示します**)**
The best way to obtain assurance that certain automated calculations comply with the regulatory requirements is to re-perform the calculation with audit software. This will allow the auditor to independently verify the accuracy and validity of the calculation and compare it with the expected results. Reviewing sign-off documentation, source code, or user acceptance test results may not provide sufficient evidence or assurance that the calculation is correct and compliant. References:
CISA Review Manual (Digital Version), page 325
CISA Questions, Answers and Explanations Database, question ID 3335

質問: **496**
データセンターにおける物理的な情報資産の保護にとって、最も重要な前提条件は次のうちどれですか？
A. 情報資産を発注するスタッフと情報資産を受け取るスタッフ間の職務分担
B. 展開済みの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発電機の可用性とテスト

D. データ保護要件に関するITスタッフの知識
正解: **B** (コメントを発表する)
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 information 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

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu 1605問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **497**
シャドー IT のリスクを軽減するための最適な制御は次のどれですか?
A. ベンダー管理レビュー
B. 侵入検知システム（IDS）
C. セキュリティ意識向上トレーニング
D. 脆弱性スキャン
正解: (正解を表示します)

質問: **498**
機密データのバックアップをクラウドベースのソリューションに移行するプロジェクトをレビューする際に、IS監査担当者が最も懸念すべき事項は次のうちどれでしょうか？
A. 使用済みバックアップメディアの保管管理体制の欠如
B. 拡張性が不十分です
C. ベンダーに対するデューデリジェンスが不十分でした
D. 保管コストの増加
正解: **(正解を表示します)**
The best answer is C. Insufficient due diligence performed on the vendor.
ISACA guidance on third-party and cloud risk repeatedly emphasizes the need for thorough vendor due diligence before entering or expanding a business relationship. When confidential backups are being migrated to a cloud solution, insufficient due diligence is the greatest concern because it can expose the organization to security, privacy, resilience, and compliance failures across the whole service arrangement.
Option A is relevant for retired media handling, but it is narrower than the overall third-party risk. Option B affects performance and growth, not necessarily confidentiality. Option D is a business issue, but not the greatest audit concern when confidential data is involved.
Vendor due diligence is the most important control at this stage.
References (Official ISACA):
ISACA, The Top 5 Cybersecurity Threats and How to Defend Against Them.
ISACA Journal, The Encrypted Truth Is Already Out There.

質問: **499**
次のパフォーマンス管理ツールのうち、IS 監査人が組織の IT 戦略の実装と実行の成功を評価するのに最も役立つものはどれですか。
A. ITベンチマーク
B. 能力成熟度モデル
C. シックスシグマ
D. ITメトリクスダッシュボード
正解: **(正解を表示します)**
Comprehensive and Detailed Explanation:
An IT metrics dashboard provides real-time monitoring and reporting on key IT performance indicators (KPIs), allowing auditors and management to evaluate the effectiveness of IT strategy implementation and execution.
* Option A (Benchmarking): Useful for comparisons with peers but not for ongoing execution.
* Option B (Maturity models): Assess long-term process maturity, not direct strategy execution.
* Option C (Six Sigma): Focuses on process improvement, not IT strategy monitoring.
* Option D: Correct - dashboards link strategy to measurable outcomes.

ISACA Reference: CISA Review Manual 27th Edition, Domain 1, section on IT strategy, governance metrics, and performance dashboards.

質問: **500**
経営改善計画の監査フォローアップを実施する際の主要な目的は、次のうちどれであるべきか？
A. 監査報告書に記載されているリスクが適切に軽減されていることを確認する
B. 組織の新たなリスクと統制を特定する。上級管理職が監査結果を認識していることを確認する。経営行動計画をビジネス要件に合わせる。
正解: **A** (コメントを発表する)

質問: **501**
以下の活動のうち、IS監査人が独立性を維持しながら統制評価(CSA)を実施できるのはどれですか？
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質問票の開発
正解: (正解を表示します)
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 and Explanations Database, Question ID 215

質問: **502**
構成管理監査により、クラウドベース環境でアプリケーションインフラストラクチャを展開および構成する際に、事前定義された自動化された手順が使用されていることが判明しました。IS監査担当者が確認すべき最も重要な項目は次のうちどれですか？
A. 構成管理ドキュメントの保管場所
B. クラウド環境仕様の変更を行うためのプロセス
C. プロビジョニングツールの保守を担当するベンダーの契約
D. クラウド管理コンソールへのアクセス権を持つ管理者の数
正解: **B** (コメントを発表する)

The IS auditor should review the processes for making changes to cloud environment specifications, as these are the inputs for the predefined automated procedures that deploy and configure the application infrastructure. The IS auditor should verify that the changes are authorized, documented, tested, and approved before they are applied to the cloud environment. The IS auditor should also check that the changes are aligned with the business requirements and do not introduce any security or performance issues.
References
ISACA CISA Review Manual, 27th Edition, page 254
Configuration Management in Cloud Computing - ScienceDirect
Cloud Configuration Management - BMC Software

質問: **503**
組織の企業ネットワークのファイアウォールセキュリティをレビューするIS監査担当者にとって、以下の調査結果のうちどれが最も懸念されるでしょうか？
A. 本番環境の構成は、企業方針に準拠していません。
B. 業界の強化に関するガイダンスは考慮されていません。
C. ファイアウォールの管理責任は、2つの異なる部門にあります。
D. ファイアウォールの設定ファイルが非常に長く複雑です。
正解: **A** (コメントを発表する)

質問: **504**
以下のクラウド機能のうち、組織が予想外に高いサービス需要に対応するのに最も適しているのはどれですか？
A. 柔軟性
B. 高可用性
C. スケーラビリティ
D. 代替ルーティング
正解: **C** (コメントを発表する)

質問: **505**
ある組織のために、外部委託で新しいシステムが開発されています。サービスの継続性を確保するために、ベンダー契約に含めるべき最も重要な要件は次のうちどれですか？
A. サポート資料はベンダーから提供される必要があります。
B. ベンダーは文書化された災害復旧計画(DRP)を策定していなければなりません。
C. ソフトウェアのソースコードはエスクローに預けなければなりません。
D. ベンダーは、組織のスタッフに新しいソフトウェアを管理するためのトレーニングを実施する必要があります。
正解: **C** (コメントを発表する)
The best answer is C: Source code for the software must be placed in escrow.

When an organization has a system developed by an external vendor, one of the key continuity risks is vendor dependency. If the vendor goes out of business, refuses support, becomes insolvent, or fails to meet contractual obligations, the organization may lose the ability to maintain, modify, or recover the software. A source code escrow agreement reduces this risk by requiring the vendor to deposit the source code with a trusted third party. The organization can access the source code if specific contractual trigger events occur, such as vendor bankruptcy, nonperformance, or failure to support the system.
This is the most important control because it directly protects the organization's ability to continue using and maintaining the application even if the vendor is no longer available.
ISACA's own CISA practice quiz states that a source code escrow agreement is recommended to protect the enterprise's software investment because the source code is held by a trusted third party and can be retrieved if the vendor goes out of business.
Option A is not the best answer because support documentation is useful, but documentation alone does not allow the organization to maintain or modify the application if the vendor fails and the source code is unavailable.
Option B is not the best answer because a vendor disaster recovery plan is important when the vendor is providing an ongoing operational or hosted service. However, the question focuses on a system being developed externally and asks what should be included in the vendor contract to ensure service continuity. A DRP does not guarantee the organization can maintain the software if the vendor becomes insolvent or stops supporting the system.
Option D is not the best answer because training the organization's staff helps internal capability, but trained staff still cannot effectively maintain or modify the application without access to the source code and related rights.
This question belongs mainly to Information Systems Acquisition, Development and Implementation because it concerns controls and contractual requirements during external system development/acquisition. ISACA's current CISA Exam Content Outline includes "Information Systems Acquisition, Development, and Implementation" as Domain 3, covering acquisition/development and control identification/design. ISACA also discusses escrow as a way to address vendor continuity risk, especially for software, where assets or software code are deposited with a third party and released under defined contractual conditions.

質問**: 506**
ゼロ トラスト アーキテクチャでは、リソースが安全にアクセスされていることを確認するために IS 監査人が評価する上で最も重要な要素はどれですか。
A. 境界ファイアウォールテストの強度と頻度
B. アクセス制御ポリシーと業界標準の整合
C. ユーザーアクセスレビューの頻度
D. リモートアクセスとデータ暗号化のためのプロトコル
正解**: B (**コメントを発表する**)**

Comprehensive and Detailed Explanation:
In Zero Trust architecture (ZTA), the principle is "never trust, always verify." The most important aspect for an IS auditor to evaluate is whether access control policies are properly designed, aligned with industry standards, and consistently enforced. These policies define how identities, devices, and contexts are authenticated and authorized before gaining access.
* Option A: Perimeter firewalls are less relevant in Zero Trust, which minimizes reliance on network boundaries.
* Option C: Access reviews are important but are periodic, not continuous enforcement.
* Option D: Secure remote protocols are necessary but part of broader access policy enforcement.
* Option B: Correct - policies are the foundation of Zero Trust security.
# ISACA Reference: ISACA's "Zero Trust and Audit Considerations" guidance; CISA Review Manual 27th Edition, Domain 5, section on identity, access, and authentication controls.

質問**: 507**
再利用するストレージメディアから機密情報を削除するのに最適な方法は次のうちどれですか？
A. 暗号シュレッディング
B. 多重上書き
C. 再フォーマット中
D. 再分割
正解**: (**正解を表示します**)**
The best method to delete sensitive information from storage media that will be reused is multiple overwriting. This is because multiple overwriting ensures that the data is practically unrecoverable by any software or hardware means. Multiple overwriting involves writing 0s, 1s, or random patterns onto all sectors of the storage media several times, making the original data unreadable or inaccessible. There arevarious software programs available that can securely delete files from storage media using multiple overwriting techniques1.
Crypto-shredding is not the best method because it only works for encrypted data. Crypto-shredding involves deleting the encryption key used to encrypt the data, making the data unreadable and unrecoverable. However, if the data is not encrypted, crypto-shredding will not erase it2.
Reformatting and re-partitioning are not the best methods because they do not erase the data completely. Reformatting and re-partitioning only delete the file system structures and pointers that make the data accessible, but thedata itself remains on the storage media and can be recovered using data recovery software

質問**: 508**

オンライン請求システムにクラウドプロバイダーを利用している組織では、顧客がウェブサイトに常時アクセスできる必要があります。組織のビジネス要件が満たされていることを確認する最良の方法は何でしょうか？
A. 5分以上の停止があった場合はベンダーに報告を求める
B. ベンダーとのサービス レベル契約 (SLA) を監視します。
C. 監査権条項を発動します。
D. ベンダーとの定期的なパフォーマンスに関する話し合いに合意する
正解: **(**正解を表示します**)**

質問: **509**
次のうち、アジャイルソフトウェア開発プロセスの原則はどれですか？
A. 明確な文書化は、進捗状況を測る主要な指標とみなされるべきである。
B. 開発段階は互いに分離されるべきである。
C. 次の段階に進む前にフェーズの完了を必要とする線形アプローチを使用する必要があります。
D. 開発プロセスの後半であっても、要求事項の変更は歓迎すべきである。
正解: **(**正解を表示します**)**
The correct answer is D. Changing requirements should be welcomed, even late in the development process.
Agile development is iterative, adaptive, and designed to respond to changing requirements. Unlike traditional linear development models, Agile expects feedback and change throughout the project. ISACA's discussion of Agile principles states that changing requirements should be welcomed, even late in development, because Agile processes harness change for the customer's competitive advantage.
Option A is incorrect because Agile values working software and useful outcomes more than extensive documentation as the primary measure of progress. Option B is incorrect because Agile encourages collaboration and iteration rather than isolated phases. Option C describes a waterfall-style approach, not Agile.
This maps to Information Systems Acquisition, Development and Implementation because ISACA's CISA Exam Content Outline includes system development methodologies under Domain 3.
References: ISACA CISA Exam Content Outline, Domain 3; ISACA Journal discussion of Agile principles.

質問: **510**
情報システム監査人は、システム所有者へのインタビューに頼るのではなく、システムから直接取得したデータインベントリリストをレビューすることを決定しました。監査人の決定を最も適切に正当化する根拠として、次のうちどれが適切ですか。
A. 証拠提供者の独立性
B. 証拠提供者の資格

C. 証拠の信頼性
D. 証拠のタイミング
正解**: (**正解を表示します**)**
System-generated data is generally more reliable than interview evidence, which is subjective and prone to bias. Audit standards emphasize evidence that is sufficient and appropriate, where appropriateness relates to relevance and reliability.
References (ISACA): ISACA Audit Standards - Evidence Collection.

質問**: 511**
IS監査担当者は、アウトソーシングされた人事アプリケーションの監査を行う際に、以下のうちどれを最初に行うべきでしょうか？
A. サービスに対して請求された料金が実施された作業に見合っていることを確認します。
B. 契約書の条項と規定を確認してください。
C. 組織のセキュリティポリシーに準拠したデータアクセス権限を実装します。
D. セキュリティインシデントレポートがタイムリーに発行されていることを確認します。
正解**: (**正解を表示します**)**
The correct answer is B. Review the terms and provisions in the contract.
When auditing an outsourced application, the auditor should first understand the contractual responsibilities, service scope, control expectations, reporting requirements, audit rights, compliance obligations, and security commitments. ISACA guidance on outsourcing and third-party assurance emphasizes that contracts are foundational because they define what the service provider is obligated to do and what the customer is entitled to review.
Option A is not first because billing validation is secondary to understanding the service arrangement and obligations.
Option C is incorrect because implementing access rights is a management responsibility, not an audit procedure.
Option D is important, but the auditor must first know whether such reporting is required, how it is defined, and under what timelines, all of which are typically governed by the contract or related agreement.
Therefore, the correct answer is B, because contract review establishes the basis for all further audit work over the outsourced HR application.
References (Official ISACA):
ISACA Journal, Third Party Assurance - highlights the importance of understanding outsourced service arrangements and related assurance expectations.
ISACA Now Blog, The Challenging Task of Auditing Social Media - states that when a function is outsourced, the contract should be reviewed to ensure it specifies required activities and expectations.

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu 1**605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **512**
以下のユーザー操作のうち、意図せずローカルネットワークにマルウェアを侵入させてしまうリスクが最も高いのはどれですか？
A. 内部サーバーにファイルをアップロードする
B. 外部アカウントからのメール添付ファイルを開く
C. ハイパーテキストマークアップ言語(HTML)ドキュメントを表示する
D. 企業ファイル共有からファイルをダウンロードしています
正解: **(**正解を表示します**)**

質問: **513**
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. 実装後の変更レビュー
B. 変更承認委員会に開発者を追加する
C. ステージング環境の作成
D. 少数の人がコードをデプロイする権限を持っています
正解: **(**正解を表示します**)**
If SoD cannot be fully implemented, an independent review of changes after deployment provides assurance that inappropriate or unauthorized code has not been introduced. Other options either weaken controls or fail to provide adequate oversight.
References (ISACA): COBIT BAI06 (Managed IT Changes).

質問: **514**
管理合計値の使用は、以下のどの管理目標を満たしますか？
A. トランザクションの整合性
B. 処理の整合性
C. 配電制御
D. システム復旧性
正解: **(**正解を表示します**)**
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 and Activities: Examples, Appropriateness
Levels and Types of Control | Principles ofManagement
CISA Review Manual 27th Edition, page 337

質問: **515**
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レビューするIS監査担当者にとって、以下のうちどれが最も懸念すべき事項でしょうか？
A. 主要業績評価指標(KPI)が継続的に監視されていない。
B. 主要な利害関係者の意見を取り入れずに指標が定義された。
C. パフォーマンスレポートには専門用語が多すぎる。
D. 指標が業界ベンチマークと一致していません。
正解: **B** (コメントを発表する)
The correct answer is B. Metrics were defined without key stakeholder input.
The greatest concern is that the metrics may not reflect what the organization's key stakeholders actually need to know. IT process performance reporting should support governance, decision-making, accountability, and alignment with business objectives. If metrics are created without stakeholder input, the reports may measure technical activity but fail to measure business value, service quality, risk, control effectiveness, or strategic alignment.
Option A is a concern because KPIs should be monitored consistently. However, even consistently monitored KPIs may be ineffective if they were not defined with stakeholder requirements in mind. Option C is a reporting-quality issue, but technical language can be improved. Option D is less important because industry benchmarking can be useful, but internal stakeholder needs and organizational objectives are more important than external comparison.
ISACA's CISA Exam Candidate Guide includes monitoring and analyzing KPIs, KRIs, and KCIs, and reporting relevant risk and control information to stakeholders to facilitate risk-based decision-making. (ISACA) ISACA's CISA Exam Content Outline also places IT performance monitoring and reporting under Governance and Management of IT. (ISACA) References: ISACA CISA Exam Content Outline, Domain 2; ISACA Exam Candidate Guide references to KPIs/KRIs/KCIs and stakeholder reporting. (ISACA)

質問: **516**
データ損失防止 (DLP) メカニズムの主な目的は次のどれですか?
A. データ損失を防ぎながらシステムパフォーマンスを向上
B. データ損失回復手順を自動化し、インシデント発生時のダウンタイムを最小限に抑える

C. 機密データの不正な送信や漏洩を防ぐ
D. データ保護に関する規制要件への準拠の確保
正解**: (**正解を表示します**)**
The central goal of DLP is to prevent sensitive data-such as PII, PHI, or intellectual property-from leaving the organization through unauthorized channels. DLP solutions monitor, detect, and block potential data exfiltration via email, endpoints, cloud applications, or removable media. While compliance (D) is often a driver, it is a secondary outcome of implementing DLP. Enhancing performance (A) and recovery automation (B) are not objectives of DLP. ISACA positions DLP as a critical control for confidentiality under DSS05 (Managed Security Services).
References (ISACA): COBIT 2019, DSS05 Managed Security Services.

質問**: 517**
複数の拠点を持つ医療機関が、患者がどこで治療を受けても患者データにアクセスできるようにしたい場合、次のうちどれが最も効率的な解決策でしょうか？
A. サービスとしてのインフラストラクチャ (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. 動的位置特定
正解**: B (**コメントを発表する**)**
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 settingsand 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

質問: **518**
情報システム監査担当者がITガバナンス監査を実施している際に、多くのイニシアチブが個々の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づいた。以下の推奨事項のうち、ITチームの成熟度向上に最も大きな影響を与えるのはどれか？
A. 正式な承認が得られ、文書化されるまで、現在進行中のすべてのITプロジェクトを中止してください。
B. ITプロセスが成熟したかどうかを確認するため、翌年にフォローアップ監査を実施する。
C. すべてのIT関連の決定事項をプロジェクト管理ツールに記録し、追跡する。
D. ITの優先順位付けと支出を監督するための学際的なIT運営委員会を設置する。
正解: **D** (コメントを発表する)
The correct answer is D. Create an interdisciplinary IT steering committee to oversee IT prioritization and spending.
The issue is not just poor documentation; it is weak IT governance. Projects are being managed informally and separately by isolated project managers. This indicates a lack of centralized prioritization, oversight, accountability, and alignment with business objectives. An interdisciplinary IT steering committee would help ensure that IT initiatives are reviewed, prioritized, funded, monitored, and aligned with enterprise strategy.
ISACA's glossary defines an IT steering committee as an executive-management-level committee that assists in delivering IT strategy, oversees day-to-day management of IT service delivery and IT projects, and focuses on implementation aspects. This directly addresses the problem described in the question.
Option A is too extreme. Stopping all projects could harm the organization and is not a mature governance response unless there is an immediate critical risk. Option B is weak because a follow-up audit only checks later whether improvement occurred; it does not create governance now. Option C may improve documentation, but a project management tool alone does not establish governance, prioritization, or business accountability.
This question maps to Governance and Management of IT because the concern is IT governance maturity, project oversight, prioritization, and spending. ISACA's CISA Exam Content Outline includes organizational structure, IT governance, IT strategy, IT resource management, and evaluation of IT project management alignment with organizational objectives.
References: ISACA CISA Exam Content Outline, Domain 2; ISACA Interactive Glossary, "IT steering committee."

質問: **519**

組織のITポートフォリオをレビューしたところ、使用されていないアプリケーションがいくつか見つかりました。このような状況の再発を防ぐ最善の方法は、次のことを実施することです。
A. 正式な提案依頼書(RFP)プロセス
B. ビジネスケース開発手順
C. 情報資産取得ポリシー
D. 資産ライフサイクル管理。
正解: **(**正解を表示します**)**
Asset life cycle management is a technique of asset management where facility managers maximize the usable life of assets throughplanning, purchasing, using, maintaining, and disposing of assets1. The mainaim of assetlife cycle management is to reduce costs and increase productivity by optimizing the performance, reliability, and lifespan of assets2. Asset life cycle management can help prevent the situation of having unused applications by ensuring that the applications are aligned with the business needs, objectives, and strategies, and that they are regularly reviewed, updated, or retired as necessary3.
The other options are not as effective as asset life cycle management for preventing unused applications. A formal request for proposal (RFP) process is a method of soliciting bids from potential vendors or suppliers for a project or service. A RFP process can help select the best application for a specific requirement, but it does not ensure that the application will be used or maintained throughout its lifecycle. Business case development procedures are a set of steps that involve defining the problem, analyzing the alternatives, and proposing a solution for a project or initiative. Business case development procedures can help justify the need and value of an application, but they do not guarantee that the application will be utilized or supported after its implementation. An information asset acquisition policy is a document that outlines the rules and standards for acquiring information assets such as applications. An information asset acquisition policy can help ensure that the applications are acquired in a consistent and compliant manner, but it does not address how the applications will be managed or disposed of after their acquisition.

