ISACA.CISM-JPN.v2026-09-04.q555

試験コード：	CISM-JPN
試験名称：	Certified Information Security Manager (CISM日本語版)
認証ベンダー：	ISACA
無料問題の数：	555
バージョン：	v2026-09-04
ページの閲覧量：	105
問題集の閲覧量：	5578

https://www.jpnshiken.com/shiken/ISACA.CISM-JPN.v2026-09-04.q555.html

質問: **1**
情報セキュリティ戦略目標の成功裡の実施に最も大きな影響を与える要因は次のうちどれですか？
A. 規制要件
B. コンプライアンスの承認
C. 経営支援
D. 予算承認
正解: **(正解を表示します)**
Management support is the factor that has the greatest influence on the successful implementation of information security strategy goals. Management support refers to the commitment and involvement of senior executives and other key stakeholders in defining, approving, funding, and overseeing the information security strategy. Management support is essential for aligning the information security strategy with the business objectives, ensuring adequate resources and budget, fostering a security-aware culture, and enforcing accountability and compliance. According to ISACA, management support is one of the critical success factors for information security governance1. The other options are not factors that influence the successful implementation of information security strategy goals, but rather outcomes or components of the information security strategy. Regulatory requirements are external obligations that the information security strategy must comply with2. Compliance acceptance is the degree to which the organization adheres to the information security policies and standards3. Budgetary approval is the process of allocating financial resources for the information security activities and initiatives4. References: 2: Information Security: Goals, Types and Applications - Exabeam 3: How to develop a cybersecurity strategy: Step-by-step guide 4: Information Security Goals And Objectives 1: The Importance of Building an Information Security Strategic Plan

質問: **2**
多国籍企業は、各事業拠点ごとに異なるセキュリティ要件を定めた政府規制を遵守する必要があります。最高情報セキュリティ責任者(CISO)が最も懸念すべき事項は次のうちどれでしょうか？

A. グローバルおよび地域的な要件を満たすセキュリティプログラムを開発する。
B. 地方規制機関との効果的なコミュニケーションを確保する。
C. 業界のベストプラクティスを活用して、現地の法的規制要件を満たします。
D. 定義されたセキュリティポリシーと標準への準拠を監視する。
正解: **A** (コメントを発表する)
= A multinational organization is required to follow governmental regulations with different security requirements at each of its operating locations. This means that the CISO has to deal with multiple and diverse legal, regulatory, and compliance issues across different jurisdictions and markets. The CISO should be most concerned with developing a security program that meets global and regional requirements, such as ISO/IEC 27001, NIST CSF, PCI DSS, GDPR, etc. These standards provide a framework for establishing, implementing, maintaining, and improving an information security management system (ISMS) that aligns with the organization's business objectives and risk appetite. The CISO should also ensure that the security program is consistent and coherent across all operating locations, and that it complies with the specific regulations of each location. Therefore, option A is the most appropriate answer. References = CISM Review Manual 15th Edition, page 255; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 234.
In this scenario, the chief information security officer (CISO) should be most concerned with developing a security program that meets the global and regional requirements of the organization. This includes considering the different legal and regulatory requirements of each operating location, and designing a security program that meets all of these requirements. The CISO should also ensure effective communication with local regulatory bodies to ensure compliance and understanding of the security program. Additionally, the CISO should use industry best practices and defined security policies and standards to ensure the program meets all applicable requirements.

質問: **3**
ソフトウェアプロジェクトのシステム開発ライフサイクル(SDLC)の開始段階では、情報セキュリティ活動において以下の点に取り組む必要があります。
A. 基本セキュリティ制御。
B. セキュリティ指標のベンチマーク。
C. セキュリティ目標。
D. 費用便益分析。
正解: (正解を表示します)
During the initiation phase of the system development life cycle (SDLC) for a software project, information security activities should address security objectives, which are derived from the business objectives and the risk assessment. Security objectives define the desired level of protection for the system and its data, and guide the selection of security controls in later phases. Baseline security controls are predefined sets of security

requirements that apply to common types of systems or environments. Benchmarking security metrics is a process of comparing the performance of security processes or controls against a standard or best practice. Cost-benefit analyses are used to evaluate the feasibility and effectiveness of security controls, and are usually performed in the acquisition/development phase or the implementation phase of the SDLC. References = CISM Review Manual, 16th Edition, page 1021; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 772 Learn more:
1. isaca.org2. amazon.com3. gov.uk

質問**: 4**
情報資産分類の最大のメリットは次のうちどれですか？
A. リカバリポイント目標(RPO)の決定を支援する
B. 必要情報開示方針を実施するための基礎を提供する
C. 職務分担の支持
D. 資源所有権の定義
正解**: (**正解を表示します**)**
The greatest benefit of information asset classification is providing a basis for implementing a need-to-know policy. Information asset classification is a process of categorizing information based on its level of sensitivity and importance, and applying appropriate security controls based on the level of risk associated with that information1. A need-to-know policy is a principle that states that access to information should be granted only to those individuals who require it to perform their official duties or tasks2. The purpose of a need-to-know policy is to limit the exposure of sensitive information to unauthorized or unnecessary parties, and to reduce the risk of data breaches, leaks, or misuse. Information asset classification provides a basis for implementing a need-to-know policy by:
*Defining the value and protection requirements of different types of information
*Labeling the information with the appropriate classification level, such as public, internal, confidential, secret, or top secret
*Establishing the roles and responsibilities of information owners, custodians, and users
*Enforcing access controls and encryption for the information
*Documenting the security policies and procedures for the information
By providing a basis for implementing a need-to-know policy, information asset classification can help organizations to protect their sensitive information, comply with rele-vant laws and regulations, and achieve their business objectives. The other options are not the greatest benefits of information asset classification.
Helping to determine the recovery point objective (RPO) is not a benefit, but rather a consequence of applying security controls based on the classification level. RPO is the acceptable amount of data loss in case of a disruption3. Supporting segregation of duties is not a benefit, but rather a prerequisite for implementing a need-to-know policy. Segregation of duties is a principle that states that no single individual should have control

over two or more phases of a business process or transaction that are susceptible to errors or fraud4.
De-fining resource ownership is not a benefit, but rather a component of information asset classification.
Resource ownership is the assignment of accountability and authority for an information asset to an individual or a group5. References: 1: Information Classifi-cation - Advisera 2: Need-to-Know Principle - NIST 3:
Recovery Point Objective - NIST 4: Segregation of Duties - NIST 5: Resource Ownership - NIST :
Information Classification in Information Security - GeeksforGeeks : Information Asset Classification Policy
- UCI

質問**: 5**
次のうち、外部脅威環境の変化の例はどれですか？
A. 業界のセキュリティ基準が変更されました。
B. 一般的に使用されている暗号化アルゴリズムが侵害されました。
C. 情報セキュリティプログラムは外部委託されました。
D. その組織は別の組織に買収されました。
正解**: D (**コメントを発表する**)**

質問**: 6**
ある組織が、災害復旧活動の実行を外部委託することを計画しています。外部委託契約に含めるべき最も重要な項目は次のうちどれでしょうか？
A. 災害宣言の基準
B. バックアップを定期的にテストするための要件
C. 復旧時間目標(RTO)
D. 災害復旧コミュニケーション計画
正解**: (**正解を表示します**)**
The most important thing to include in the outsourcing agreement for disaster recovery activities is the recovery time objectives (RTOs). RTOs are the maximum acceptable time frames within which the critical business processes and information systems must be restored after a disaster or disruption. RTOs are based on the business impact analysis (BIA) and the risk assessment, and they reflect the business continuity requirements and expectations of the organization. By including the RTOs in the outsourcing agreement, the organization can ensure that the service provider is aware of and committed to meeting the agreed service levels and minimizing the downtime and losses in the event of a disaster.
The other options are not as important as the RTOs, although they may be relevant and useful to include in the outsourcing agreement depending on the scope and nature of the disaster recovery services. References = CISM Review Manual 15th Edition, page 2471;

CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 1033

質問: **7**
フォレンジック調査を実施する前に、情報セキュリティ管理者は以下のことを行う必要があります。
A. クリーンなシステムで元のハードディスクを起動します。
B. 新しいメディア上に元のデータのイメージを作成する。
C. バックアップメディアからデータを複製します。
D. サーバーをシャットダウンして移設します。
正解: **(**正解を表示します**)**
= A forensic examination is a process of collecting, preserving, analyzing, and presenting digital evidence in a manner that is legally acceptable. The first step in conducting a forensic examination is to create an image of the original data on new media, such as a hard disk, a CD-ROM, or a USB drive. This is done to ensure that the original data is not altered, damaged, or destroyed during the examination. An image is an exact copy of the data, including the file system, the slack space, and the deleted files. Creating an image also allows the examiner to work on a duplicate of the data, rather than the original, which may be needed as evidence in court. Booting the original hard disk on a clean system is not a good practice, as it may change the data on the disk, such as the timestamps, the registry entries, and the log files. Duplicating data from the backup media is not sufficient, as the backup media may not contain all the data that is relevant to the investigation, such as the deleted files, the temporary files, and the swap files. Shutting down and relocating the server is not advisable, as it may cause data loss, corruption, or tampering. The server should be kept running and isolated from the network until an image is created.
References = CISM Review Manual 15th Edition, page 204-205.
Prior to conducting a forensic examination, an information security manager should create an image of the original data on new media. This is done in order to preserve the evidence, as making changes to the original data could potentially alter or destroy the evidence. Creating an image of the data also helps to ensure that the data remains intact and free from any interference or tampering.

質問: **8**
情報セキュリティプログラムの主な役割は何ですか？
A. 定期的なリスク評価および事業影響分析(BIA)を実施する
B. 組織のセキュリティリスク管理に関するガイダンスを提供する
C. 事業に関連する情報セキュリティ要件を承認する
D. 情報セキュリティ要件に関して関係者を教育する。
正解: **(**正解を表示します**)**

The primary role of the information security program is to provide guidance in managing organizational security risk (B). In CISM, the security program translates governance direction, policies, and risk appetite into coordinated activities, controls, and practices that enable the organization to manage risk consistently and effectively. Performing risk assessments and BIAs (A) are important activities but are not the program's primary purpose. Approving security requirements (C) is typically a management or governance responsibility, while education and awareness (D) are supporting components of the program. CISM emphasizes that the security program acts as the mechanism for operationalizing risk management, ensuring alignment with business objectives and continuous improvement of the security posture.
References: ISACA CISM Review Manual (Program development and management-program purpose and scope); CISM Exam Content Outline (Domain 3).

質問: **9**
事業継続計画(BCP)を策定する際の最初のステップはどれですか？
A. 最短の復旧時間目標(RTO)を持つアプリケーションを特定します。
B. 事業復旧戦略を決定する
C. 利用可能な資源を特定する。
D. 重要なビジネスプロセスを特定する。
正解: **(正解を表示します)**

質問: **10**
組織全体の新しい情報セキュリティプログラムへの支持を得るための最良の方法は、次のうちどれですか？
A. 類似の業界団体とのベンチマーク
B. 情報セキュリティ意識向上キャンペーンを実施する。
C. 情報セキュリティRACIチャートを公開する。
D. 情報セキュリティ戦略委員会を設置する。
正解: **(正解を表示します)**
= Establishing an information security strategy committee is the best way to obtain support for a new organization-wide information security program because it involves the participation and collaboration of key stakeholders from different business functions and levels who can provide input, guidance, and endorsement for the security program. An information security strategy committee is a governance body that oversees the development, implementation, and maintenance of the security program and aligns it with the organization's strategic objectives, risk appetite, and culture. An information security strategy committee can help to obtain support for the security program by: Communicating the vision, mission, and goals of the security program to the organization and demonstrating its value and benefits.

Establishing roles and responsibilities for the security program and ensuring accountability and ownership.
Securing adequate resources and budget for the security program and allocating them appropriately.
Resolving conflicts and issues that may arise during the security program execution and ensuring alignment with other business processes and initiatives.
Monitoring and evaluating the performance and effectiveness of the security program and ensuring continuous improvement and adaptation.
Benchmarking against similar industry organizations is a useful technique to compare and improve the security program, but it is not the best way to obtain support for a new organization-wide information security program. Benchmarking involves measuring and analyzing the security program's processes, practices, and outcomes against those of other organizations that have similar characteristics, objectives, or challenges. Benchmarking can help to identify gaps, strengths, weaknesses, opportunities, and threats in the security program and to adopt best practices and standards that can enhance the security program's performance and maturity. However, benchmarking alone does not guarantee the support or acceptance of the security program by the organization, as it may not reflect the organization's specific needs, risks, or culture.
Delivering an information security awareness campaign is a vital component of the security program, but it is not the best way to obtain support for a new organization-wide information security program. An information security awareness campaign is a set of activities and initiatives that aim to educate and inform the organization's workforce and other relevant parties about the security program's policies, standards, procedures, and guidelines, as well as the security risks, threats, and incidents that may affect the organization. An information security awareness campaign can help to increase the security knowledge, skills, and behaviors of the organization's members and to foster a security risk-aware culture. However, an information security awareness campaign is not sufficient to obtain support for the security program, as it may not address the strategic, operational, or financial aspects of the security program or the expectations and interests of the different stakeholders.
Publishing an information security RACI chart is a helpful tool to define and communicate the security program's roles and responsibilities, but it is not the best way to obtain support for a new organization-wide information security program. A RACI chart is a matrix that assigns the level of involvement and accountability for each task or activity in the security program to each role or stakeholder. RACI stands for Responsible, Accountable, Consulted, and Informed, which are the four possible levels of participation. A RACI chart can help to clarify the expectations, obligations, and authority of each role or stakeholder in the security program and to avoid duplication, confusion, or conflict. However, a RACI chart does not ensure the support or commitment of the roles or stakeholders for the security program, as it may not address the benefits, challenges, or resources of the security program or the feedback and input of the roles or stakeholders. References =

CISM Review Manual 15th Edition, pages 97-98, 103-104, 107-108, 111-112 Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition
- ISACA1
Information Security Strategy: The Key to Success - ISACA2
Deliver an information security awareness campaign is the BEST approach to obtain support for a new organization-wide information security program. An information security awareness campaign is a great way to raise awareness of the importance of information security and the impact it can have on an organization. It helps to ensure that all stakeholders understand the importance of information security and are aware of the risks associated with it. Additionally, an effective awareness campaign can help to ensure that everyone in the organization is aware of the cybersecurity policies, procedures, and best practices that must be followed.

質問**: 11**
企業ガバナンスと情報セキュリティガバナンスの整合性を示す最良の証拠は、次のうちどれですか？
A. セキュリティの主要業績評価指標(KPI)
B. プロジェクトリソースの最適化
C. 定期的なセキュリティポリシーの見直し
D. 上級管理職による支援
正解**: D (**コメントを発表する**)**
Alignment between corporate and information security governance means that the information security program supports the organizational goals and objectives, and is integrated into the enterprise governance structure. The best evidence of alignment is the senior management sponsorship, which demonstrates the commitment and support of the top-level executives and board members for the information security program.
Senior management sponsorship also ensures that the information security program has adequate resources, authority, and accountability to achieve its objectives and address the risks and issues that affect the organization. Senior management sponsorship also helps to establish a culture of security awareness and compliance throughout the organization, and to communicate the value and benefits of the information security program to the stakeholders.
References =
CISM Review Manual 15th Edition, page 1631
CISM 2020: Information Security & Business Process Alignment, video 22
Certified Information Security Manager (CISM), page 33

質問**: 12**

本国を拠点とする電子商取引事業を展開する組織が、厳格なセキュリティ法を持つ別の国に新たなオフィスを開設した。このような状況において、全体的なセキュリティ戦略は以下の点に基づいて策定されるべきである。
A. 国際セキュリティ基準。
B. リスク評価結果。
C. セキュリティ組織構造。
D. 最も厳しい要件。
正解: **(**正解を表示します**)**

質問: **13**
情報分類体系の第一の目的は何であるべきか？
A. 法令および規制要件を満たすため
B. 資産目録を作成する
C. データ保持要件を定義する
D. リスクに見合った管理策を実施する
正解: **(**正解を表示します**)**
The correct answer is D because the primary objective of an information classification scheme is to ensure that information receives protection appropriate to its sensitivity, criticality, value, and risk. Classification labels such as public, internal, confidential, and restricted help determine required controls for access, storage, transmission, encryption, retention, monitoring, and disposal. Legislative and regulatory requirements may influence classification rules, but compliance is not the only objective. Developing an asset inventory is important because organizations need to know what information assets they have, but classification goes further by assigning protection levels. Defining data retention requirements may be supported by classification, but retention is only one control area. In CISM risk management, controls should be risk-based and cost-effective. Overprotecting low-risk data wastes resources, while underprotecting sensitive data increases exposure. A classification scheme enables consistent, proportionate, and risk-aligned protection of information assets. Therefore, the primary objective is to implement controls proportionate to risk.
Reference: CISM Information Risk Management; information classification, data protection, risk-based controls, asset management, and control proportionality principles.

質問: **14**
アプリケーション開発中にセキュリティが確実に統合されるようにするには、次のうちどれが最も効果的でしょうか？
A. 開発プロセスにおいてグローバルなセキュリティ基準を採用する
B. プログラマー向けに安全な開発手法に関する研修を提供する
C. 受け入れテスト中にアプリケーションセキュリティテストを実施する
D. 開始段階でのセキュリティ要件の導入

正解: **D** (コメントを発表する)
Introducing security requirements during the initiation phase would BEST ensure that security is integrated during application development because it would allow the security objectives and controls to be defined and aligned with the business needs and risk appetite before any design or coding is done. This would also facilitate the security by design approach, which is the most effective method to enhance the security of applications and application development activities1. Introducing security requirements early would also enable the collaboration between security professionals and developers, the identification and specification of security architectures, and the integration and testing of security controls throughout the development life cycle2. Employing global security standards during development processes (A) would help to ensure the consistency and quality of security practices, but it would not necessarily ensure that security is integrated during application development. Providing training on secure development practices to programmers (B) would help to raise the awareness and skills of developers, but it would not ensure that security is integrated during application development. Performing application security testing during acceptance testing © would help to verify the security of the application before deployment, but it would not ensure that security is integrated during application development. It would also be too late to identify and remediate any security issues that could have been prevented or mitigated earlier in the development process.
References = 1: Five Key Components of an Application Security Program - ISACA1; 2: CISM Domain - Information Security Program Development | Infosec2

質問: **15**
情報セキュリティプログラムの主要な成果として、次のうちどれが適切でしょうか？
A. 戦略的整合性
B. リスク排除
C. コスト削減
D. 脅威の軽減
正解: (正解を表示します)
According to the CISM Review Manual (Digital Version), Chapter 3, Section 3.2.1, strategic alignment is the primary outcome of an information security program1. Strategic alignment means that the information security program supports and is tailored to the organization's objectives and business strategy1. It also means that the information security program is aligned with other assurance functions, such as physical, human resources, quality, and IT1.
The CISM Review Manual (Digital Version) also states that strategic alignment is essential for achieving a competitive advantage, enhancing customer trust, reducing legal and regulatory risks, and improving organizational performance1. Strategic alignment requires effective communication and collaboration among all stakeholders, including senior management, information owners, information security managers, information security steering committees, and external partners1.

The CISM Exam Content Outline also covers the topic of strategic alignment in Domain 3 - Information Security Program Development and Management (33% exam weight)2. The subtopics include:
3.2.1 Information Security Strategy
3.2.2 Information Security Governance
3.2.3 Information Security Risk Management
3.2.4 Information Security Compliance
I hope this answer helps you prepare for your CISM exam. Good luck! #

質問**: 16**
インシデント対応チームのトレーニングを強化するための最良の方法は、次のうちどれですか？
A. 事後検証を実施する。
B. インシデントの主要業績評価指標(KPI)を設定する。
C. 組織単位へのインタビューを実施する。
D. 緊急対応活動に参加する。
正解**: (**正解を表示します**)**
Performing post-incident reviews is the best way to enhance training for incident response teams because it allows them to identify the strengths and weaknesses of their response, learn from the lessons and best practices, and implement corrective actions and improvement plans for future incidents. Post-incident reviews also help to evaluate the effectiveness and efficiency of the incident response process and procedures, and to update them as needed.
References: The CISM Review Manual 2023 states that "post-incident reviews are an essential part of the incident response process" and that "they provide an opportunity to assess the performance of the incident response team, identify areas for improvement, and document lessons learned and best practices" (p. 191).
The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Performing post-incident reviews is the best way to enhance training for incident response teams, as it enables them to learn from their experience and improve their skills and knowledge" (p. 97).

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu ｶ193問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **17**
IT利用規約において最も重要な目的は次のうちどれですか？
A. 事業部門を情報セキュリティポリシーに準拠させる
B. 従業員が情報セキュリティポリシーを理解していることを示すため
C. 組織リソースへの第三者アクセスを管理する
D. 組織のリソースを活用する際の期待事項を文書化する
正解: **(**正解を表示します**)**
The correct answer is D because the primary purpose of an acceptable use policy is to define and document expectations for how users may use organizational information systems, networks, devices, applications, internet access, email, data, and other resources. It communicates permitted and prohibited activities, user responsibilities, monitoring expectations, privacy limitations, disciplinary consequences, and requirements for protecting information assets. Aligning business units to the information security policy is a broader governance objective, not the specific objective of an acceptable use policy. Employee acknowledgement is useful evidence that users have received or accepted the policy, but acknowledgement is not the primary purpose. Managing third-party access is usually addressed through access management, vendor agreements, and third-party risk controls. In CISM governance, policies define expected behavior and provide a foundation for accountability. The acceptable use policy specifically sets expectations for appropriate use of organizational resources. Therefore, documenting expectations for resource use is the most important objective.
Reference: CISM Information Security Governance; acceptable use policy, user responsibilities, policy communication, and accountability.

質問: **18**
情報セキュリティフレームワークの目的が達成されていることを保証する最終的な責任は、以下の者にあります。
A. 情報セキュリティ責任者。
B. 運営委員会。
C. 取締役会。
D. 内部監査マネージャー。
正解: **(**正解を表示します**)**
The ultimate responsibility for ensuring the objectives of an information security framework are being met belongs to the board of directors, as they are accountable for the governance of the organization and the oversight of the information security strategy. The board of directors should ensure that the information security framework aligns with the business objectives, supports the business processes, and complies with the legal and

regulatory requirements. The board of directors should also monitor the performance and effectiveness of the information security framework and provide guidance and direction for its improvement.
References = CISM Review Manual, 16th Edition eBook1, Chapter 1: Information Security Governance, Section: Enterprise Governance, Subsection: Board of Directors, Page 18.

質問: **19**
組織がクラウドサービスのセキュリティ体制を評価する上で、最も有効な手段は次のうちどれですか？
A. 業界のピアレビュー
B. サービスプロバイダー証明書
C. 侵入テストレポート
D. 第三者監査報告書
正解: **(**正解を表示します**)**
Third-party audit reports (D) provide the most reliable evaluation of a cloud provider's security posture because they offer independent assurance of control design and effectiveness. Peer reviews (A) and attestations (B) are less objective, while penetration test reports (C) focus narrowly on technical vulnerabilities. CISM emphasizes independent assurance mechanisms when assessing third-party security, particularly for cloud services.
References: ISACA CISM Review Manual (Governance-third-party assurance and cloud risk); CISM Exam Content Outline (Domain 2).

質問: **20**
リスクオーナーが以下の事項について責任を負うことを理解することが最も重要です。
A. リスク指標と管理コンプライアンス状況を情報セキュリティマネージャーに報告する
B. 意思決定運営委員会に対するリスクに関連する管理上の欠陥の拡大
C. 利害関係者と協力して、リスクに関連する管理策の有効性を評価する。
D. リスクに関連する管理策の有効性を監督および監視する
正解: **D (**コメントを発表する**)**
It is most important that risk owners understand they are accountable for overseeing and monitoring the effectiveness of controls associated with the risk. In CISM, risk ownership means accountability for managing a risk within the organization's risk appetite. The risk owner does not necessarily operate every control, but must ensure that appropriate treatment is selected, controls are effective, residual risk is understood, and issues are addressed. Reporting metrics to the information security manager is useful, but it is only part of oversight and does not fully define accountability. Escalating deficiencies may be required when risks exceed tolerance, but escalation alone is not the primary accountability. Collaborating with stakeholders is important, but accountability remains with the risk owner. CISM separates control ownership from risk ownership:

control owners may operate controls, while risk owners remain accountable for the business risk and outcomes. Therefore, overseeing and monitoring the effectiveness of related controls is the most important accountability for risk owners.
References:
ISACA CISM Review Manual, Information Risk Management - risk ownership, control monitoring, and accountability ISACA CISM Exam Content Outline, Domain 1: Information Risk Management

質問**: 21**
情報セキュリティに関する報告書を上級管理職がレビューする主な理由として、次のうちどれが挙げられますか？
A. セキュリティプログラムの有効性を評価する
B. 十分なセキュリティリソースが確保されるようにする
C. セキュリティ監査が定期的に実施されていることを確認する
D. セキュリティリスクを費用対効果の高い方法で管理することを保証する
正解**: A (**コメントを発表する**)**
The correct answer is A because senior management reviews information security reports to determine whether the security program is achieving its objectives and effectively supporting the organization's business goals. Reporting provides visibility into program performance, risk trends, incident activity, compliance status, control effectiveness, and progress against security objectives. Ensuring adequate resources is an important management responsibility, but resource decisions should be based on an understanding of program effectiveness and risk. Confirming regular audits is useful, but audits are only one source of assurance.
Ensuring risk is managed cost-effectively is also important, but it is a broader outcome of governance and decision-making. The primary purpose of reporting is to give senior management enough information to evaluate whether the program is performing as intended. In CISM governance, reporting enables oversight, accountability, informed decision-making, and alignment between security and enterprise objectives.
Therefore, assessing the effectiveness of the security program is the best answer.
Reference: CISM Information Security Governance; management reporting, program effectiveness, governance oversight, and performance measurement principles.

質問**: 22**
情報セキュリティガバナンスフレームワークが正常に実装されたことを最もよく示すのは、次のうちどれですか？
A. このフレームワークは、内部リソースと外部リソースを整合させます。
B. このフレームワークは、セキュリティプロセスを業界のベストプラクティスに合わせます。

C. このフレームワークは、セキュリティ組織内の管理機能とその他の機能を整合させます。
D. このフレームワークには、市販の既製セキュリティソリューションが含まれています。
正解: **(**正解を表示します**)**
The best indicator that an information security governance framework has been successfully implemented is A). The framework aligns internal and external resources. This is because the framework should ensure that the information security strategy, policies, and objectives are aligned with the business goals, stakeholder expectations, and regulatory requirements. The framework should also enable the effective allocation and coordination of internal and external resources, such as people, processes, technology, and finances, to support the information security program and its activities.
The framework should ensure that the information security strategy, policies, and objectives are aligned with the business goals, stakeholder expectations, and regulatory requirements. The framework should also enable the effective allocation and coordination of internal and external resources, such as people, processes, technology, and finances, to support the information security program and its activities. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 1, Section 1.2.1, page 181; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 49, page 14

質問: **23**
上級管理職は、ミッションクリティカルなシステムの災害復旧計画 (DRP) を徹底的にテストしたいと考えています。
次のどれが最も信頼性の高い結果をもたらすでしょうか?
A. シミュレーションテスト
B. 構造化されたウォークスルー
C. 完全中断テスト
D. 並列テスト
正解: **(**正解を表示します**)**

質問: **24**
日々の監視レポートによると、IT担当者が変更管理プロセスを経ずにファイアウォールルールを変更したことが判明しました。情報セキュリティマネージャーがこの問題に対処するための最初のステップは次のとおりです。
A. 変更を元に戻すよう要求する
B. 変更管理プロセスをレビューする
C. 変化の分析を行う
D. この出来事を上級管理職に報告する
正解: **C (**コメントを発表する**)**

Performing an analysis of the change is the first step in addressing the issue of an IT employee making a change to a firewall rule outside of the change control process because it helps to understand the reason, impact, and risk of the change and to decide whether to approve, reject, or reverse it. Requiring that the change be reversed is not the first step because it may cause more disruption or damage without proper analysis and testing. Reviewing the change management process is not the first step because it does not address the specific issue or incident at hand, but rather focuses on improving the process for future changes.
Reporting the event to senior management is not the first step because it does not resolve the issue or incident, but rather escalates it without sufficient information or recommendation. References: https://www.isaca.org /resources/isaca-journal/issues/2018/volume-3/change-management-in-the-age-of-digital-transformation
https://www.isaca.org/resources/isaca-journal/issues/

質問**: 25**
情報セキュリティプログラムの要件を雇用および人員配置プロセスと整合させることで、組織にとって最も大きなメリットは何でしょうか？
A. セキュリティインシデント報告手順に従います。
B. 警備員の離職率が低下します。
C. 情報資産は適切に分類されている。
D. アクセスはタスクの要件に基づいて許可されます。
正解**: D (**コメントを発表する**)**
The PRIMARY benefit to an organization when information security program requirements are aligned with employment and staffing processes is that access is granted based on task requirements. This means that the organization can ensure that the employees have the appropriate level and scope of access to the information assets and systems that they need to perform their duties, and that the access is granted, reviewed, and revoked in accordance with the security policies and standards. This can help to reduce the risk of unauthorized access, misuse, or leakage of information, as well as to comply with the principle of least privilege and the segregation of duties12. Security incident reporting procedures are followed (A) is a benefit to an organization when information security program requirements are aligned with employment and staffing processes, but it is not the PRIMARY benefit. Security incident reporting procedures are the steps and guidelines that the employees should follow when they detect, report, or respond to a security incident. Aligning the information security program requirements with the employment and staffing processes can help to ensure that the employees are aware of and trained on the security incident reporting procedures, and that they are enforced and monitored by the management. This can help to improve the effectiveness and efficiency of the incident response process, as well as to comply with the legal and contractual obligations12.

Security staff turnover is reduced (B) is a benefit to an organization when information security program requirements are aligned with employment and staffing processes, but it is not the PRIMARY benefit.
Security staff turnover is the rate at which the security personnel leave or join the organization. Aligning the information security program requirements with the employment and staffing processes can help to reduce the security staff turnover by ensuring that the security roles and responsibilities are clearly defined and communicated, that the security personnel are adequately compensated and motivated, and that the security personnel are evaluated and developed regularly. This can help to retain the security talent and expertise, as well as to reduce the costs and risks associated with the security staff turnover12. Information assets are classified appropriately © is a benefit to an organization when information security program requirements are aligned with employment and staffing processes, but it is not the PRIMARY benefit. Information asset classification is the process of assigning a security level or category to the information assets based on their value, sensitivity, and criticality to the organization. Aligning the information security program requirements with the employment and staffing processes can help to ensure that the information assets are classified appropriately by establishing the ownership and custody of the information assets, the criteria and methods for the information asset classification, and the roles and responsibilities for the information asset classification. This can help to protect the information assets according to their security level or category, as well as to comply with the regulatory and contractual requirements12. References = 1: CISM Review Manual
15th Edition, page 75-76, 81-82, 88-89, 93-941; 2: CISM Domain 1: Information Security Governance (ISG)
[2022 update] 2

質問**: 26**
情報セキュリティ手順の開発において、最も重要な関与が必要なグループは次のうちどれですか？
A. 監査管理
B. 上級管理職
C. 運用部隊
D. エンドユーザー
正解**: (**正解を表示します**)**
The correct answer is C because procedures describe specific operational steps for carrying out security requirements, and operational units are the groups that must execute those steps in practice. Procedures must be realistic, workable, and aligned with day-to-day business and technical processes. Involving operational units helps ensure that procedures reflect actual workflows, system dependencies, resource constraints, and control responsibilities. Audit management may review procedures for compliance or control adequacy, but auditors should not be the primary developers of operational

procedures. Senior management approves direction and policy, but it usually does not define detailed procedural steps. End users may provide useful feedback for procedures affecting them, but operational units have the strongest understanding of how processes are performed and controlled. In CISM, effective security program management requires translating policies and standards into practical procedures that can be implemented consistently. Therefore, operational units are the most important group to involve in procedure development.
Reference: CISM Information Security Program Development and Management; procedures, operational control implementation, policy hierarchy, and process ownership principles.

質問: **27**
経営陣が企業戦略を変更する場合、既存の情報セキュリティ対策を評価し、新たな情報セキュリティ対策を選択するために、以下のどのプロセスを使用すべきでしょうか？
A. 構成管理
B. リスク管理
C. アクセス制御管理
D. 変更管理
正解: **D (**コメントを発表する**)**
According to the CISM Review Manual (Digital Version), Chapter 3, Section 3.2.2, change management is the process of identifying, assessing, approving, implementing, and monitoring changes to information systems and information security controls1. Change management is essential for ensuring that changes are aligned with the organization's business strategy and objectives, as well as complying with applicable laws and regulations1.
The CISM Review Manual (Digital Version) also states that change management should be performed in conjunction with other processes, such as configuration management, access control management, and risk management1. Configuration management is the process of identifying, documenting, controlling, and verifying the configuration items (CIs) of an information system1. Access control management is the process of granting or denying access to information systems and information assets based on predefined policies and procedures1. Risk management is the process of identifying, analyzing, evaluating, treating, monitoring, and communicating risks to information systems and information assets1.
The CISM Exam Content Outline also covers the topic of change management in Domain 3 - Information Security Program Development and Management (27% exam weight)2. The subtopics include:
3.2.2 Change Management
3.2.3 Change Control
3.2.4 Change Implementation
3.2.5 Change Monitoring

I hope this answer helps you prepare for your CISM exam. Good luck! #

質問: **28**
組織内でセキュリティインシデントが報告された場合、情報セキュリティ管理者はいつ情報所有者に連絡すべきでしょうか？
A. 事件が収束した後
B. 事件が確認された後。
C. 潜在的なインシデントが切り替えられた後
D. 事件が収束した後
正解: **(**正解を表示します**)**
= An information security manager should contact the information owner after the incident has been confirmed, as this is the point when the impact and severity of the incident can be assessed and communicated. The information owner is responsible for the business value and use of the information and should be involved in the decision making process regarding the incident response. Contacting the information owner after the incident has been mitigated or contained may be too late, as the information owner may have different priorities or expectations than the security team. Contacting the information owner after the potential incident has been logged may be premature, as the incident may turn out to be a false positive or a minor issue that does not require the information owner's attention.
References = 1: CISM Review Manual, 16th Edition by Isaca (Author), page 292.

質問: **29**
ある組織では、災害発生時に業務上重要なアプリケーションを30分以内に復旧させることを要求しています。この要件を管理するために、事業継続計画(BCP)において定義すべき指標は次のうちどれでしょうか？
A. 復旧時間目標(RTO)
B. リカバリポイント目標(RPO)
C. 最大許容ダウンタイム(MTD)
D. サービスレベル契約(SLA)
正解: **A (**コメントを発表する**)**
The Recovery Time Objective (RTO) specifies the maximum acceptable downtime before operations must resume. A 30-minute requirement directly defines the RTO for those systems.
"RTO defines the duration within which systems must be restored following an outage to prevent unacceptable business impact."
- CISM Review Manual 15th Edition, Chapter 3: Business Continuity Planning, Section: Continuity Metrics*

質問: **30**

情報セキュリティチームは、最近の侵入テストの結果を軽減するための作業を開始しました。
次のどれが組織にとって最大のリスクをもたらしますか?
A. 評価後、一部の所見は低リスクに再分類されました
B. 侵入テストレポートのすべての発見事項が修正されたわけではありません
C. 侵入テストレポートには、高リスクの発見事項は含まれていませんでした
D. 侵入テスト結果のリスク分類は実行されませんでした
正解: **D** (コメントを発表する)
The greatest risk comes from not performing risk classification on the findings. Without classification, the organization cannot prioritize remediation efforts, allocate resources effectively, or understand the business impact of the vulnerabilities.
"Risk classification helps determine the priority for mitigating vulnerabilities and enables risk-informed decisions."
- CISM Review Manual 15th Edition, Chapter 2: Risk Assessment and Analysis* Even if some findings are unfixed or reclassified, the lack of any classification process undermines the whole risk management effort.

質問: **31**
SIEM システムの有効性を最も低下させる可能性のあるものはどれですか?
A. 複雑なユーザーインターフェース
B. アラートしきい値の設定ミス
C. 弱い暗号化ログファイル
D. システムアクセスに対する多要素認証 (MFA) の欠如
正解: **B** (コメントを発表する)
The effectiveness of a SIEM (Security Information and Event Management) system heavily relies on properly configured alert thresholds. Misconfiguration of alert thresholds can result in missed detection of significant incidents (false negatives) or an overwhelming number of false positives, making it difficult to identify real threats. According to the CISM Review Manual, 16th Edition, Domain 4: Information Security Incident Management, the configuration and tuning of monitoring tools like SIEMs are crucial for timely and accurate detection of incidents.
Reference:ISACA CISM Review Manual, 16th Edition, Page 304-305, "Security Event Management Tools and Techniques".

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu ｷ193問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **32**
情報セキュリティプログラムに対する組織全体の支持を得るために、以下のうちどれを最も重要視すべきでしょうか？
A. セキュリティポリシーの成熟度
B. セキュリティ上の役割と責任の明確化
C. 企業文化
D. 企業リスクフレームワーク
正解: **C** (コメントを発表する)
Corporate culture is the most important factor to consider when trying to gain organization-wide support for an information security program because it reflects the values, beliefs, and behaviors of the organization and its members. Corporate culture influences how the organization perceives, prioritizes, and responds to information security risks and issues, and how it adopts and implements information security policies and practices. By understanding and aligning with the corporate culture, the information security manager can communicate the benefits and value of the information security program, and foster a positive and collaborative security culture across the organization.
References: The CISM Review Manual 2023 states that "corporate culture is the set of shared values, beliefs, and behaviors that characterize the organization and its members" and that "corporate culture affects how the organization views and manages information security risks and issues, and how it supports and implements information security policies and practices" (p. 81). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Corporate culture is the correct answer because it is the most important factor to consider when trying to gain organization-wide support for an information security program, as it reflects the values, beliefs, and behaviors of the organization and its members, and influences how they perceive, prioritize, and respond to information security risks and issues, and how they adopt and implement information security policies and practices" (p. 23). Additionally, the article Building a Culture of Security from the ISACA Journal 2019 states that "corporate culture is the key factor that determines the success or failure of an information security program" and that "corporate culture can be either an enabler or a barrier for information security, depending on how well it aligns with the information security objectives, values, and practices of the organization" (p. 1)

質問: **33**
組織が情報セキュリティリスクの状況を継続的に評価するために最も有効な方法はどれですか？
A. 主要リスク指標(KRI)
B. 業界規制の遵守

C. リスク登録簿の定期的な見直し
D. 上級管理職の支援度
正解: **(**正解を表示します**)**

質問: **34**
ランサムウェア攻撃後にクリーンなデータを復元できる能力を確保するための最良の方法は、次のうちどれですか？
A. サイバー保険を購入する
B. 機密性の高い生産データを暗号化する
C. バックアップの整合性チェックを実行する
D. 複数のオフラインバックアップを維持する
正解: **(**正解を表示します**)**
The best way to ensure the capability to restore clean data after a ransomware attack is to maintain multiple offline backups. Offline backups are backups that are not connected to the network or the internet, and therefore are not accessible by ransomware. Multiple offline backups provide redundancy and allow the organization to choose the most recent and uncorrupted backup to restore the data. Offline backups should be stored in a secure location and tested regularly to ensure their integrity and availability.
Purchasing cyber insurance may help the organization cover some of the costs associated with a ransomware attack, such as ransom payment, data recovery, legal fees, etc., but it does not guarantee the capability to restore clean data. Cyber insurance policies may have exclusions, limitations, or conditions that affect the coverage and reimbursement. Moreover, cyber insurance does not prevent or mitigate the ransomware attack itself, and it may not cover all the losses or damages caused by the attack.
Encrypting sensitive production data may protect the confidentiality of the data from unauthorized access or disclosure, but it does not prevent ransomware from encrypting the data again. Ransomware does not need to decrypt the data to encrypt it, and it may use a different encryption algorithm or key than the one used by the organization. Encrypting production data may also increase the complexity and time required for data recovery, especially if the encryption keys are lost or compromised.
Performing integrity checks on backups may help the organization verify that the backups are not corrupted or tampered with, but it does not ensure the capability to restore clean data after a ransomware attack. Integrity checks are a preventive measure that should be done before the attack, not after. If the backups are already infected or encrypted by ransomware, performing integrity checks will not help to recover the data. Integrity checks should be complemented by other measures, such as isolation, versioning, and offline storage, to protect the backups from ransomware. References = CISM Certified Information Security Manager Study Guide, Chapter 9: Business Continuity and Disaster Recovery, page 3081; CISM Foundations: Module 4 Course, Part Two: Business Continuity and Disaster Recovery Plans2; Ransomware recovery: 8 steps to successfully restore from backup3; Ransomware Recovery: 5 Steps to Recover Data4

質問: **35**
新たなリスクの影響を評価する際に、最も大きな課題となるのは次のうちどれですか？
A. 新たなリスクの複雑性
B. 新たなリスクに関するデータが不十分
C. 時代遅れのリスク管理戦略
D. リスク評価を実施するためのリソース不足
正解: **(**正解を表示します**)**
The greatest challenge in assessing emerging risk is insufficient data (B). Emerging risks, by definition, lack historical incidents, loss data, and proven impact metrics, making accurate assessment difficult. CISM emphasizes that uncertainty and data scarcity are inherent challenges in emerging risk management.
Complexity (A) and resource constraints (D) are common issues, but without sufficient data, even skilled analysts and mature processes struggle to estimate likelihood and impact. An outdated strategy (C) affects overall effectiveness but does not specifically hinder impact assessment as much as data scarcity does.
References: ISACA CISM Review Manual (Risk management-emerging risks, uncertainty, and assessment challenges); CISM Exam Content Outline (Domain 1).