質問: **520**
ある組織は最近、規制当局から報告データに重大な矛盾があるとの通知を受けた。
予備調査の結果、不一致の原因は組織のデータ品質の問題であることが判明しました。経営陣はデータ品質チームに対し、プログラムの改善を指示しました。監査委員会は内部監査部門に対し、このプロセスに関するアドバイザーとなるよう要請しました。経営陣の懸念事項に対処するため、内部監査部門はどのデータセットを最初にレビューすべきと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. 規制機関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

正解: (正解を表示します)
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 and Explanations Database, Question ID: 262

質問: **521**
システムを自社開発する場合と比較して、ソフトウェアパッケージを購入する場合、エンドユーザーによるテストの必要性は以下のようになります。
A. 削除済み
B. 変更なし
C. 増加
D. 縮小
正解: (正解を表示します)
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. Enduser 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

質問: **522**
情報システム監査担当者が、インターネットに接続された重要なシステムが攻撃に対して脆弱であり、かつパッチが提供されていないことを発見した。
監査人はまず何を行うべきだと勧告すべきでしょうか？
A. パッチを適用できる新しいシステムを実装します。
B. システムを保護するために追加のファイアウォールを実装します。
C. サーバーを廃止します。
D. 関連するリスクを評価します。
正解: **(**正解を表示します**)**
The first step in addressing a vulnerability is to evaluate the associated risk, which involves assessing the likelihood and impact of a potential exploit. Based on the risk assessment, the appropriate mitigation strategy can be determined, such as implementing a new system, addingfirewalls, or decommissioning the server. References: ISACA CISA Review Manual 27th Edition, page 280

質問: **523**
ブラックボックス侵入テストを計画する際に、最も重要な確認事項は次のうちどれですか？
A. 戦術、技術、手順は決定済みです。
B. 組織のネットワークアーキテクチャの図が利用可能です。
C. 試験結果は文書化され、経営陣に報告されます。
D. クライアント組織の経営陣がテスト範囲を承認しました。
正解: **(**正解を表示します**)**
The correct answer is D. The management of the client organization has approved the scope of testing.
Before any penetration test begins, especially a black-box test, the most important requirement is formal management approval of the scope. Penetration testing can be disruptive and may involve activities that resemble real attacks. Therefore, the tester must

have clear authorization, approved scope, rules of engagement, timing, target systems, restrictions, and escalation procedures before testing starts.
ISACA guidance on penetration testing emphasizes the importance of clear documentation of project scope, rules of engagement, and client authorization to demonstrate that testing is being conducted legally and ethically. ISACA also explains that planning security testing requires defining scope and out-of-scope items, including what will be tested, where testing will occur from, when testing should not be performed, which hosts are restricted, and who will perform the testing.
Option A is useful because tactics, techniques, and procedures help define how the test will be performed, but they should not override approved scope and authorization. Option B is not required for a black-box penetration test because black-box testing intentionally gives the tester little or no internal knowledge of the environment. Option C is important because results must be documented and communicated, but reporting happens after testing; formal authorization and scope approval must come first.
This question maps mainly to Protection of Information Assets, because penetration testing is a security testing technique used to evaluate vulnerabilities and the effectiveness of security controls. ISACA's CISA Exam Content Outline includes security testing tools and techniques, threat and vulnerability management, and security monitoring under Domain 5.
References: ISACA CISA Exam Content Outline, Domain 5; ISACA white paper on penetration testing scope, rules of engagement, and client authorization; ISACA Journal, Planning for Information Security Testing: A Practical Approach.

質問**: 524**
クラウド環境におけるアプリケーションの統制を評価するための監査を計画する際、IS監査担当者が最も理解すべきことは以下のとおりです。
A. サービスレベル契約 (SLA) に違反した場合の不履行料金。
B. クラウドプラットフォームアーキテクチャからの可用性レポート。
C. クラウドプロバイダーと組織間の責任共有モデル。
D. クラウドシステムによってサポートされるビジネスプロセス再設計。
正解**: (**正解を表示します**)**
In cloud environments, responsibility for controls is split between the provider and the customer. The division depends on the service model (IaaS, PaaS, SaaS). Misunderstanding the shared responsibility model can create gaps in control coverage, where critical risks may not be managed by either party. SLA penalties (A) are contractual issues, not audit priorities. Availability reports (B) and business process redesign (D) are relevant but not as fundamental as defining control ownership. ISACA's cloud audit guidelines stress that proper scoping begins with understanding shared responsibilities to avoid assurance gaps.
References (ISACA): ISACA Cloud Computing Audit Program; ISACA Journal - Shared Responsibility in Cloud.

質問: **525**
組織におけるシャドウITの根本原因として最も可能性が高いのは、次のうちどれですか？
A. 技術投資に対する長期にわたる承認
B. ソフトウェアライセンス料を削減する機会
C. クラウドベースのアプリケーションとサービスの使いやすさ
D. 承認済みソフトウェアがユーザー要件を満たしていません
正解: **D** (コメントを発表する)
Shadow IT often arises when approved software does not meet user requirements (Option D), leading employees to seek alternative solutions.
ISACA CISA Reference: IT governance frameworks stress the need for user-centric IT policies to mitigate shadow IT risks.
Risk Implication: Shadow IT introduces security vulnerabilities, compliance risks, and potential data breaches.

質問: **526**
侵入テストのどの段階で、ホスト検出とドメインネームシステム(DNS)照会が実施されますか？
A. 発見
B. 攻撃
C. 計画
D. レポート
正解: **A** (コメントを発表する)
Penetration testing is a method of evaluating the security of a system or network by simulating an attack from a malicious source. Penetration testing typically consists of four phases: planning, discovery, attacks, and reporting. In the discovery phase, penetration testers gather information about the target system or network, such as host detection, domain name system (DNS) interrogation, port scanning, service identification, operating system fingerprinting, vulnerability scanning, etc. This information can help to identify potential entry points, weaknesses, or vulnerabilities that can be exploited in the subsequent attack phase. Host detection and DNS interrogation are techniques that can be used in the discovery phase to determine the active hosts and their IP addresses and hostnames on the target network. References: [ISACA CISA Review Manual 27th Edition], page 368.

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジン

を手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu 1605問、３０%ディスカウント、特別な割引コード: JPNshiken」

質問: **527**
新しいデータの分類を検討する際に、最も優れた情報源は次のうちどれですか？
A. データ管理者による入力
B. セキュリティポリシー要件
C. リスク評価結果
D. 現在の保護レベル
正解: **(**正解を表示します**)**
The best source ofinformation for examining the classification of new data is the risk assessment results, because they provide an objective and consistent basis for determining the value, sensitivity, and criticality of the data, as well as the potential impact of unauthorized disclosure, modification, or loss of the data12. The risk assessment results can help to definethe appropriate classification levels and criteria for the data, such as public, internal, confidential, or restricted12. Input by data custodians, security policy requirements, and current levelof protection are not the best sources of information for examining the classification of new data, because they may not reflect the actual risk exposure or business needs of the data. References: 1: CISA Review Manual (Digital Version), Chapter 5, Section5.4.2 2: CISA Online Review Course, Module 5, Lesson 4

質問: **528**
大規模システムアップグレード後の導入後レビューを実施するIS監査担当者にとって、以下のうちどれが最も懸念すべき事項でしょうか？
A. 変更は開発グループによって本番環境に反映されます。
B. 変更承認は正式には文書化されていません。
C. オブジェクトコードは開発グループがアクセスできます。
D. 開発者はテスト環境にアクセスできます。
正解: **A (**コメントを発表する**)**

質問: **529**
IS監査担当者がフォローアップ監査を実施しており、いくつかの重大な不備が対処されていないことに気づいた。監査担当者の最善の行動は次のうちどれか。
A. 欠陥に対処しないことによる影響を評価する。
B. 文書管理の欠陥に対処しない理由。
C. 新しい推奨事項を提供します。
D. 不備が解消されるまで監査を延期する。
正解: **A (**コメントを発表する**)**

質問: **530**
IS監査担当者は、IT部門とビジネス部門が実施した最新のアプリケーションユーザーアクセスレビューに関連する文書を評価しています。その結果、ユーザーリストがシステムによって生成されたものではないことが判明しました。以下のうち、最も懸念すべき事項はどれでしょうか？
A. ユーザーリストの完全性を確認しました
B. ユーザーリストの可用性を確認しました
C. ユーザーリストの機密性を確認しました
D. ユーザーリストの出典元を確認しました
正解: **(正解を表示します)**

質問: **531**
ネットワーク活動を監視するサードパーティサービスプロバイダーのIS監査を計画する際に、最初に行うべき手順は次のうちどれですか？
A. 第三者の監視ログとインシデント対応状況を確認する
B. 第三者プロバイダーの役割と責任を確認する
C. 組織の第三者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判断します
正解: **(正解を表示します)**
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.

質問: **532**
ITバランススコアカードは主に以下の目的で使用されます。
A. ITプロジェクトポートフォリオの評価
B. IT戦略パフォーマンスの測定
C. IT予算とリソースの割り当て
D. IT関連プロセスにおけるリスクの監視
正解: **(正解を表示します)**
An IT balanced scorecard is primarily used for measuring IT strategic performance. An IT 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. An IT 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 otheroptions are not the primary uses of an IT 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. References: CISA Review Manual (Digital Version)1, Chapter 1, Section 1.2.3

質問: **533**
ネットワークサブネットでウイルス感染が発生したとの通知をインシデント対応チームに受けました。次のステップとして取るべき行動は次のうちどれですか？
A. 被害を最小限に抑えることに注力する。
B. 事件を記録してください。
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. 影響を受けたシステムを削除して復元します。
正解: **(**正解を表示します**)**

質問: **534**
以下のうち、第三者サービスプロバイダーの情報セキュリティ管理が効果的であることをIS監査人が最もよく証明できる証拠はどれですか？
A. サービスプロバイダのセキュリティ構成制御に関するドキュメント
B. サービス提供者のポリシーと手順のレビュー
C. 外部監査人による内部統制の監査報告書
D. サービスプロバイダーの上級管理職へのインタビュー
正解: **C (**コメントを発表する**)**
Toverify the effectivenessof a third-party provider'ssecurity controls, anindependent external audit reportis thestrongestevidence.
Option A (Incorrect):Security configuration documentsare helpful butdo not confirm effectivenesswithout validation.
Option B (Incorrect):Policies and procedures outlineintent, but anaudit confirms actual implementation.
Option C (Correct):External audit reports (e.g., SOC 2, ISO 27001)provideindependent assurancethat security controls are effective.
Option D (Incorrect):Management interviews providequalitativeinsights but arenot objective evidenceof control effectiveness.
Reference:ISACA CISA Review Manual -Domain 3: Information Systems Acquisition, Development, and Implementation- Coversthird-party risk assessments and audit assurance.

質問: **535**
IT監査計画に含めるプロジェクトを選択する際に、IS監査担当者にとって最も有用な情報を提供するのは次のうちどれですか？

A. プロジェクト憲章
B. プロジェクト計画
C. プロジェクト課題ログ
D. プロジェクトのビジネスケース
正解**: (**正解を表示します**)**
A project business case is a document that describes the rationale and justification for initiating a project, based on its expected costs, benefits, risks, and feasibility. A project business case provides the most useful information to an IS auditor when selecting projects for inclusion in an IT audit plan, because it helps the IS auditor to:
Understand the purpose, scope, objectives, and deliverables of the project Assess the alignment of the project with the organization's strategy, vision, and goals Evaluate the value proposition and return on investment of the project Identify the key stakeholders, sponsors, and owners of the project Analyze the potential risks and issues associated with the project Compare and prioritize the project with other competing projects The other possible options are:
A). Project charter: A project charter is a document that formally authorizes and defines the high-level scope, roles, responsibilities, and authority of a project. A project charter provides some useful information to an IS auditor when selecting projects for inclusion in an IT audit plan, but it is not the most useful information. A project charter does not provide enough details about the costs, benefits, risks, and feasibility of the project, which are essential for evaluating its suitability for an IT audit plan.
B). Project plan: A project plan is a document that outlines the detailed scope, schedule, budget, resources, quality, and communication plans of a project. A project plan provides some useful information to an IS auditor when selecting projects for inclusion in an IT audit plan, but it is not the most useful information. A project plan does not provide enough information about the rationale, justification, value proposition, and alignment of the project with the organization's strategy and goals, which are important for assessing its relevance for an IT audit plan.
C). Project issue log: A project issue log is a document that records and tracks the issues that arise during a project's execution and how they are resolved. A project issue log provides some useful information to an IS auditor when selecting projects for inclusion in an IT audit plan, but it is not the most useful information. A project issue log does not provide enough information about the purpose, objectives, benefits, and feasibility of the project, which are critical for determining its priority for an IT audit plan.

質問**: 536**
以下の弱点のうち、境界ファイアウォールの効果的な運用に最も大きな影響を与えるのはどれでしょうか？
A. ファイアウォールルールの設定ミス
B. ファイアウォールソフトウェアへの潜在的なバックドア
C. ファイアウォールアクティビティのアドホック監視

D. デフォルト設定でのステートフルファイアウォールの使用
正解: **(**正解を表示します**)**

質問: **537**
セキュリティ脆弱性管理プログラムを成功裏に確立するために、以下のうち最も重要なものはどれですか？
A. 堅牢な卓上運動計画
B. 包括的な資産目録
C. テスト済みのインシデント対応計画
D. 承認されたパッチ適用ポリシー
正解: **A (**コメントを発表する**)**
A comprehensive asset inventory is the most important factor for the successful establishment of a security vulnerability management program. A security vulnerability management program is a systematic process of identifying, assessing, prioritizing, and remediating vulnerabilities in the organization's IT environment1. A comprehensive asset inventory is a complete and accurate record of all the hardware, software, and network components that the organization owns or uses2. A comprehensive asset inventory helps the organization to:
Know what assets are in scope for vulnerability scanning and assessment3.
Identify the vulnerabilities that affect each asset and their severity level4.
Prioritize the remediation of vulnerabilities based on the criticality and value of each asset.
Track the status and progress of vulnerability remediation for each asset.
Measure the effectiveness and maturity of the vulnerability management program.
A robust tabletop exercise plan is a simulated scenario that tests the organization's preparedness and response capabilities for a potential cyberattack or incident. A tabletop exercise plan is useful for validating and improving the organization's incident response plan, but it is not essential for establishing a security vulnerability management program.
A tested incident response plan is a documented process that defines the roles, responsibilities, and actions of the organization's personnel in the event of a cyberattack or incident. A tested incident response plan is important for minimizing the impact and restoring normal operations after a security breach, but it is not critical for establishing a security vulnerability management program.
An approved patching policy is a set of rules and guidelines that governs how the organization applies patches and updates to its IT systems and applications. An approved patching policy is a key component of the remediation phase of the vulnerability management program, but it is not sufficient for establishing a security vulnerability management program.

質問: **538**
プライバシー監査において、情報システム監査人の最も重要なステップは次のどれですか?
A. データ管理のために実施されている制御を評価します。

B. 従業員に対してプライバシートレーニングが実施されているかどうかを判断します。
C. 適切な個人情報 (PII) 保護対策についてサードパーティ契約を確認します。
D. 個人を特定できる情報 (PII) データのライフ サイクルのすべての段階を分析して、潜在的なリスクを特定します。
正解: **(**正解を表示します**)**
Comprehensive and Detailed Explanation:
The most important step in a privacy audit is to ensure that all risks associated with PII handling are identified. This requires analyzing the entire PII data life cycle-from collection, processing, storage, and transfer to retention and destruction.
* Option A: Reviewing data management controls is part of the audit but is narrower than life cycle coverage.
* Option B: Privacy training is necessary, but training alone doesn't ensure compliance.
* Option C: Reviewing third-party agreements is important but only covers outsourced risks.
* Option D: Provides comprehensive coverage of privacy risks across all stages.
# ISACA Reference: CISA Review Manual 27th Edition, Domain 5, section on data privacy, data life cycle, and PII risks.

質問: **539**
IS監査担当者は、ロボティック ・プロセス ・オートメーション(RPA)の実装を監査する際に、まず最初に以下のどれを行うべきでしょうか？
A. ロボットが使用する認証情報と、それらが保存されている場所を特定します。
B. ソリューション全体のアーキテクチャを評価します。
C. ロボットが実行した一連の動作を分析します。
D. ロボットによって自動化されたビジネスプロセスを理解する。
正解: **(**正解を表示します**)**

質問: **540**
ITガバナンスフレームワークを使用していない組織にとって、以下のうち最も重大な影響はどれですか？
A. 主要リスク指標(KRIS)の適切な測定
B. IT計画と事業目標の整合性が不十分
C. 不十分な事業影響分析(BIA)の結果と予測
D. 主要業績評価指標(KPI)の測定が不十分である
正解: **B (**コメントを発表する**)**
The most significant impact to an organization that does not use an IT governance framework is inadequate alignment of IT plans and business objectives. IT governance is a framework for the governance and management of enterprise information and technology (IandT) that supports enterprise goal achievement1. IT governance helps to ensure that IT investments and activities are aligned with the business strategy, vision, and values of the

organization. IT governance also helps to optimize the value of IT, manage IT-related risks, and measure and monitor IT performance1.
Without an IT governance framework, an organization may face challenges such as:
Lack of clarity and direction for IT decision making
Inconsistent or conflicting IT priorities and demands
Inefficient or ineffective use of IT resources and capabilities
Poor quality or delivery of IT services and products
Increased exposure to IT-related threats and vulnerabilities
Reduced customer satisfaction and trust in IT
Missed opportunities for innovation and competitive advantage
Therefore, an organization that does not use an IT governance framework may fail to achieve its business objectives and may lose its competitive edge in the market.
References:
COBIT 2019 Framework Introduction and Methodology, Section 1.1: What Is Governance of Enterprise IandT?
IT Governance: Definitions, Frameworks and Planning, Section 1: What Is IT Governance?

質問**: 541**
IS監査担当者が、あるデータベース管理システム(DBMS)から別のDBMSへの移行に伴うリスクを評価しています。変更全体を通してシステムの整合性を確保するために、次のうちどれが最も役立つでしょうか？
A. 同じデータ分類を保持する
B. 同じデータ入力を保持する
C. 同じデータ構造を保持する
D. 同じデータインターフェースを保持する
正解**: C (**コメントを発表する**)**
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.

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu　**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **542**
ITプロジェクトポートフォリオ管理の目的として適切なものはどれですか？
A. 追跡メカニズムの確立
B. プロジェクトの成功裡の実施
C. 健全で戦略的に整合性の取れた投資機会の選定
D. ビジネスケースのメリットの検証
正解: **(**正解を表示します**)**

質問: **543**
2つの組織が合併した後、IS監査担当者が行うべき最も重要な業務は次のうちどれですか？
A. アクセス権限が審査済みであることを確認しています
B. 有効期限のアクセス権限を調査中
C. 重要資源の継続性計画を更新中
D. セキュリティポリシーを更新しています
正解: **A (**コメントを発表する**)**
The most important task for an IS auditor to perform after the merger of two organizations is to verify that access privileges have been reviewed. Access privileges are the permissions granted to users, groups, or roles to access, modify, or manage IT resources,

such as systems, applications, data, or networks. After a merger, the IS auditor should ensure that the access privileges of both organizations are aligned with the new business objectives, policies, and processes, and that there are no conflicts, overlaps, or gaps in the access rights. The IS auditor should also verify that the access privileges are based on the principle of least privilege, which means that users are granted only the minimum level of access required to perform their tasks.
The other options are not as important as verifying that access privileges have been reviewed:
Investigating access rights for expiration dates is a useful task, but it is not the most important one. Expiration dates are the dates when access rights are automatically revoked or suspended after a certain period of time or after a specific event. The IS auditor should check that the expiration dates are set appropriately and enforced consistently, but this is not as critical as reviewing the access privileges themselves.
Updating the continuity plan for critical resources is a necessary task, but it is not the most urgent one. A continuity plan is a document that outlines the procedures and actions to be taken in the event of a disruption or disaster that affects the availability of IT resources. The IS auditor should update the continuity plan to reflect the changes and dependencies introduced by the merger, but this can be done after verifying that the access privileges are secure and compliant.
Updating the security policy is an essential task, but it is not the most immediate one. A security policy is a document that defines the rules and guidelines for securing IT resources and protecting information assets.
The IS auditor should update the security policy to incorporate the best practices and standards of both organizations, and to address any new risks or threats posed by the merger, but this can be done after verifying that the access privileges are aligned with the policy.