質問: **36**
機密情報をホストするサーバー向けに、インシデント対応計画が策定されています。情報漏洩が発生した場合、誰がシステムのシャットダウンを決定すべきでしょうか？
A. サービスオーナー
B. オペレーションマネージャー
C. 情報セキュリティマネージャー
D. インシデント対応チーム
正解: **(**正解を表示します**)**

質問: **37**
組織における高度な持続的脅威(APT)を監視するための最良の方法は次のうちどれですか？
A. 業界の同業者とネットワークを築き、情報を共有する。
B. インターネットで潜在的なイベントのチームを検索
C. 環境中の異常を探索する
D. 環境内の脅威シグネチャを検索します。
正解: **(**正解を表示します**)**
An advanced persistent threat (APT) is a stealthy and sophisticated attack that aims to compromise and maintain access to a target network or system over a long period of time, often for espionage or sabotage purposes. APTs are difficult to detect by conventional security tools, such as antivirus or firewalls, that rely on signatures or rules to identify

threats. Therefore, the best way to monitor for APTs is to search for anomalies in the environment, such as unusual network traffic, user behavior, file activity, or system configuration changes, that may indicate a compromise or an ongoing attack. References: https://www.isaca.
org/credentialing/cism https://www.nist.gov/publications/information-security-handbook-guide-managers

質問**: 38**
情報セキュリティマネージャーが新しいセキュリティプロジェクトの承認を得られる可能性が最も高いのは、ビジネスケースに以下の証拠が示されている場合である。
A. 組織的整合性
B. IT戦略の整合性
C. 組織に対する脅威
D. 既存の管理コスト
正解**: (**正解を表示します**)**
A new security project is more likely to be approved if it aligns with the organization's goals, objectives, and strategies. This shows that the project supports the business needs and adds value to the organization. Organizational alignment is one of the key elements of a business case for information security, as stated in the CISM Review Manual, 16th Edition1, page 41. IT strategy alignment, threats to the organization, and existing control costs are also important factors to consider, but they are not as persuasive as organizational alignment in obtaining approval for a new security project. References = 1: CISM Review Manual, 16th Edition by Isaca (Author) Learn more:
1. isaca.org2. amazon.com3. gov.uk

質問**: 39**
企業におけるセキュリティ技術への投資に関する推奨事項は、主に以下の点に基づいて策定されるべきである。
A. 国際規格への準拠
B. 資金の確保
C. 組織のリスク許容度
D. ビジネスニーズとの整合性
正解**: (**正解を表示します**)**
Verified answer: According to the CISM Review Manual, 15th Edition, Chapter 3, Section 3.2.1.1, " Recommendations for enterprise investment in security technology should be primarily based on the organization's risk tolerance. " 1 The organization's risk tolerance is the degree of uncertainty that the organization is willing to accept in order to pursue its objectives. It reflects the organization's appetite for risk and its ability to cope with potential losses or disruptions. The higher the risk tolerance, the more aggressive and innovative the security investments can be, as they can help achieve faster growth or competitive advantage. The lower the risk tolerance, the more conservative and defensive the security

investments should be, as they can help protect the organization's assets and reputation from potential threats.
References: 1: CISM Review Manual, 15th Edition, Chapter 3, Section 3.2.1.1

質問: **40**
従業員がメール内の悪意のあるリンクをクリックした結果、会社のデータが漏洩しました。今後、このようなリスクを軽減するための最善策は何でしょうか？
A. フィッシング対策に関する意識向上トレーニングを実施する。
B. 懲戒手続きを実施する。
C. 利用規約を策定する。
D. スパムフィルタリングルールを評価し、更新します。
正解: **(**正解を表示します**)**
Phishing awareness training is the best way to mitigate the risk of employees clicking on malicious links in emails, as it educates them on how to recognize and avoid phishing attempts. (From CISM Review Manual
15th Edition)
References: CISM Review Manual 15th Edition, page 179, section 4.3.2.2.

質問: **41**
ビジネス要件に合致した費用対効果の高い情報セキュリティ戦略を策定する上で、最も役立つのは次のうちどれですか？
A. 情報資産の分類
B. 政策基準の策定
C. データ保持の強制
D. 業界他社とのベンチマーク
正解: **(**正解を表示します**)**

質問: **42**
遠隔地に支社を持つ国際組織が、個人識別情報(PII)を管理するための企業セキュリティポリシーを導入しています。情報セキュリティマネージャーの主な懸念事項は次のうちどれでしょうか？
A. 地方条例
B. データバックアップ戦略
C. 啓発プログラムの一貫性
D. 組織報告構造
正解: **(**正解を表示します**)**
Local regulations are the main concern for the information security manager when implementing a corporate security policy for managing PII, as different countries or regions may have different legal, regulatory or contractual requirements for the protection, processing, storage and transfer of PII. The information security manager should ensure

that the policy complies with the applicable local regulations and respects the rights and preferences of the data subjects. The policy should also address the risks and challenges of cross-border data transfers and the use of cloud services.
References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.2.1, page 2191; CISM Online Review Course, Module 4, Lesson 2, Topic 12; Comparitech, PII Compliance: What is it and How to Implement it3

質問: **43**
情報リスクに関して上級管理職に伝えるのに最も適切なのは次のうちどれですか？
A. 新興セキュリティ技術
B. リスクプロファイルの変化
C. リスク許容度の定義
D. 脆弱性スキャンの進捗状況
正解: **(**正解を表示します**)**
Risk profile changes are the most appropriate to communicate to senior management regarding information risk because they reflect the current level and nature of the risks that the organization faces and how they may affect its objectives and performance. Senior management needs to be aware of any changes in the risk profile so that they can make informed decisions and allocate resources accordingly. Risk profile changes also help senior management monitor the effectiveness of the risk management process and identify any gaps or weaknesses that need to be addressed.
References = Communicating Information Security Risk Simply and Effectively, Part 1, CISM Domain 2:
Information Risk Management (IRM) [2022 update]

質問: **44**
多国籍企業がセキュリティガバナンスフレームワークを導入しようとしています。情報セキュリティマネージャーは、地域によってセキュリティ対策が異なることを懸念しています。最初に評価すべき項目は次のうちどれでしょうか？
A. 国境を越えたデータモビリティ
B. 現地の規制要件
C. フレームワークのトレーニング要件
D. グローバルフレームワーク基準
正解: **(**正解を表示します**)**

質問: **45**
新たなセキュリティプロジェクトについて上級管理職の賛同を得るための提案は、以下の内容を含んでいる場合に最も効果的です。
A. 投資収益率(ROI)の予測。
B. 業界ベンチマークギャップ分析。

C. 現在の脅威状況の分析。
D. 報告された事件の履歴データ。
正解: **(**正解を表示します**)**

質問: **46**
最悪の混乱シナリオを特定する上で、以下のうちどれが最も役立つでしょうか？
A. 事業影響分析(BIA)
B. ビジネスプロセス分析
C. SWOT分析
D. 費用便益分析
正解: **(**正解を表示します**)**
A business impact analysis (BIA) is the process of identifying and evaluating the potential effects of disruptions to critical business functions or processes. A BIA helps to determine the recovery priorities, objectives, and strategies for the organization in the event of a disaster or crisis. A BIA also helps to identify the worst-case disruption scenarios, which are the scenarios that would cause the most severe impact to the organization in terms of financial, operational, reputational, or legal consequences. By conducting a BIA, the organization can assess the likelihood and impact of various disruption scenarios, and plan accordingly to mitigate the risks and ensure business continuity and resilience. References = CISM Review Manual 15th Edition, page 181, page 183.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu ↾**193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **47**
ある組織がデジタル変革プロセスを進めており、IT部門はこれまで経験したことのないリスク環境に置かれています。情報セキュリティマネージャーは、ITリスク管理プロセスを主導する任務を負っています。次のうち、最も優先順位を高くすべきものはどれでしょうか？
A. リスクの特定
B. 制御ギャップの分析
C. 主要リスク指標(KRI)の設計
D. リスク治療オプションの選択
正解: **(**正解を表示します**)**

= Identification of risk is the first and most important step in the IT risk management process, especially when the organization is undergoing a digital transformation that introduces new technologies, processes, and business models. Identification of risk involves determining the sources, causes, and potential consequences of IT-related risks that may affect the organization's objectives, assets, and stakeholders. Identification of risk also helps to establish the risk context, scope, and criteria for the subsequent risk analysis, evaluation, and treatment. Without identifying the risks, the information security manager cannot effectively assess the risk exposure, prioritize the risks, implement appropriate controls, monitor the risk performance, or communicate the risk information to the relevant parties.
References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Identification, page 841; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question
34, page 352.

質問: **48**
リスク管理策を実施する際に、リスクオーナーから意見を収集する最も重要な理由は次のうちどれですか？
A. リスク軽減コストを削減するため
B. エンタープライズアーキテクチャ(EA)の脆弱性を解決する
C. リスクを許容可能なレベルに管理する
D. ビジネスに影響を与える脅威を排除する
正解: **(**正解を表示します**)**
According to the Certified Information Security Manager (CISM) Study Manual, risk owners are responsible for managing a risk, including taking corrective action to reduce the risk to an acceptable level. When implementing controls, it is essential to obtain input from risk owners to ensure that the controls are effective in managing the risk to an acceptable level. By obtaining input from risk owners, the organization can ensure that the controls are tailored to the specific risks and are effective in reducing the risk to an acceptable level. This can help to minimize the impact of the risk on the organization and reduce the potential for financial or reputational damage.

質問: **49**
以下のうち、効果的かつ迅速なインシデント対応を最も効果的にサポートするのはどれですか？
A. 内部および外部のステークホルダーの関与
B. 文書化されたインシデント対応計画を策定しておくこと
C. 法医学的インシデント対応専門家の任命
D. SIEMソリューションの維持管理
正解: **(**正解を表示します**)**

The correct answer is B because a documented incident response plan provides the structured guidance needed for effective and timely response. The plan defines roles, responsibilities, escalation paths, communication procedures, severity classifications, containment strategies, evidence handling, notification requirements, and recovery coordination. Without a documented plan, response activities may be delayed, inconsistent, duplicated, or incomplete. Involving internal and external stakeholders is important, but stakeholder involvement must be organized through the incident response plan. Appointing a forensic specialist may be necessary for certain investigations, but not every incident requires forensic expertise. A SIEM solution is useful for monitoring and detection, but technology alone does not ensure that people know how to respond. CISM incident management principles emphasize preparation, documented procedures, communication, role clarity, and repeatable response processes. A documented plan enables responders to act quickly and consistently under pressure. Therefore, having a documented incident response plan in place best supports effective and timely incident response.
Reference: CISM Information Security Incident Management; incident response planning, documentation, escalation, communication, and response readiness principles.

質問: **50**
ある組織の研究部門は、顧客名と購入履歴を含む大規模なデータセットに機械学習アルゴリズムを適用することを計画しています。個人データ漏洩のリスクは大きな影響があると考えられます。この状況で最適なリスク処理オプションは次のどれですか?
A. 保険を購入することでリスクを移転します。
B. メリットが潜在的な結果を上回るため、リスクを受け入れます。
C. データ セット内の顧客名を暗号化することでリスクを軽減します。
D. データ セットに匿名化を適用してリスクを軽減します。
正解: **(**正解を表示します**)**

質問: **51**
次のうち、発生しつつある事態を示す最も適切な指標はどれですか？
A. 組織の情報システム内で発見された弱点
B. システムのパッチ適用を試みた結果、エラーが発生しました
C. ウェブサイトが利用できないことに関する顧客からの苦情
D. 業界の競合他社で最近発生したセキュリティインシデント
正解: **(**正解を表示します**)**

質問: **52**
組織がインシデントの分類とカテゴリ化のレベルを定義する際に考慮すべき最も適切なのは次のうちどれですか?
A. インシデント対応活動の成熟度

B. 脅威環境
C. 影響を受ける資産の数量
D. インシデントの影響
正解: **(**正解を表示します**)**
Incident impact is the primary factor for classification and categorization. It ensures incidents are addressed based on their potential to disrupt the organization.
"Incident impact should be the primary factor in defining categorization levels to ensure appropriate prioritization and response."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Incident Classification and Prioritization* ISACA practice database stresses that focusing on impact ensures incidents receive the proper response priority.

質問: **53**
ある組織が競合組織を買収しようとしている。買収前に情報セキュリティデューデリジェンスを実施する主な理由は以下のとおりである。
A. セキュリティリスクを特定する。
B. セキュリティ部門の業務を統合する能力を評価する。
C. 国際規格への準拠を確保する。
D. セキュリティポリシーと基準を評価する。
正解: **(**正解を表示します**)**
Information security due diligence is the process of assessing the current state of information security in an organization, identifying any gaps, risks, or vulnerabilities, and estimating the costs and efforts required to remediate them. Performing information security due diligence prior to making the purchase is important to determine the security exposures that may affect the value, reputation, or liability of the organization, as well as the feasibility and compatibility of integrating the security systems and processes of the two organizations.
References = CISM Review Manual 2022, page 361; CISM Exam Content Outline, Domain 1, Task 1.22; Information Security Due Diligence Questionnair

質問: **54**
SaaS(Software as a Service)モデルを採用する際に、クライアント組織のみが責任を負うべき事項は次のうちどれですか？
A. ホストパッチ適用
B. 侵入テスト
C. インフラ強化
D. データ分類
正解: **(**正解を表示します**)**
Data classification is the sole responsibility of the client organization when adopting a Software as a Service (SaaS) model. Data classification is the process of categorizing data

based on its sensitivity, value and criticality to the organization. Data classification helps to determine the appropriate level of protection, access control and retention for different types of data. Data classification is an essential part of data governance and risk management, as it enables the organization to comply with legal and regulatory requirements, protect its intellectual property and reputation, and optimize its data storage and usage costs.
In a SaaS model, the client organization has the least control and responsibility over the cloud infrastructure, platform and application, as these are fully managed by the cloud service provider (CSP). The client organization only has control and responsibility over its own data and users. Therefore, the client organization is responsible for defining and implementing data classification policies and procedures, and ensuring that its data is properly labeled and handled according to its classification level. The client organization is also responsible for educating its users about the importance of data classification and the best practices for data security and privacy.
The other options are not the sole responsibility of the client organization in a SaaS model, as they are either shared with or delegated to the CSP. Host patching, penetration testing and infrastructure hardening are all related to the security and maintenance of the cloud infrastructure and platform, which are the responsibility of the CSP in a SaaS model. The CSP is expected to provide regular updates, patches and fixes to the host operating system, network and application components, and to conduct periodic security assessments and audits to identify and remediate any vulnerabilities or weaknesses in the cloud environment. The client organization may have some responsibility to monitor and verify the CSP's performance and compliance with the service level agreement (SLA) and the cloud security standards and regulations, but it does not have direct control or access to the cloud infrastructure and platform. References = Understanding the Shared Responsibilities Model in Cloud Services - ISACA, Figure 1 CISM Review Manual, Chapter 3, page 121

質問**: 55**
緊急システム変更によって生じる混乱のリスクを軽減する最善の方法は次のどれでしょうか?
A. 変更の実装がスケジュールされていることを確認します。
B. 変更要求が承認されたことを確認します。
C. ロールバック計画が実施されていることを確認します。
D. 変更の影響を受けるユーザーに通知します。
正解**: (**正解を表示します**)**
The best way to reduce the risk of disruption from an emergency system change is to confirm rollback plans are in place. According to the CISM Review Manual, having an effective rollback (or backout) plan ensures that if the emergency change causes unexpected issues, the organization can quickly revert to a known, stable state. This minimizes downtime and impact to business operations. Approval and communication are

important, but only a rollback plan directly addresses risk reduction during unexpected disruptions.
Reference:ISACA CISM Review Manual, 16th Edition, Page 210, "Change Management - Rollback Planning".

質問: **56**
組織の情報セキュリティ目標に従業員の行動を合わせるために、最初に検討すべき制御タイプは次のうちどれですか？
A. 技術的なセキュリティ対策
B. アクセスセキュリティ制御
C. 管理セキュリティ制御
D. 物理的なセキュリティ対策
正解: **C (コメントを発表する)**

質問: **57**
情報セキュリティ部門は、ウェアラブルテクノロジーも含まれるようになった最近更新されたBYOD(Bring Your Own Device)ポリシーに対応するため、新しいツールへの投資が必要です。戦略委員会に提出して検討してもらう際に、リスク管理への投資対効果(ROI)を最も効果的に示すのは、次のうちどれでしょうか？
A. ビジネスケース
B. リスク評価
C. リスク監査報告書
D. 事業影響分析(BIA)
正解: **(正解を表示します)**
A business case best demonstrates return on investment in risk management when requesting investment in new tools. In CISM, a business case connects the proposed investment to business objectives, risk reduction, cost, benefits, alternatives, and expected value. For a BYOD policy expanded to include wearable technologies, management needs to understand why new tools are required, what risks they reduce, what costs are involved, and how the investment supports acceptable risk levels. A risk assessment is an important input because it identifies and analyzes risks associated with wearable technologies, but it does not itself demonstrate ROI. A risk audit report provides assurance or findings, not the investment justification. A BIA supports continuity planning and impact prioritization, but it is not the best document for presenting investment value. The strategy committee needs a decision-oriented justification. Therefore, the business case is the best answer because it translates security needs and risk reduction into management-level investment rationale.
References:
ISACA CISM Review Manual, Information Security Program Development and Management - business cases and security investment justification ISACA CISM Exam Content Outline, Domain 3: Information Security Program Development and Management

質問: **58**
インシデント後の調査で、ユーザーの操作ミスが重大な情報漏洩の原因であることが判明しました。調査において最も重要な判断事項は次のうちどれですか？
A. 侵害が発生した日時と場所
B. ユーザーによる過去の事件の証拠
C. ユーザーエラーの根本的な原因
D. ユーザーエラーに対する適切な懲戒手続き
正解: **(正解を表示します)**
The underlying reason for the user error is the most important factor to determine during the post-incident review, as this helps the information security manager to understand the root cause of the breach, and to implement corrective and preventive actions to avoid similar incidents in the future. The underlying reason for the user error may be related to the lack of training, awareness, guidance, or motivation of the user, or to the complexity, usability, or design of the system or process that the user was using. By identifying the underlying reason for the user error, the information security manager can address the human factor of the information security program, and improve the security culture and behavior of the organization. The time and location that the breach occurred, evidence of previous incidents caused by the user, and appropriate disciplinary procedures for user error are not the most important factors to determine during the post-incident review, as they do not provide a comprehensive and holistic understanding of the breach, and may not help to prevent or reduce the likelihood or impact of future incidents. References = CISM Review Manual 2023, page
1671; CISM Review Questions, Answers & Explanations Manual 2023, page 382; ISACA CISM - iSecPrep, page 233

質問: **59**
残存リスクを受け入れるかどうかを決定する際に、最も重要な基準は次のうちどれですか？
A. 資産の交換費用
B. 追加緩和策の費用
C. 年間損失期待値(ALE)
D. 年間発生率
正解: **(正解を表示します)**
= Annual loss expectancy (ALE) is the most important criterion when deciding whether to accept residual risk, because it represents the expected monetary loss for an asset due to a risk over a one-year period. ALE is calculated by multiplying the annual rate of occurrence (ARO) of a risk event by the single loss expectancy (SLE) of the asset. ARO is the estimated frequency of a risk event occurring within a one-year period, and SLE is the estimated cost of a single occurrence of a risk event. ALE helps to compare the cost and benefit of different risk responses, such as avoidance, mitigation, transfer, or acceptance.

Risk acceptance is appropriate when the ALE is lower than the cost of other risk responses, or when the risk is unavoidable or acceptable within the organization's risk appetite and tolerance. ALE also helps to prioritize the risks that need more attention and resources.
References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Assessment, page 831; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question
22, page 242

質問: **60**
ある組織は、アプリケーションの脆弱性によって生じるリスクを軽減するための対策を実施しました。すべての脆弱性が対処された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. 脆弱性評価を実施する
B. 内部監査を実施する
C. 侵入テストを実施する
D. 補償制御の準備
正解: **C (**コメントを発表する**)**
Penetration testing simulates real-world attacks to identify any remaining exploitable vulnerabilities after controls are implemented. It validates that mitigation has been successful from an attacker's perspective.
"Penetration testing is essential to verify the effectiveness of remediation efforts and ensure vulnerabilities can no longer be exploited."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Security Testing and Evaluation* Vulnerability assessments and audits are valuable, but pen testing provides practical assurance.

質問: **61**
セキュリティ手順を文書化しておくべき最も重要な理由は次のうちどれですか？
A. 政策要件の実施を指導する
B. 情報セキュリティ指標の報告プロセスを円滑化するため
C. 標準作業手順に関する規制要件を満たすため
D. ビジネスセキュリティ目標との整合性を示すため
正解: **(**正解を表示します**)**
The most important reason to have documented security procedures is to guide the implementation of policy requirements. In CISM governance, policies define management's high-level expectations, standards define mandatory minimum requirements, and procedures provide the step-by-step instructions needed to execute those requirements consistently. Without documented procedures, employees and operational teams may interpret policy requirements differently, resulting in inconsistent control implementation and increased risk.

Metrics reporting, regulatory support, and demonstrating alignment with business objectives are useful secondary benefits, but they are not the primary purpose of procedures. Procedures operationalize governance by translating policy intent into repeatable actions, enabling accountability, consistency, and effective control execution. CISM emphasizes that an effective information security framework requires a clear hierarchy of policies, standards, procedures, and guidelines to ensure management direction is implemented across the organization. Therefore, documented procedures are essential because they tell personnel how to perform required security activities in alignment with approved policies.
References:
ISACA CISM Review Manual, Information Security Governance - policy, standards, and procedures hierarchy ISACA CISM Exam Content Outline, Domain 2: Information Security Governance

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu **193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **62**
ランサムウェア攻撃の成功リスクを最小限に抑えるための最適なセキュリティ対策は、次のうちどれですか？
A. 申請拒否リスト
B. ウェブセキュリティゲートウェイ
C. ホスト侵入検知システム
D. アプリケーション許可リスト
正解: **(正解を表示します)**
The correct answer is D because application allow listing is one of the most effective preventive controls against ransomware execution. Allow listing permits only approved and authorized applications, scripts, or executables to run, thereby reducing the likelihood that malicious ransomware code can execute on endpoints or servers. An application deny list blocks known malicious applications, but it is less effective because attackers can modify filenames, hashes, or code to bypass known deny rules. A web security gateway can help reduce exposure to malicious downloads, phishing links, and compromised websites, but it does not fully prevent ransomware introduced through other channels. A host intrusion detection system may detect suspicious activity, but detection is reactive and may occur after ransomware has already started execution or encryption. CISM risk management

principles favor preventive controls where feasible, especially for high- impact threats. Since ransomware success often depends on unauthorized code execution, application allow listing provides stronger protection than the other options.
Reference: CISM Information Risk Management; malware prevention, ransomware risk, endpoint controls, and preventive security control principles.

質問: **63**
あるグローバル企業が、本社所在地国よりもデータ保護規制が厳しい国へ事業を拡大する計画を立てています。これらの新たな要件に対応するための最適なアプローチは次のうちどれでしょうか？
A. 新しい国での潜在的な侵害やインシデントをカバーするサイバーセキュリティ保険に加入する。
B. 現地の事業運営が本社の地理データ保護法に準拠していることを確認する。
C. 法務部門と協力して、現地の規制要件を解釈し、適用可能な管理策を実施する。
D. 新しい国の規制に合わせて、組織全体のセキュリティポリシーを調整する。
正解: **(**正解を表示します**)**

質問: **64**
重要インフラにおけるセキュリティ制御のテストの主な目的は次のうちどれですか？
A. セキュリティチームのパフォーマンス上の問題点を特定し、対処する
B. ITサービスの継続的な回復力とセキュリティの確保
C. 本番環境で障害を引き起こすセキュリティ導入の割合を削減する
D. 資源を最適化するために、管理評価の数を削減する
正解: **B (**コメントを発表する**)**
The correct answer is B because the primary objective of testing security controls in critical infrastructure is to ensure that IT services remain secure, resilient, and available. Critical infrastructure supports essential business, public, or operational services, so control failures may have severe consequences. Testing verifies whether controls are designed and operating effectively, whether they reduce risk as intended, and whether they support continuity of critical services. Identifying security team performance issues may be a secondary outcome of testing, but it is not the primary objective. Reducing failed deployments is useful for operational quality, but security control testing focuses on assurance and resilience rather than deployment statistics.
Reducing the number of assessments may save resources, but fewer assessments do not necessarily improve security. In CISM program management, controls must be monitored and tested to ensure they continue to meet control objectives and support business requirements. For critical infrastructure, resilience and security of services are the central goals.
Reference: CISM Information Security Program Development and Management; control testing, critical infrastructure protection, resilience, and service security principles.

質問: **65**
データベース内の情報をどのように分類すべきかを判断するのに最も適任なのは誰でしょうか？
A. データベースアナリスト
B. データベース管理者(DBA)
C. 情報セキュリティアナリスト
D. データ所有者
正解: **(**正解を表示します**)**
= Data owner is the best suited to determine how the information in a database should be classified, because data owner is the person who has the authority and responsibility for the data and its protection. Data owner is accountable for the business value, quality, integrity, and security of the data. Data owner also defines the data classification criteria and levels based on the data sensitivity, criticality, and regulatory requirements.
Data owner assigns the data custodian and grants the data access rights to the data users. Data owner reviews and approves the data classification policies and procedures, and ensures the compliance with them.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:
Data Classification, page 331

質問: **66**
次のうち、Webアプリケーションファイアウォールの主な機能はどれですか？
A. 悪意のあるトラフィックに基づいて、事前定義された設定を自動的に変更する
B. プライベートネットワーク内での外部トラフィックの制限
C. 分散型サービス拒否攻撃のリダイレクト
D. 受信ハイパーテキスト転送プロトコルトラフィックのフィルタリング
正解: **D (**コメントを発表する**)**
The correct answer is D because the primary function of a web application firewall is to inspect, filter, and block malicious HTTP and HTTPS traffic directed at web applications. A WAF is specifically designed to protect web applications from attacks such as SQL injection, cross-site scripting, malicious requests, and protocol abuse. It operates at the application layer and evaluates web requests and responses based on rules, signatures, behavior, and application-specific policies. Automatically modifying its configuration may be a feature of some advanced adaptive tools, but it is not the main defining feature of a WAF. Restricting external traffic within a private network is more closely related to network firewalls or segmentation controls.
Redirecting distributed denial-of-service attacks is usually handled by DDoS protection services, content delivery networks, or traffic scrubbing solutions. In CISM terms, the correct control must match the risk and technology layer being protected. Since a WAF protects web applications by filtering web traffic, option D is the best answer.

Reference: CISM Information Security Program Development and Management; technical security controls, application protection, and web application security principles.

質問: **67**
予算が限られている小規模組織が新しい情報セキュリティマネージャーを雇用したところ、同じITスタッフがシステム管理者、セキュリティ管理者、データベース管理者(DBA)、およびアプリケーション管理者の責任を兼任していることが分かりました。マネージャーにとって最善の行動は何でしょうか？
A. ユーザープロビジョニング活動を厳格に管理する。
B. IT管理者の活動を監視する。
C. IT管理者の活動を正式に文書化する。
D. ユーザープロビジョニング活動を自動化する。
正解: **B (**コメントを発表する**)**

質問: **68**
組織が情報セキュリティガバナンスをコーポレートガバナンスと統合していることを示す最も適切な指標は、次のうちどれですか？
A. セキュリティパフォーマンス指標は、ビジネス目標に対して測定されます。
B. ITリスクを評価する際、影響は事業損失に基づいて測定されます。
C. セキュリティポリシーは、事業目標が変更されるたびに見直されます。
D. セキュリティベンダーのサービスレベルは、ビジネスニーズに応じて定義されます。
正解: **(**正解を表示します**)**
Security performance metrics are quantitative or qualitative measures that indicate the effectiveness and efficiency of the information security program in achieving the organization's security goals and objectives.
Measuring security performance metrics against business objectives is the best indication that an organization has integrated information security governance with corporate governance, as it demonstrates that the security program is aligned with and supports the business strategy, value delivery, and risk management. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 37, section 1.3.2.2.

質問: **69**
ある組織が人事管理プロセスに情報セキュリティを統合したいと考えています。最初のステップとして取るべきなのは次のうちどれでしょうか？
A. ベストプラクティスと比較してプロセスをベンチマークし、ギャップを特定します。
B. 投資収益率(ROI)を計算します。
C. 人事部にセキュリティ意識向上トレーニングを実施する。
D. プロセスのビジネス目標を評価する。
正解: **(**正解を表示します**)**

The first step when integrating information security into HR management processes is to assess the business objectives of the processes, which means understanding the purpose, scope, and expected outcomes of the HR functions and activities, and how they relate to the organization's strategy and goals. The assessment will help to identify the information security requirements, risks, and controls that are relevant and applicable to the HR processes, and to align the information security objectives with the business objectives. References = CISM Review Manual 15th Edition, CISM: Overview of domains [updated 2022]

質問: **70**
情報セキュリティマネージャーが、組織のワークステーションを新しいオペレーティングシステムバージョンにアップグレードしたいと考えています。アップグレードに対する上級管理職の支持を得るために、次のうちどれが最も役立つでしょうか？
A. リスクに基づいた現行オペレーティングシステムの評価
B. 新オペレーティングシステムにおけるパフォーマンス改善点の概要
C. 現在のオペレーティングシステムに問題があることを示すユーザー調査の結果
D. 新しいオペレーティングシステムの最新セキュリティ機能一覧
正解: **(**正解を表示します**)**
An assessment of the current operating system based on risk (A) is most effective for gaining senior management support because CISM emphasizes risk-based decision-making at the executive level. Senior management is primarily concerned with exposure, potential impact, and alignment with risk appetite-not technical features or user convenience. Performance improvements (B), user surveys (C), and feature lists (D) provide supporting detail but do not clearly articulate business risk. A risk-based assessment demonstrates why the upgrade is necessary to reduce unacceptable risk. References: ISACA CISM Review Manual (Governance-executive communication, risk-based justification); CISM Exam Content Outline (Domain 2).

質問: **71**
規制の厳しい環境下で情報セキュリティ対策のビジネスケースを作成する際に、最初に行うべきことは次のうちどれですか？
A. 競合他社との比較
B. 法律顧問に相談する
C. 実現可能性調査を実施する
D. リスク評価を実施する
正解: **D (**コメントを発表する**)**
The correct answer is D because a business case for an information security initiative should first be based on risk. Conducting a risk assessment identifies the threats, vulnerabilities, likelihood, business impact, regulatory exposure, control gaps, and potential consequences that justify the initiative. In a highly regulated environment, legal and

compliance obligations are important inputs, but the business case should still be driven by risk to the organization, including compliance risk. Benchmarking against competitors may provide context, but it does not define the organization's specific need. Consulting legal counsel may be necessary to interpret regulatory obligations, but it is not as complete as a risk assessment for developing a business case.
A feasibility study is useful after the need and risk have been established. CISM emphasizes that security investments should be risk-based, business-aligned, and cost-justified. Therefore, the first step is to conduct a risk assessment to support the business case.
Reference: CISM Information Risk Management; risk assessment, business case development, regulatory risk, cost justification, and security investment principles.

質問**: 72**
情報セキュリティプログラムを成功させる上で、最も重要な要素は次のうちどれですか？
A. このプログラムは業界のベストプラクティスに準拠しています。
B. このプログラムは、綿密に練られた戦略に基づいています。
C. このプログラムは費用対効果が高く、予算内です。
D. このプログラムはリスク管理に重点を置いています。
正解**: (**正解を表示します**)**
A successful information security program is one that aligns with the business objectives and strategy, supports the business processes and functions, and protects the information assets from threats and vulnerabilities. The most important factor of such a program is that it is focused on risk management, which means that it identifies, assesses, treats, and monitors the information security risks that could affect the business continuity, reputation, and value. Risk management helps to prioritize the security activities and resources, allocate the appropriate budget and resources, implement the necessary controls and measures, and evaluate the effectiveness and efficiency of the program. Risk management also enables the program to adapt to the changing business and threat environment, and to continuously improve the security posture and performance. A program that follows industry best practices, is based on a well-developed strategy, and is cost-efficient and within budget are all desirable attributes, but they are not sufficient to ensure the success of the program without a risk management focus. References = CISM Review Manual 15th Edition, page 411; CISM Practice Quiz, question 1242

質問**: 73**
情報セキュリティガバナンスプログラムに対する経営陣のコミットメントを得る上で最も重要な要素は次のとおりです。
A. 定義されたセキュリティフレームワーク。
B. プロセス改善モデル
C. 確立されたセキュリティ戦略。

D. 特定されたビジネス推進要因。
正解: **(**正解を表示します**)**
The most important element in achieving executive commitment to an information security governance program is to align the program with the identified business drivers of the organization. Business drivers are the factors that influence the strategic objectives, goals, and priorities of the organization. They reflect the needs and expectations of the stakeholders, customers, regulators, and other parties that are relevant to the organization's mission and vision. By aligning the information security governance program with the business drivers, the executive can demonstrate the value and benefits of information security to the organization's performance, reputation, and competitiveness. The other options are not the most important element, although they may be part of an information security governance program. A defined security framework is a set of standards, guidelines, and best practices that provide a structure and direction for implementing information security. A process improvement model is a methodology that helps to identify, analyze, and improve the processes related to information security. Established security strategies are the plans and actions that define how information security supports and enables the business objectives and goals. These elements are important for developing and executing an information security governance program, but they do not necessarily ensure executive commitment unless they are aligned with the business drivers

質問: **74**
セキュリティ意識向上プログラムを組織のビジネス戦略に整合させる際に、最も重要な考慮事項は次のうちどれですか？
A. 規制と基準
B. 人々と文化
C. 経営陣および取締役会の指示
D. プロセスと技術
正解: **B (**コメントを発表する**)**
A security awareness program is a set of activities designed to educate and motivate employees to adopt secure behaviors and practices. A security awareness program should be aligned with the organization's business strategy, which defines the vision, mission, goals and objectives of the organization. The most important factor to consider when aligning a security awareness program with the business strategy is the people and culture of the organization, because they are the primary target audience and the key enablers of the program. The people and culture of the organization influence the level of awareness, the attitude and the behavior of the employees towards information security. Therefore, a security awareness program should be tailored to the specific needs, preferences, values and expectations of the people and culture of the organization, and should use appropriate methods, channels, messages and incentives to engage and influence them. A security awareness program that is aligned with the people and culture of the organization will have

a higher chance of achieving its objectives and improving the overall security posture of the organization.
References =
CISM Review Manual 15th Edition, page 1631
CISM 2020: Information Security & Business Process Alignment, video 22

質問: **75**
以下のバックアップ方法のうち、アプリケーションのデータ復元に最も時間がかかるのはどれですか？
A. フルバックアップ
B. インクリメンタル
C. 微分
D. ディスクミラーリング
正解: **(**正解を表示します**)**
= An incremental backup method only backs up the data that has changed since the last backup, whether it was a full or an incremental backup. This method requires the least amount of time and storage space for backup, but it requires the most time to restore data for an application. To restore data from an incremental backup, the latest full backup and all the subsequent incremental backups are needed. A full backup method backs up all the data in a system or an application at a point in time. This method requires the most amount of time and storage space for backup, but it requires the least time to restore data for an application. To restore data from a full backup, only the latest full backup is needed. A differential backup method backs up the data that has changed since the last full backup. This method requires more time and storage space for backup than the incremental method, but less than the full backup method. It also requires less time to restore data for an application than the incremental method, but more than the full backup method. To restore data from a differential backup, the latest full backup and the latest differential backup are needed. A disk mirroring method creates an exact copy of a disk on another disk in real time. This method provides the highest level of availability and fault tolerance, but it also requires twice the amount of disk space. To restore data from a disk mirroring method, the mirrored disk can be used as the primary disk in case of a failure. References = CISM Review Manual 15th Edition, page 201-202.
The method that requires the MOST time to restore data for an application is a Full Backup. Full backups contain all the data that is required to restore an application, but the process of restoring the data is the most time-consuming as it involves copying all the data from the backup to the application. Incremental backups only backup the changes made since the last backup, differential backups only backup changes made since the last full backup, and disk mirroring provides real-time data replication, so the data is immediately available.

質問: **76**

組織内に高度な技術的フォレンジック調査を実施するための専門知識が不足している場合、情報セキュリティインシデント発生後に効果的かつ迅速な調査を確実に行うための最善の方法は何でしょうか？
A. 事件が発生する前に鑑識会社を雇う。
B. インシデント対応ポリシーでフォレンジック会社を雇うことが認められていることを確認してください。
C. 鑑識標準作業手順書を購入する。
D. 情報セキュリティチームにフォレンジック研修を提供する。
正解: **B** (コメントを発表する)

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu **193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **77**
組織文化が情報セキュリティプログラムの有効性に及ぼす主な影響は、次のうちどれですか？
A. 文化は情報セキュリティに対する行動を形成する。
B. 文化は、プログラム実施に必要な責任を定義する。
C. 文化は情報セキュリティ対策の予算を決定するのに役立ちます。
D. 情報セキュリティ管理が遵守されている限り、文化の影響は最小限です。
正解: **A** (コメントを発表する)
A culture that supports security encourages behaviors that protect information assets.
"Organizational culture has a significant impact on how employees approach security, influencing their behavior and adherence to policies."
- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Security Culture*

質問: **78**
情報セキュリティ管理者は、情報資産管理プログラムをレビューする際に、まず何を検証すべきでしょうか？
A. システム所有者が特定されました。
B. 重要なアプリケーションが確保されました。
C. 情報資産は分類されています。
D. 情報資産の目録が作成されました。

正解: (正解を表示します)
According to the CISM Review Manual, information asset classification is the first step in an information asset management program, as it provides the basis for determining the level of protection required for each asset. System owners, key applications and information asset inventory are subsequent steps that depend on the classification of the assets.
References = CISM Review Manual, 27th Edition, Chapter 1, Section 1.4.2, page 381.

質問: **79**
標準的なセキュリティ構成を導入する主な目的は何ですか？
A. サポート対象外のシステムに対する潜在的なリスクを軽減するために、柔軟なアプローチを維持する。
B. サポート対象外システムの管理および監視に伴う運用上の負担を最小限に抑える。
C. 脆弱性を制御し、構成変更による脅威を軽減します。
D. サポート対象システムとサポート対象外システムの構成を比較します。
正解: (正解を表示します)
The primary objective of implementing standard security configurations is to control vulnerabilities and reduce threats from changed configurations. Standard security configurations are the baseline settings and parameters that define the desired security level and functionality of information systems and devices. By implementing standard security configurations, the organization can ensure that the information systems and devices are configured in a consistent and secure manner, and that any deviations or changes from the standard are detected and corrected. This can help to prevent or mitigate potential security incidents caused by misconfigurations, unauthorized modifications, or malicious attacks.
References: The CISM Review Manual 2023 states that "the information security manager is responsible for ensuring that the security configuration of information systems is in compliance with the security policies and standards of the organization" and that "the information security manager should establish and implement standard security configurations for information systems and devices, and monitor and review the security configuration on a regular basis and take corrective actions when deviations or violations are detected" (p.
138). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Control vulnerabilities and reduce threats from changed configurations is the correct answer because it is the primary objective of implementing standard security configurations, as it helps to maintain the security posture and functionality of information systems and devices, and to prevent or mitigate potential security incidents caused by misconfigurations, unauthorized modifications, or malicious attacks" (p. 63). Additionally, the article Standard Security Configurations from the ISACA Journal 2017 states that "standard security configurations are the baseline settings and

parameters that define the desired security level and functionality of information systems and devices" and that "standard security configurations can help to control vulnerabilities and reduce threats from changed configurations by ensuring that the information systems and devices are configured in a consistent and secure manner, and that any deviations or changes from the standard are detected and corrected" (p. 1)

質問: **80**
データ損失防止(DLP)ソリューションを導入する主なメリットは以下のとおりです。
A. 組織のウイルス対策を強化する。
B. データ損失のリスクを排除します。
C. 組織の探偵管理を補完する。
D. セキュリティ意識向上プログラムの必要性を軽減する。
正解: **(正解を表示します)**
A data loss prevention (DLP) solution is a type of detective control that monitors and prevents unauthorized transmission or leakage of sensitive data from the organization. A DLP solution can enhance the organization' s antivirus controls by detecting and blocking malicious code that attempts to exfiltrate data, but this is not its main benefit. A DLP solution cannot eliminate the risk of data loss, as there may be other sources of data loss that are not covered by the DLP solution, such as physical theft, accidental deletion, or natural disasters. A DLP solution also does not reduce the need for a security awareness program, as human factors are often the root cause of data loss incidents. A security awareness program can educate and motivate employees to follow security policies and best practices, and to report any suspicious or anomalous activities. References = ISACA, CISM Review Manual, 16th Edition, 2020, page 79.
ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1003.

質問: **81**
組織の自動セキュリティ監視ツールが、過剰に大量の誤検知を生成しています。監視プロセスを最適化するための最適な方法は次のうちどれですか？
A. 重大なアラートのみを報告します。
B. 変更報告のしきい値。
C. ログ記録を再設定します。
D. 特定の時間枠内で発生した事象を監視します。
正解: **(正解を表示します)**
Changing reporting thresholds is the best method to optimize the monitoring process when the automated security monitoring tool generates an excessively large amount of false positives. Changing reporting thresholds means adjusting the criteria or parameters that trigger the alerts, such as the severity level, the frequency, the source, or the destination of the events. Changing reporting thresholds can help to reduce the number of false

positives, filter out the irrelevant or benign events, and focus on the most critical and suspicious events that require further investigation or response.
References = Cybersecurity tool sprawl leading to burnout, false positives: report, Security tools' effectiveness hampered by false positives

質問: **82**
情報セキュリティマネージャーが取締役会に伝えるべき最も重要な内容は次のうちどれですか？
A. 脆弱性評価
B. 露出レベル
C. 固有リスクのレベル
D. 脅威評価
正解: **(**正解を表示します**)**

質問: **83**
セキュリティインシデントを分類する最も重要な理由は以下のとおりです。
A. インシデント解決の効率と効果を向上させる。
B. セキュリティイベントとインシデントのログ記録をより適切に管理する。
C. インシデント対応計画を企業方針に合わせる。
D. インシデントリーダーへのインシデント状況の報告を強化する。
正解: **(**正解を表示します**)**
The correct answer is A because incident classification enables the organization to prioritize, escalate, assign, and resolve incidents efficiently and effectively. Classification helps determine severity, business impact, required response time, communication needs, legal or regulatory involvement, evidence handling, and appropriate containment actions. Without classification, all incidents may be treated the same, which can waste resources on low-risk events or delay response to high-impact incidents. Better logging is useful, but it is not the most important reason for classification. Aligning the incident response plan with corporate policy is important during plan development, not the primary purpose of classifying individual incidents. Reporting incident status to the incident lead may be improved through classification, but that is a supporting benefit.
CISM incident management principles emphasize that incidents must be identified, categorized, prioritized, escalated, and resolved based on business impact and risk. Proper classification ensures that resources are directed to the most important incidents and that response actions are appropriate.
Reference: CISM Information Security Incident Management; incident classification, prioritization, escalation, severity, and resolution principles.