質問: **544**
IS監査の結果、ITアプリケーションのパフォーマンスが低下しており、データ不整合やデータ整合性の問題が発生していることが判明しました。最も可能性の高い原因は何でしょうか？
A. データベースクラスタリング
B. データキャッシュ
C. データベーステーブルのインデックス再構築
D. ロードバランシング
正解: **(**正解を表示します**)**
Data caching is the most likely cause of poor performance, data inconsistency and integrity issues in an IT application, because it involves storing frequently accessed data in a temporary memory location (cache) to reduce the latency and bandwidth consumption of retrieving data from the original source. However, data caching can also introduce problems such as stale data (when the cache is not updated with changes made to the

original source), cache coherence (when multiple caches store copies of the same data and need to be synchronized), and cache corruption (when the cache is damaged or tampered with).
Database clustering is not a likely cause of poor performance, data inconsistency and integrity issues, because it involves distributing data across multiple servers or nodes to improve availability, scalability and load balancing of database operations. Database clustering can also enhance data consistency and integrity by using replication and synchronization mechanisms to ensure that all nodes have the same view of the data.
Reindexing of the database table is not a likely cause of poor performance, data inconsistency and integrity issues, because it involves rebuilding or reorganizing indexes on tables or views to improve query performance and reduce fragmentation of index pages. Reindexing can also improve data consistency and integrity by ensuring that indexes reflect the current state of the data in the tables or views.
Load balancing is not a likely cause of poor performance, data inconsistency and integrity issues, because it involves distributing workloads across multiple servers or resources to optimize resource utilization, throughput and response time of applications. Load balancing can also enhance data consistency and integrity by using algorithms and protocols to route requests to the most appropriate server or resource based on availability, capacity and performance.
References:
Data Caching
Database Clustering
Reindexing Database Tables in SQL Server
[Load Balancing]

質問: **545**
ある組織が社内でWebアプリケーションを開発しました。以下のうち、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情報システム監査担当者に最もよく示す証拠となるのはどれでしょうか？
A. データベースアプリケーション監視ログ
B. Webアプリケーションファイアウォール(WAF)の実装
C. 侵入テスト結果
D. 第三者によるコードレビュー
正解: **(正解を表示します)**

質問: **546**
不正ログイ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. 時間外利用の制限
D. 自動パスワード生成器をインストールしています

正解: (正解を表示します)
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

質問: **547**
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良の方法は次のうちどれですか？
A. 組織の機密データへのアクセスログを適時に確認する。
B. BYOD(私物端末の持ち込み)セキュリティ手順に利用制限を含める。
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. 従業員にセキュリティ手順を正式に承認させる。
正解: (正解を表示します)

質問: **548**
組織が事業影響分析(BIA)を実施する際に、最も重要な考慮事項は次のうちどれですか？
A. 技術的リスクによって引き起こされる混乱の影響に焦点を当てる。
B. IT管理部門が設定した復旧時間目標(RTO)を検証する。
C. 様々な部門のプロセスオーナーを巻き込む。
D. 規制要件を満たすために不可欠なハードウェアを特定する。
正解: (正解を表示します)
The correct answer is C. Involving process owners from various departments.
A business impact analysis is a business-driven activity, not only an IT exercise. The purpose of a BIA is to evaluate the impact of losing business processes, information assets, resources, and supporting systems.
Process owners from different departments are best positioned to explain business criticality, operational dependencies, financial impact, legal/regulatory impact, customer impact, reputational impact, and minimum recovery requirements.
ISACA defines BIA as the process of evaluating the criticality and sensitivity of information assets by determining the impact of losing support of any resource. It also establishes loss escalation over time, identifies minimum resources needed to recover, and prioritizes

recovery of processes and supporting systems. ISACA also notes that BIA captures income loss, unexpected expense, legal issues, interdependent processes, and loss of public confidence.
Option A is incorrect because BIA should not focus only on technological risks. It must consider business impacts from many types of disruptions, including people, facilities, suppliers, applications, infrastructure, data, and external events.
Option B is incorrect because RTOs should not simply be "set by IT management." Recovery objectives must be driven by business needs and validated with business/process owners. ISACA's contingency planning guidance states that the BIA helps prioritize recovery activities and define metrics such as MTD, RTO, and RPO.
Option D is too narrow. Hardware may be important, but BIA is broader than identifying critical hardware; it identifies business process impacts, dependencies, recovery priorities, and minimum recovery resources.
References: ISACA CISA Exam Content Outline, Domain 4; ISACA Interactive Glossary, "Business impact analysis"; ISACA Journal, Information System Contingency Planning Guidance.

質問**: 549**
ビジネスインテリジェンスシステムを通じて不正確または誤解を招くデータが拡散するリスクを軽減するための最善の方法は何ですか？
A. データをある形式から別の形式に変換するためのルールを確立する
B. 新規および既存のアプリケーションにデータ入力制御を実装する
C. 一貫性のあるデータベースインデックス戦略を実装する
D. メタデータを保存およびアクセスするためのメタデータリポジトリを開発する
正解**: (**正解を表示します**)**
The best way to reduce the risk of inaccurate or misleading data proliferating through business intelligence systems is to establish rules for converting data from one format to another, because this ensures that the data quality and integrity are maintained throughout the data transformation process. Data conversion rules define the standards, procedures, and methods for transforming data from different sources and formats into a common format andstructure that can be used by the business intelligence systems12.
Implementing data entry controlsfor new and existing applications, implementing a consistent database indexing strategy, and developing a metadata repository to store and access metadata are not the best ways to reduce the risk of inaccurate or misleading dataproliferating through business intelligence systems, becausethey do not address the issue of dataconversion, which is a critical step in the data integration process for business intelligence systems. References: 1: CISA Review Manual (Digital Version), Chapter 4, Section 4.3.3 2: CISA Online Review Course, Module 4, Lesson 3

質問**: 550**

IS監査担当者は、提案されている新しいコンピュータハードウェアの取得について監査を依頼されました。監査担当者の主な懸念事項は次のとおりです。
A. 実装計画はユーザーの要求を満たしています。
B. 完全な監査証跡が含まれます。
C. 重要なビジネスケースが確立されました。
D. 新しいハードウェアは確立されたセキュリティ基準を満たしています
正解: **(**正解を表示します**)**
The IS auditor's primary concern when auditing the proposed acquisition of new computer hardware is that a clear business case has been established. A business case is a document that justifies the need, feasibility, and benefits of a proposed project or investment. A clear business case can help to ensure that the acquisition of new computer hardware is aligned with the organization's goals, objectives, and requirements, and that it provides value for money and return on investment. The other options are not as important as establishing a clear business case, as they do not address the rationale or justification for acquiring new computer hardware. References: CISA Review Manual, 27th Edition, page 467

質問: **551**
構成管理データベース(CMDB)を導入する最も適切な理由は次のうちどれですか？
A. ソフトウェア構成アイテムのライセンスを保存するため
B. 構成項目のリアルタイムネットワーク監視を提供する
C. 構成アイテムの物理的な位置を追跡するため
D. 構成項目間の関係を文書化する
正解: **(**正解を表示します**)**
The best answer is D. To document relationships between configuration items.
ISACA's configuration management guidance identifies the value of a CMDB in maintaining information about configuration items and their relationships. That relationship view is what supports effective impact analysis, change management, incident response, and dependency understanding across the environment.
Option A is too narrow. Option B describes monitoring rather than configuration management. Option C may be one data element in some environments, but the defining value of a CMDB is not physical location tracking. The central purpose is documenting configuration items and how they relate to one another.
References (Official ISACA):
ISACA Glossary / configuration management references.

質問: **552**
組織内でプライバシー関連の管理策を実施する際の主な目的は次のうちどれですか？
A. 機密データの損失を防ぐため
B. 法的および規制上の要件を遵守するため

C. 暗号化のために保存データと転送データを識別する
D. 個人が自身のデータの利用に関して選択肢を持てるようにする
正解: **B (**コメントを発表する**)**
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

質問: **553**
ベンダーが重要な業務アプリケーションへの特権アクセスを必要としています。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. 特権ロールのリアルタイムアクティビティ監視を実装する
B. ベンダー契約に監査権を含める
C. 特権的な役割と責任のレビューを実施する
D. ベンダーに特権ロールのジョブローテーションの実装を要求する
正解: **(**正解を表示します**)**
A vendor requires privileged access to a key business application. The best recommendation to reduce the risk of data leakage is to implement real-time activity monitoring for privileged roles. This is because real-time activity monitoring can provide visibility and accountability for the actions performed by the vendor with privileged access, such as creating, modifying, deleting, or copying data. Real-time activity monitoring can also enable timely detection and response to any unauthorized or suspicious activities that may indicate data leakage. Including the right-to-audit in the vendor contract is a good practice, but it may not be sufficient to prevent or detect data leakage in a timely manner, as audits are usually performed periodically or on-demand.
Performing a review of privileged roles and responsibilities is also a good practice, but it may not address the specific risk of data leakage by the vendor with privileged access. Requiring the vendor to implement job rotation for privileged roles may reduce the risk of collusion or fraud, but it may not prevent or detect data leakage by any individual with privileged access. References: CISA Review Manual (Digital Version),
[ISACA Privacy Principles and Program Management Guide]

質問: **554**

ある組織は最近、社内会計ソフトウェアシステムへのカスタムコードのデプロイにアジャイルモデルを採用しました。本番環境へのコードデプロイに関する既存の手順を見直す際、対処すべき最も重要なセキュリティ上の懸念事項は次のうちどれでしょうか？

A. ソフトウェアの脆弱性スキャンは、必要に応じて随時実施されます。

B. 変更管理には、品質保証 (QA) によるテストと承認は含まれません。

C. 本番環境へのコードデプロイは自動化されていません。

D. 現在のDevSecOpsプロセスは独立して検証されていません。

正解: **(**正解を表示します**)**

Change control is the process of managing and documenting changes to an information system or its components. Change control aims to ensure that changes are authorized, tested, approved, implemented, and reviewed in a controlled and consistent manner. Change control is an essential part of ensuring the security, reliability, and quality of an information system.

One of the key elements of change control is testing and approval from quality assurance (QA). QA is the function that verifies that the changes meet the requirements and specifications, comply with the standards and policies, and do not introduce any errors or vulnerabilities. QA testing and approval provide assurance that the changes are fit for purpose, function as expected, and do not compromise the security or performance of the system.

An organization that has recently moved to an agile model for deploying custom code to its in-house accounting software system should still follow change control procedures, including QA testing and approval.

Agile development methods emphasize flexibility, speed, and collaboration, but they do not eliminate the need for quality and security checks. In fact, agile methods can facilitate change control by enabling frequent and iterative testing and feedback throughout the development cycle.

However, if change control does not include testing and approval from QA, this poses a significant security concern for the organization. Without QA testing and approval, the changes may not be properly validated, verified, or evaluated before being deployed to production. This could result in introducing bugs, defects, or vulnerabilities that could affect the functionality, availability, integrity, or confidentiality of the accounting software system. For example, a change could cause data corruption, performance degradation, unauthorized access, or data leakage. These risks could have serious consequences for the organization's financial operations, compliance obligations, reputation, or legal liabilities.

Therefore, change control that does not include testing and approval from QA is the most significant security concern to address when reviewing the procedures in place for production code deployment in an agile model.

References:

Change Control - ISACA

Quality Assurance - ISACA
Agile Development - ISACA
10 Agile Software Development Security Concerns You Need to Know

質問: **555**
ITガバナンスにおける効果的なリスク管理に必要なものは次のうちどれですか？
A. リスク評価は現地の管理者のみが責任を負います。
B. ITリスク管理は企業リスク管理とは別個のものです。
C. リスク管理戦略は監査委員会によって承認されました。
D. リスク評価は管理プロセスに組み込まれています。
正解: **(**正解を表示します**)**
The necessary condition for effective risk management in IT governance is that risk evaluation is embedded in management processes. Risk evaluation is the process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. Risk evaluation should be integrated into the management processes of planning, implementing, monitoring, and reviewing the IT activities and resources. This will ensure that risk management is aligned with the business objectives, strategies, and values, and that risk responses are timely, appropriate, and effective. References:
CISA Review Manual (Digital Version)
CISA Questions, Answers and ExplanationsDatabase

質問: **556**
物理セキュリティ監査の際、情報システム監査担当者に、企業オフィスビル内の特定の3つのフロアへのアクセスを許可する近接バッジが支給されました。以下の問題のうち、最も懸念すべきものはどれでしょうか？
A. 監査の現場作業の最初の2日間は、近接バッジが機能しませんでした。
B. 野外調査中に同行者を必要とする規定はありませんでした。
C. アクセス違反の試みが失敗に終わった場合、フォローアップは行われませんでした。
D. 近接バッジにより、制限区域へのアクセスが誤って許可されました。
正解: **D (**コメントを発表する**)**
The proximity badge incorrectly granting access to restricted areas is the most concerning issue, as it indicates a failure of the access control system to enforce the principle of least privilege and protect the sensitive or critical assets of the organization. The proximity badge should only grant access to the areas that are necessary for the IS auditor to perform the audit fieldwork, and not to any other areas that may contain confidential information, valuable equipment, or hazardous materials. The incorrect access could result in unauthorized disclosure, modification, or destruction of the assets, as well as potential safety or legal issues.
References

ISACA CISA Review Manual, 27th Edition, page 254
Office and Workplace Physical Security Assessment Checklist
Physical Security: Planning, Measures and Examples

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu　**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **557**
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. キー承認者のバックアップが特定されていません。
B. 財務管理システムはクラウドベースです。
C. 主要なレポートを生成する手順が承認されていません。
D. システム容量はテストされていません。
正解: **A** (コメントを発表する)

質問: **558**
新しいシステムにおいて、職務分掌違反を特定する最も効率的な方法は次のうちどれですか？
A. システム内のセキュリティ権限に関するレポートを確認します。
B. ビジネスプロセスのパフォーマンスを監視します。
C. 認可の競合を特定するプロセスを開発する。
D. 最近のシステムアクセス権限違反を調査します。
正解: **A** (コメントを発表する)
The most efficient way to identify segregation of duties violations in a new system is to review a report of security rights in the system. Segregation of duties is a control principle that aims to prevent or detect errors, fraud, or abuse by ensuring that no single individual has the ability to perform incompatible or conflicting functions or activities within a system or process. A report of security rights in the system can provide a comprehensive and accurate overview of the roles, responsibilities, and access levels assigned to different users or groups in the system, and can help to identify any potential segregation of duties violations or risks. The other options are not as efficient as reviewing a report of security rights in the system, because they either rely on observation or testing rather than analysis, or they focus on existing rather than potential violations. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.2

質問: **559**
ある組織が、人事アプリケーションをプライベートクラウド上のIaaS(Infrastructure as a Service)モデルに移行しようとしています。デプロイ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
正解: **(正解を表示します)**
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

質問: **560**
災害対応計画において、最も重要な考慮事項は次のうちどれですか？
A. IT資産保護
B. 十分なリソース容量
C. 収益損失
D. 人員の安全
正解: **D (コメントを発表する)**

質問: **561**

組織の情報システム管理が客観的にレビューされたことを統治機関に最も確実に保証できるのは、次のうちどれの結果でしょうか？
A. 行政監査。
B. 外部監査。
C. フォレンジック監査。
D. 内部監査。
正解: **(**正解を表示します**)**
The correct answer is B. External audit.
An external audit provides the strongest assurance of objectivity because it is performed by an independent party outside the organization. A governing body, such as the board or audit committee, relies on independent assurance to determine whether information system controls have been reviewed without management bias or internal influence. Option A is not the best answer because an administrative audit generally focuses on administrative procedures or operational compliance and does not necessarily provide independent assurance over IS controls. Option C is not the best answer because a forensic audit is usually performed to investigate suspected fraud, misconduct, or evidence-related matters. Option D is valuable, but internal audit is still part of the organization; therefore, an external audit generally provides stronger objective assurance to the governing body.
This maps to Information Systems Auditing Process , because ISACA's CISA Exam Content Outline includes IS audit standards, audit execution, evidence, reporting, and assurance activities under Domain 1. (ISACA) References: ISACA CISA Exam Content Outline, Domain 1; ISACA Interactive Glossary, "Audit," "Audit evidence," and assurance-related terms. (ISACA)

質問: **562**
ある組織は、バックアップドライブを外部の保管施設へ輸送するために、第三者と提携した。
ドライブを発送する前に、以下のうちどれが最も重要ですか？
A. 輸送中のドライブに付随する保管管理記録を作成する
B. データ保護がデータ分類ポリシーに準拠していることを確認する
C. 強力な保護基準でドライブを暗号化します
D. ドライブが改ざん防止機構に収められていることを確認する
正解: **(**正解を表示します**)**
Before sending backup drives to an offsite storage facility, the most important thing to do is to encrypt the drive with strong protection standards. This is because encryption ensures effective security where information cannot be intercepted and used to harm the organization or its customers. Encryption also protects the data from unauthorized access, modification, or deletion in case the drive is lost, stolen, or damaged during transit or storage. Encryption of backup drives is especially important for public safety organizations

that handle sensitive or personally identifiable information, such as medical records, criminal records, or emergency communications12.

質問: **563**
監査の結果、コンピュータシステムが発注依頼に連番の発注番号を割り当てていないことが判明しました。IS監査担当者は、経営陣がこの指摘事項を留保しているかどうかを確認するため、監査フォローアップを実施しています。次のうち、最も信頼性の高いフォローアップ手順はどれですか？
A. 連番を実装するための変更の撤回に関する文書を確認してください。
B. システムが連続した注文番号を生成するように構成およびテストされているかどうかを管理者に確認してください。
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. 経営陣から入手したシステム生成の購買発注書のサンプルを調査する
正解: **(**正解を表示します**)**
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

質問: **564**
災害による取引損失のリスクを最小限に抑えるには、次のうちどれが最適でしょうか？
A. トランザクションログのコピーを毎日オフサイトストレージに送信する
B. 耐火金庫に取引ログのコピーを保管する
C. トランザクションログのコピーを暗号化してローカルサーバーに保存します
D. トランザクションログのコピーに署名し、ローカルサーバーに保存します
正解: **(**正解を表示します**)**
Sending a copy of the transaction logs to offsite storage on a daily basis would minimize the risk of losing transactions as a result of a disaster. This is because offsite storage provides a backup of the data that can be recovered in case of a catastrophic event that destroys or damages the onsite data. Storing a copy of the transaction logs onsite in a fireproof vault (B) would not protect the data from other types of disasters, such as floods, earthquakes, or theft. Encrypting or signing (D) a copy of the transaction logs and storing them on a local server would not prevent the loss of data if the server is affected by the disaster. Encryption and digital signatures are security measures that protect the confidentiality and integrity of the data, but not the availability.

Reference: CISA - Certified Information Systems Auditor Study Guide1, Chapter 5: Protection of Information Assets, Section 5.2: Backup and Recovery Concepts, Page 353.

質問: **565**
アプリケーションシステムの導入後レビューを実施する際に、IS監査人の独立性を最も損なう可能性が高いのは、次のうちどれでしょうか？
A. IS監査担当者は、アプリケーションシステムのベストプラクティスに関するコンサルティングアドバイスを提供しました。
B. IS監査担当者はアプリケーションシステムプロジェクトチームの一員として参加しましたが、運用上の責任は負いませんでした。
C. IS監査担当者は、アプリケーションシステムの監査専用の組み込み監査モジュールを設計しました。
D. IS監査担当者は、アプリケーションシステムの開発中に特定のコントロールを実施しました。
正解: **(**正解を表示します**)**
The IS auditor's independence would be most likely impaired if they implemented a specific control during the development of an application system. This is because the IS auditor would be auditing their own work, which creates a self-review threat that could compromise their objectivity and impartiality. The IS auditor should avoid participating in any operational or management activities that could affect their ability to perform an unbiased audit. The other options do not pose a significant threat to the IS auditor's independence, as long as they follow the ethical standards and guidelines of the profession.

質問: **566**
IS監査担当者が、クラウドシステムを使用してデータベースをホスティングしている組織の運用データベース管理をレビューしています。監査担当者が重点的に調査すべき主な領域は次のうちどれでしょうか？
A. クラウドベンダーのセキュリティ認証
B. プロビジョニングコストの自動スケーリング
C. セキュリティ設定の構成
D. 大規模データ転送
正解: **(**正解を表示します**)**
Comprehensive and Detailed in-Depth Explanation:
The primary focus when reviewing operational database management in a cloud environment should be the security settings configuration. Cloud environments often have complex and customizable security configurations, and any misconfiguration can lead to data breaches or unauthorized access. Ensuring proper security settings helps maintain data confidentiality, integrity, and availability.