質問: **84**
脆弱性スキャナーが不完全な結果を返す最も可能性の高い理由は次のうちどれですか？

A. ゼロデイ脆弱性のシグネチャが取り込まれていません。
B. スキャン結果はセキュリティ情報およびイベント管理(SIEM)ツールに取り込まれません。
C. 認証なしの脆弱性スキャンが実行されています。
D. ホスト名が完全に列挙されていません。
正解: **C** (コメントを発表する)

質問: **85**
ある組織が、新たな先端技術への投資を検討しています。情報セキュリティマネージャーがその影響を評価する際に、最も重要な考慮事項は次のうちどれでしょうか？
A. システム互換性
B. 当該技術に関する業界関係者による評価
C. 安全な構成
D. 技術の脆弱性
正解: **D** (コメントを発表する)

質問: **86**
ある組織は、重要なアプリケーションのセキュリティ脆弱性を修正するには費用がかかりすぎるため現実的ではないと判断したが、その影響は事業にとって重大である。次のうち、最も適切なリスク対策はどれか？
A. アプリケーションの継続使用に伴うリスクを受け入れる。
B. アプリケーションの使用を中止してください。
C. アプリケーションに対する補償制御を実装します。
D. サイバーセキュリティ保険に加入してください。
正解: (正解を表示します)

質問: **87**
情報セキュリティマネージャーは、組織の給与処理業務を外部委託する際の契約に関するセキュリティ上の観点からのガイダンスを提供するよう依頼されました。以下のうち、対処すべき最も重要な事項はどれですか？
A. ベンダーが最も厳格なデータセキュリティ規制を遵守していること
B. ベンダーが業界で認められたセキュリティ基準に準拠していること
C. ベンダーが組織の情報セキュリティポリシーを遵守していること
D. ベンダーが組織のサービスレベル契約要件を遵守していること
正解: (正解を表示します)
The correct answer is C because an outsourced payroll provider will process sensitive employee information, and the contract must require the vendor to comply with the organization's information security policies or equivalent security requirements. Payroll data may include personally identifiable information, salary details, tax information, bank account data, and employment records. The organization remains accountable for

protecting this information even when processing is outsourced. Recognized industry standards are useful, but they may not fully reflect the organization's specific policy requirements, risk appetite, privacy obligations, access rules, incident notification needs, or data handling expectations. The most stringent regulations may not always be applicable, and contract requirements should be based on relevant legal, regulatory, and organizational obligations. Service level agreements are important for performance and availability, but they do not fully address security governance. In CISM third-party risk management, contracts should include security requirements aligned with organizational policies, compliance obligations, audit rights, confidentiality, incident reporting, and control expectations. Therefore, vendor compliance with the organization's information security policies is most important.
Reference: CISM Information Risk Management; third-party risk, outsourcing, payroll data protection, contractual security requirements, and vendor compliance principles.

質問: **88**
既存の管理体制がコンプライアンス要件を満たし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. 独立監査の実施
B. コンプライアンス指標の設定
C. セキュリティポリシーの見直し
D. リスク評価の実施
正解: **(正解を表示します)**
The correct answer is A because independent audits provide objective assurance that existing controls meet compliance requirements. Independent auditors can evaluate whether controls are appropriately designed, implemented, documented, and operating effectively against regulatory, contractual, or policy requirements.
Establishing compliance metrics is useful for monitoring trends and reporting status, but metrics may not provide sufficient independent validation. Reviewing security policies confirms whether requirements are documented, but it does not prove that controls are operating effectively. Performing risk assessments helps identify and evaluate risk, but risk assessment is not the same as compliance assurance. In CISM governance, independent assurance is important because management needs reliable evidence that controls are effective and obligations are being met. Audits also help identify gaps, exceptions, and remediation needs. Because compliance requires evidence and objective evaluation, independent audits provide the greatest assurance among the listed options.
Reference: CISM Information Security Governance; independent assurance, compliance audits, control effectiveness, and governance oversight principles.

質問: **89**

インシデントハンドラーがハードドライブのフォレンジックイメージを準備しています。このイメージがオリジナルの完全なコピーであることを証明するには、以下のどれを必ず実行する必要がありますか？
A. ファイル数の手動検証を実行します。
B. イメージにはオリジナルと同じハードウェアを使用します。
C. コピーする前にハードドライブを暗号化してバックアップします。
D. オリジナルと画像のデジタル ハッシュを実行します。
正解: **(**正解を表示します**)**

質問: **90**
情報セキュリティポリシーの策定に最も大きな影響を与えるべき要素はどれでしょうか？
A. ビジネス戦略
B. 過去および現在の脅威
C. ITセキュリティフレームワーク
D. 業界標準
正解: **(**正解を表示します**)**
Business strategy is the overarching driver for any organizational initiative, including security. Information security policies must align with the strategic goals of the organization to ensure relevance, support, and effectiveness.
Security policies that do not consider the business context may hinder operations or fail to protect key objectives. Business-driven policies are more likely to gain executive support and compliance from stakeholders, creating a strong foundation for governance.
"Information security policies must be aligned with business goals and objectives to ensure that they support the overall mission and are embraced by stakeholders."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Strategy Alignment*

質問: **91**
以下の指標のうち、組織のセキュリティ意識向上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. マルウェアに感染した従業員のコンピュータおよびデバイスの割合
B. エンドユーザーが閲覧したフィッシングメールの数
C. ヘルプデスクに報告されたセキュリティインシデントの件数
D. 定期的にセキュリティ研修に参加している従業員の割合
正解: **(**正解を表示します**)**

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

す。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu ↾**193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **92**
重大なシステム障害が報告された場合、インシデント対応担当者が最初に行うべきことは以下のとおりです。
A. 関係者に通知する
B. 事件の範囲を特定する
C. インシデントを検証する
D. システムの電源を切る
正解: **C** (コメントを発表する)
The correct answer is C because the first step after an incident is reported is to validate whether the reported event is actually an incident. Validation helps prevent unnecessary escalation, disruption, or incorrect response actions. The incident handler should confirm the event by reviewing available evidence, logs, alerts, user reports, system behavior, or other indicators. After validation, the handler can classify the incident, determine severity, assess scope, notify appropriate parties, and begin containment or eradication according to the incident response plan. Notifying parties before validation may cause confusion or unnecessary escalation.
Determining scope is important, but it should occur after confirming that an incident exists. Powering off the system may destroy volatile evidence, disrupt business operations, or worsen the situation if done without analysis. CISM incident management principles require orderly identification, validation, classification, escalation, and response. Therefore, validating the incident is the correct first action for the incident handler.
Reference: CISM Information Security Incident Management; incident identification, validation, classification, escalation, and response handling principles.

質問: **93**
ビジネスインパクト分析(BIA)BESTは、組織が以下のことを確立することを可能にします。
A. 復旧の優先順位。
B. 復旧方法
C. 年間損失期待値(ALE)。
D. 総所有コスト(TCO)。
正解: **A** (コメントを発表する)

質問: **94**
経営陣の支援と事業との連携に加え、情報セキュリティガバナンスにとって最も重要な要素は次のうちどれですか？

A. セキュリティの所有権
B. 方針の遵守
C. システムの監査可能性
D. 研修資源の配分
正解: **A** (コメントを発表する)
Information security governance is the process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations. In addition to executive sponsorship and business alignment, a critical factor for effective information security governance is ownership of security, which means that the roles and responsibilities for information security are clearly defined and assigned to the appropriate stakeholders, such as business owners, information owners, information custodians, and users. Ownership of security also implies accountability for the protection of information assets and the management of security risks.
References: https://www.isaca.org/credentialing/cism
https://www.nist.gov/publications/information-security- handbook-guide-managers

質問: **95**
新たに導入されたプライバシー規制が事業に影響を与える場合、情報セキュリティマネージャーが最初にとるべき行動は次のうちどれでしょうか？
A. ITスタッフと相談し、彼らの推奨事項に基づいてリスクを評価する。
B. 規制要件に基づいてセキュリティポリシーを更新する
C. 事業が規制を遵守することを確実にするための適切な管理策を提案する
D. 事業目標の観点からリスクを特定し、評価する
正解: (正解を表示します)
Identify and assess the risk in the context of business objectives. Before making any changes to the security policy or introducing any new controls, the information security manager should first identify and assess the risk that the new privacy regulation poses to the business. This should be done in the context of the overall business objectives so that the security measures introduced are tailored to meet the specific needs of the organization.

質問: **96**
組織の情報セキュリティ文化を向上させるために、経営陣にとって最も重要なことは以下のとおりです。
A. セキュリティポリシーを承認する
B. セキュリティ予算とリソースの見直し
C. セキュリティ研修に参加する
D. 優れたセキュリティ対策を実践する
正解: **D** (コメントを発表する)

The correct answer is D because security culture is strongly influenced by leadership behavior. Senior management must set the tone from the top by consistently demonstrating good security practices, following policies, supporting security initiatives, and making risk-aware decisions. Employees are more likely to adopt secure behavior when they see executives and managers treating security as a business priority. Approving security policies is important, but approval alone does not create culture unless leaders also model expected behavior. Reviewing budget and resources supports the program, but it does not directly shape everyday security behavior. Participating in security training is positive and visible, but demonstrating good security practices on an ongoing basis has a broader cultural impact. In CISM governance, management commitment, accountability, communication, and example-setting are essential for embedding information security into the organization's values and operations. Therefore, leadership behavior is the most important factor in improving information security culture.
Reference: CISM Information Security Governance; security culture, tone at the top, senior management commitment, and organizational behavior principles.

質問: **97**
ある組織がシステムのセキュリティ上の欠陥を修正しました。次に取るべき行動は次のうちどれですか？
A. 残存リスクを評価する。
B. 組織内で得られた教訓を共有する。
C. システムのドキュメントを更新します。
D. 侵入テストのための予算を割り当てる。
正解: **(正解を表示します)**
Residual risk is the risk that remains after applying controls to mitigate the original risk. It is important to assess the residual risk after remediation to ensure that it is within the acceptable level and tolerance of the organization. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 181, section 4.3.2.4.

質問: **98**
情報セキュリティガバナンス委員会の主な責任は次のうちどれですか？
A. 月次の情報セキュリティ指標のレビュー
B. 情報セキュリティリスク登録簿の見直し
C. 情報セキュリティ戦略の変更を承認する
D. 今後の情報セキュリティプロジェクトについて話し合う
正解: **(正解を表示します)**

質問: **99**
クラウドサービスに関する新たな規制要件の影響を判断するために、最初に行うべきことは次のうちどれですか？

A. リスク評価を実施する
B. 情報資産目録を確認する。
C. 適用性を判断する。
D. ギャップ分析を実施する。
正解: **(**正解を表示します**)**
The correct answer is C because before assessing impact, performing a gap analysis, or conducting a risk assessment, the organization must first determine whether the new regulatory requirement applies to its cloud services, data, jurisdictions, customers, industry, and processing activities. Applicability establishes whether the regulation is relevant and which systems, processes, contracts, business units, or data types are in scope. A risk assessment is important after applicability is confirmed, but performing it too early may waste resources or miss the correct scope. Reviewing the asset inventory may support scoping, but it should follow or support the applicability analysis. A gap analysis compares current practices against requirements, but this cannot be done properly until the organization confirms that the requirement applies and understands its scope. CISM risk management emphasizes identifying legal, regulatory, and contractual obligations as part of risk and compliance management. Therefore, determining applicability is the first step in understanding the impact of a new regulatory requirement.
Reference: CISM Information Risk Management; regulatory compliance, cloud risk, applicability analysis, and risk assessment scoping principles.

質問: **100**
ある組織では、災害発生時にビジネスクリティカルなアプリケーションを30分以内に復旧することが求められています。この要件を満たすために、事業継続計画（BCP）に組み込むべき指標は次のどれですか。
A. 最大許容ダウンタイム（MTD）
B. サービスレベル契約（SLA）
C. 復旧ポイント目標 (RPO)
D. 復旧時間目標（RTO）
正解: **(**正解を表示します**)**
The Recovery Time Objective (RTO) defines the maximum acceptable downtime for a business function or system following a disruption. If the organization requires recovery in 30 minutes, that is the system's RTO.
This metric guides the selection of technologies, staffing, and procedures needed to meet recovery expectations.
"RTO defines the target time set for the recovery of IT and business activities after a disruption. It is a key BCP design parameter."
- CISM Review Manual 15th Edition, Chapter 3: Business Continuity and Disaster Recovery Planning*

質問: **101**
情報セキュリティマネージャーは、サードパーティプロバイダーが作業範囲記述書(SOW)を遵守していないことに気づきました。次のうち、最も適切な対応策はどれですか？
A. 上級管理職にこの問題を報告してください。
B. 問題を法務担当者に報告してください。
C. 契約再交渉を開始する。
D. 問題の深刻度を評価する。
正解: **(正解を表示します)**
The first course of action when the information security manager becomes aware that a third-party provider is not in compliance with the SOW is to assess the extent of the issue, which means determining the nature, scope, and impact of the non-compliance on the security of the enterprise's data and systems. The assessment should also identify the root cause of the non-compliance and the possible remediation actions. The assessment will help the information security manager to decide the next steps, such as notifying senior management, reporting the issue to legal personnel, initiating contract renegotiation, or terminating the contract.
References = Ensuring Vendor Compliance and Third-Party Risk Mitigation, A Risk-Based Management Approach to Third-Party Data Security, Risk and Compliance

質問: **102**
BYOD (個人所有デバイスの持ち込み) プログラムに関連するリスクを軽減する最善の方法は次のどれですか?
A. 従業員に効果的なマルウェア対策アプリのインストールを義務付けます。
B. 安全なモバイル デバイスの運用方法について従業員にトレーニングを提供します。
C. モバイル デバイス管理 (MDM) ソリューションを実装します。
D. モバイル デバイスのポリシーと標準を実装します。
正解: **(正解を表示します)**

質問: **103**
情報セキュリティ管理者は、パッチを適用できないWeb接続型のレガシーアプリケーション上のデータを保護するための選択肢を検討しています。以下のうち、補償制御の有効性について最も適切な情報を提供するものはどれでしょうか？
A. 脅威評価
B. 侵入検知システムのログ
C. 侵入テスト
D. ファイアウォールルール
正解: **(正解を表示します)**
The correct answer is C because penetration testing provides practical evidence of whether compensating controls can resist real-world attack techniques against the legacy application. When an application cannot be patched, compensating controls such as web

application firewalls, network segmentation, access restrictions, monitoring, or virtual patching may be used to reduce risk. However, the effectiveness of those controls should be validated through testing that simulates attacker behavior. A threat assessment identifies potential threats, but it does not prove whether controls are working. Intrusion detection system logs may show detected activity, but they provide only a partial and reactive view. Firewall rules can be reviewed, but rule review alone does not demonstrate whether the total control environment prevents exploitation. Penetration testing is more useful because it tests the application and compensating controls together under realistic conditions. CISM emphasizes risk-based control validation, especially where vulnerabilities cannot be remediated directly. Therefore, penetration testing provides the best information about compensating control effectiveness.
Reference: CISM Information Risk Management; compensating controls, vulnerability management, penetration testing, and control effectiveness principles.

質問**: 104**
組織のサイバーセキュリティプログラムがビジネスニーズを満たすことを確実にするために、以下のうちどれを最も重要視すべきでしょうか？
A. リスク評価プログラム
B. 情報セキュリティ意識向上トレーニング
C. 情報セキュリティガバナンス
D. 情報セキュリティ指標
正解**: (**正解を表示します**)**
= Information security governance is the process of establishing and maintaining the policies, standards, frameworks, and best practices that guide the information security program of an organization. Information security governance helps to ensure that the information security program meets the needs of the business by aligning it with the organization's risk appetite, objectives, and strategy. Information security governance also helps to coordinate and integrate various assurance functions, such as risk management, compliance, audit, and incident response, to provide a holistic view of the information security posture. Information security governance is essential for achieving a positive return on investment (ROI) from information security investments, as well as for enhancing the trust and confidence of internal and external stakeholders. References = CISM Review Manual (Digital Version), Chapter 1: Introduction to Information Security Management, Section 1.1: Overview of Information Security Management1. CISM Review Manual (Print Version), Chapter 1: Introduction to Information Security Management, Section 1.1: Overview of Information Security Management2. CISM ITEM DEVELOPMENT GUIDE, Domain 1: Information Security Governance, Task Statement 1.1, p. 193.
Information security governance is MOST important to have in place to help ensure an organization's cybersecurity program meets the needs of the business. This is because information security governance provides the strategic direction, oversight and accountability for the cybersecurity program. It also ensures that the program aligns with

the business objectives, risk appetite and compliance requirements of the organization. Information security governance involves defining roles and responsibilities, establishing policies and standards, setting goals and metrics, allocating resources and monitoring performance of the cybersecurity program.

質問**: 105**
一般的なIaaS(Infrastructure as a Service)モデルにおける以下のサービス提供のうち、クラウドサービスプロバイダーがセキュリティインシデントからの復旧時に顧客を支援するのに最も適しているのはどれでしょうか？
A. Webアプリケーションファイアウォールログの可用性。
B. オンライン仮想マシン解析機能
C. 最新のインフラストラクチャドキュメントの入手可能性
D. 仮想マシンのスナップショットを取得する機能
正解**: D (**コメントを発表する**)**
A snapshot is a point-in-time copy of the state of a virtual machine (VM) that can be used to restore the VM to a previous state in case of a security incident or a disaster. A snapshot can capture the VM's disk, memory, and device configuration, allowing for a quick and easy recovery of the VM's data and functionality.
Snapshots can also be used to create backups, clones, or replicas of VMs for testing, analysis, or migration purposes. Snapshots are a common service offering in Infrastructure as a Service (IaaS) models, where customers can provision and manage VMs on demand from a cloud service provider (CSP). A CSP that offers the capability to take snapshots of VMs can assist customers when recovering from a security incident by providing them with the following benefits12:
Faster recovery time: Snapshots can reduce the downtime and data loss caused by a security incident by allowing customers to quickly revert their VMs to a known good state. Snapshots can also help customers avoid the need to reinstall or reconfigure their VMs after an incident, saving time and resources.
Easier incident analysis: Snapshots can enable customers to perform online or offline analysis of their VMs after an incident, without affecting the production environment. Customers can use snapshots to examine the VM's disk, memory, and logs for evidence of compromise, root cause analysis, or forensic investigation.
Customers can also use snapshots to test and validate their incident response plans or remediation actions before applying them to the production VMs.
Enhanced security posture: Snapshots can improve the security posture of customers by enabling them to implement best practices such as backup and restore, disaster recovery, and business continuity. Snapshots can help customers protect their VMs from accidental or malicious deletion, corruption, or modification, as well as from environmental or technical disruptions. Snapshots can also help customers comply with regulatory or contractual requirements for data retention, availability, or integrity. References = What is

Disaster Recovery as a Service? | CSA - Cloud Security Alliance, What Is Cloud Incident Response (IR)?
CrowdStrike

質問: **106**
次のうち、インシデント発生後のレビュー活動において最も重要な目的はどれですか？
A. 証拠収集
B. 継続的な改善
C. インシデントトリアージ
D. インシデント記録
正解: **B (**コメントを発表する**)**
The primary goal of post-incident review (PIR) is continuous improvement. After an incident has been contained, eradicated, and systems recovered, a formal review helps identify:
What went wrong or could have been done better
What controls failed or were missing
How the response process can be improved
The goal is not only to learn from the incident but also to enhance incident response capabilities, update plans, and prevent future occurrences.
"Post-incident reviews are a key activity for improving incident response processes. The goal is continuous improvement and prevention of repeat incidents."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Post-Incident Activities* While incident documentation and evidence collection are components of the process, they are supportive to the broader strategic objective: learning and improving the overall security posture.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu 問**193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **107**
情報セキュリティチームが、既存ベンダーのセキュリティ評価を計画しています。評価範囲を適切に設定するために、次のうちどの方法が最も役立ちますか？
A. 最もリスクの高いインフラに焦点を当ててレビューを実施する
B. ベンダー契約書に記載されている管理事項を確認する

C. ベンダーが選択されたセキュリティフレームワークのルールに従っているかどうかを判断する
D. ベンダーのセキュリティポリシーを確認する
正解**: D (**コメントを発表する**)**
Reviewing controls listed in the vendor contract is the most helpful approach for properly scoping the security assessment of an existing vendor because it helps to determine the security requirements and expectations that the vendor has agreed to meet. A vendor contract is a legal document that defines the terms and conditions of the business relationship between the organization and the vendor, including the scope, deliverables, responsibilities, and obligations of both parties. A vendor contract should also specify the security controls that the vendor must implement and maintain to protect the organization's data and systems, such as encryption, authentication, access control, backup, monitoring, auditing, etc. Reviewing controls listed in the vendor contract helps to ensure that the security assessment covers all the relevant aspects of the vendor's security posture, as well as to identify any gaps or discrepancies between the contract and the actual practices. Therefore, reviewing controls listed in the vendor contract is the correct answer.
References:
https://medstack.co/blog/vendor-security-assessments-understanding-the-basics/
https://www.ncsc.gov.uk/files/NCSC-Vendor-Security-Assessment.pdf
https://securityscorecard.com/blog/how-to-conduct-vendor-security-assessment

質問**: 108**
成功するセキュリティプログラムにとって、最も重要な要件は次のうちどれですか？
A. セキュリティプロセスをベースラインセキュリティ標準にマッピングする
B. 主要システムに対する侵入テスト
C. 資産価値に関する経営判断
D. 従業員との秘密保持契約(NDA)
正解**: (**正解を表示します**)**
"A successful security program requires management support and involvement. One of the key aspects of management support is to decide on the value of assets and the acceptable level of risk for them. This will help define the security objectives and priorities for the program. The other options are possible activities within a security program, but they are not as important as management decision on asset value."

質問**: 109**
ある組織が最近、事業継続計画(BCP)を発動しました。従業員には事案発生時に通知されましたが、一部の従業員はコミュニケーション計画を完全に遵守しませんでした。このような事態の再発を防ぐための最善策は何でしょうか？
A. BCPにおける外部コミュニケーションに関する指示を強化する
B. 適切な従業員とともに卓上テストを実施する。

C. 計画に従った従業員にインセンティブを与える
D. 事業影響分析(BIA)を更新する
正解**: (**正解を表示します**)**
Tabletop testing with appropriate employees (B) is the best way to prevent recurrence because it reinforces roles, communication paths, and expectations through realistic practice. CISM stresses regular testing and exercises to ensure plans are understood and executable under pressure. Updating the BIA (D) or incentivizing behavior (C) does not address understanding gaps. Enhancing instructions (A) alone is insufficient without practice.
References: ISACA CISM Review Manual (Program management-BCP testing and exercises); CISM Exam Content Outline (Domain 3).

質問**: 110**
ある組織が、機密性の高いアーカイブデータを第三者にホスティングしてもらうことを検討しています。契約を結ぶ前に、以下の項目のうちどれを検証することが最も重要ですか？
A. ベンダーのデータセンターは同じ地理的地域にあります。
B. 暗号化キーはベンダーに提供されません。
C. ベンダーの管理体制は組織のセキュリティ基準に準拠しています。
D. ベンダーの業務に対する独立監査が定期的に実施されます。
正解**: (**正解を表示します**)**
The most important thing to verify before entering into a relationship with a third party to host sensitive archived data is the vendor's controls are in line with the organization's security standards. This is because the organization is ultimately responsible for the security and privacy of its data, even if it is stored or processed by a third party. The organization should ensure that the vendor has adequate and effective controls to protect the data from unauthorized access, modification, disclosure, or destruction. The organization should also ensure that the vendor complies with the applicable laws and regulations regarding data protection, such as the General Data Protection Regulation (GDPR) in the European Union. The organization should conduct a thorough risk assessment of the vendor and its services, and establish a clear contract that defines the roles, responsibilities, expectations, and obligations of both parties.
References = CISM Review Manual 15th Edition, Chapter 3, Section 3.2.1, page 1341; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 2, page 2

質問**: 111**
分散型サービス拒否(DDoS)攻撃の影響を軽減するために、次のうちどれが最も効果的でしょうか？
A. サーバーに状態制限を課す。
B. サイトを複数のISPに分散させる。

C. 攻撃の発生源で攻撃を阻止する。
D. ネットワークセキュリティを強化する。
正解: **B (**コメントを発表する**)**
The answer to the question is B. Spread a site across multiple ISPs. This is because spreading a site across multiple Internet service providers (ISPs) can help to reduce the impact of a distributed denial of service (DDoS) attack by increasing the bandwidth and redundancy of the site, and making it harder for the attacker to target and overwhelm a single point of failure. Spreading a site across multiple ISPs can also help to distribute the traffic load and balance the performance of the site, and to mitigate the effects of regional or network-specific outages or disruptions. Spreading a site across multiple ISPs can be done by using various techniques, such as anycast routing, content delivery networks (CDNs), or cloud-based services12.
Spreading a site across multiple ISPs can help to reduce the impact of a DDoS attack by increasing the bandwidth and redundancy of the site, and making it harder for the attacker to target and overwhelm a single point of failure. (From CISM Manual or related resources)
References = CISM Review Manual 15th Edition, Chapter 4, Section 4.2.1, page 2091; DDoS Attacks-A Cyberthreat and Possible Solutions2

質問: **112**
情報セキュリティの価値を経営陣に伝えるための最善の方法は何でしょうか？
A. セキュリティ意識向上トレーニングのメリットを説明する
B. セキュリティがビジネス目標の達成にどのように貢献するかを説明する
C. 妥協がもたらす潜在的な影響について説明する
D. 証券投資の予想収益率
正解: **B (**コメントを発表する**)**
The most effective way to communicate the value of information security to senior management is to describe how security enables business objectives (B). CISM emphasizes that executives view security as valuable when it supports revenue generation, operational resilience, customer trust, and strategic goals. Discussing training benefits (A), potential impacts (C), or ROI (D) alone frames security as a cost or fear-based function.
Positioning security as a business enabler aligns it with executive priorities and promotes sustained support.
References: ISACA CISM Review Manual (Governance-executive communication and value realization); CISM Exam Content Outline (Domain 2).

質問: **113**
情報セキュリティ管理者が情報セキュリティリソースの要件を特定する際に、最も重要な考慮事項は次のうちどれですか？
A. 現在のリソースレベル
B. 情報セキュリティインシデント

C. 潜在資源の利用可能性
D. 情報セキュリティ戦略
正解: **(**正解を表示します**)**

質問: **114**
以下のうち、インシデント対応計画のテスト実施を保証する責任を負うのは誰ですか？
A. ビジネスプロセスオーナー
B. 事業継続マネージャー
C. インシデント対応チームのメンバー
D. 情報セキュリティマネージャー
正解: **(**正解を表示します**)**
The correct answer is D because the information security manager is accountable for ensuring that the incident response capability is maintained, tested, and improved. Incident response plans must be tested periodically to confirm that roles, escalation paths, communication procedures, containment steps, and recovery coordination work as intended. Business process owners are responsible for business processes and may participate in tests, especially where business impact is involved, but they are not normally accountable for the information security incident response plan itself. The business continuity manager may be accountable for business continuity or disaster recovery exercises, but this question specifically refers to incident response. Incident response team members perform response activities and participate in exercises, but accountability for ensuring the plan is tested belongs to the manager responsible for the incident management program. CISM emphasizes that information security management includes establishing, maintaining, testing, and improving incident management processes to reduce organizational impact when incidents occur.
Reference: CISM Information Security Incident Management; incident response planning, testing, accountability, and continuous improvement principles.

質問: **115**
最近発生したセキュリティインシデントの調査で、根本原因はシステム管理者がインシデントアラートを不注意に処理したことにあると判明しました。この問題に対処するにはどうすればよいでしょうか？
A. リスク評価を実施し、その結果を上級管理職と共有する。
B. 業務プロセスに合わせてインシデント対応計画を改訂する。
C. データ管理者に対してインシデント対応トレーニングを実施する。
D. データ所有者に対してインシデント対応トレーニングを実施する。
正解: **(**正解を表示します**)**
The best action for the system admin manager to address the issue of negligent handling of incident alerts by system admins is to provide incident response training to data custodians because it helps to improve their awareness and skills in recognizing and

reporting security incidents, and following the incident response procedures and protocols. Conducting a risk assessment and sharing the result with senior management is not a good action because it does not address the root cause of the issue or provide any solutions or improvements. Revising the incident response plan to align with business processes is not a good action because it does not address the root cause of the issue or provide any solutions or improvements. Providing incident response training to data owners is not a good action because data owners are not responsible for handling incident alerts or performing incident response tasks. References: https://www.isaca.org/resources /isaca-journal/issues/2017/volume-5/incident-response-lessons-learned https://www.isaca.org/resources/isaca- journal/issues/2018/volume-3/incident-response-lessons-learned

質問**: 116**
災害復旧計画(DRP)テストを実施する際に、最も大きな内在リスクは次のうちどれですか？
A. 結果と教訓の文書化が不十分である。
B. 影響を受けるユーザーへの情報伝達不足
C. 生産環境の混乱
D. 各部署間の連携不足
正解**: (**正解を表示します**)**
A disaster recovery plan (DRP) test is a simulation of a disaster scenario to evaluate the effectiveness and readiness of the DRP. The greatest inherent risk when performing a DRP test is the disruption to the production environment, which could cause operational issues, data loss, or system damage. Therefore, it is essential to plan and execute the DRP test carefully, with proper backup, isolation, and rollback procedures.
Poor documentation, lack of communication, and lack of coordination are also potential risks, but they are not as severe as disrupting the production environment. References = CISM Review Manual 15th Edition, page
253; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 224.
The greatest inherent risk when performing a disaster recovery plan (DRP) test is disruption to the production environment. A DRP test involves simulating a disaster scenario to ensure that the organization ' s plans are effective and that it is able to recover from an incident. However, this involves running tests on the production environment, which has the potential to disrupt the normal operations of the organization. This inherent risk can be mitigated by running tests on a non-production environment or by running tests at times when disruption will be minimized.

質問**: 117**
リスクを適切に軽減するための予防的対策が実行不可能な場合、情報セキュリティ管理者にとって最も重要な行動は次のうちどれですか？

A. 影響の管理
B. 許容できないリスクレベルの特定
C. 脆弱性の評価
D. 潜在的な脅威の評価
正解: **(**正解を表示します**)**
When preventive controls to appropriately mitigate risk are not feasible, the most important action for the information security manager is to manage the impact, which means taking measures to reduce the likelihood or severity of the consequences of the risk. Managing the impact can involve using alternative controls, such as engineering, administrative, or personal protective controls, that can lower the exposure or harm to the organization. The other options, such as identifying unacceptable risk levels, assessing vulnerabilities, or evaluating potential threats, are part of the risk assessment process, but they are not actions to mitigate risk when preventive controls are not feasible. References:
https://bcmmetrics.com/risk-mitigation-evaluating-your-controls/
https://www.osha.gov/safety-management/hazard-prevention
https://www.cdc.gov/niosh/topics/hierarchy/default.html

質問: **118**
高可用性を必要とする電子ビジネスの場合、次の設計原則のうちどれが最適ですか?
A. ユーザーのニーズを満たす別のeビジネスのウェブサイトへの手動フェイルオーバー
B. トランザクションを迅速に受信して処理できる単一のエントリポイント
C. ダウンしたシステムから代替システムにトランザクションを誘導するインテリジェントミドルウェア
D. 隣接するコールドサイトと、重要なデータのミラーコピーを備えたスタンバイサーバーの可用性
正解: **C (**コメントを発表する**)**
Intelligent middleware enables dynamic rerouting and automated load balancing, which is crucial for high availability. This minimizes downtime and ensures continuity without manual intervention.
"Middleware solutions can provide automated failover capabilities, improving system resilience and availability."
- CISM Review Manual 15th Edition, Chapter 3: Program Development and Management, Section:
Availability and Resilience*
Manual failover and cold sites introduce delays, which are not suitable for e-business environments requiring near-zero downtime.

質問: **119**
情報セキュリティチームは、ユーザーが機密情報を含むアプリケーションへのログインアカウントを共有していることを発見しました。これはアクセスポリシーに違反する行為で

す。経営陣は、この行為が業務効率化につながると主張しています。情報セキュリティマネージャーにとって最適な対応策は何でしょうか？
A. ポリシーを施行する。
B. 方針を変更する。
C. 経営陣にリスクを提示する。
D. 逸脱に対する例外を作成します。
正解: **C** (コメントを発表する)
The information security manager's best course of action is to present the risk to senior management, because this is a case of conflicting objectives and priorities between the information security team and the business management. The information security manager should explain the potential impact and likelihood of a security breach due to the violation of the access policy, as well as the possible legal, regulatory, and reputational consequences. The information security manager should also provide alternative solutions that can achieve both operational efficiency and security compliance, such as implementing single sign-on, role- based access control, or multi-factor authentication. The information security manager should not enforce the policy without senior management's approval, because this could cause operational disruption and business dissatisfaction. The information security manager should not modify the policy without a proper risk assessment and approval process, because this could weaken the security posture and expose the organization to more threats. The information security manager should not create an exception for the deviation without a formal risk acceptance and documentation process, because this could create inconsistency and ambiguity in the policy enforcement and accountability. References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 127-128, 138-139, 143-144.

質問: **120**
マルウェア攻撃の発見と駆除後、最も重要な判断事項は次のうちどれですか？
A. 関与しているマルウェアの種類
B. マルウェアの侵入経路
C. マルウェアの検出方法
D. マルウェアの作成者
正解: (正解を表示します)

質問: **121**
ある企業が、情報セキュリティプログラムを支援するために、第三者ベンダーからセキュリティサービスを調達することを決定しました。ベンダー選定基準に含めるべき最も重要な項目は次のうちどれですか？
A. ベンダーの過去の顧客からのフィードバック
B. ベンダーの事業目標と企業のセキュリティ目標との整合性
C. ベンダーの内部統制環境の成熟度

D. ベンダーのネットワークに対する侵入テスト
正解: **B (**コメントを発表する**)**
The most important thing to include in the vendor selection criteria when procuring security services from a third-party vendor is B. Alignment of the vendor's business objectives with enterprise security goals. This is because the vendor should be able to understand and support the enterprise's security vision, mission, strategy, and policies, and provide services that are consistent and compatible with them. The vendor should also be able to demonstrate how their services add value, reduce risk, and enhance the performance and maturity of the enterprise's information security program. The alignment of the vendor's business objectives with enterprise security goals can help to ensure a successful and long-term partnership, and avoid any conflicts, gaps, or issues that may arise from misalignment or divergence.
The vendor should be able to understand and support the enterprise's security vision, mission, strategy, and policies, and provide services that are consistent and compatible with them. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 3, Section 3.2.1, page 1341; Third-Party Vendor Selection: If Done Right, It's a Win-Win2; Vendor Selection Criteria: Key Factors in Procurement Success3

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu **1193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **122**
事業継続計画(BCP)の改善において、以下のうち最も重要なものはどれですか？
A. 経営レビューの実施
B. ITレジリエンスソリューションの実装
C. 重要な業務プロセスの文書化
D. 学んだ教訓を取り入れる
正解: **(**正解を表示します**)**

質問: **123**
どのタイプの計画が、発生する可能性のあるセキュリティインシデントの影響を軽減することを主な目的としていますか？
A. セキュリティ意識向上計画
B. インシデント対応計画

C. 事業継続計画(BCP)
D. 災害復旧計画(DRP)
正解: **(**正解を表示します**)**

質問: **124**
侵害が発生し、リスクが特定され、フォレンジックプロセスが実行された後、次に実行すべきことは次のうちどれですか?
A. Web サーバーを隔離します。
B. 最後に検証されたバックアップからサーバーを再構築します。
C. 計画的にサーバーをシャットダウンします。
D. 元のメディアから関連するパッチを使用してサーバーを再構築します。
正解: **(**正解を表示します**)**
= After a breach where the risk has been isolated and forensic processes have been performed, the next step should be to rebuild the server from the last verified backup. This will ensure that the server is restored to a known and secure state, and that any malicious code or data that may have been injected or compromised by the attacker is removed. Rebuilding the server from the original media may not be sufficient, as it may not include the latest patches or configurations that were applied before the breach. Placing the web server in quarantine or shutting it down may not be feasible or desirable, as it may disrupt the business operations or services that depend on the server. Rebuilding the server from the last verified backup is the best option to resume normal operations while maintaining security. References = CISM Review Manual 15th Edition, page 118: "Recovery is the process of restoring normal operations after an incident. Recovery activities may include rebuilding systems, restoring data, applying patches, changing passwords, and testing functionality." Data Breach Experts Share The Most Important Next Step You Should Take After A Data Breach in 2014 &
2015, snippet: "Restore from backup. If you have a backup of your system from before the breach, wipe your system clean and restore from backup. This will ensure that any backdoors or malware installed by the hackers are removed."

質問: **125**
事業継続計画 (BCP) には次の内容を含める必要があります。
A. ハードウェアとソフトウェアのインベントリ
B. データ復元手順
C. 駆除活動に関する情報
D. アクティベーションの基準
正解: **(**正解を表示します**)**
Criteria for activation are essential to ensure that the BCP is triggered appropriately in response to a disruption.

"The BCP should include clearly defined activation criteria to ensure that plans are invoked when necessary."
- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Business Continuity Planning* ISACA's practice questions confirm that criteria for activation are core to a BCP's effectiveness.

質問: **126**
セキュリティレビューの結果、ファイルサーバー上の機密情報が組織内の権限のないユーザーによってアクセスされたことが判明しました。情報セキュリティマネージャーは、まず次のうちどれを行うべきでしょうか？
A. インシデント対応計画を発動する
B. ロールベースアクセス制御(RBAC)を実装する
C. 情報へのアクセスを削除する
D. ファイルサーバーから情報を削除します
正解: **(**正解を表示します**)**
The first step is to invoke the incident response plan to ensure a systematic, controlled, and compliant response to the security incident.
"The incident response plan should be activated immediately to investigate, contain, and resolve incidents of unauthorized access."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Incident Response Plan Execution* ISACA practice questions also reinforce that invoking the incident response plan is the essential first response to contain the breach.

質問: **127**
情報セキュリティインシデントを検出する最も効果的な方法はどれですか?
A. セキュリティイベントログ記録の定期的な分析
B. 定期的なセキュリティ意識向上プログラムの実施
C. ネットワークアクティビティのリアルタイム監視
D. 主要リスク指標 (KRI) のしきい値設定
正解: **C (**コメントを発表する**)**

質問: **128**
以下のうち、インシデント対応計画の効果的な実行を最も促進するのはどれですか？
A. この計画はリスク評価の結果に基づいています。
B. 対応チームは計画に基づいて訓練を受けている
C. この計画は業界のベストプラクティスに基づいています。
D. インシデント対応計画は、IT災害復旧計画(DRP)と整合しています。
正解: **B (**コメントを発表する**)**
The effective execution of an incident response plan depends largely on the competence and readiness of the response team, who are responsible for carrying out the tasks and

activities defined in the plan. Therefore, the best way to facilitate the effective execution of an incident response plan is to ensure that the response team is trained on the plan, and that they are familiar with their roles, responsibilities, procedures, and tools. Training the response team on the plan will also help to improve their confidence, communication, coordination, and collaboration during an incident response. The other options are not the best ways to facilitate the effective execution of an incident response plan, although they may be important factors for developing or improving the plan. The plan should be based on risk assessment results and industry best practice, but these do not guarantee that the plan will be executed effectively. The incident response plan should align with the IT disaster recovery plan, but this does not ensure that the response team is prepared and capable of executing the plan. References = CISM Review Manual, 16th Edition, page 1031 The best way to facilitate the effective execution of an incident response plan is to ensure that the response team is trained on the plan. An incident response plan is a set of instructions that defines the roles, responsibilities, procedures, and tools for detecting, responding to, and recovering from security incidents. An incident response team is a group of individuals that are assigned to perform specific tasks and activities during an incident response process. The response team may include security analysts, IT staff, legal counsel, public relations, and other stakeholders. To execute an incident response plan effectively, the response team needs to be trained on the plan, which means they need to be familiar with the following aspects of the plan:
The scope and objectives of the plan The roles and responsibilities of each team member The communication and escalation protocols The incident classification and prioritization criteria The incident response procedures and tools The incident documentation and reporting requirements The incident review and improvement processes By training the response team on the plan, the organization can ensure that the team members are prepared and confident to handle any security incidents that may occur, and that they can perform their tasks efficiently and consistently. The other options are not the best way to facilitate the effective execution of an incident response plan, although they may be some steps or outcomes of the process.
The plan being based on risk assessment results is a desirable practice, as it ensures that the plan is aligned with the organization's risk profile and addresses the most relevant and likely threats and vulnerabilities.
However, it does not guarantee that the plan will be executed effectively unless the response team is trained on the plan. The plan being based on industry best practice is a desirable practice, as it ensures that the plan follows established standards and guidelines for incident response. However, it does not guarantee that the plan will be executed effectively unless the response team is trained on the plan. The incident response plan aligning with the IT disaster recovery plan (DRP) is a desirable practice, as it ensures that the plans are consistent and coordinated in terms of objectives, scope, roles, procedures, and tools. However, it does not guarantee that the plan will be executed effectively unless the response team is trained on the plan

質問: **129**
経営陣は、組織の侵入防止システム(IPS)が繰り返し業務を妨害する可能性があることを懸念しています。情報セキュリティマネージャーがこの懸念に対処するためにシステムを調整したことを最もよく示しているのは次のうちどれですか？
A. 偽陰性の増加
B. 偽陰性を減らす
C. 偽陽性の減少
D. 偽陽性の増加
正解: **C (**コメントを発表する**)**
Decreasing false positives is the best indicator that the information security manager has tuned the system to address senior management's concern that the organization's intrusion prevention system (IPS) may repeatedly disrupt business operations. False positives are alerts generated by the IPS when it mistakenly blocks legitimate traffic or activity, causing disruption or downtime. Decreasing false positives means that the IPS has been configured to reduce such errors and minimize unnecessary interruptions. Increasing false negatives is not a good indicator because it means that the IPS has failed to detect or block malicious traffic or activity, increasing the risk of compromise or damage. Decreasing false negatives is not a good indicator because it does not affect business operations, but rather improves security detection or prevention. Increasing false positives is not a good indicator because it means that the IPS has increased its errors and interruptions, worsening senior management's concern. References: https://www.isaca.org/resources/isaca-journal/issues /2017/volume-6/the-value-of-penetration-testing https://www.isaca.org/resources/isaca-journal/issues/2016 /volume-5/security-scanning-versus-penetration-testing

質問: **130**
組織がプライバシー規制を遵守し続けるために、最初に行うべきセキュリティ対策は次のうちどれでしょうか？
A. セキュリティ意識向上トレーニングの開発
B. セキュリティ情報およびイベント管理(SIEM)の実装
C. データ分類フレームワークの実装
D. データ損失防止(DLP)ソリューションのインストール
正解: **(**正解を表示します**)**
A data classification framework (C) is the foundational step for privacy compliance because organizations must first understand what data they have, its sensitivity, and how it is regulated. Privacy obligations vary by data type (e.g., personal, sensitive, regulated), and classification enables appropriate handling, protection, retention, and access controls. Awareness training (A), SIEM (B), and DLP (D) are all valuable controls, but they are ineffective or misaligned without knowing which data requires protection and at what level.

CISM governance guidance emphasizes that compliance and control selection must be risk- and data-driven, making classification an essential prerequisite for privacy programs. References: ISACA CISM Review Manual (Governance-data governance, privacy, information asset classification); CISM Exam Content Outline (Domain 2).