Cloud vendor security certifications (Option A) are important but do not directly address how security is configured. Auto-scaling of provisioning costs (Option B) relates to resource management rather than security. Large-scale data transfers (Option D) may be relevant, but security settings directly impact data protection.
ISACA CISA Reference: Domain 5 - Protection of Information Assets

質問: **567**
ITプロジェクトにおいて、期待される効果が得られないリスクを軽減する上で、主に責任を負う役割は次のうちどれですか？
A. プロジェクトスポンサー
B. 品質保証(QA)マネージャー
C. 最高リスク責任者(CRO)
D. プロジェクトマネージャー
正解: **(正解を表示します)**

質問: **568**
データ損失防止(DLP)ツールは、以下のものに対して最大限の保護を提供します。
A. 未知のマルウェアのインストール。
B. 組織のシステム上で実行されている悪意のあるプログラム。
C. 従業員による機密情報のデバイスへのダウンロード。
D. 破損したデータファイルを電子メールで外部の関係者に送信すること。
正解: **(正解を表示します)**
DLP (Data Loss Prevention) toolsare designed toprevent unauthorized access, transfer, or leakage of sensitive data, especially byinsider threatsorunauthorized downloads.
Preventing Unauthorized Downloads (Correct Answer - C)
DLP solutionsblock or log attemptsto transfer sensitive files.
Example:A DLP tool detects andblocks an employee from copying confidential data to a USB drive.
Preventing Malware Installation (Incorrect - A, B)
Antivirus and endpoint protection tools, not DLP, handle malware threats.
Preventing Corrupt Data Transmission (Incorrect - D)
DLP focuses ondata protection, not detecting corrupt files.
References:
ISACA CISA Review Manual
NIST 800-53 (Data Protection Controls)
CIS (Center for Internet Security) DLP Best Practices

質問: **569**
オンラインアプリケーションのセキュリティアーキテクチャを監査する際、IS監査担当者はまず以下の点を確認する必要があります。

A. ファイアウォール規格。
B. ファイアウォールの設定
C. ファイアウォールのファームウェアバージョン
D. ネットワーク内におけるファイアウォールの位置
正解**: D (**コメントを発表する**)**
The security architecture of an online application is a design that describes how various security components and controls are integrated and configured to protect the application from internal and external threats. When auditing the security architecture of an online application, an IS auditor should first review the location of the firewall within the network, as this determines how effectively the firewall can filter and monitor the traffic between different network segments and zones. The firewall standards, configuration, and firmware version are also important aspects to review, but they are secondary to the location of the firewall.

質問**: 570**
次の公開鍵インフラストラクチャ (PKI) 要素のうち、侵害された秘密鍵の対処方法について詳しく説明しているのはどれですか。
A. 認証実務規定
B. 証明書ポリシー
C. PKI開示声明
D. 証明書失効リスト
正解**: A (**コメントを発表する**)**
Comprehensive and Detailed Explanation:
A Certification Practice Statement (CPS) is a detailed document that describes the practices a Certificate Authority (CA) uses when issuing and managing digital certificates. It includes procedures for handling compromised private keys, revocation, renewal, and security controls.
Certificate policy (B): High-level rules governing certificate usage, but not operational details.
PKI disclosure statement (C): Provides users with general PKI-related information.
Certificate revocation list (D): A technical mechanism listing revoked certificates, but not the procedures for managing compromise.
ISACA Reference: CISA Review Manual 27th Edition, Domain 5, section on PKI components and certificate lifecycle management.

質問**: 571**
ワンタイムパスワードを使用する主な利点は何ですか？
A. 傍受されたパスワードは再利用できません
B. アプリケーションのセキュリティは自動化できます
C. ユーザーは複雑なパスワードを記憶する必要はありません

D. ユーザーはアカウントから締め出されることはありません
正解: **(**正解を表示します**)**
The primary benefit of using one-time passwords is that an intercepted password cannot be reused, as it is valid only for a single login session or transaction. One-time passwords enhance the security of authentication by preventing replay attacks or password guessing. The other options are not the primary benefits of using one-time passwords. Security for applications can be automated with or without one-time passwords. Users may still have to memorize complex passwords or use a device or software to generate one-time passwords. Users can still be locked out of an account if they enter an incorrect or expired one-time password. References: CISA Review Manual (Digital Version), Chapter 6, Section 6.1

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu 「**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **572**
サンプリング方法の選択に最も影響を与えるリスクの種類はどれですか？
A. 固有の
B. 残差
C. コントロール
D. 検出
正解: **(**正解を表示します**)**
The type of risk that would most influence the selection of a sampling methodology is detection risk (option D). This is because:
Detection risk is the risk that the auditor will not detect a material misstatement that exists in an assertion1. Detection risk depends on the effectiveness of the audit procedures and how well they are applied by the auditor1.
The selection of a sampling methodology is part of the design of audit procedures, which aims to reduce detection risk to an acceptable level1. The auditor should consider the following factors when selecting a sampling methodology23:
The objectives of the audit procedure and the related assertions.
The characteristics of the population from which the sample will be drawn, such as its size, homogeneity, and structure.
The sampling technique to be used, such as random, systematic, haphazard, or judgmental.
The sample size and the method of selecting sample items.

The evaluation of the sample results and the projection of errors to the population.
The auditor should also consider the advantages and disadvantages of different sampling methodologies, such as statistical and non-statistical sampling23. Statistical sampling is a sampling technique that uses random selection and probability theory to evaluate sample results. Non-statistical sampling is a sampling technique that does not use random selection or probability theory to evaluate sample results. Some of the advantages and disadvantages are as follows23:
Statistical sampling allows the auditor to measure and control sampling risk, which is the risk that the sample is not representative of the population. Statistical sampling also allows the auditor to quantify the precision and reliability of the sample results. However, statistical sampling requires more technical knowledge and skills, as well as more time and cost, than non-statistical sampling.
Non-statistical sampling relies on the auditor's professional judgment and experience to select and evaluate sample items. Non-statistical sampling is more flexible and less complex than statistical sampling. However, non-statistical sampling does not provide an objective basis for measuring and controlling sampling risk, nor does it allow the auditor to quantify the precision and reliability of the sample results.
Therefore, the type of risk that would most influence the selection of a sampling methodology is detection risk (option D), as it determines how effective and efficient the audit procedures should be in order to provide sufficient appropriate audit evidence.
References: 1: Audit Sampling - Overview, Purpose, Importance, and Types 2: Audit Sampling | Auditing and Attestation | CPA Exam FAR 3: Audit Sampling | ACCA Qualification | Students | ACCA Global

質問**: 573**
非構造化データのリスクを最小限に抑えるために、以下のうちどれを最初に行うべきですか？
A. 非構造化データのリポジトリを特定します。
B. 非構造化データを分析するためのツールを購入する。
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. 非構造化データに対するユーザーアクセス制御を実装します。
正解**: A (**コメントを発表する**)**
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

質問: **574**
ネットワークサービスのサービスレベル契約(SLA)を策定する上で、以下のうちどれが課題となるでしょうか？
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する。
B. 適切に測定可能なパフォーマンス指標を見つける
C. クライアントによってネットワークコンポーネントが変更されないようにする
D. ネットワークへの入り口の数を減らす
正解: **B** (コメントを発表する)
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

質問: **575**
IS監査担当者は、企業資源計画(ERR)システムにおいて3者一致が発生したことを検証する際に、次のうちどれを使用すべきでしょうか？
A. 銀行確認
B. 商品配送通知
C. 購入依頼書
D. 発注書
正解: (正解を表示します)
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 and Example4
What Is Three-Way Matching and Why Is It Important? | NetSuite1
Enterprise Resource Planning (ERP) - Definition, Types, Uses2

質問**: 576**
IS監査担当者は、リスク管理手法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レビューするよう依頼されました。監査担当者が最も懸念すべき事項は次のうちどれでしょうか？
A. ログフィードはバッチ処理で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施されていません。
C. ログデータは正規化されていません。
D. データ暗号化規格は考慮されていません。
正解**: (**正解を表示します**)**
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 and Monitoring Relation in Cybersecurity4 3: Log Aggregation: What It Is and How It Works | Datadog3 4: Data Flow Testing - GeeksforGeeks1

質問**: 577**
データベースが完全に破損した後、ある組織は最新のバックアップから顧客データを復旧しました。しかし、顧客データの不一致に関する苦情が多数寄せられるようになりました。

このような状況で、情報システム監査担当者が最も確認すべき事項は次のうちどれでしょうか？
A. サービスレベル契約(SLA)
B. 最大許容停電時間(MTO)
C. 復旧時間目標(RTO)
D. リカバリポイント目標(RPO)
正解: **(**正解を表示します**)**
The correct answer is D. Recovery point objective (RPO) because the issue is related to data loss or data inconsistency after recovery, not simply the time taken to restore the database. RPO defines the point in time to which data must be recoverable after an outage or disruption. In practical terms, it answers: "How much data can the business afford to lose?" ISACA's contingency planning guidance explains that RPO represents the point in time prior to disruption to which business data can be recovered using the most recent backup, and it is directly related to the amount of data loss the business can tolerate.
The organization restored from the most recent available backup, but customers are reporting discrepancies.
This suggests the backup/recovery strategy may not meet the organization's acceptable data-loss requirement.
For example, if the business can tolerate losing only 15 minutes of transactions but backups are taken every
24 hours, recovered customer data may be outdated or incomplete. That is an RPO failure.
Option A is not the best answer because an SLA defines agreed service expectations, but the immediate audit concern is whether the backup point met the required data recovery point. Option B is not the best answer because MTO, also commonly discussed as maximum tolerable downtime, relates to the maximum outage period the business can tolerate, not the point to which data must be restored. Option C is not the best answer because RTO focuses on how quickly a system must be restored, while this case is about the correctness and completeness of recovered data.
This question maps mainly to Information Systems Operations and Business Resilience, because ISACA's CISA Exam Content Outline includes Database Management, Data Backup, Storage, and Restoration, Business Continuity Plan, and Disaster Recovery Plans under Domain 4.
References: ISACA CISA Exam Content Outline, Domain 4; ISACA Journal, Information System Contingency Planning Guidance.

質問: **578**
コンピュータのパフォーマンスを分析する際に、次のうちどれが最も役立つでしょうか？
A. 設備利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報告
C. システムソフトウェアの調整によるリソース使用量の最適化
D. オフピーク時の利用状況と応答時間のレポート

正解: **A** (コメントを発表する)
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

質問: **579**
システム開発プロジェクトにおけるメリット実現プロセスを最も効果的に促進するのは、次のうちどれですか？
A. プロジェクトの指標は、プロジェクト開始前に選択されています。
B. プロジェクト予算には、プロジェクトの実行費用とソリューションに関連する費用が含まれます。
C. 事業上のメリットの推定値は、過去に完了した同様のプロジェクトによって裏付けられています。
D. 指標はプロジェクト実施直後に評価されます。
正解: (正解を表示します)
A benefits realization process is a systematic way of identifying, defining, planning, tracking and realizing the benefits from a project or program. Benefits are the measurable improvements that result from the delivery of project outputs and outcomes. Benefits realization management (BRM) is the practice of ensuring that benefits are derived from outputs and outcomes.
One of the best practices for BRM is to select metrics for the project before it begins. Metrics are the indicators that measure the performance and value of the project and its benefits. By selecting metrics in advance, the project team can align the project objectives with the expected benefits, establish a baseline for comparison, and monitor and evaluate

the progress and results of the project. Metrics also help to communicate the value of the project to stakeholders and justify the investment.
The other options are not as effective as selecting metrics before the project begins. Project budget is an important factor for BRM, but it does not enable the benefits realization process by itself. It only reflects the costs of executing the project and delivering the solution, not the benefits or value that are expected from them. Estimates of business benefits are useful for planning and forecasting, but they are not sufficient for BRM. They need to be validated by actual data and evidence from similar projects or other sources. Metrics are evaluated after the project has been implemented, but this is only one part of the benefits realization process. BRM requires continuous monitoring and evaluation throughout the project life cycle and beyond, to ensure that benefits are sustained and optimized.
References:
ISACA, CISA Review Manual, 27th Edition, 2019, p. 3261
PMI, Benefits Realization Management: A Practice Guide, 20192
APM, What is benefits management and project success?, 20213

質問**: 580**
組織のノートパソコン上のデータを保護するための最良の方法は次のうちどれですか？
A. 無効化されたUSBポート
B. フルディスク暗号化
C. 生体認証アクセス制御
D. 二段階認証
正解**: B (**コメントを発表する**)**
The best method to safeguard data on an organization's laptop computers is full disk encryption. Full disk encryption is a technique that encrypts all the data stored on a harddrive, including the operating system, applications, files, and folders. This means that if the laptop is lost, stolen, or accessed by an unauthorized person, they will not be able to read or modify any data without knowing the encryption key or password. Full disk encryption provides a strong level of protection for data at rest, as it prevents data leakage or exposure in case of physical theft or loss of the device.
References:
How to Protect theData on Your Laptop
6 Steps to Practice Strong Laptop Security

質問**: 581**
IS監査担当者は、経営陣に対し、新しいシステムを本番環境で使用する前にテストを実施することを推奨しています。経営陣がテスト計画を策定する際の最適なアプローチは、以下の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. 生産エンティティと顧客によってシミュレートされます。
正解: **D (**コメントを発表する**)**
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.

質問: **582**
セキュリティログに含まれるマシン識別情報が意図せず漏洩した場合に生じる可能性のあるデータプライバシーの懸念に対処するための最善の方法は、次のうちどれですか？
A. ログの使用は、収集された目的のみに限定する。
B. ホストマシンからオンラインストレージへのログファイルの転送を制限する
C. ビジネス上重要なサーバーからのみログを収集します。
D. ログ収集をセキュリティ活動が活発な期間のみに制限する。
正解: **(**正解を表示します**)**
Limiting the use of logs to only those purposes for which they were collected is the best way to address potential data privacy concerns associated with inadvertent disclosure of machine identifier information contained within security logs, because it minimizes the risk of unauthorized access, misuse, or leakage of personal data that may be embedded in the logs. Logs should be collected and processed in accordance with the data protection principles and regulations, such as theGeneral Data Protection Regulation (GDPR)
12. Restricting the transfer of log files from host machine to online storage, only collecting logs from servers classified as business critical, and limiting log collection toonly periods of increased security activity are not effective ways to address data privacy concerns, because they do not prevent or mitigate the potential disclosure of personal datain the logs. References: 1: CISA Review Manual (DigitalVersion), Chapter 5, Section 5.4.4 2: CISA Online Review Course, Module 5, Lesson 4

質問: **583**
キャパシティ管理ツールは主に以下のことを保証するために使用されます。
A. 利用可能な資源が効率的かつ効果的に使用されている。
B. コンピュータシステムはほとんどの場合、最大容量で使用されています
C. 多数のユーザーによる同時使用が有効になっています

D. 提案されたハードウェア調達は容量要件を満たしている
正解: **(**正解を表示します**)**
Capacity management tools are primarily used to ensure that available resources are used efficiently and effectively to meet the current and future demands of the business. Capacity management tools can help monitor, analyze and optimize the performance and utilization of IT resources such as CPU, memory, disk, network, etc. The other options are not the primary purpose of capacity management tools, although they may be related or derived from them. References:
ISACA, CISA Review Manual, 27th Edition,chapter 4, section 4.32
ISACA, COBIT 2019 Framework: Introduction and Methodology, section 3.2

質問: **584**
フォローアップ監査の優先順位付けにおける主要な基準として、以下のうちどれを用いるべきでしょうか？
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. 経営陣からの提言
D. 過去の監査結果に基づく残存リスク
正解: **(**正解を表示します**)**
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 managementare not valid criteria for prioritizingfollow-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

質問: **585**
IS環境において効果的な変更管理が確実に実施されるようにするには、次のうちどれが最も適切でしょうか？
A. アプリケーションへのアクセスに関するユーザー認証手順は確立されています。
B. ソフトウェアの受け入れテストのための、ユーザーが作成した詳細なテスト基準。
C. 開発チームによって適切なテストが実施されました。
D. 本番環境のソースプログラムおよびオブジェクトプログラムへのアクセスは厳密に管理されています。
正解: **D (**コメントを発表する**)**

Access to production source and object programs is the best way to ensure that effective change management is in place in an IS environment, as it prevents unauthorized or accidental changes to the production code that could affect the functionality, performance, or security of the system. Access to production source and object programs should be restricted to authorized personnel only, and any changes should follow a formal change management process that includes documentation, approval, testing, and review.
References
ISACA CISA Review Manual, 27th Edition, page 254
Change Management Best Practices for the Engineering and ...
Change Management - an overview | ScienceDirect Topics

質問: **586**
次の監査まで是正措置のテストを延期する最も適切な理由はどれですか？
A. 監査を実施し、スケジュールに同意した監査担当者が組織を退職しました。
B. 観察結果の相対的な重要性を考慮すると、経営陣の計画された行動は十分である。
C. 被監査企業の経営陣は、監査人が報告したすべての所見を受け入れました。
D. 監査環境は大きく変化しました。
正解: **D (**コメントを発表する**)**
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

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジン

を手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu 1605問、３０%ディスカウント、特別な割引コード: JPNshiken」

質問: **587**
情報システム監査担当者が、企業資源計画(ERP)システムにおいて職務分掌の不備を発見しました。この設定ミスが再発するのを防ぐための最善の方法は次のうちどれですか？
A. 定期的にアクセス権限を監視する
B. 標準ユーザーアクセスマトリックスを参照
C. ロールベースモデルを使用してユーザーアクセスを許可する
D. 職務分掌の矛盾を是正する
正解: **C** (コメントを発表する)
The best way to prevent the misconfiguration from recurring is to grant user access using a role-based model. A role-based access control (RBAC) model is an access control method that assigns permissions to end-users based on their role within the organization1. RBAC provides fine-grained control, offering a simple, manageable approach to access management that is less error-prone than individually assigning permissions1. RBAC also enforces the principle of least privilege, which means that users only have the minimum access required to perform their tasks2.
A role-based model can help prevent segregation of duties (SoD) issues in an ERP system by restricting user access to conflicting activities within the application. SoD is a central issue for enterprises to ensure compliance with laws and regulations, and to reduce the risk of fraud and unauthorized transactions3. SoD requires that no single individual or group of individuals should havecontrol over two or more parts of a process or an asset3. For example, a user who can create and approve purchase orders should not be able to process payments or modify vendor records.
By using a role-based model, user access provisioning is based on the needs ofa group (e.g., accountingdepartment) based on common responsibilities and needs1. This means each role has a given set of permissions, and individuals can be assigned to one or more roles. For example, you may designate a user as an accounts payable clerk, an accounts receivable clerk, or a financial manager, and limit access to specific resources or tasks. The user-role and role-permissions relationships make it easy to perform role assignment because individual users no longer have unique access rights, rather they have privileges that conform to the permissions assigned to their specific role or job function1.
The other options are not the best way to prevent the misconfiguration from recurring. Monitoring access rights on a regular basis (option A) is a detective control that can help identify SoD issues after they occur, but it does not prevent them from happening in the first place. Referencing a standard user-access matrix (option B) is a tool that can help document and analyze user access rights, but it does not ensure that the user access rights are configured correctly or consistently. Correcting the segregation of duties conflicts

(option D) is a corrective action that can resolve SoD issues once they are detected, but it does not prevent them from happening again.
References: 3: Implementing Segregation of Duties: A Practical Experience Based on Best Practices 1: What is Role-Based Access Control (RBAC)? Examples, Benefits, and More 2: What is Azure role-based access control (Azure RBAC)?

質問: **588**
以下の指標のうち、組織のプライバシー保護プログラムの有効性を最もよく示すものはどれですか？
A. プライバシー研修を修了した従業員の割合。
B. プライバシー侵害未遂件数。
C. プライバシー影響評価(PIA)の完了率。
D. 顧客からの情報削除依頼件数。
正解: **(正解を表示します)**
The correct answer is C. Percentage of privacy impact assessments (PIAs) completed.
A privacy impact assessment is a proactive privacy risk-management activity. ISACA defines a PIA as the overall process of identifying, analyzing, evaluating, consulting, communicating, and planning the treatment of potential privacy impacts related to processing personally identifiable information within the broader enterprise risk management framework. Therefore, the percentage of required PIAs completed is a strong indicator that the privacy program is being applied to systems, processes, and data-processing activities.
Option A is not the best answer because training completion measures participation or awareness, not whether privacy risks are being assessed and treated. Option B is not the best answer because attempted privacy breaches may reflect the threat environment rather than the effectiveness of the privacy program. Option D is not the best answer because deletion requests are data subject activity; they do not directly demonstrate whether the privacy program is effective.
This question maps mainly to Protection of Information Assets, because ISACA's CISA Exam Content Outline includes information asset security, privacy principles, data protection, and security monitoring under Domain 5.
References: ISACA CISA Exam Content Outline, Domain 5; ISACA Interactive Glossary, "Privacy impact assessment."

質問: **589**
情報システム監査人が組織のDevSecOpsアプローチを評価しています。脆弱性を特定するためのプロアクティブなアプローチとして最も適切なのは、次のうちどれですか？
A. 継続的インテグレーション/継続的デリバリー（CI/CD）プロセス内のオープンソースの依存関係チェック
B. 最新の開発フレームワークとライブラリの使用

C. アプリケーション導入後の脆弱性スキャン
D. 継続的インテグレーション/継続的デリバリー(CI)への自動化セキュリティテストツールの統合
/CD)プロセス
正解: **(**正解を表示します**)**

質問: **590**
データ復元プロセスの有効性を検証する最良の方法はどれですか？
A. バックアップメディアへの物理的アクセスに関する定期的なレビューの実施
B. 定期的な完全データ復元を実行します
C. ソフトウェアユーティリティを使用して新しいバックアップを検証する
D. データ復元ポリシーを毎年見直し、更新する
正解: **(**正解を表示します**)**
The best way to verify the effectiveness of a data restoration process is to perform periodic complete data restorations. This is the process of transferring backup data to the primary system or data center and verifying that the restored data is accurate, complete, and functional. By performing periodic complete data restorations, the auditee can test the reliability and validity of the backup data, the functionality and performance of the restoration tools and procedures, and the compatibility and integrity of the restored data with the primary system. This will also help identify and resolve any issues or errors that may occur during the restoration process, such as corrupted or missing files, incompatible formats, or configuration problems.
Performing periodic reviews of physical access to backup media (option A) is not the best way to verify the effectiveness of a data restoration process, as it only ensures the security and availability of the backup media, not the quality or usability of the backup data. Physical access reviews are important for preventing unauthorized access, theft, damage, or loss of backup media, but they do not test the actual restoration process or verify that the backup data can be successfully restored.
Validating offline backups using software utilities (option C) is also not the best way to verify the effectiveness of a data restoration process, as it only checks the integrity and consistency of the backup data, not the functionality or compatibility of the restored data. Software utilities can help detect and correct any errors or inconsistencies in the backup data, such as checksum errors, duplicate files, or incomplete backups, but they do not test the actual restoration process or verify that the restored data can work with the primary system.
Reviewing and updating data restoration policies annually (option D) is also not the best way to verify the effectiveness of a data restoration process, as it only ensures that the policies are current and relevant, not that they are implemented and followed. Data restoration policies are important for defining roles and responsibilities, objectives and scope, standards and procedures, and metrics and reporting for the restoration process,

but they do not test the actual restoration process or verify that it meets the expected outcomes.
Therefore, option B is the correct answer.
References:
Whatis backup and disaster recovery? | IBM
Backup and Recovery of Data: The Essential Guide | Veritas
Database Backup and Recovery Best Practices - ISACA

質問: **591**
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示す最良の指標は、次のうちどれですか？
A. 継続的で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インフラサーバー数の増加
D. 情報セキュリティインシデント件数の減少
正解: **(**正解を表示します**)**
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 and business strategy | CIO Robust Governance - KPMG Global

質問: **592**
組織の災害復旧計画プロセスの全体的な有効性を評価する際、IS監査人が検証すべき最も重要な事項は次のうちどれですか？
A. 管理部門は、ウォームサイトサービスに関して第三者と契約を締結します。
B. 経営陣は年次机上演習を計画する。
C. 経営陣は計画書を作成し、全従業員にコピーを配布する。
D. 経営陣は、計画を毎年または変更が生じた場合に見直し、更新します。
正解: **(**正解を表示します**)**
The overall effectiveness of an organization's disaster recovery planning process depends on how well the plan reflects the current and future needs and risks of the organization, and how well the plan is tested, communicated, and maintained. Among the four options

given, the most important one for the IS auditor to verify is that management reviews and updates the plan annually or as changes occur.
A disaster recovery plan is not a static document that can be created once and forgotten. It is a dynamic and evolving process that requires regular review and update to ensure that it remains relevant, accurate, and effective. A disaster recovery plan should be reviewed and updated at least annually, or whenever there are significant changes in the organization's structure, operations, environment, or regulations. These changes could affect the business impact analysis, risk assessment, recovery objectives, recovery strategies, roles and responsibilities, or resources of the disaster recovery plan. If the plan is not updated to reflect these changes, it could become obsolete, incomplete, or inconsistent, and fail to meet the organization's recovery needs or expectations.
The other three options are not as important as reviewing and updating the plan, although they may also contribute to the effectiveness of the disaster recovery planning process. Contracting with a third party for warm site services is a possible recovery strategy that involves using a partially equipped facility that can be quickly activated in case of a disaster. However, this strategy may not be suitable or sufficient for every organization or scenario, and it does not guarantee the success of the disaster recovery plan. Scheduling an annual tabletop exercise is a good practice that involves simulating a disaster scenario and testing the plan in a hypothetical setting. However, this exercisemay not be enough to evaluate the feasibility or readiness of the plan, and it should be complemented by other types of tests, such as walkthroughs, drills, or full-scale exercises. Documenting and distributing a copy of the plan to all personnel is an essential step that ensures that everyone involved in or affected by the plan is aware of their roles and responsibilities, and has access to the relevant information and instructions. However, this step alone does not ensure that the plan is understood or followed by all personnel, and it should be accompanied by proper training, education, and awareness programs.
Therefore, reviewing and updating the plan annually or as changes occur is the best answer.

質問: **593**
IS監査担当者は、ITマネージャーがコスト削減のために最近SaaS(Software as a Service)プロバイダーとの契約を変更したことを発見しました。新しい契約では、インシデントの解決に要する時間が増加しています。監査担当者が最も懸念すべき事項は次のうちどれでしょうか？
A. 業務プロセスへの影響は評価されていません。
B. 新しい契約はITセキュリティポリシーに準拠していません。
C. 対応するサービスレベル契約(SLA)は変更されていません。
D. 代替のコスト削減方法は検討されなかった。
正解: **(**正解を表示します**)**

The greatest concern is whether the increased incident resolution time will adversely affect the organization's business operations and whether that impact was properly assessed before the contract change. In ISACA terms, service arrangements should be aligned with business needs and service objectives. If a contract change weakens incident response commitments, the key audit concern is not simply the wording of the SLA, but whether management evaluated the resulting business impact. ISACA guidance notes that support agreements and SLAs should be aligned with internal service expectations and business requirements.
Option A is correct because incident resolution times directly affect availability, continuity, user support, and operational resilience. If the contract now permits slower restoration or resolution, the organization may be exposed to longer outages or degraded services. The central risk is whether management made that trade-off knowingly after analyzing the impact on critical business processes. This is the most important concern from an audit and governance perspective.
Option B is not the best answer because noncompliance with IT security policy could be serious, but the question specifically highlights a change in incident resolution time. Unless there is evidence of an actual policy violation, the more direct concern is operational impact on the business.
Option C is also not the greatest concern. In practice, if the contract terms changed, the SLA may need revision or alignment, but that is more of a documentation and governance symptom. The deeper issue is whether the revised service commitments are acceptable to the business. ISACA guidance stresses alignment of support agreements and SLAs with organizational needs.
Option D is the weakest answer because considering alternative cost-reduction methods is a management decision, not the primary audit concern. Auditors focus on risk and control implications, not whether management explored every possible commercial option.
Therefore, A is the best answer because the most significant issue is whether the organization evaluated the impact of slower incident resolution on business processes before accepting the lower-cost contract.
References (Official ISACA):
* ISACA, A Framework for SIEM Implementation - support agreements should be aligned with internal SLAs.
* ISACA, Top Risks and Rewards of Moving to the Cloud - auditors should review cloud provider SLAs and evaluate continuity implications.
* ISACA Journal, Is Business Continuity Management Still Relevant? - audit concern centers on business impact and risk acceptance.
* ISACA Journal, Understanding Software Metric Use - SLAs should use metrics that are monitored and measured.

質問: **594**
クラウド環境において、データ漏洩のリスクが最も高いのは次のうちどれですか？

A. データ保持ポリシーの欠如
B. 同一データベース内でのマルチテナント
C. ロールベースのアクセス権限がない
D. セキュリティ証明書の有効期限切れ
正解**: (**正解を表示します**)**
Multi-tenancy within the same database (B) presents the greatest risk of data leakage in the cloud environment, because it means that multiple customers share the same physical database and resources. This can lead to data isolation and security issues, such as unauthorized access, cross-tenant attacks, or data leakage due to misconfiguration or human error. To prevent data leakage in a multi-tenant database, cloud providers need to implement strict access control policies, encryption, isolation mechanisms, and auditing tools.
Lack of data retention policy (A) is not the greatest risk of data leakage in the cloud environment, because it mainly affects the availability and compliance of data, not its confidentiality or integrity. Data retention policy defines how long data should be stored and when it should be deleted or archived. Without a data retention policy, cloud customers may face legal or regulatory issues, storage costs, or performance degradation.
Lack of role-based access is not the greatest risk of data leakage in the cloud environment, because it can be mitigated by implementing proper authentication and authorization mechanisms. Role-based access control (RBAC) is a security model that assigns permissions and privileges to users based on their roles and responsibilities. Without RBAC, cloud customers may face unauthorized access, privilege escalation, or data misuse.
Expiration of security certificate (D) is not the greatest risk of data leakage in the cloud environment, because it can be easily detected and renewed. A security certificate is a digital document that verifies the identity and authenticity of a website or service. It also enables secure communication using encryption. If a security certificate expires, it may cause trust issues, warning messages, or connection errors, but not necessarily data leakage.
References:
7 Ways to Prevent Data Leaks in the Cloud | OTAVA
An analysis of data leakage and prevention techniques in cloud environment

質問**: 595**
ネットワークプリンタの廃棄プロセスをレビューする情報システム監査担当者にとって、以下のうちどれが最も懸念すべき事項でしょうか？
A. 廃棄に関する方針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去されたことを検証する証拠はありません。
C. 事業部門はプリンターを直接廃棄することが許可されています

D. 動作しないプリンターは、セキュリティ対策が施されていない場所に保管されています。
正解: **B** (コメントを発表する)
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

質問: **596**
ビジネス上重要なアプリケーションの監査の質を高める上で、次のうちどれが最も貢献しますか？
A. 監査を独立した外部監査人に委任する
B. アプリケーション所有者から報告された過去の調査結果を確認する
C. 開発チームが犯した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
正解: (正解を表示します)
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

質問: **597**
ソフトウェア開発ライフサイクルのどの段階で、セキュリティ対策を推奨してもらうために情報システム監査人に相談すべきでしょうか？
A. 設計と開発
B. 最終受入試験
C. ソフトウェアの実装
D. 要件定義
正解: (正解を表示します)

An IS auditor should be consulted during the requirements definition phase to recommend security controls.
This ensures that security considerations are integrated from the beginning of the software development life cycle, leading to more secure software design and implementation.
References
ISACA CISA Review Manual 27th Edition, Page 240-241 (SDLC Phases)

質問: **598**
小売企業の倉庫従業員が、在庫管理システムに破損または紛失した在庫品の調整を入力することで、在庫品の盗難を隠蔽することに成功した。小売環境において、このような不正行為を最も効果的に防止できる管理策はどれか？
A. トランザクション入力のための個別の承認
B. 調整取引の統計的サンプリング
C. 紛失した在庫品目の予定外監査
D. 在庫取引の有効性に関する編集チェック
正解: **(**正解を表示します**)**
Separate authorization for input of transactions. This control would have best prevented this type of fraud in a retail environment by ensuring that the warehouse employee who handles the inventory items does not have the authority to enter adjustments to the inventory system. This would create a segregation of duties that would reduce the risk of collusion and concealment of theft.
The other options are not as effective as option A in preventing this type of fraud. Option B, statistical sampling of adjustment transactions, is a detective control that may help identify fraudulent transactions after they have occurred, but it does not prevent them from happening in the first place. Option C, unscheduled audits of lost stock lines, is also a detective control that may reveal discrepancies between the physical and recorded inventory, but it does not address the root cause of the fraud. Option D, an edit check for the validity of the inventory transaction, is a preventive control that may help verify the accuracy and completeness of the transaction data, but it does not prevent unauthorized or fraudulent adjustments.
References:
ISACA, CISA Review Manual, 27th Edition, 2019
ISACA, CISA Review Questions, Answers and Explanations Database - 12 Month Subscription Different Types of Inventory Fraud and How to Prevent Them1
6 Ways to Prevent Inventory Fraud in Your Business2

質問: **599**
情報セキュリティプログラムにおいて資産分類が不可欠である主な理由は、次のうちどれですか？
A. 資産に対する適切なレベルの保護を確保するため
B. 資産保護対策が業界標準に準拠していることを確認するため

C. リスク軽減策が適切であることを確認するため
D. 情報セキュリティに十分なリソースが割り当てられるようにする。
正解: **(**正解を表示します**)**
The best answer is A. To ensure the appropriate level of protection to assets.
ISACA guidance explains that asset categorization indicates the level of concern that should be given to an asset, and that identifying and classifying critical assets is done to avoid adverse effects from theft, loss, compromise, or misuse. In other words, classification tells the organization how much protection a given asset requires.
Option B may be a by-product, but alignment to standards is not the primary reason.
Option C is broader than the specific purpose of classification. Option D may follow from classification, but classification is primarily about matching protection strength to asset importance and sensitivity.
References (Official ISACA):
ISACA Journal, IT Asset Valuation, Risk Assessment and Control Implementation Model
ISACA Journal, Effective Reporting to the BoD on Critical Assets

質問: **600**
データ損失防止(DLP)監査の計画段階において、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た。IS監査担当者は、関連するリスクとして次のうちどれを特定すべきか？
A. いつでもどこでもアクセスできるため、脆弱性が増大する
B. 利用者の意識向上トレーニングの必要性が高まっている
C. クラウドの利用がITの可用性に悪影響を与える
D. ITインフラストラクチャおよびアプリケーションに対するガバナンスと監督の欠如
正解: **(**正解を表示します**)**

質問: **601**
以下の生体認証アクセス制御のうち、偽陰性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
正解: **B (**コメントを発表する**)**
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

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu　**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **602**
リスクベースの監査計画における重要な領域を特定する最良の方法は、次のうちどれですか？
A. 同業他社とのベンチマーク結果を確認します。
B. 最近の監査報告書から未解決の問題を確認する。
C. 事業に関連する利害関係者にインタビューを行う。
D. CIO と共にリスク調査を実施する。
正解: **(**正解を表示します**)**
The best answer is C. Interview relevant stakeholders in the business.
ISACA guidance on risk-based audit planning emphasizes understanding the business context, identifying risk themes, and engaging stakeholders to determine what matters most. One ISACA example describes interviewing hundreds of leaders to identify risk themes for audit planning. Stakeholder interviews give the auditor a direct view of business objectives, current risks, process changes, emerging concerns, and management priorities across the enterprise.
Option A. Review peer benchmarking results can provide context, but benchmarking does not reveal the organization's own risk drivers.
Option B. Review open issues from recent audit reports is useful input, but it is backward-looking and incomplete by itself.
Option D. Conduct a risk survey with the CIO is too narrow because risk-based audit planning should reflect the broader business, not only the CIO's perspective.
Therefore, C is the correct answer because interviewing relevant business stakeholders is the best way to identify the key areas that should shape a risk-based audit plan.
References (Official ISACA):
ISACA Journal, Transforming the IT Audit Function-Taking the Digital Journey.

ISACA Journal, IS Audit Basics: Risk-based Audit Planning for Beginners.
ISACA Journal, Business Skills for the IT Audit and Assurance Professional.
ISACA, The Future of Cybersecurity Assessments Is Here - includes stakeholder interviews as part of risk assessment.

質問: **603**
IS監査担当者が新しいサーバーのインストールをレビューしています。IS監査担当者の主な目的は、
A. セキュリティパラメータは製造元の基準に従って設定されます。
B. 購入前に詳細な事業計画が正式に承認されました。
C. セキュリティパラメータは組織のポリシーに従って設定されます。
D. 調達プロジェクトには、少なくとも3つの異なるサプライヤーからの融資者が招待されました。
正解: **C (**コメントを発表する**)**
The primary objective of an IS auditor when reviewing the installation of a new server is to ensure that security parameters are set in accordance with the organization's policies. Security parameters are settingsor options that control the security level and behavior of the server, such as authentication methods, encryption algorithms, access rights, audit logs, firewall rules, or password policies7. The organization's policies are documents that define the security goals, requirements, standards, and guidelines for the organization's information systems. An IS auditor should verify that security parameters are set in accordance with the organization's policies to ensure that the new server complies with the organization's security expectations and regulations. The other options are less important or incorrect because:
A). Security parameters should not be set in accordance with the manufacturer's standards alone, as they may not reflect the organization's specific security needs and environment. The manufacturer's standards are general recommendations or best practices for configuring the server's security parameters based on common scenarios and threats. An IS auditor should compare the manufacturer's standards with the organization's policies and identify any gaps or conflicts that need to be resolved.
B). A detailed business case should have been formally approved prior to the purchase of a new server rather than during its installation. A business case is a document that justifies the need for a new server based on its expected benefits, costs, risks, and alternatives. A business case should be approved by senior management before initiating a project to acquire a new server.
D). The procurement project should have invited tenders from at least three different suppliers before purchasing a new server rather than during its installation. A tender is a formal offer or proposal to provide a product or service at a specified price and quality. Inviting tenders from multiple suppliers helps to ensure a fair and competitive procurement process that can result in the best value for money and quality for the organization.

References: Server Security - ISACA, [Information Security Policy - ISACA], [Server Hardening - ISACA] , [Business Case - ISACA], [Tender - ISACA] , [Procurement Management - ISACA]

質問: **604**
ITガバナンスフレームワークの利用の重要性を経営陣に強調する上で、IS監査担当者が最も適切な理由は次のうちどれですか？
A. フレームワークにより、競合他社に対するITベンチマークが可能になります
B. フレームワークは、さまざまな組織に合わせてカスタマイズおよび最適化できます。
C. フレームワークは、自己評価(CSA)を容易にするのに役立ちます
D. フレームワークは、組織がITリスクを理解し、管理するのに役立ちます。
正解: **B (**コメントを発表する**)**
The best reason for an IS auditor to emphasize to management the importance of using an IT governance framework is that frameworks can be tailored and optimized for different organizations. An IT governance framework is a set of principles, guidelines, and processes that help an organization align its IT strategy with its business goals, manage IT risks and performance, and deliver value from IT investments. An IT governance framework can be adapted and customized to suit the specific needs, context, and culture of each organization, taking into account factors such as size, industry, maturity, objectives, and stakeholders. An IT governance framework can also help an organization adopt best practices and standards from various sources, such as COBIT2, ITIL3, ISO/IEC 200004, and others.
The other options are not as good as option B, as they may not capture the full scope or benefits of using an IT governance framework. Frameworks enable IT benchmarks against competitors, but this is not the main purpose or advantage of using an IT governance framework. Frameworks help facilitate control self- assessments (CSAs), but this is only one aspect or tool of an IT governance framework. Frameworks help organizations understand and manage IT risk, but this is also only one outcome or objective of an IT governance framework.
References:
1: What is ITIL? Your guide to the IT Infrastructure Library | CIO
2: IT Governance Framework | Components | Framework | Terminology - EDUCBA
3: IT Governance: Definitions, Frameworks and Planning - ProjectManager
4: What Is IT Governance? - Definition from Techopedia
5: What is IT Governance? A formal way to align IT and business strategy | CIO
6: What Is IT Governance? - Definition from WhatIs.com
7: ISO/IEC 20000 Information Technology Service Management Systems Standard - ISO/IEC 20000 Portal
8: COBIT | Control Objectives for Information Technologies | ISACA

質問: **605**
複数の国に地域事務所を持つグローバル組織のデータ保持ポリシーを評価する際に、最も重要な考慮事項は次のうちどれですか？
A. この方針は、企業の方針および慣行と一致しています。
B. この方針は、世界的なベストプラクティスに沿っています。
C. この方針は、事業目標および目的に合致しています。
D. この方針は現地の法律および規制に準拠しています。
正解: **D** (コメントを発表する)
The data retention policy for a global organization with regional offices in multiple countries should align with local laws and regulations, as they may vary significantly from one country to another and may impose different requirements and penalties for non-compliance. The policy should also consider the corporate policies and practices, the global best practices, and the business goals and objectives, but these are secondary to the legal compliance. References: CISA Review Manual (Digital Version), Chapter 5: Protection of InformationAssets, Section 5.3: Data Classification and Protection

質問: **606**
大量のソフトウェア変更全体にわたって一貫性を最も効果的に実現できるのは、次のうちどれですか？
A. ソフトウェア展開のベストプラクティスに関する継続的な啓発キャンペーン
B. 継続的インテグレーションおよびデプロイメントパイプラインの使用
C. 開発およびリリース管理に関する改訂版ポリシーの公開
D. リリース済みコードの詳細な例外レポートに対する経営陣によるレビュー
正解: (正解を表示します)