質問**: 131**
事業継続管理において、最も重要な考慮事項は次のうちどれでしょうか？
A. 人間の安全を確保する
B. 重要なビジネスプロセスの特定
C. バックアップデータの信頼性を確保する
D. 重要な情報資産の保護
正解**: (**正解を表示します**)**
= Business continuity management (BCM) is the process of planning and implementing measures to ensure the continuity of critical business processes in the event of a disruption. The most important consideration of BCM is ensuring human safety, as this is the primary responsibility of any organization and the basis of ethical conduct. Human safety includes protecting the health and well-being of employees, customers, suppliers, and other stakeholders who may be affected by a disruption. Identifying critical business processes, ensuring the reliability of backup data, and securing critical information assets are also important aspects of BCM, but they are secondary to human safety. References = CISM Review Manual, 16th Edition, ISACA,
2020, p. 2111; CISM Online Review Course, Domain 4: Information Security Incident Management, Module
4: Business Continuity and Disaster Recovery, ISACA2

質問**: 132**
情報セキュリティマネージャーは、システム管理者がサーバー管理者アカウントをデフォルトのユーザー名から変更していないことに気づきました。ビジネスマネージャーは、これらの変更を義務付けるポリシーを作成し承認しました。情報セキュリティマネージャーが最初にとるべき行動は次のうちどれでしょうか？
A. 情報セキュリティ意識向上資料に要件を含める
B. ポリシー遵守状況の評価を実施する
C. ポリシーがシステム管理者に伝達されていることを確認する
正解**: (**正解を表示します**)**
The first course of action is to ensure the policy has been communicated to the system administrators (C).
CISM governance principles require that policies be formally communicated and understood before enforcement or compliance assessment occurs. Conducting assessments (B) or training (A) is ineffective if administrators are not aware of the policy requirements. Effective governance follows a sequence: approval # communication #

implementation # monitoring and enforcement. Communication ensures accountability and supports consistent adoption of security requirements.
References: ISACA CISM Review Manual (Governance-policy lifecycle, communication and enforcement); CISM Exam Content Outline (Domain 2).

質問**: 133**
外部委託業者が組織の業務上重要なデータを取り扱っています。クライアント組織が委託業者のセキュリティ対策について確証を得るための最も効果的な方法は次のうちどれですか？
A. ベンダーに事業継続計画(BCP)の提出を求める
B. ベンダーからの最近の情報セキュリティ開示内容を確認する
C. 定期的な独立した第三者による審査を義務付ける
D. ベンダーのサービスレベル契約(SLA)を確認する
正解**: (**正解を表示します**)**
The most effective way to obtain assurance of a vendor's security practices is requiring periodic independent third-party reviews (C). In CISM governance and third-party risk management, independent assurance is the strongest mechanism to validate that security controls are not only documented but also designed appropriately and operating effectively. Third-party reviews (such as SOC reports or independent audits) provide objective evidence and reduce reliance on vendor self-reporting.
Requiring BCPs (A) focuses primarily on availability and resilience, not the overall security posture.
Reviewing security disclosures (B) is reactive and limited to known issues disclosed by the vendor.
Reviewing SLAs (D) confirms contractual expectations but does not validate actual control effectiveness.
CISM emphasizes that governance over outsourced services must include ongoing, independent assurance activities to ensure continued alignment with risk appetite and regulatory obligations.
Periodic independent reviews also support accountability, enable risk-based decision-making, and provide defensible evidence of due diligence to senior management and regulators.
References:
ISACA CISM Review Manual, Information Security Governance - third-party risk management and assurance ISACA CISM Exam Content Outline, Domain 2: Information Security Governance

質問**: 134**
情報セキュリティガバナンスを企業統治の枠組みに組み込むことによる最大のメリットは、次のうちどれですか？
A. 情報セキュリティ戦略に対する意識の高まり

B. 攻撃発生時のプロセス回復力の向上
C. セキュリティ・バイ・デザインの原則をビジネスに推進する
D. 情報セキュリティに対する経営陣の責任
正解: **(**正解を表示します**)**
The greatest benefit of incorporating information security governance into the corporate governance framework is D. Management accountability for information security. This is because management accountability for information security means that the senior management and the board of directors are responsible for defining, overseeing, and supporting the information security strategy, policies, and objectives of the organization, and ensuring that they are aligned with the business goals, stakeholder expectations, and regulatory requirements. Management accountability for information security also means that the senior management and the board of directors are accountable for the performance, value, and effectiveness of the information security program, and for the management and mitigation of the information security risks and incidents. Management accountability for information security can help to foster a culture of security awareness and responsibility, and to enhance the trust and confidence of the customers, partners, and regulators in the organization's information security capabilities.
Management accountability for information security means that the senior management and the board of directors are responsible for defining, overseeing, and supporting the information security strategy, policies, and objectives of the organization, and ensuring that they are aligned with the business goals, stakeholder expectations, and regulatory requirements. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 1, Section 1.2.1, page 181; CISM domain 1: Information security governance [Updated 2022] | Infosec2; Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition3

質問: **135**
自動化されたIDおよびアクセス管理(1AM)システムを使用する大規模な多国籍企業にとって、以下のうちどれが最大の課題となるでしょうか？
A. 組織内での多数のアプリケーション
B. 業界平均を大幅に上回る従業員離職率
C. 雇用期間中のユーザーロールの頻繁な変更
D. 人事部(HR)からの不正確な従業員データ
正解: **D (**コメントを発表する**)**

質問: **136**
ある組織が、顧客データを分析するためのビッグデータソリューションの導入可能性を検討している。この取り組みを支援するために、情報セキュリティマネージャーはまず最初に以下のことを行うべきである。
A. ソリューションによって処理される在庫関連の顧客データ。

B. 情報セキュリティのリソースと予算要件を決定する。
C. 組織に対する潜在的な情報セキュリティリスクを評価する。
D. ビッグデータソリューションの情報セキュリティ要件を策定する。
正解: **C** (コメントを発表する)
Assessing potential information security risk to the organization is the first step that the information security manager should take when considering the feasibility of implementing a big data solution to analyze customer data, as it helps to identify and evaluate the threats, vulnerabilities, and impacts that may arise from the collection, processing, storage, and sharing of large volumes and varieties of customer data. Assessing risk also helps to determine the risk appetite and tolerance of the organization, and to prioritize the risk treatment options and security controls that are needed to protect the customer data and the big data solution. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 64, section 2.2.1.2; Big Data Security and Privacy Issues in Healthcare1, page 1, section 1. Introduction.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu **193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **137**
ある重大なセキュリティインシデントへの対応中に、情報セキュリティマネージャーは、現在のインシデント対応計画にいくつかの不備があることに気づきました。計画を更新する最適なタイミングはいつでしょうか？
A. 事件への対応中
B. 卓上演習中
C. 事後検証中
D. リスク再評価後
正解: **C** (コメントを発表する)
During post-incident review is the best time to update the incident response plan after observing several deficiencies in the current plan while responding to a high-profile security incident. A post-incident review is a process of analyzing and evaluating the incident response activities, identifying the lessons learned, and documenting the recommendations and action items for improvement. Updating the incident response plan during post-incident review helps to ensure that the plan reflects the current best practices, addresses the gaps and weaknesses, and incorporates the feedback and suggestions

from the incident response team and other stakeholders. Therefore, during post-incident review is the correct answer.
References:
https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf
https://www.techtarget.com/searchsecurity/feature/5-critical-steps-to-creating-an-effective-incident-response-plan
https://www.integrify.com/blog/posts/incident-response-plan-need-an-update/

質問: **138**
ある組織は、自社の環境における外部からのブルートフォース攻撃の脅威が増大していることを認識しました。組織の重要システムに対するこのリスクを軽減するための最も効果的な方法は次のうちどれですか？
A. 多要素認証を実装する。
B. ログの監視と分析の頻度を増やす。
C. セキュリティ情報およびイベント管理システム(SIEM)を導入し、
D. 侵入検知システム(IDS)の感度を高める。
正解: **(**正解を表示します**)**
A brute force attack is a type of cyberattack that attempts to gain unauthorized access to an account, file, or other protected information by trying different combinations of usernames and passwords until finding the correct one. Brute force attacks can be very effective if the target system has weak or default passwords, or if the attacker has access to a large number of potential credentials. To mitigate this risk, an organization should implement multi-factor authentication (MFA) for its critical systems. MFA is a security method that requires users to provide more than one piece of evidence to verify their identity before accessing a system or service.
For example, MFA can involve using a password in addition to a code sent to a phone or email, or using a biometric factor such as a fingerprint or face scan. MFA can significantly reduce the impact of brute force attacks by making it harder for attackers to guess or obtain valid credentials, and by increasing the time and effort required for them to compromise the system. References = CISM Review Manual (Digital Version), Chapter 3: Information Security Risk Management, Section 3.1: Risk Identification, p. 115-1161. CISM Review Manual (Print Version), Chapter 3: Information Security Risk Management, Section 3.1: Risk Identification, p. 115-1162. CISM ITEM DEVELOPMENT GUIDE, Domain 3: Information Security Program Development and Management, Task Statement 3.1, p. 193.

質問: **139**
災害復旧計画(DRP)を成功裏に実行する能力に最も大きな影響を与えるのは、次のうちどれですか？
A. 計画の机上演習を実施する

B. 計画を定期的に更新する
C. 計画をすべての関係者に伝える
D. エスカレーション手順の見直し
正解: **C** (コメントを発表する)
The CISM Review Manual emphasizes that the success of a DRP (Disaster Recovery Plan) depends greatly on clear communication of the plan to all stakeholders. Stakeholders must be aware of their roles and responsibilities during an incident to ensure the plan can be effectively executed. While testing, updating, and reviewing the plan are also important, communication is critical to effective execution.
Reference:ISACA CISM Review Manual, 16th Edition, Page 250-251, " Disaster Recovery Planning - Key Success Factors " .

質問: **140**
情報セキュリティ戦略を策定する際に考慮すべき最も重要な制約は次のうちどれですか？
A. 法的および規制上の要件
B. 確立されたセキュリティポリシーと基準
C. 国際セキュリティ基準への準拠
D. 情報セキュリティアーキテクチャ
正解: (正解を表示します)
Legal and regulatory requirements are the most important constraint to be considered when developing an information security strategy, as they define the minimum level of security that the organization must comply with to avoid legal sanctions, fines, or reputational damage. Legal and regulatory requirements may vary depending on the jurisdiction, industry, and type of data that the organization handles, and they may impose specific security controls, standards, or frameworks that the organization must follow.
References = CISM Review Manual, 16th Edition, Chapter 1, Section 1.2.1.11

質問: **141**
組織の会計システムの健全性を確保するために最も効果的な方法は、次のうちどれですか？
A. 経理スタッフへのセキュリティ意識向上トレーニングの実施
B. 二要素認証の実装
C. 監査ログのセキュリティレビューを頻繁に実施する
D. システムの年次セキュリティ監査を実施する
正解: (正解を表示します)
Frequent security reviews of the audit log (C) most directly assure the integrity of an accounting system by enabling detection of unauthorized or inappropriate transactions and configuration changes. Integrity focuses on accuracy, completeness, and protection from unauthorized modification, and audit logs provide evidence of system activity that can be reviewed for anomalies, fraud, or policy violations. Awareness training (A) is preventive but indirect. Two-factor authentication (B) strengthens access control, but does not detect

improper changes made by authorized users. Annual audits (D) are periodic and retrospective, making them less effective for ongoing integrity assurance. CISM emphasizes that detective controls, such as log monitoring and review, are critical for high-integrity systems like financial and accounting applications where timely detection is essential.
References: ISACA CISM Review Manual (Program management-control types, monitoring, integrity assurance); CISM Exam Content Outline (Domain 3).

質問: **142**
以下のうち、インシデント対応プロセスの有効性に最も悪影響を与えるのはどれですか？
A. 曖昧な重症度基準
B. 組織のリスク許容度が高い
C. 分散型インシデント監視
D. 手動によるインシデント報告プロセス
正解: **(正解を表示します)**
The correct answer is A because ambiguous severity criteria can cause inconsistent classification, delayed escalation, inappropriate response actions, and poor prioritization during an incident. Incident response depends heavily on clear criteria for determining severity, impact, urgency, ownership, escalation paths, and communication requirements. If severity levels are unclear, responders may underestimate a serious incident or overreact to a minor event. This directly reduces the effectiveness of the response process. High organizational risk tolerance may influence response thresholds, but it does not necessarily make the process ineffective. Decentralized monitoring can create coordination challenges, but it can still be effective if roles and escalation processes are clear. Manual reporting may be slower than automated reporting, but it can still work if the process is well-defined. CISM emphasizes that incident response processes require classification, prioritization, escalation, and communication procedures. Clear severity criteria are foundational to effective incident management because they guide timely and appropriate response decisions.
Reference: CISM Information Security Incident Management; incident classification, severity criteria, escalation, and response process principles.

質問: **143**
経営幹部が情報セキュリティ戦略計画をレビューし承認する主な理由は、以下の点を確実にするためです。
A. 組織は計画を実行するために必要な資金を保有しています。
B. 法律および規制要件の遵守。
C. 情報セキュリティ活動への職員の参加。
D. この計画はコーポレートガバナンスに合致しています。
正解: **(正解を表示します)**

The main reason for having senior management review and approve an information security strategic plan is to ensure that the plan aligns with the corporate governance of the organization. Corporate governance is the set of responsibilities and practices exercised by the board and executive management to provide strategic direction, ensure objectives are achieved, manage risks appropriately and verify that the organization's resources are used responsibly1. An information security strategic plan is a document that defines the vision, mission, goals, objectives, scope and approach for the information security program of the organization2. The plan should be aligned with the organization's business strategy, risk appetite, culture, values and objectives3. By reviewing and approving the plan, senior management demonstrates their commitment and support for the information security program, ensures its alignment with the corporate governance, and provides the necessary resources and authority for its implementation4. References = 1: CISM Review Manual 15th Edition, ISACA, 2017, page 172: CISM Review Manual 15th Edition, ISACA, 2017, page 253:
CISM Review Manual 15th Edition, ISACA, 2017, page 264: CISM Review Manual 15th Edition, ISACA,
2017, page 27.
Senior management review and approval of an information security strategic plan is important to ensure that the plan is aligned with the organization ' s overall corporate governance objectives. It is also important to ensure that the plan takes into account any legal and regulatory requirements, as well as the resources and staff needed to properly implement the plan.

質問**: 144**
インシデント対応計画、事業継続計画(BCP)、および災害復旧計画(DRP)間の統合を維持するために、次のうちどれが最も重要ですか？
A. 資産分類
B. 復旧時間目標(RTO)
C. 保管管理記録
D. エスカレーション手順
正解**: (**正解を表示します**)**
Recovery time objectives (RTOs) are the maximum acceptable time that an organization can be offline or unavailable after a disruption. RTOs are important to maintain integration among the incident response plan, business continuity plan (BCP), and disaster recovery plan (DRP) because they help align the recovery goals and strategies of each plan. By defining clear and realistic RTOs, an organization can ensure that its IT infrastructure and systems are restored as quickly as possible after a disaster, minimizing the impact on business operations and customer satisfaction.
References = CISM Manual, Chapter 6: Incident Response Planning, Section 6.2: Recovery Time Objectives (RTOs), page 971
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles

質問: **145**
情報セキュリティマネージャーは、新たに発表された業界標準のセキュリティ基準に多数の例外があると判断しました。次に取るべき行動は次のうちどれですか？
A. リスク受容に関する文書を作成する。
B. 組織のセキュリティポリシーを改訂する。
C. 不遵守の結果を評価する。
D. 情報セキュリティ監査を実施する。
正解: **(正解を表示します)**
Assessing the consequences of noncompliance is the next step that should be done after determining that there are a significant number of exceptions to a newly released industry-required security standard. The information security manager should evaluate the potential impact and exposure of the organization due to the noncompliance with the security standard. The assessment should consider the legal, regulatory, contractual, and reputational implications of the noncompliance, as well as the likelihood and severity of the incidents or penalties that may result from the noncompliance. The assessment should also compare the cost and benefit of complying with the security standard versus accepting the risk of noncompliance. The assessment should provide the basis for making informed and rational decisions about how to address the noncompliance issue and prioritize the actions and resources needed to achieve compliance. Documenting risk acceptances, revising the organization's security policy, and conducting an information security audit are all possible actions that may be taken to address the noncompliance issue, but they are not the next steps that should be done. These actions should be performed after assessing the consequences of noncompliance, and based on the results and recommendations of the assessment. Documenting risk acceptances may be appropriate if the organization decides to accept the risk of noncompliance, and if the risk is within the risk appetite and tolerance of the organization. Revising the organization's security policy may be necessary if the organization decides to comply with the security standard, and if the policy needs to be updated to reflect the new requirements and expectations. Conducting an information security audit may be useful if the organization wants to verify the level of compliance and identify the gaps and weaknesses in the security controls and processes. Therefore, assessing the consequences of noncompliance is the next step that should be done after determining that there are a significant number of exceptions to a newly released industry-required security standard, as it helps the information security manager to understand the risk and impact of the noncompliance and to make informed and rational decisions about how to address it.
References = CISM Review Manual
2023, page 43 1; CISM Practice Quiz 2

質問: **146**

特定の脅威と脆弱性の組み合わせに対するリスクを、対策を適用する前に判断することは、次のように表現できます。
A. 脅威が脆弱性を悪用した場合の可能性と影響の関数。
B. 脅威が脆弱性を悪用した場合の影響の大きさ。
C. 脆弱性に対する制御のコストと有効性の関数。
D. 特定の脅威が脆弱性を悪用しようとする可能性
正解**: (**正解を表示します**)**
= According to the CISM Manual1, risk is defined as the combination of the probability of an event and its consequence. Therefore, determining the risk for a particular threat/vulnerability pair before controls are applied can be expressed as a function of the likelihood and impact, should a threat exploit a vulnerability.
Likelihood is the probability or frequency of a threat occurring, while impact is the magnitude or severity of the harm or loss that would result from a threat exploiting a vulnerability. The higher the likelihood and impact, the higher the risk. The lower the likelihood and impact, the lower the risk.
The other options are not correct because they do not capture the full expression of risk. Option B only considers the impact, but not the likelihood, of a threat exploiting a vulnerability. Option C confuses the risk with the risk response, which is the action taken to reduce or mitigate the risk. Option D only considers the likelihood, but not the impact, of a threat attempting to exploit a vulnerability.
References = CISM Manual1, Chapter 2: Information Risk Management (IRM), Section 2.1: Risk Concepts2
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles 2: 2

質問**: 147**
以下のうち、インシデント対応チームの準備態勢にとって最も大きなリスクとなるのはどれですか？
A. 正式なインシデント対応シナリオの欠如
B. 情報セキュリティ管理の変化
C. 時代遅れのインシデント対応計画
D. ハッカーが使用する新たな攻撃手法
正解**: A (**コメントを発表する**)**
The correct answer is A because formal incident response scenarios are essential for preparing the incident response team to recognize, coordinate, escalate, contain, and recover from realistic incident situations.
Preparedness is built through planning, exercises, role clarity, communications testing, and scenario-based practice. Without formal scenarios, the team may not be able to test whether procedures are practical, whether roles are understood, or whether communications and escalation paths work under pressure. A change in information security management may affect leadership, but it does not automatically reduce team

preparedness if processes remain sound. Outdated incident response plans are a serious concern; however, the question focuses on team preparedness, and scenario-based training is a direct mechanism for preparing the team. New attack vectors are expected in a changing threat environment, but a well-prepared team with practiced response scenarios can adapt more effectively. CISM emphasizes testing, exercises, and lessons learned as key elements of incident response capability.
Reference: CISM Information Security Incident Management; incident response preparedness, scenario testing, exercises, and team readiness principles.

質問: **148**
マルウェア感染事故のトリアージを行う際に、最初に行うべき手順は次のうちどれですか？
A. 影響を受けたシステムを含む
B. 法医学的画像の保存
C. バックアップと本番環境の比較
D. マルウェアの削除
正解: **(正解を表示します)**
The first step when performing triage of a malware incident is to contain the affected system, which means isolating it from the network and preventing any further communication or data transfer with the attacker or other compromised systems. Containing the affected system helps to limit the scope and impact of the incident, preserve the evidence, and prevent the spread of the malware to other systems.
References = NIST SP 800-61 Revision 2, CISM Review Manual 15th Edition

質問: **149**
サイバー攻撃に関する情報を提示し、経営陣から対策強化への支持を得るために、最も重要な強調事項は次のうちどれですか？
A. 同業種における最近のデータ漏洩
B. 内部システムに対する脅威
C. 残留リスクへの曝露
D. 多層防御アーキテクチャにおける制御ギャップ
正解: **C (コメントを発表する)**
The correct answer is C because senior management is primarily responsible for risk oversight and business decision-making. When seeking support for control enhancements, the information security manager should emphasize residual risk exposure, meaning the level of risk that remains after existing controls are considered.
This allows senior management to understand whether current risk is within the organization's risk appetite and whether additional investment is justified. Recent industry breaches may provide useful context, but they do not directly show the organization's own exposure. Threats against internal systems are important, but threats alone do not explain business impact or whether current controls are sufficient. Control gaps in a defense-in-

depth architecture may be technically relevant, but senior management needs the issue translated into business risk. CISM governance principles emphasize business-aligned reporting, risk-based decision- making, and communication in terms meaningful to executives. Residual risk exposure best connects cyberattack information to business impact, risk appetite, and the need for control enhancements.
Reference: CISM Information Security Governance; senior management reporting, residual risk, risk appetite, control enhancement justification, and business alignment principles.

質問: **150**
インシデント後の検証を実施する際の主な目的は、以下の点を特定することです。
A. 追加のサイバーセキュリティ予算が必要
B. インシデント対応計画の弱点
C. 上級管理職と共有する情報
D. 追加トレーニングが必要な個人
正解: **(**正解を表示します**)**
The core objective of a post-incident review (PIR) is to identify gaps and weaknesses in the response process.
This includes missteps, delays, communication failures, or policy limitations - all of which provide insight to improve future incident handling.
" Post-incident reviews focus on identifying root causes and areas for improvement to enhance the organization's preparedness for future incidents."
- CISM Review Manual 15th Edition, Chapter 4: Post-Incident Activities* Though training, reporting, and budgeting may follow, they are secondary outcomes of this process.