質問: **607**
ユーザーアカウントポリシーをレビューする際に、IS監査担当者が最も懸念すべき事項は次のうちどれでしょうか？
A. 従業員の退職時にシステムへのアクセス権を取り消すポリシーはありません。
B. 継続的なセキュリティ意識向上トレーニングに関する方針は存在しません。
C. 従業員に秘密保持契約(NDA)への署名を義務付ける方針はありません。
D. 従業員が役割を変更した際に、以前のアクセス権限を取り消すポリシーはありません。
正解: **A** (コメントを発表する)
Failure torevoke access upon terminationposes the greatest security risk, as ex-employees could still access sensitive data or systems.
No Policy to Revoke Access (Correct Answer - A)
A terminated employee retaining access can lead todata breaches or insider threats.
Example:A former employee misuses active credentials to access financial systems.
Lack of Security Awareness Training (Incorrect - B)

Important but does not pose an immediate security risk like an active ex-employee account.
No NDAs (Incorrect - C)
Protects intellectual property but is not as critical as system access.
No Access Revocation for Role Changes (Incorrect - D)
Still a concern, but ex-employees with active access are ahigherrisk.
References:
ISACA CISA Review Manual
NIST 800-53 (Access Control)

質問: **608**
IS監査担当者が、総勘定元帳システムのデータ品質をレビューするよう依頼されました。以下のうち、監査担当者にとって最も有意義な結果をもたらすのはどれでしょうか？
A. 事業主との最大口座残高に関する話し合い
B. システム脆弱性評価
C. システム所有者および運用者へのインタビュー
D. ソースドキュメントに対する整合性チェック
正解: **(**正解を表示します**)**

質問: **609**
組織のIT機能の俊敏性を測定するのに最適な指標は次のうちどれですか？
A. ITスタッフ1人あたりの平均学習 研修時間数
B. 最新の基準とガイドラインに対するセキュリティ評価の頻度
C. 戦略的なIT目標を合意され承認されたイニシアチブに変換するまでの平均時間
D. 職務に必要な能力を満たすのに十分なIT関連スキルを持つスタッフの割合
正解: **(**正解を表示します**)**
The metric that would best measure the agility of an organization's IT function is average time to turn strategic IT objectives into an agreed upon and approved initiative. IT agility is the ability of an IT function to respond quickly and effectively to changing business needs and opportunities. By measuring how fast an IT function can translate strategic IT objectives into actionable initiatives, such as projects or programs, an organization can assess how well its IT function can align with and support its business strategy. Average number of learning and training hours per IT staff member, frequency of security assessments against the most recent standards and guidelines, and percentage of staff with sufficient IT-related skills for the competency required of their roles are metrics that may indicate other aspects of IT performance, such as capability development, security maturity, and skills gap analysis, but they do not directly measure IT agility. References:
ISACA Journal Article: Measuring IT Agility

質問: **610**

ソーシャルエンジニアリングによる被害を防ぐための最善の方法は、次のうちどれですか？
A. オンボーディングおよび年次セキュリティ意識向上プログラムを維持する。
B. ユーザーのワークステーションで最新バージョンのウイルス対策ソフトウェアが実行されていることを確認してください。
C. 職務記述書にセキュリティに関する責任事項を含め、署名入りの確認書を要求してください。
D. 厳格なメールセキュリティゲートウェイ制御を適用する
正解: **(**正解を表示します**)**
Maintaining an onboarding and annual security awareness program is the best way to prevent social engineering incidents because it can educate the users about the common techniques and tactics used by social engineers and how to avoid falling victim to them. Ensuring user workstations are running the most recent version of antivirus software, including security responsibilities in job descriptions and requiring signed acknowledgment, and enforcing strict email security gateway controls are all good security practices, but they do not directly address the human factor that is exploited by social engineering.
References:
ISACA, CISA Review Manual, 27th Edition, 2020, p. 3671
ISACA, CISA Review Questions, Answers and Explanations Database - 12 Month Subscription2

質問: **611**
データベース管理の評価中に、IS監査担当者は、データベース管理者(DBA)権限を持つ一部のアカウントに、ログイン失敗回数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。監査担当者にとって最適な対応策は次のうちどれですか？
A. ログイン失敗回数が過剰なアカウントを特定し、無効化を要求します。
B. ITマネージャーに管理者セキュリティパラメータの変更と調査結果の更新を依頼する
C. 発見事項を文書化し、不適切なセキュリティ設定の管理者アカウントを持つことのリスクを説明する
正解: **(**正解を表示します**)**
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

質問: **612**
組織のITプロセスの現状を、最先端のベストプラクティスと比較して測定する上で、最も適した方法はどれですか？
A. ITポリシー
B. 同業他社ベンチマーク
C. 制御フレームワーク
D. 成熟度モデル
正解: **(正解を表示します)**
The best answer is D. Maturity model.
ISACA states that maturity models are becoming the common language used by organizations to understand the current state of their COBIT implementations and to support gap analysis and road maps for improvement.
That is exactly what this question asks: measuring the current state of IT processes against leading practices.
Option A provides direction, but policies do not measure current state. Option B can provide comparison with peers, but benchmarking is not the primary mechanism for assessing process capability or maturity against good practice levels. Option C provides structure for controls, but a control framework alone does not inherently measure present maturity. A maturity model is the specific tool for assessing where the organization currently stands and how far it is from desired practice levels.
References (Official ISACA):
ISACA Journal, Building a Maturity Model for COBIT 2019 Based on CMMI.
ISACA Journal, A Holistic Approach to Controls, Risk and Maturity.
ISACA, Effective Capability and Maturity Assessment Using COBIT 2019.

質問: **613**
IS監査担当者は、複数の事業部門にサービスを提供するIT組織がすべてのイニシアチブに等しい優先順位を付けているため、プロジェクト資金の確保に遅延が生じるリスクがあることを発見しました。事業目標をサポートする形で、プロジェクトやサービスの需要と利用可能なリソースをマッチングさせるのに最も役立つのは次のうちどれでしょうか？
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
正解: **(正解を表示します)**
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 and Explanations Database - 12 Month Subscription

質問**: 614**
システムがRFIDを使用している場合、IS監査担当者が最も懸念すべき事項は次のうちどれですか？
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
正解**: (**正解を表示します**)**
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.

質問: **615**
IS監査担当者は、3か月後に廃止予定のレガシーアプリケーションが、現行ポリシーで定められたセキュリティ要件を満たしていないことを発見しました。この問題に対処するための最善の方法(または監査担当者が取るべき最善の方法)は何でしょうか？
A. 要件を満たすよう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. ポリシー違反についてITディレクターに報告してください。
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か月後に廃止されるため、何もする必要はありません。
正解: **C** (コメントを発表する)
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 and Explanations Database - 12 Month Subscription Cybersecurity Engineering for Legacy Systems: 6 Recommendations - SEI Blog How to Secure Your Company's Legacy Applications - iCorps

質問: **616**

開発者が本番環境への書き込み権限を必要とする小規模なITウェブ開発会社において、IS監査担当者が推奨する最善策は次のとおりである。
A. 本番環境への移行を実行するために別の担当者を雇用します。
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権限を削除します。
D. 開発チーム向けにユーザーアクセスレビューを実施する
正解: **(**正解を表示します**)**
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

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu 「**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **617**
ソースコードリポジトリは、以下の目的で設計されるべきである。
A. 既存のコードへの変更の組み込みを防止します。
B. 開発者が安全なソースコードにアクセスできないようにします。
C. 既存のコードに対して安全なバージョン管理とバックアップ機能を提供します。

D. 変更されたコードの自動的な組み込みと配布を提供します。
正解: **C (**コメントを発表する**)**
A source code repository is a system that stores and manages the source code of a software project. A source code repository should be designed to provide secure versioning and backup capabilities for existing code, as these are essential features for concurrent development, code quality, and disaster recovery. Versioning allows developers to track, compare, and revert changes to the code over time. Backup ensures that the code is safely stored and can be restored in case of data loss or corruption.
References
Source Code Repositories: What is a Source Code Repository?
Git Source Code Repository Design Considerations
Best practices for repositories - GitHub Docs

質問: **618**
仮想マシン上に暗号化されずに保存されているデータの機密性と完全性を保護するために、最も効果的な対策は次のうちどれですか？
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てください。
正解: **(**正解を表示します**)**
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.

質問: **619**
IS監査担当者が組織のIT戦略と計画を評価しています。次のうち、最も懸念されるのはどれでしょうか？
A. 明確なITセキュリティポリシーがありません。
B. 事業戦略会議の議事録は配布されません。
C. IT部門は事業戦略計画に関与していません。
D. IT戦略計画に関する文書化が不十分です。
正解: **(正解を表示します)**
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

質問: **620**
組織の業務上重要なサーバーハードウェアのオンサイト予防保守をレビューするIS監査担当者にとって、以下のうちどれが最も懸念事項となるでしょうか？
A. 予防保守費用が事業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。
正解: **(正解を表示します)**
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 MaintenanceAudit?

質問: **621**
法医学的データ収集および保存手順において、最も重要な項目は次のうちどれですか？
A. デバイスの物理的セキュリティを確保する
B. データ整合性の維持
C. 保管管理の連鎖を維持する
D. 使用するツールの決定
正解: **(**正解を表示します**)**
The most important thing to include in forensic data collection and preservation procedures is preserving data integrity. Data integrity is the property that ensures that data is accurate, complete, and consistent throughout its lifecycle. Preserving data integrity is essential for forensic data collection and preservation procedures because it ensures that the data can be used as valid and reliable evidence in legal proceedings or investigations. Preserving data integrity can be achieved by using methods such as hashing, checksums, digital signatures, write blockers, tamper-evident seals, or timestamps. The other options are not as important as preserving data integrity in forensic data collection and preservation procedures, as they do not affect the validity or reliability of the data. Assuring the physical security of devices is a security measure that protects devices from unauthorized access, theft, damage, or destruction, but it does not ensure that the data on the devices is accurate, complete, and consistent. Maintaining chain of custody is a documentation technique that records and tracks the handling and transfer of devices or data among different parties involved in forensic activities, but it does not ensure that the data on the devices is accurate, complete, and consistent. Determining tools to be used is a planning activity that selects and prepares the appropriate tools for forensic data collection and preservation procedures, but it does not ensure that the data collected and preserved by

the tools is accurate, complete, and consistent. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.4

質問: **622**
電子メールで送信される情報の機密性を保護するには、次のうちどれが適切でしょうか？
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
正解: **(正解を表示します)**
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]

質問: **623**
IS監査担当者が、組織が機密情報をデータベースレベルで暗号化していることを確認する必要がある場合、次のうちどれが最も確実な保証となるでしょうか？
A. ホストサーバーのドライブ設定を確認しています
B. 平文送信のネットワークトラフィックをチェックしています
C. 重要なフィールドのサンプルを検証しています
D. 組織の暗号化ポリシーを確認する
正解: **(正解を表示します)**
The best assurance is obtained by verifying a sample of critical fields. If the question is specifically about encryption at the database level, the auditor should test the actual data elements in the database that are expected to be encrypted. ISACA privacy and data-

protection guidance discusses encryption of sensitive data fields as a protection mechanism, which supports validating field-level protection directly.
Option C is correct because it provides direct evidence that sensitive database fields are actually encrypted.
This is stronger than reviewing policies or peripheral settings because it tests the implemented control itself.
Option A is incorrect because drive settings usually relate to disk or full-volume encryption on the host server, not necessarily to database-level encryption of specific sensitive fields.
Option B is incorrect because checking network traffic for clear text transmissions only helps verify encryption in transit, not whether the data is encrypted within the database.
Option D is incorrect because a policy only states intent or requirement. It does not prove the database is actually encrypting sensitive fields.
Therefore, C is the best answer because direct verification of sensitive fields provides the strongest assurance that encryption is implemented at the database level.
References (Official ISACA):
ISACA Journal, Practical Data Security and Privacy for GDPR and CCPA - discusses encryption of sensitive client data fields.
ISACA Journal, Privacy-Preserving Analytics and Secure Multiparty Computation - discusses encryption of sensitive data fields throughout the data life cycle.
ISACA, Cloud Data Sovereignty: Governance and Risk Implications of Cross-Border Cloud Storage - distinguishes encryption at rest and in transit, supporting why network checks alone are insufficient for database-level assurance.

質問**: 624**
アップグレードされた企業資源計画(ERP)システムの導入において、稼働開始の決定に関して最も重要な考慮事項は次のうちどれですか？
A. ロールバック戦略
B. テストケース
C. 導入後レビューの目的
D. ビジネスケース
正解**: (**正解を表示します**)**
The most important consideration for a go-live decision when implementing an upgraded enterprise resource planning (ERP) system is the business case. The business case is the document that defines and justifies the need, value, feasibility, and risks of the project. It also outlines the expected costs, benefits, outcomes, and impacts of the project. The business case provides the basis for measuring and evaluating the success of the project. Therefore, before deciding to go live with an upgraded ERP system, it is essential to review and validate the business case to ensure that it is still relevant, accurate, realistic, and achievable.
A rollback strategy, test cases, and post-implementation review objectives are not the most important considerations for a go-live decision when implementing an upgraded ERP

system. These are important elements of project planning, execution, and evaluation, but they are not sufficient to determine whether the project is worth pursuing or delivering. These elements should be aligned with and derived from the business case.

質問: **625**
次のうち、新たな脅威に対する最も効果的な保護策はどれですか？
A. 非武装地帯(DMZ)
B. ヒューリスティック侵入検知システム(IDS)
C. ウイルス対策ソフトウェアのリアルタイム更新
D. シグネチャベースの侵入検知システム(IDS)
正解: **B (**コメントを発表する**)**
A heuristic intrusion detection system (IDS) provides the most protection against emerging threats, as it uses behavioral analysis and anomaly detection to identify unknown or zero-day attacks. A heuristic IDS can adapt to changing patterns and learn from previous incidents, making it more effective than a signature-based IDS, which relies on predefined rules and signatures to detect known attacks. A demilitarized zone (DMZ) is a network segment that separates the internal network from the external network, and it can provide some protection against external threats, but not against internal or emerging threats. Real-time updating of antivirus software is important to protect against malware, but it may not be sufficient to prevent new or sophisticated attacks that exploit unknown vulnerabilities. References: CISA Review Manual (Digital Version) 1, page 452-453.

質問: **626**
組織にとってマルウェアに対する最善の防御策は次のどれですか?
A. 侵入防止システム (IPS)
B. 文書化されたセキュリティ手順
C. 侵入検知システム (IDS)
D. セキュリティ意識向上トレーニング
正解: **(**正解を表示します**)**

質問: **627**
次のうち、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しているのはどれですか？
A. インシデント解決時間の短縮
B. IT管理部門によるレビュー対象インシデント数の増加
C. ヘルプデスクへの電話件数の減少
D. 報告された重大インシデント数の増加
正解: **(**正解を表示します**)**

質問: **628**

事件発生時に法的手続きを最も円滑に進めるには、次のうちどれが最適でしょうか？
A. 電子情報開示を行う権利
B. 法律顧問からの助言
C. 保管管理の連鎖を維持する
D. 根本原因分析の結果
正解: **C** (コメントを発表する)
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:
CISAReview Manual (Digital Version)
CISA Questions, Answers and Explanations Database

質問: **629**
IS監査担当者が、一部の従業員がパブリッククラウドベースのAIツールを使用していることを発見しました。以下のうち、最も懸念されるのはどれですか？
A. データ信頼性
B. コスト超過
C. 著作権侵害
D. データ漏洩
正解: **D** (コメントを発表する)
The best answer is D.
ISACA guidance on shadow AI and emerging technology risk highlights data breaches, privacy risk, and data leakage as major concerns when employees use unapproved public AI tools. Public cloud AI use can expose sensitive data through prompts, uploads, or output handling, making data leakage the greatest immediate concern from an audit and control perspective.
Option A is a concern because AI outputs can be inaccurate, but poor reliability usually does not create the same immediate confidentiality exposure as leaking internal data. Option B is less severe. Option C can matter in some use cases, but the most significant enterprise risk identified in ISACA's public guidance is unauthorized disclosure of data.
References (Official ISACA):
* ISACA, From Shadow IT to Shadow AI: Navigating the New Frontier of Enterprise Risk.
* ISACA, Navigating the Hype and Risk of Emerging Technologies.
* ISACA, Collaboration and the New Triad of AI Governance.

質問: **630**

データセンターの物理的なセキュリティを評価する上で、最も効果的な方法はどれですか？
A. データセンターの見学ツアーを実施します。
B. データセンターのカメラ映像を確認する。
C. データセンターのアクセスログを確認してください。
D. データセンターの関係者にインタビューを行う。
正解: **(**正解を表示します**)**

質問: **631**
ソフトウェア製品のベータテストに参加することの最も重要な利点は次のうちどれですか？
A. 新しいテクノロジーを使った仕事を好む従業員を組織が維持する能力を高めます。
B. ベンダーのサポートとトレーニングを改善します。
C. セキュリティと機密性を強化します。
D. 組織が新製品とその機能に慣れることを可能にします。
正解: **(**正解を表示します**)**
Beta testing is the process of releasing a near-final version of a software product to a group of external users, known as beta testers, who provide feedback and report bugs based on their real-world experiences. Beta testingoffers various benefits for both the developers and the users of the software product. Some of these benefits are:
It reduces product failure risk via customer validation12.
It helps to test post-launch infrastructure1.
It helps to improve product quality via customer feedback12.
It allows for thorough bug detection and issue resolution3.
It enhances usability and user experience3.
It increases customer satisfaction and loyalty3.
Based on these benefits, the most important advantage of participating in beta testing of software products is D). It enables an organization to gain familiarity with new products and their functionality. By being involved in beta testing, an organization can learn how to use the new product effectively, discover its features and benefits, and provide suggestions for improvement. This can help the organization to adopt the new product faster, easier, and more efficiently when it is officially released. It can also give the organization a competitive edge over other users who are not familiar with the new product.

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジン

を手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu 1605問、３０%ディスカウント、特別な割引コード: JPNshiken」

質問: **632**
監査業務の準備段階で、監査目標を文書化する主な目的は何ですか？
A. 検討対象の活動に関連する全体的なリスクに対処するため
B. 材料問題が発生する可能性が比較的高い領域を特定する
C. 監査業務中に監査リソースを最大限に活用できるよう支援するため
D. 監査対象者との会議の優先順位付けとスケジュール設定を支援する
正解: **(**正解を表示します**)**
The primary purpose of documenting audit objectives when preparing for an engagement is to identify areas with relatively high probability of material problems. Audit objectives are statements that describe what the audit intends to accomplish or verify during the engagement. Audit objectives help the IS auditor to focus on the key areas of risk or concern, to design appropriate audit procedures and tests, and to evaluate audit evidence and results. By documenting audit objectives, the IS auditor can identify areas with relatively high probability of material problems that may affect the achievement of audit goals or business objectives.
Addressing the overall risk associated with the activity under review, ensuring maximum use of audit resources during the engagement and prioritizing and scheduling auditee meetings are also purposes of documenting audit objectives, but they are not as primary as identifying areas with high probability of material problems. References:
CISA Review Manual, 27th Edition, page 1111
CISA Review Questions, Answers and Explanations Database - 12 Month Subscription

質問: **633**
データベース内でデータ定義標準を適用することで、次のうちどれが最も効果的にサポートされますか？
A. データ破棄
B. データ保持
C. データフォーマット
D. データ機密性
正解: **(**正解を表示します**)**
Data definition standards within a database primarily support data formatting by establishing how data elements must be structured, represented, and stored. In practical terms, these standards define characteristics such as data type, field length, allowable values, precision, naming conventions, and valid formats. ISACA glossary material includes format checking as a control concept, which directly relates to verifying that data conforms to a prescribed format. That is the closest and strongest match to what data definition standards support.

Option C is correct because data definition standards are about consistency of data structure and representation. When an organization enforces common definitions for fields and attributes, it improves the consistency and usability of data across systems and applications. ISACA governance and data management material emphasizes that defining the format in which data are presented is part of giving data meaning and ensuring quality and usability.
Option A is incorrect because data disposal concerns end-of-life handling of data, such as destruction, archival expiration, and secure deletion. Those activities are governed by retention, records management, privacy, and disposal requirements, not by database data definition standards. ISACA privacy and data lifecycle guidance treats disposal as a separate lifecycle issue.
Option B is incorrect because data retention relates to how long data should be kept for business, legal, regulatory, or operational purposes. Retention policies may rely on data classification and legal obligations, but they are not what data definition standards primarily address.
Option D is incorrect because data confidentiality is mainly supported by access controls, encryption, classification, segregation of duties, and related security controls. Although well-defined data may indirectly help governance, confidentiality is not the main purpose of data definition standards.
Therefore, the best answer is C because enforcing data definition standards within a database most directly supports correct and consistent data formatting.
References (Official ISACA):
ISACA Glossary - Format checking.
ISACA, Unearthing and Enhancing Intelligence and Wisdom Within the COBIT 5 Governance of Information Model - discusses defining the format in which data are presented.
ISACA Journal, IS Audit Basics: Data Management Body of Knowledge-A Summary for Auditors - supports the role of data management standards and quality.
ISACA, SOC Reports for Cloud Security and Privacy - distinguishes use, retention, and disposal from data structure concerns.

質問**: 634**
情報システム監査人がITプロジェクトをレビューしたところ、プロジェクトの進捗報告の一環として、アーンドバリュー分析（EVA）が定期的に実施されていないことが判明しました。この状況から生じる最大のリスクは次のどれですか？
A. 時間と予算の超過がタイムリーに特定されない可能性があります。
B. リソースが適切なタイミングで割り当てられず、優先順位が付けられない可能性があります。
C. プロジェクトはプロジェクト管理標準に準拠していない可能性があります。
D. ビジネス要件が適切にベンチマークされていない可能性があります。

正解: (正解を表示します)

質問: **635**
文書管理システムのアクセス制御のレビューを実施するIS監査担当者にとって、次のうちどれが最も役立ちますか？
A. 部門長から提供された文書の管理に関する方針と手順
B. システムが生成した、スタッフとそのプロジェクト割り当て、役割、責任の一覧。
C. 他の部署による同一システムの使用に関する過去の監査報告書
D. 監査チームリーダーから提供された情報と、部門で使用されている認証システムに関する情報
正解: (正解を表示します)
The answer B is correct because a system-generated list of staff and their project assignments, roles, and responsibilities is the most useful to an IS auditor performing a review of access controls for a document management system. A document management system is a software that helps organizations store, manage, and share documents electronically. Access controls are the mechanisms that restrict or allow access to the documents based on predefined criteria, such as user identity, role, or project. An IS auditor needs to verify that the access controls are properly configured and implemented to ensure the security, confidentiality, and integrity of the documents.
A system-generated list of staff and their project assignments, roles, and responsibilities can help the IS auditor to perform the following tasks:
Identify the users who have access to the document management system and their level of access (e.g., read- only, edit, delete, etc.).
Compare the actual access rights of the users with their expected or authorized access rights based on their roles and responsibilities.
Detect any anomalies, discrepancies, or violations in the access rights of the users, such as excessive or unauthorized access, segregation of duties conflicts, or dormant or inactive accounts.
Evaluate the effectiveness and efficiency of the access control policies and procedures, such as user provisioning, deprovisioning, authentication, authorization, auditing, etc.
The other options are not as useful as option B. Policies and procedures for managing documents provided by department heads (option A) are not reliable sources of information for an IS auditor because they may not reflect the actual practices or compliance status of the document management system. Previous audit reports related to other departments' use of the same system (option C) are not relevant for an IS auditor because they may not address the specific issues or risks associatedwith the current department's use of the document management system. Information provided by the audit team lead on the authentication systems used by the department (option D) is not sufficient for an IS auditor because authentication is only one aspect of access control and it does not provide information on the authorization or auditing of the document access.
References:

Overview of document management in SharePoint
Setting Up a Document Control System: 6 Basic Steps
Access Control Management: Purpose, Types,Tools, and Benefits
9 Best Document Management Systems of 2023

質問: **636**
2人のユーザーが同時に同じデータベースレコードにアクセスした場合、以下のうちどれが最も大きなリスクとなりますか？
A. 可用性の完全性
B. データ整合性
C. エンティティの整合性
D. 参照整合性
正解: **(正解を表示します)**
The greatest risk if two users have concurrent access to the same database record is data integrity. Data integrity is the property that ensures that the data is accurate, complete, consistent, and valid throughout its lifecycle. If two users have concurrent access to the same database record, they may modify or delete the data in a conflicting or inconsistent manner, resulting in data corruption, loss, or duplication. This can affect the reliability and quality of the data, and cause errors or anomalies in the database operations and functions. The IS auditor should verify that the database has adequate controls to prevent or resolve concurrent access issues, such as locking mechanisms, transaction isolation levels, concurrency control protocols, or timestamping methods. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.7

質問: **637**
リスク管理の観点から、大規模かつ複雑なデータセンターITインフラストラクチャを導入する際に、次のうちどれが最適なアプローチでしょうか？
A. 概念実証に成功したビッグバン展開
B. 展開前に新しいインフラストラクチャをシミュレーションする
C. プロトタイピングと1段階展開
D. 段階的に構成された展開計画
正解: **(正解を表示します)**
From a risk management standpoint, the best approach for implementing a large and complex data center infrastructure is a deployment plan based on sequenced phases. ISACA guidance repeatedly supports phased implementation for complex, high-risk changes because it allows the organization to manage dependencies, reduce disruption, validate results incrementally, and maintain operational continuity while lessons from earlier phases can inform later ones.
Option D is correct because phased deployment reduces concentration of implementation risk. Instead of exposing the organization to a single large-scale failure point, phased

rollout allows testing, adjustment, monitoring, and controlled transition. ISACA material discussing complex implementations emphasizes structured, phased approaches to handle technical debt, compatibility issues, and continuity concerns.
Option A is incorrect because a big bang deployment concentrates risk, even if a proof of concept was successful. A proof of concept demonstrates feasibility in limited conditions, but it does not eliminate the operational risks of a full-scale one-time cutover in a complex environment. For large infrastructure changes, CISA logic generally prefers phased approaches over big bang implementations.
Option B is useful, but simulation alone is not the best answer. Simulation can support planning and testing, yet it does not by itself provide the controlled risk reduction that phased deployment offers during actual implementation. In CISA questions, the best risk-management choice is usually the one that combines control and gradual exposure reduction, which is phased rollout.
Option C is incorrect because "prototyping and a one-phase deployment" still culminates in a single-phase rollout, which is riskier than sequenced deployment. A prototype can improve design understanding, but it does not replace the value of incremental implementation in a complex production environment.
Therefore, D is the best answer because a sequenced, phased deployment is the most effective risk- management approach for large and complex infrastructure implementations.
References (Official ISACA):
ISACA, Passwordless Authentication: Risk, Reward, and Readiness - supports a carefully crafted phased implementation to manage complexity and maintain continuity.
ISACA Journal, Working Toward a White Box Approach - highlights the risks created by complexity in large IT initiatives.
ISACA Journal, Essential Frameworks and Methodologies to Maximize the Value of IT - supports structured project and program management sequencing.
ISACA Journal, A Strategic Risk-Based Approach to Systems Security Engineering - supports using a risk- based approach for complex systems change.

質問: **638**
組織のソフトウェア開発ライフサイクルにおける実践を能力成熟度モデルに照らし合わせてベンチマークすることの主な利点は、次のうちどれですか？
A. 再現可能なソフトウェア開発手順が確立されている。
B. 信頼できる製品を保証します。
C. プログラマーの効率が向上します。
D. ソフトウェア開発プロセスにセキュリティ要件が追加されます。
正解: **(**正解を表示します**)**

質問: **639**

データ分類スキームをレビューする際に、IS監査担当者が最も重要視するのは、以下の点です。
A. 各情報資産は、異なる分類に割り当てられます。
B. 各分類のセキュリティ基準が明確に文書化されています
C. 上級IT管理者は情報所有者として特定されます。
D. 情報所有者は資産へのアクセスを承認する必要があります
正解: **(**正解を表示します**)**
When reviewing a data classification scheme, it is most important for an IS auditor to determine if the security criteria are clearly documented for each classification. This will help the IS auditor to evaluate if the data classification scheme is consistent, comprehensive, and aligned with the organizational objectives and regulatory requirements. The security criteria should define the level of confidentiality, integrity, and availability for each data classification, aswell as the corresponding controls such as access control, rights management, and cryptographic protection1. The other options are less important or incorrect because:
A). Each information asset is not necessarily assigned to a different classification. Data classification schemesusually have a limited number of categories, such as "Sensitive," "Confidential," and "Public," and multiple information assets can belong to the same category2.
C). Senior IT managers are not necessarily identified as information owners. Information owners are typically the business units or functions that create, use, or maintain the information assets, and they may or may not be senior IT managers3.
D). The information owner is not required to approve access to the asset. The information owner is responsible for defining the access requirements and rules for the asset, but the actual approval of access requests may be delegated to other roles, such as data custodians or administrators3. References: Simplify and Contextualize Your Data Classification Efforts - ISACA, 3.7: Establish and Maintain a Data Classification Scheme, Data Classification and Practices - NIST, CISA Exam Content Outline |CISA Certification | ISACA

質問: **640**
IS監査担当者が監査業務中に発見された問題の是正において果たす主な役割は以下のとおりです。
A. ソリューションを提供することで、監査対象企業の経営陣を支援します。
B. 更新されたポリシーを経営陣に提示し、承認を得る。
C. 調査結果を説明し、一般的なアドバイスを提供する。
D. 問題の責任を負い、是正措置を監督する。
正解: **C (**コメントを発表する**)**

質問: **641**

セキュリティ監査において、情報システム監査担当者は、企業侵入防御システム(IPS)から取得したログエントリをレビューする任務を負います。監査担当者が、IPS構成のエラーを示す可能性のある一連のログイベントを見落とす可能性に関連するリスクの種類はどれでしょうか？
A. サンプリングリスク
B. 検出リスク
C. リスク管理
D. 固有のリスク
正解: **(**正解を表示します**)**
The type of risk associated with the potential for the auditor to miss a sequence of logged events that could indicate an error in the IPS configuration is detection risk. 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. Detection risk can be affected by factors such as the nature, timing, and extent of the audit procedures, the quality and sufficiency of the audit evidence, and the auditor's professional judgment and competence. Detection risk can be reduced by applying appropriate audit techniques, such as sampling, testing, observation, inquiry, and analysis. References:
CISA Review Manual (Digital Version)
CISA Questions, Answers and Explanations Database

質問: **642**
データバックアッププロセスをレビューする際に、最も重要な発見事項は次のうちどれでしょうか？
A. 復旧テストは実施されません。
B. テープはオフサイトで定期的にローテーションされていません。
C. データバックアッププロセスは文書化されていません。
D. データセーフの鍵はバックアップ管理者が保管しています。
正解: **A (**コメントを発表する**)**

質問: **643**
経営陣は、今後数年以内に組織のデータセンター付近で洪水が発生する可能性が高いという情報を受け取りました。その結果、データセンターの運用をより高い場所にある別の施設に移転することが決定されました。どのようなアプローチが採用されたのでしょうか？
A. リスク回避
B. リスク移転
C. リスク受容
D. リスク軽減
正解: **(**正解を表示します**)**
The approach adopted by management in this scenario is risk avoidance. Risk avoidance is the elimination of a risk by discontinuing or not undertaking an activity that poses a

threat to the organization3. By moving data center operations to another facility on higher ground, management is avoiding the potential flooding risk that could disrupt or damage the data center. Risk transfer, risk acceptance and risk reduction are other possible approaches for dealing with risks, but they do not apply in this case. References:
CISA Review Manual, 27th Edition, page 641
CISA Review Questions, Answers and Explanations Database - 12 Month Subscription

質問: **644**
以下の懸念事項のうち、本番環境のソースライブラリを保護することで最も適切に対処できるのはどれですか？
A. 本番環境の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. 生産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、本番環境のソースライブラリの誤ったバージョンに適用されています。
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。
正解: **D** (コメントを発表する)
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 and Explanations Database, Question ID 213

質問: **645**
情報セキュリティ監査の過程で、IS監査担当者は、組織の方針として、すべての従業員が毎年新年の最初の週に情報セキュリティ研修を受講しなければならないことを知りました。1月以降に採用された従業員がセキュリティ意識に関する適切な指導を受けられるようにするための、監査担当者の最善の推奨事項は何でしょうか？
A. 新規従業員が利用規約を読み、同意書に署名していることを確認してください。
B. 入社時のセキュリティ研修を含めるようにポリシーを改訂してください。
C. すべての従業員に対し、6か月ごとにセキュリティ研修を実施するよう方針を改訂する。
D. 新入社員の管理者にセキュリティ意識の概要説明を義務付ける。
正解: (正解を表示します)
This directly addresses the gap for new hires, creates a consistent expectation regardless of hiring date, and formalizes the process within organizational policy.

References
ISACA CISA Review Manual (Current Edition) - Chapters on Information Security Policies, Training and Awareness Industry Best Practices for Security Awareness - Emphasize the importance of timely and comprehensive training for new employees.

質問: **646**
従業員を対象に実施したフィッシングシミュレーションテストの有効性を監査する際、IS監査担当者が最も懸念すべき所見は次のうちどれでしょうか？
A. テストに不合格だった職員はフォローアップ教育を受けなかった。
B. 検査結果は職員に伝えられませんでした。
C. 職員には事前にテストについて通知されていませんでした。
D. 試験前にセキュリティ意識向上トレーニングは実施されませんでした。
正解: **(正解を表示します)**
The IS auditor should be most concerned about the lack of follow-up education for staff members who failed the phishing simulation test. Phishing simulation tests are designed to assess the level of awareness and susceptibility of staff members to phishing attacks, and to provide feedback and training to improve their security behavior. If staff members who failed the test do not receive follow-up education, they will not learn from their mistakes and may continue to fall victim to real phishing attacks, which could compromise the security of the organization.
The other options are less concerning for the IS auditor:
Test results were not communicated to staff members. This is not ideal, as staff members should receive feedback on their performance and learn from the test results. However, this does not necessarily mean that they did not receive any training or education on how to avoid phishing attacks.
Staff members were not notified about the test beforehand. This is a common practice for phishing simulation tests, as it mimics the real-world scenario where staff members do not know when they will receive a phishing email. The purpose of the test is to measure their spontaneous reaction and awareness, not their preparedness or compliance.
Security awareness training was not provided prior to the test. This is not a major concern, as the test can serve as a baseline measurement of the current level of awareness and susceptibility of staff members, and as a starting point for providing tailored training and education based on the test results.

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジン

を手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu 1605問、３０%ディスカウント、特別な割引コード: JPNshiken」

質問: **647**
事業部門がITリスク管理に異なる方法を使用している場合、組織全体のITリスク許容度を決定するための最適なアプローチは次のうちどれですか？
A. 事業部門のITリスクレベルを平均する
B. 事業部門の中で最も高いITリスクレベルを特定します
C. 組織のITリスクシナリオに優先順位を付ける
D. グローバルなITリスク評価基準を確立する
正解: **(**正解を表示します**)**
The best approach for determining the overall IT risk appetite of an organization when business units use different methods for managing IT risks is to prioritize the organization's IT risk scenarios. IT risk appetite is the amount and type of IT risk that an organization is willing to accept in pursuit of its objectives. IT risk scenarios are hypothetical situations that describe the potential impact of IT risk events on the organization's objectives, processes, and resources. By prioritizing the organization's IT risk scenarios, the IS auditor can identify the most significant IT risks that affect the organization as a whole, and align them with the organization's strategic goals, values, and culture. Prioritizing the organization's IT risk scenarios can also help to communicate and monitor the IT risk appetite across the organization, and facilitate consistent and informed decision making. The other approaches (A, B and D) are not effective for determining the overall IT risk appetite of an organization, as they do not consider the impact and likelihood of IT risks on the organization's objectives, nor do they account for the diversity and complexity of IT risks across different business units. References: CISA Review Manual (Digital Version), Chapter 2: Governance and Management of Information Technology, Section 2.3: Information Technology Risk Management

質問: **648**
ソフトウェア取得プロセスにIS監査担当者を関与させる主な理由は次のうちどれですか？
A. プロジェクト管理プロセスがポリシーと手順に準拠していることを確実にするため
B. 提案された契約およびサービスレベル契約(SLA)が主要な要素に対応していることを確認するため
C. ハードウェアとオペレーティングシステムの要件が考慮されるようにするため
D. 一般的な脅威やリスクに対処するための適切な管理策が検討されるようにするため
正解: **(**正解を表示します**)**

質問: **649**
アプリケーションプログラミングインターフェース(API)クエリによるデータ漏洩のリスクを軽減するために、以下の設計上の考慮事項のうち、最も重要なものはどれですか？

A. データ保持
B. データ最小化
C. データ品質
D. データ整合性
正解**: B (**コメントを発表する**)**
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

質問: **650**
データカンターの喉の評価をレビューするIS監査担当者が最も懸念するのは、次のような場合です。
A. 特定された脅威の中には、発生する可能性が低いものもあります。
B. 特定された脅威はすべて外部の組織に関連しています。
C. 演習は現地管理によって完了しました。
D. 近隣組織の活動も含まれています。
正解: **(**正解を表示します**)**
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

質問: **651**
小規模な社内ITチームが開発した新しい複雑なシステムの変更管理およびリリース管理の統制に関する監査を実施するIS監査担当者にとって、以下の観察事項のうちどれが最も懸念すべきでしょうか？
A. 変更テスト戦略と結果へのアクセスは、ITチーム以外のスタッフに限定されません。
B. ITチームのメンバーによって、一部のユーザー受け入れテスト(IJAT)が完了しました。
C. IT管理者は本番環境と開発環境にアクセスできます
D. すべてのシステムリリースに対して、実装後のテストは実施されません。
正解: **(**正解を表示します**)**
Post-implementation testing is the process of verifying and validating the functionality, performance, and security of a system after it has been deployed to the production environment1. Post-implementation testing is important for ensuring that the system meets the user requirements and expectations, as well as the operational and business objectives. Post-implementation testing also helps to identify and resolve any defects, errors, or issues that may have occurred during the deployment process or that may have been missed during the previous testing stages2.
Therefore, the observation that post-implementation testing is not conducted for all system releases should be of greatest concern to an IS auditor performing an audit of change and release management controls for a new complex system developed by a small in-house IT team. This observation indicates that the system may have quality, reliability, or security problems that could affect the user satisfaction, system performance, or data integrity. This observation also suggests that the change and release management controls are not adequate or effective, as they do not ensure that all system releases are properly tested and validated before and after deployment.
Option A is not correct because access to change testing strategy and results is not restricted to staff outside the IT team is not a major concern for an IS auditor. While it is good practice to limit access to sensitive or confidential information, such as test data or test cases, to authorized personnel only, access to change testing strategy and results may not pose a significant risk to the system or the organization. Moreover, access to change testing strategy and results may be beneficial for some stakeholders outside the IT team, such as business users, project managers, or auditors, who may need to review or evaluate the testing process or outcomes.
Option B is not correct because some user acceptance testing (UAT) was completed by members of the IT team is not a major concern for an IS auditor. User acceptance testing is the process of verifying and validating that the system meets the user requirements and expectations by involving actual or representative users in the testing process3. While it is preferable to have independent and unbiased users perform UAT, it may not be feasible or practical for some organizations, especially those with small or limited resources.

Therefore, some UAT may be completed by members of the IT team, as long as they have sufficient knowledge and experience of the user needs and expectations, and as long as they follow the UAT plan and criteria.
Option C is not correct because IT administrators have access to the production and development environment is not a major concern for an IS auditor. IT administrators are responsible for managing and maintaining the IT infrastructure, including the production and development environments4. Therefore, it is reasonable and necessary for them to have access to both environments, as long as they follow the appropriate policies and procedures for accessing, using, and securing them. Moreover, IT administrators may need to perform tasks such as backup, restore, patching, or troubleshooting in both environments.
References:
What Is Post Implementation Testing?1
Post Implementation Review (PIR) - Definition and Process2
User Acceptance Testing (UAT): Definition and Examples3
What Is an IT Administrator? Definition and Examples4

質問: **652**
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レビューするIS監査担当者にとって、以下のうちどれが最も懸念すべき事項でしょうか？
A. 指標は利害関係者のレビューなしに定義された。
B. パフォーマンスレポートには技術用語が多すぎる
C. 指標が業界ベンチマークと一致していません
D. 主要業績評価指標(KPI)はわずか1ヶ月で達成されました
正解: **D (**コメントを発表する**)**

質問: **653**
ビジネスデータベースのトランザクション記録が誤って削除されたため、システムオペレーターはスナップショットコピーから復元することにしました。以下のうち、BESTトランザクションが正常に復元されたことを保証するものはどれですか？
A. トランザクション回復ログを確認し、エラーが記録されていないことを確認してください。
B. トランザクション記録を再カウントして、記録の欠落がないことを確認します。
C. バックアップマシンでプロセスを再実行して、結果が同じであることを確認します。
D. 取引値を外部明細書と比較して正確性を検証します。
正解: **(**正解を表示します**)**
Recounting the transaction records to ensure no records are missing provides assurance that the best transactions were recovered successfully from a snapshot copy. This is because recounting the transaction records can verify that the number of records in the restored database matches the number of records in the snapshot copy, which represents

the state of the database before the deletion occurred. Recounting the transaction records can also detect any data corruption or inconsistency that may have occurred during the restore process1.
Reviewing transaction recovery logs to ensure no errors were recorded is not the best answer, because transaction recovery logs may not capture all the details or issues that may affect the data quality or integrity. Transaction recovery logs are mainly used to monitor and troubleshoot the restore process, but they may not reflect the actual content or accuracy of the restored data2.
Rerunning the process on a backup machine to verify the results are the same is not the best answer, because rerunning the process may introduce additional errors or inconsistencies that may affect the data quality or integrity. Rerunning theprocess may also consume more time and resources than necessary, and it may not guarantee that the results are identical to the original data3.
Comparing transaction values against external statements to verify accuracy is not the best answer, because external statements may not be available or reliable for all transactions. External statements are documents or reports that provide information about transactions from a third-party source, such as a bank, a vendor, or a customer. However, external statements may not cover all transactions, or they may have differentformats, standards, or timeliness than the internal data

質問: **654**
データベースセキュリティ監査で判明した以下の所見のうち、重大なセキュリティ侵害のリスクが最も高いのはどれですか？
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。
正解: **(正解を表示します)**
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

質問: **655**
あるグローバル企業が所在する国で、最近、個人データの国境を越えた移転を禁止する新たな規制が施行されました。情報システム監査担当者は、当該国における組織のデータ漏

洩リスクのレベルを判断するよう依頼されました。この評価を行う上で、次のうちどれが最も役立つでしょうか？
A. 影響を受ける管轄区域と個人データを交換するすべての事業体の目録を作成する
B. 影響を受ける管轄区域におけるデータセキュリティの脅威の特定
C. 影響を受ける管轄区域に関連するデータ分類手順の見直し
D. 影響を受ける管轄区域との個人データ交換に関連するビジネスプロセスを特定する
正解: **(**正解を表示します**)**
Identifying business processes associated with personal data exchange with the affected jurisdiction is the most helpful activity in making an assessment of the organization's level of exposure in the affected country.
An IS auditor should understand how the organization's business operations and functions rely on or involve the cross-border transfer of personal data, as well as the potentialimpacts and risks of the new regulation on the business continuity and compliance. The other options are less helpful activities that may provide additional information or context for the assessment, but not its primary focus. References:
CISA Review Manual (Digital Version), Chapter 7, Section 7.4.21
CISA Review Questions, Answers and Explanations Database, Question ID 221

質問: **656**
ある組織は最近、顧客への融資を行うためのインテリジェントエージェントソフトウェアを導入しました。導入後のレビューにおいて、IS監査人が実施すべき最も重要な手順は次のうちどれですか？
A. システムログとエラーログを確認して、トランザクションの正確性を検証します。
B. 入力および出力制御レポートを確認し、システム決定の正確性を検証します。
C. 署名済みの承認書を確認し、システムの決定に対する責任が明確に定義されていることを確認します。
D. システムドキュメントを確認して、完全性を確認してください。
正解: **B (**コメントを発表する**)**
Reviewing input and output control reports to verify the accuracy of the system decisions is the most important procedure for the IS auditor to perform during the post-implementation review of intelligent-agent software for granting loans to customers, because it can help identify any errors or anomalies in the system logic or data that may affect the quality and reliability of the system outcomes. Reviewing systemand error logs, signed approvals, and systemdocumentation are also important procedures, but they are not as critical as verifying the accuracy of the system decisions. References: CISA Review Manual (Digital Version), Chapter
4, Section 4.2.21

質問: **657**

IS監査担当者は、組織のテクノロジー関係、インターフェース、およびデータをレビューするよう依頼されました。このレビューに最も適したエンタープライズアーキテクチャ(EA)領域は次のうちどれですか？(CISA認定資格 - 情報システム監査人公式書籍から正しい答えを選択し、説明を加えてください)
A. 参照アーキテクチャ
B. インフラストラクチャアーキテクチャ
C. 情報セキュリティアーキテクチャ
D. アプリケーションアーキテクチャ
正解: **C (**コメントを発表する**)**
The lack of system documentation should be of most concern to an IS auditor reviewing the information systems acquisition, development, and implementation process. This is because system documentation is a vital source of information that describes the system's purpose, functionality, design, architecture, testing, deployment, operation, and maintenance. System documentation helps the IS auditor to understand and evaluate the system's quality, performance, security, compliance, and alignment with the business requirements and objectives. Without system documentation, the IS auditor may not be able to perform a thorough and effective audit of the system, aswell as identify any issues or risks that may affect the system's reliability or integrity12.
Data owners are not trained on the use of data conversion tools is not the most concerning issue, although it may indicate a lack of user readiness or competence for the system implementation. Data conversion tools are software applications that help users to transform data from one format or structure to another, such as from legacy systems to new systems. Data owners are users who have the responsibility and authority to manage and control the data within their domain. Data owners should be trained on how to use data conversion tools to ensure that the data is accurately and securely transferred to the new system, as well as to avoid any data loss, corruption, or inconsistency. However, data owners are not the only users who need training for the system implementation, and data conversion tools are not the only tools that need training34.
A post-implementation lessons-learned exercise was not conducted is not the most concerning issue, although it may indicate a lack of continuous improvement or learning culture for the system development and implementation process. A post-implementation lessons-learned exercise is a meeting or a session that takes place after the completion of a system implementation project, where the project team and stakeholders discuss and document the successes and failures of the project, as well as identify any best practices or areas for improvement for future projects. Apost-implementation lessons-learned exercise can help to enhance the project management skills, knowledge, and performance of the project team and stakeholders, as well as to avoid repeating the same mistakes or problems in future projects56.
System deployment is routinely performed by contractors is not the most concerning issue, although it may pose some challenges or risks for the system implementation process. System deployment is the final stage of the system development life cycle (SDLC), where

the system is installed and configured on the target environment and made available for use by end-users. System deployment can be performed by internal staff or external contractors, depending on the availability, expertise, and cost of resources. System deployment by contractors may offer some benefits such as faster delivery, lower cost, or higher quality than internal staff. However, system deployment by contractors mayalso introduce some risks such as loss of control, dependency, or security breaches over the system implementation process

質問: **658**
機密データが保存されていたフラッシュドライブの最適な廃棄方法は次のうちどれですか？
A. 破壊
B. 消磁
C. 暗号的消去
D. 上書き
正解: **(**正解を表示します**)**

質問: **659**
フォローアップ監査中に、IS監査担当者はいくつかの重要な推奨事項がIS監査担当者の最善の行動方針であることを発見しました。
A. 被監査者に対し、勧告事項に全面的に対応するよう求める。
B. 年次リスク評価をそれに応じて調整する。
C. 経営陣のリスク受容度を評価する。
D. 経営陣のリスク受容度に基づいて監査プログラムを更新する。
正解: **(**正解を表示します**)**
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 and Explanations Database

質問: **660**
ドキュメントをハッシュする目的は何ですか?
A. コンテンツの不正な開示を防ぐため
B. ファイルを内部使用のみに分類する

C. ファイルのサイズを圧縮する
D. ファイルの内容の整合性を検証する
正解: **(**正解を表示します**)**

質問: **661**
企業向け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際、成長するビジネス環境にとって最も重要な要件は次のうちどれですか？
A. バックアップと復元機能
B. スケーラブルなアーキテクチャとシステム
C. ネットワークスロットリング
D. サービスディスカバリ
正解: **(**正解を表示します**)**

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu 1**605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **662**
無人コンピュータ室における最も適切かつ効果的な消火方法はどれですか？
A. 散水器
B. 消火器
C. 二酸化炭素(CO2)
D. 乾燥したパイプ
正解: **(**正解を表示します**)**
The most appropriate and effective fire suppression method for an un-staffed computer room is carbon dioxide (CO2). Carbon dioxide is a gaseous clean agent that extinguishes fire by displacing oxygen and reducing the combustion process. Carbon dioxide is suitable for un-staffed computer rooms because it does not leave any residue, damage, or corrosion on the electronic equipment, and it does not require water or other chemicals that could harm the environment or human health. However, carbon dioxide can pose a risk of asphyxiation to any person who may enter the computer room during or after the discharge, so proper safety precautions and warning signs should be in place.
The other options are not as appropriate or effective as carbon dioxide for an un-staffed computer room:
Water sprinkler. This is a common fire suppression method that uses water to cool down and extinguish fire.

However, water sprinkler is not suitable for un-staffed computer rooms because it can cause severe damage to the electronic equipment, such as short circuits, corrosion, or data loss. Water sprinkler can also create a risk of electric shock to any person who may enter the computer room during or after the discharge.
Fire extinguishers. These are portable devices that contain a pressurized agent that can be sprayed on a fire to put it out. However, fire extinguishers are not effective for un-staffed computer rooms because they require manual operation by a trained person who can identify the type and location of the fire, and use the appropriate extinguisher. Fire extinguishers can also cause damage to the electronic equipment if they contain water or chemical agents.
Dry pipe. This is a type of sprinkler system that uses pressurized air or nitrogen in the pipes instead of water until a fire is detected. When a fire is detected, the air or nitrogen is released and water flows into the pipes and sprinklers. However, dry pipe is not ideal for un-staffed computer rooms because it still uses water as the extinguishing agent, which can damage the electronic equipment as mentioned above. Dry pipe also has a slower response time than wet pipe sprinkler systems, which can allow the fire to spread more quickly.

質問: **663**
導入前レビューの過程で、情報システム監査担当者は、いくつかのシナリオがテストされていないことに気づいた。
経営陣は、このプロジェクトは極めて重要であり、延期は不可能であると述べている。監査人が取るべき最善の行動は次のうちどれか？
A. 実装前に残りのシナリオテストを完了できるよう、管理部門を支援します。
B. 実装後、本番環境で残りのシナリオテストを実行します。
C. すべてのシナリオがテストされるまで、プロジェクトの実施を延期することを推奨します。
D. テストされたシナリオが最も重要なプロジェクトリスクを網羅しているかどうかを判断します。
正解: **(**正解を表示します**)**

質問: **664**
次のうち、融資実行プロセスにおけるデータ分析の活用例として適切なものはどれですか？
A. ローン記録がバッチファイルに含まれているか、またサービスシステムによって検証されているかを評価する。
B. 融資実行システムに入力された融資の母集団と、サービス管理システムに記録された融資を比較する
C. 2つのシステム間の照合が実行され、不一致が調査されているかどうかを検証する
D. 送信障害発生時に適切な担当者に通知するためのエラー処理制御の見直し

正解: **B** (コメントを発表する)
Data analytics can be used to compare data from different sources and identify any discrepancies or anomalies. In this case, comparing a population of loans input in the origination system to loans booked on the servicing system can help detect any errors or frauds in the loan origination process. The other options are not examples of data analytics, but rather controls for data integrity, reconciliation, and error handling.
References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3.2

質問: **665**
取引内容をレビューしている際に、情報システム監査担当者がリレーショナルデータベースに矛盾を発見しました。監査担当者にとって最適な推奨事項は次のうちどれでしょうか？
A. データ辞書を更新します。
B. 編集チェックを実装します。
C. データモデリングを実行します。
D. データ所有者向けのトレーニングを実施する。
正解: (正解を表示します)
Comprehensive and Detailed in-Depth Explanation:
Implementing edit checks ensures data validity and integrity by verifying inputs and reducing inconsistencies in the database.
Updating the data dictionary (Option A) does not resolve inconsistency issues. Data modeling (Option C) and training (Option D) are less relevant to addressing data accuracy directly.
ISACA CISA Reference: Domain 4 - Information Systems Operations, Maintenance, and Support

質問: **666**
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。このポリシーへの準拠を最も確実に保証できる指標は次のうちどれでしょうか？
A. 研修を修了した新規採用者の割合。
B. 企業セキュリティポリシーに違反した新規採用者の数。
C. 新規採用者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した新規採用者の割合
正解: (正解を表示します)
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

質問: **667**
組織のエンタープライズリスクマネジメント(ERM)プログラムに対する責任は誰が負うのか？
A. 取締役会
B. 経営幹部
C. 運営委員会
D. 最高リスク責任者(CRO)
正解: **(**正解を表示します**)**

質問: **668**
ネットワーク外部に設置されたセンサーシステムからのデータは、サーバーの開いているポートで受信されます。センサーシステムから収集されるデータの完全性を確保するための最良の方法は次のうちどれですか？
A. センサーシステム上でネットワークアドレス変換を実装します。
B. センサーデータを仮想プライベートネットワーク(VPN)経由でサーバーに送信します。
C. センサーシステムから送信されるデータをハッシュ化します。
D. センサーシステムからのトラフィックをプロキシサーバー経由でルーティングします。
正解: **C (**コメントを発表する**)**

質問: **669**
システムインターフェース全体でデータの整合性を確保する上で、次のうちどれが最も役立ちますか？
A. 環境分離
B. 和解
C. システムバックアップ
D. アクセス制御
正解: **(**正解を表示します**)**
The best way to ensure data integrity across system interfaces is to perform reconciliation. Reconciliation is the process of comparing and verifying the data from different sources or systems to ensure that they are consistent, accurate, and complete. Reconciliation can help to identify and resolve any discrepancies, errors, or anomalies in the data that could affect the quality, reliability, or validity of the information. Reconciliation can also help to detect and prevent any unauthorized or fraudulent data manipulation or modification. References:
CISA Review Manual (Digital Version)

質問: **670**
新規システム導入の過程で、各マイルストーンにおけるリスク管理をレビューするために情報システム監査担当者が任命されました。監査担当者は、プロジェクトのメリットに対するいくつかのリスクが未解決であることを発見しました。これらのリスク管理の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. 情報セキュリティ責任者
D. プロジェクトマネージャー
正解: **(正解を表示します)**
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 foroverseeing 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

質問: **671**
ある組織が、以前の中央集権型セキュリティ管理システムに代わる分散型セキュリティ管理システムを導入しました。以下のうち、最も大きな潜在的な懸念事項はどれでしょうか？
A. セキュリティ手順が変更をサポートするのに不十分な場合があります
B. 分散型セキュリティシステムは本質的に脆弱なセキュリティシステムである
C. 新システムのエンドユーザーによる受け入れは難しいかもしれない
D. 新しいシステムには追加のリソースが必要になります
正解: **(正解を表示します)**
A distributed security administration system is a system that allows different administrators to manage the security of different parts of the network or organization. This can provide more flexibility, scalability, and efficiency than a centralized system, where one

administrator is responsible for the entire security. However, a distributed security administration system also presents some potential challenges and risks, such as: Inconsistency and conflict among different security policies and standards Lack of coordination and communication among different administrators Difficulty in monitoring and auditing the overall security status and performance Increased complexity and cost of security management and maintenance Therefore, the greatest potential concern for implementing a distributed security administration system is that the security procedures may be inadequate to support the change. Security procedures are the rules and guidelines that define how security is implemented and enforced in an organization. They include policies, standards, processes, roles, responsibilities, controls, and metrics. Security procedures should be aligned with the business objectives, risks, and requirements of the organization, as well as the best practices and regulations in the industry. Security procedures should also be reviewed and updated regularly to reflect the changes in the environment, technology, and threats.
If the security procedures are not adequate to support the change from a centralized to a distributed security administration system, the organization may face increased security risks, such as unauthorized access, data breaches, compliance violations, reputation damage, and financial losses. Therefore, it is essential to ensure that the security procedures are revised and adapted to suit the new system, and that they are communicated and enforced effectively across the organization.
References:
1: Security in Distributed System - GeeksforGeeks
2: Distributed System Security Architecture - Wikipedia
3: Distributed Systems Security: Issues, Processes and Solutions

質問**: 672**
セキュリティ管理者は、深夜にオンコール中のプログラマーから電話を受けました。複数のプログラムが失敗しており、プログラマーは稼働中のシステムへのアクセスを求めています。最善の対応策は何でしょうか？
A. 変更要求が完了し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用の緊急IDを与え、アクティビティを確認する
C. プログラマーに問題調査のための読み取り専用アクセス権限を与える
D. 翌日にアクティビティログを確認し、不審なアクティビティを調査します。
正解**: B (**コメントを発表する**)**
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

質問**: 673**
高度にセキュリティが確保されたエリアへの訪問者のアクセスを制御する上で、最も効果的な方法はどれですか？
A. 訪問者は、許可された職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ています
D. 訪問者はデッドマンドアを通って入場する必要があります。

正解: **A** (コメントを発表する)
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

質問: **674**
以下のサンプリング方法のうち、1つのエラーが見つかった場合にサンプル全体が不規則であるとみなされるのはどれですか？
A. 発見サンプリング
B. 変数サンプリング
C. ストップ -オア -ゴー -サンプリング
D. 判断サンプリング
正解: **A** (コメントを発表する)
The sampling method in which the entire sample is considered to be irregular if a single error is found is discovery sampling. Discovery sampling is a type of statistical sampling that is used to test for the existence of at least one occurrence of a specific characteristic or condition in a population. Discovery sampling is often used when the auditor expects the characteristic or condition to be very rare or nonexistent, and when any occurrence would have a significant impact on the audit objective. For example, discovery sampling can be used to test for fraud, noncompliance, or material misstatement.
Discovery sampling works by setting a very low tolerable error rate (the maximum rate of occurrence of the characteristic or condition that the auditor is willing to accept) and a high confidence level (the degree of assurance that the auditor wants to obtain). The auditor then selects a sample from the population using a random or systematic method, and examines each item in the sample for the presence or absence of the characteristic or

condition. If no error is found in the sample, the auditor can conclude with a high level of confidence that the characteristic or condition does not exist or is very rare in the population. However, if one or more errors are found in the sample, the auditor cannot draw any conclusion about the population and must either expand the sample size or perform alternative procedures.
Discovery sampling differs from other sampling methods in that it does not allow for any errors in the sample.
Other sampling methods, such as variable sampling, stop-or-go sampling, or judgmental sampling, can tolerate some errors in the sample and use them to estimate the error rate or amount in the population.
However, discovery sampling is designed to test for zero-tolerance situations, where any error would be unacceptable or material. Therefore, discovery sampling considers the entire sample to be irregular if a single error is found.
References:
Audit Sampling - Overview, Purpose, Importance, and Types1
Audit Sampling - What Is It, Methods, Example, Advantage, Reason2
ISA 530: Audit sampling | ICAEW3
Audit Sampling - AICPA4

質問: **675**
IS監査担当者がネットワーク図を確認しています。ファイアウォールを設置するのに最適な場所は次のうちどれでしょうか？
A. セキュリティレベルの異なるネットワークセグメントの境界
B. 仮想ローカルエリアネットワーク (VLAN) 間
C. 非武装地帯(DMZ)内
D. 各ホストとローカルネットワークスイッチ/ハブの間
正解: **(**正解を表示します**)**

質問: **676**
組織の機密データがクラウドコンピューティング環境に保存され、暗号化されている場合、IS監査担当者にとって最も懸念すべき事項は次のうちどれでしょうか？
A. 暗号化キーは二重管理下にありません。
B. 暗号化には対称鍵が使用されます。
C. データ暗号化キーはサービスプロバイダがアクセスできます。
D. クラウドベンダーは複数地域に拠点を持っていません。
正解: **(**正解を表示します**)**

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu　**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **677**
IS監査担当者は、リスク管理手法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レビューするよう依頼されました。監査担当者が最も懸念すべき事項は次のうちどれでしょうか？
A. ログデータは正規化されていません。
B. ログフィードはバッチ処理でアップロードされます。
C. データ暗号化規格(DES)は考慮されていません。
D. ログデータに対して完全性テストは実施されていません。
正解: **(**正解を表示します**)**
The correct answer is D. Completeness testing has not been performed on the log data. For an event log aggregation system, the auditor must first be concerned with whether the log data is complete. If completeness testing has not been performed, the organization may not know whether all required logs are being collected, whether sources are missing, whether log feeds are interrupted, or whether critical events are excluded. Incomplete log data weakens monitoring, investigation, incident response, and risk management.
Option A is a concern because non-normalized logs can make correlation and analysis more difficult.
However, incomplete logs are a more fundamental problem because missing data cannot be analyzed at all.
Option B may be acceptable if batch uploads meet monitoring and investigation requirements. Option C is not the best answer because DES is an outdated encryption standard, but the question is mainly about whether the aggregated log data is complete and reliable for risk management.
This maps to Information Systems Operations and Business Resilience because ISACA's CISA Exam Content Outline includes operational log management, incident/problem management, and IT operations under Domain 4.
References: ISACA CISA Exam Content Outline, Domain 4; ISACA Interactive Glossary, audit evidence and control concepts.

質問: **678**
IT運営委員会の主な役割は次のうちどれですか？
A. 定期的なIT監査の承認
B. ビジネス部門とIT部門間の連携を促進する

C. 事業部門がIT目標を確実にサポートしていることを確認する
D. ITパフォーマンスについて事業部門に定期的に報告する
正解: **B** (コメントを発表する)

有効的な**CISA-JPN**問題集はJPNTest.com提供され、**CISA-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISA-JPN**試験問題集を提供します。JPNTest.com CISA-JPN試験問題集はもう更新されました。ここで**CISA-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISA-JPN-mondaishu 「**1605**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」