質問: **151**
ある組織の情報セキュリティマネージャーがソーシャルメディアで、最近購入したベンダー製品が侵害され、顧客データがオンラインに投稿されたという情報を目にしました。情報セキュリティマネージャーはまず何をすべきでしょうか？
A. 事業影響分析(BIA)を実施する。
B. 違反があった場合は、地元の法執行機関に通知してください。
C. インシデント対応プログラムを起動します。
D. 組織に対するリスクを検証する。
正解: **D (**コメントを発表する**)**
The first thing that the information security manager should do after reading about a vendor product compromise on social media is to validate the risk to the organization. This means verifying the source and credibility of the information, determining if the organization uses the affected product, and assessing the potential impact and likelihood of the compromise on the organization's data and systems. Validating the risk to the organization will help the information security manager to decide on the appropriate course

of action, such as activating the incident response program, notifying relevant stakeholders, or performing a BIA.
References: The CISM Review Manual 2023 states that "the information security manager is responsible for identifying and assessing the risks associated with the use of third-party products and services" and that "the information security manager should monitor and review the security performance and incidents of third-party products and services on a regular basis and take corrective actions when deviations or violations are detected" (p. 138). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Validating the risk to the organization is the correct answer because it is the first and most important step to take after reading about a vendor product compromise on social media, as it will help the information security manager to confirm the accuracy and relevance of the information, and to evaluate the potential consequences and probability of the compromise on the organization's data and systems" (p. 63). Additionally, the article Defending Against Software Supply Chain Attacks from the CISA website states that "the first step in responding to a software supply chain attack is to validate the risk to the organization by verifying the source and credibility of the information, determining if the organization uses the affected software, and assessing the potential impact and likelihood of the compromise on the organization's data and systems" (p. 2)

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu ↾**193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **152**
定量的リスク分析を用いる際の重要な考慮事項は、以下の点である。
A. 情報資産のリスク分析に関するベストプラクティスに準拠しています。
B. 情報資産のエクスポージャーに数値を割り当てます。
C. 情報資産に一般的に使用されるラベルを適用します。
D. 情報資産の重要度分析に基づいています。
正解: **(**正解を表示します**)**
A key consideration in the use of quantitative risk analysis is that it assigns numeric values to exposures of information assets, such as the probability of occurrence, the frequency of occurrence, the impact of occurrence, and the monetary value of the assets. These numeric values help to measure and compare the risks in a more objective and consistent

way, and to support the decision-making process based on cost-benefit analysis. Quantitative risk analysis also requires reliable and accurate data sources, and it may involve the use of statistical tools and techniques.
References = CISM Review Manual, 16th Edition eBook1, Chapter 2: Information Risk Management, Section: Risk Analysis, Subsection: Quantitative Risk Analysis, Page 84.

質問: **153**
情報セキュリティマネージャーは、リスク登録簿に記載されている未解決事項について、上級管理職に報告している。
これらのリスクに関して、最も重要なコミュニケーション事項は次のうちどれですか？
A. 責任主体
B. 主要リスク指標(KRIS)
C. 補償制御
D. 潜在的なビジネスへの影響
正解: **(**正解を表示します**)**
The most important information to communicate with regard to the open items from the risk register to senior management is the potential business impact of these risks. The potential business impact is the estimated consequence or loss that the organization may suffer if the risk materializes or occurs. The potential business impact can be expressed in quantitative or qualitative terms, such as financial, operational, reputational, legal, or strategic impact. Communicating the potential business impact of the open items from the risk register helps senior management to understand the severity and urgency of these risks, and to prioritize the risk response actions and resources accordingly. Communicating the potential business impact also helps senior management to align the risk management objectives and activities with the business objectives and strategies, and to ensure that the risk appetite and tolerance of the organization are respected and maintained.
References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Assessment, page 831; CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Reporting, page 1012.

質問: **154**
技術的な対策がない場合、会社支給の携帯端末における不正なテキストメッセージの送受信を減らすための最善の方法は何でしょうか？
A. 利用規約に関する定期的なリマインダーを伝達する
B. セキュリティ意識向上トレーニングに、禁止されているテキストメッセージの送信に関するトピックを含める。
C. 組織が管理体制を導入できるようになるまで、モバイル端末の提供を停止する
D. 事業影響分析(BIA)を実施し、その報告書を経営陣に提出する。
正解: **(**正解を表示します**)**

In the absence of technical controls, the best way to reduce unauthorized text messaging is to include the topic of prohibited texting in security awareness training. CISM recognizes that when automated or technical enforcement is unavailable, user behavior must be influenced through targeted awareness and training.
Training is stronger than simple reminders because it can explain the policy requirement, business rationale, examples of prohibited behavior, consequences of noncompliance, and proper alternatives. Regular reminders of the acceptable use policy may help reinforce expectations, but they are less effective than structured training. Stopping mobile device use would likely disrupt business and may not be proportionate to the risk.
Conducting a BIA is unrelated because the issue is user behavior and policy compliance, not continuity prioritization. CISM emphasizes that awareness and training programs should be tailored to specific roles, technologies, and behaviors. Therefore, incorporating prohibited texting into security awareness training is the best compensating measure when technical controls are not available.
References:
ISACA CISM Review Manual, Information Security Program Development and Management - security awareness and acceptable use ISACA CISM Exam Content Outline, Domain 3: Information Security Program Development and Management

質問**: 155**
ビジネスインパクト分析(BIA)プロセスの一環としてインタビューを実施する最も重要な理由は次のうちどれですか？
A. BIA後の定性的なリスク評価を容易にするため
B. 主要関係者の情報セキュリティ意識を高める
C. 意見を提供する利害関係者が関連リスクを負うことを保証する
D. できるだけ多くの関係者から意見を収集する
正解**: (**正解を表示します**)**
The most important reason to conduct interviews as part of the business impact analysis (BIA) process is to obtain input from as many relevant stakeholders as possible. A BIA is a process of identifying and analyzing the potential effects of disruptive events on the organization's critical business functions, processes, and resources. A BIA helps to determine the recovery priorities, objectives, and strategies for the organization's continuity planning. Interviews are one of the methods to collect data and information for the BIA, and they involve direct and interactive communication with the stakeholders who are involved in or affected by the business functions, processes, and resources. By conducting interviews, the information security manager can obtain input from as many relevant stakeholders as possible, such as business owners, managers, users, customers, suppliers, regulators, and partners. This can help to ensure that the BIA covers the full scope and complexity of the organization's business activities, and that the BIA reflects the accurate, current, and comprehensive views and expectations of the stakeholders. Interviews can also help to validate, clarify, and supplement the data and information

obtained from other sources, such as surveys, questionnaires, documents, or systems. Interviews can also help to build rapport, trust, and collaboration among the stakeholders, and to increase their awareness, involvement, and commitment to the information security and continuity planning.
References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Business Impact Analysis (BIA), pages 178-1801; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 65, page 602.

質問**: 156**
以下の要因のうち、組織の情報セキュリティガバナンスの形態に最も大きな影響を与えるのはどれでしょうか？
A. アウトソーシングされたプロセス
B. セキュリティ予算
C. 従業員数
D. 企業文化
正解**: D (**コメントを発表する**)**
The corporate culture of an organization is the set of values, beliefs, norms, and behaviors that shape how the organization operates and interacts with its stakeholders. The corporate culture can have a significant impact on an organization's information security governance mode, which is the way the organization establishes, implements, monitors, and evaluates its information security policies, standards, and objectives. A strong information security governance mode requires a supportive corporate culture that fosters a shared vision, commitment, and accountability for information security among all levels of the organization. A supportive corporate culture can also help to overcome resistance to change, promote collaboration and communication, encourage innovation and learning, and enhance trust and confidence in information security12. References = CISM Review Manual (Digital Version), Chapter 1: Information Security Governance CISM Review Manual (Print Version), Chapter 1: Information Security Governance

質問**: 157**
情報セキュリティ戦略の主要な基盤となるべきものは、次のうちどれでしょうか？
A. 組織のビジョンとミッション
B. 包括的なギャップ分析の結果
C. 情報セキュリティポリシー
D. 監査および規制要件
正解**: (**正解を表示します**)**
The organization's vision and mission should be the PRIMARY basis for an information security strategy, as they define the purpose and direction of the organization and its information security needs. A comprehensive gap analysis is a tool to identify the current state and desired state of information security, and the actions needed to close the gap.

Information security policies are the high-level statements of management's intent and expectations for information security, and are derived from the information security strategy. Audit and regulatory requirements are external factors that influence the information security strategy, but are not the primary basis for it. References = CISM Review Manual, 16th Edition, pages 17-181; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 782 The primary basis for an information security strategy should be the organization ' s vision and mission. The organization ' s vision and mission should be the foundation for the security strategy, and should inform and guide the security policies, procedures, and practices that are implemented. The results of a comprehensive gap analysis, information security policies, and audit and regulatory requirements should all be taken into consideration when developing the security strategy, but should not be the primary basis.

質問: **158**
情報セキュリティの第一の目標として、次のうちどれが適切でしょうか？
A. データガバナンス
B. ビジネスとの整合性
C. 情報管理
D. 規制遵守
正解: **(**正解を表示します**)**

質問: **159**
あるグローバル組織がインシデント対応チームを編成しています。組織は、すべてのインシデントについて本部に情報を提供し、広範囲に分散した事象に対して統一的な対応ができるようにしたいと考えています。これらの目的を最も効果的にサポートするのは次のうちどれですか？
A. 仮想インシデント対応チーム
B. 分散型インシデント対応チーム
C. 外部委託のインシデント対応チーム
D. 中央集中型インシデント対応チーム
正解: **D (**コメントを発表する**)**
A centralized incident response team ensures consistent communication, coordination, and a unified approach to managing incidents across the organization.
"A centralized incident response team provides a consistent and coordinated approach to incident handling and ensures that management is kept informed."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Incident Response Organization Models*

質問: **160**

ある組織は、最近の災害で収益の損失を被りました。組織の復旧に向けて、次のうちどれが最も適切な準備となるでしょうか？
A. 災害復旧計画(DRP)
B. 事業影響分析(BIA)
C. インシデント対応計画
D. 事業継続計画(BCP)
正解: **(正解を表示します)**

質問: **161**
インシデント対応ポリシーには以下が含まれるべきである。
A. 試験方法の説明。
B. 通知要件。
C. インフラストラクチャ図。
D. 復旧時間目標(RTO)。
正解: **(正解を表示します)**
Comprehensive and Detailed Step-by-Step Explanation:
Incident response policies must provide clear and actionable steps to ensure effective handling of incidents.
Notification requirements are critical to ensure timely communication with stakeholders during an incident.
A). A description of testing methodology: While testing is important, it is typically addressed in incident response plans, not the policy itself.
B). Notification requirements: This is the BEST answer as it ensures that key stakeholders are informed promptly, allowing for coordination and mitigation efforts.
C). An infrastructure diagram: This is useful for understanding system architecture but is not a core policy requirement.
D). Recovery time objectives (RTOs): RTOs are part of business continuity and disaster recovery plans, not incident response policies.
Reference: CISM Job Practice Area 4 (Information Security Incident Management) emphasizes the importance of clear communication and notification procedures in incident response.

質問: **162**
組織内にセキュリティ文化を構築するための主要な目標として、次のうちどれが適切でしょうか？
A. 情報セキュリティ対策のためのリソースを確保する
B. 組織内のセキュリティを最優先事項とする
C. リスクを許容レベルまで低減する
D. 上級管理職に対し、統制の有効性を示すため
正解: **(正解を表示します)**

The primary objective of creating a security culture is to reduce risk to acceptable levels (C) by influencing employee behavior and decision-making. CISM stresses that culture is a means to an end-not the end itself.
Prioritization (B), resource acquisition (A), and reporting (D) are outcomes or enablers, but the ultimate purpose is effective risk reduction aligned with business objectives. A strong security culture helps prevent incidents, improves compliance, and strengthens resilience through consistent, risk-aware behavior at all levels of the organization.
References: ISACA CISM Review Manual (Program management-security culture and behavior); CISM Exam Content Outline (Domain 3).

質問: **163**
財務部門の責任者が組織の予算申請業務を外部委託することを決定し、候補となる業者を特定しました。情報セキュリティマネージャーは、次のうちどれを最初に行うべきでしょうか？
A. 新しいソリューションに必要なセキュリティ制御を決定する
B. プロバイダーの災害復旧計画(DRP)を確認する
C. サービスプロバイダーのホスティング環境に関する監査レポートを入手する
D. 組織とサービスプロバイダーの統計情報の役割を整合させる。
正解: **(**正解を表示します**)**
Before outsourcing any application or service, an information security manager should first determine the required security controls for the new solution, based on the organization's risk appetite, security policies and standards, and regulatory requirements. This will help to evaluate and select the most suitable provider, as well as to define the security roles and responsibilities, service level agreements (SLAs), and audit requirements. References: https://www.isaca.org/credentialing/cism https://www.wiley.com/en-us /CISM+Certified+Information+Security+Manager+Study+Guide-p-9781119801948

質問: **164**
組織内で望ましい情報セキュリティ文化を醸成するために、次のうちどれが最も役立ちますか？
A. 情報セキュリティ意識向上トレーニングおよびキャンペーン
B. 効果的な情報セキュリティポリシーと手順
C. 情報セキュリティの役割と責任の委任
D. 適切な情報セキュリティ関連行動に対するインセンティブ
正解: **(**正解を表示します**)**
Information security awareness training and campaigns are the best way to enable the desired information security culture within an organization because they help to educate, motivate and influence the behavior and attitude of the employees towards information security. They also help to raise the awareness of the risks, threats and best practices of information security among the staff and stakeholders.

References = Organizational Culture for Information Security: A Systemic Perspective on the Articulation of Human, Cultural and Social Systems, CISM Exam Content Outline

質問: **165**
組織の外部Webアプリケーションに対する侵入テストで、複数の脆弱性が発見されました。以下のうち、最も懸念されるのはどれですか？
A. 侵入テスト実施前に交戦規定書に署名がなかった。
B. 内部テストでは脆弱性は発見されませんでした
C. 脆弱性は、不十分なユーザー受け入れテスト(UAT)によって引き起こされました。
D. 脆弱性の1つに対するエクスプロイトコードが公開されている。
正解: **D (**コメントを発表する**)**
Exploit code for one of the vulnerabilities is publicly available presents the greatest concern because it means that anyone can easily exploit the vulnerability and compromise the web application. This increases the risk of data breach, denial of service, or other malicious attacks. Therefore, exploit code for one of the vulnerabilities is publicly available is the correct answer.
References:
https://www.imperva.com/learn/application-security/penetration-testing/
https://www.netspi.com/blog/technical/web-application-penetration-testing/are-you-testing-your-web-application-for-vulnerabilities/

質問: **166**
ビジネスインパクト分析(BIA)を実施する主な理由は次のうちどれですか？
A. リスク軽減策の決定
B. 重要なプロセスの優先順位付け
C. 復旧目標時点(RPO)の設定
D. 情報感度の判定
正解: **B (**コメントを発表する**)**
The primary reason for performing a business impact analysis (BIA) is to prioritize critical business processes (B). In CISM, the BIA is a foundational activity for business continuity and resilience planning, designed to identify which business functions are most critical to organizational survival and must be restored first following a disruption. The BIA evaluates the impact of outages over time, enabling management to rank processes based on operational, financial, legal, and reputational consequences.
While establishing recovery point objectives (RPOs) (C) is an important output of the BIA, it is secondary to identifying and prioritizing critical processes. Determining risk mitigation options (A) is part of risk treatment, not the primary purpose of a BIA. Determining information sensitivity (D) relates to data classification, which is a separate governance activity.

CISM guidance clearly positions the BIA as a business-driven exercise that informs recovery priorities, recovery time objectives (RTOs), and continuity strategies. Without first prioritizing critical processes, recovery objectives and continuity planning cannot be effectively aligned with business needs.
References:
ISACA CISM Review Manual, Information Security Program Development and Management - Business Impact Analysis (BIA) objectives and outcomes ISACA CISM Exam Content Outline, Domain 3: Information Security Program Development and Management

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu **193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **167**
セキュリティに関する責任を職務記述書に組み込むことが重要な主な理由は以下のとおりです。
A. アクセス管理をサポートします。
B. セキュリティ意識向上プログラムの開発を簡素化します。
C. セキュリティを人事(HR)機能に整合させる。
D. 従業員の責任感を強化する。
正解: **(**正解を表示します**)**
Employee accountability is the degree to which employees are responsible for their actions and outcomes related to information security. It reflects the extent to which employees understand their roles and responsibilities, follow the policies and procedures, report incidents and breaches, and comply with legal and regulatory requirements. Embedding security responsibilities into job descriptions helps to clarify the expectations and obligations of employees, as well as the consequences of non-compliance or negligence. It also helps to align the security objectives with the business goals and strategies, and to foster a culture of security awareness and responsibility.
References: 1: CISM Review Manual, 15th Edition, Chapter 3, Section 3.2.1.2

質問: **168**
戦略的な情報セキュリティに関する意思決定を行うための最適なアプローチは、次のうちどれですか？

A. 定期的な情報セキュリティ状況報告体制を確立する。
B. 情報セキュリティ運営委員会を設置する。
C. 事業部門のセキュリティワーキンググループを設置する。
D. 定期的な上級管理職会議を開催する。
正解**: (**正解を表示します**)**
= According to the CISM Review Manual (Digital Version), page 9, an information security steering committee is a group of senior managers from different business units and functions who provide guidance and oversight for the information security program. An information security steering committee is the best approach to make strategic information security decisions because it can:
Ensure alignment of information security strategy with business objectives and risk appetite1 Facilitate communication and collaboration among different stakeholders and promote information security awareness and culture2 Provide direction and support for information security initiatives and projects3 Monitor and review the performance and effectiveness of the information security program4 Resolve conflicts and issues related to information security policies and practices5 Establishing regular information security status reporting, business unit security working groups, and periodic senior management meetings are useful activities for information security management, but they are not sufficient to make strategic information security decisions without the involvement and guidance of an information security steering committee. References = 1: CISM Review Manual (Digital Version), page
9 2: 1 3: 2 4: 3 5: 4
An Information Security Steering Committee is a group of stakeholders responsible for providing governance and guidance to the organization on all matters related to information security. The committee provides oversight and guidance on security policies, strategies, and technology implementation. It also ensures that the organization is in compliance with relevant laws and regulations. Additionally, it serves as a forum for discussing security-related issues and ensures that security is taken into account when making strategic decisions.

質問**: 169**
情報セキュリティガバナンスフレームワークの有効性を最大限に高めるには、以下の条件を満たす必要があります。
A. コンサルタントが情報セキュリティガバナンスフレームワークをレビューします。
B. 経営陣は法令遵守の文化を推進している。
C. リスク管理は、業務活動および戦略活動に組み込まれています。
D. IS監査担当者はガバナンス活動を評価する権限を与えられている
正解**: (**正解を表示します**)**
The effectiveness of an information security governance framework will best be enhanced if risk management is built into operational and strategic activities. This is because risk

management is a key component of information security governance, which is the process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations, and are effectively managed and measured. Risk management involves identifying, analyzing, evaluating, treating, monitoring, and communicating information security risks that may affect the organization's objectives, assets, and stakeholders. By integrating risk management into operational and strategic activities, the organization can ensure that information security risks are considered and addressed in every decision and action, and that the information security governance framework is aligned with the organization's risk appetite and tolerance. This also helps to optimize the allocation of resources, enhance the performance and value of information security, and improve the accountability and transparency of information security governance.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:
Information Security Governance Framework, page 181; CISM Review Manual, 16th Edition, Chapter 2:
Information Risk Management, Section: Risk Management, page 812; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 53, page 493.

質問**: 170**
限られたリソースしかない組織において、情報セキュリティプログラムの資金調達競争で勝つための最良の方法は次のうちどれですか？
A. 事業継続計画(BCP)の有効性を実証する。
B. 主要業績評価指標(KPI)の動向を報告する。
C. このプログラムがビジネス活動を可能にすることを実証する。
D. 同業他社におけるセキュリティインシデントの増加を示す証拠を提示する。
正解**: (**正解を表示します**)**
Comprehensive and Detailed Step-by-Step Explanation:
The goal of securing funding for an information security program often requires aligning the program with business goals and demonstrating its value to the organization. Here ' s an analysis of each option:
A). Demonstrate the effectiveness of business continuity plans (BCPs): While important, this focuses on continuity rather than the overall value of the information security program to business objectives. This is not the strongest method to justify funding.
B). Report key performance indicator (KPI) trends: KPI trends are useful for tracking performance but may not directly demonstrate how the program supports business activities or adds value.
C). Demonstrate that the program enables business activities: This is the BEST option because it ties the information security program directly to business operations. When

security is seen as an enabler (e.g., reducing risks in critical areas like customer data protection), stakeholders are more likely to allocate resources.
D). Provide evidence of increased security events at peer organizations: This may indicate a general threat landscape but does not provide concrete evidence of the program ' s value or relevance to the organization's specific goals.
Reference: CISM Job Practice Area 1 (Information Security Governance) emphasizes aligning information security strategies with organizational objectives to gain stakeholder support.

質問**: 171**
組織が使用しているクラウドアプリケーションに深刻な脆弱性が発見されました。リスクを評価した後、情報セキュリティマネージャーが取るべき最善の行動は次のうちどれでしょうか？
A. ベンダーに侵入テストを実施するよう指示してください。
B. ファイアウォールでアプリケーションへの接続を一時停止する
C. アプリケーションのビジネスオーナーに状況を報告してください。
D. 組織のインシデント対応プロセスを開始する。
正解**: (**正解を表示します**)**
= Initiating the organization's incident response process is the best course of action for the information security manager when a cloud application used by the organization is found to have a serious vulnerability.
The incident response process is a set of predefined steps and procedures that aim to contain, analyze, resolve, and learn from security incidents. The information security manager should follow the incident response process to ensure that the vulnerability is properly reported, assessed, mitigated, and communicated to the relevant stakeholders. The incident response process should also involve the cloud service provider (CSP) and the business owner of the application, as they are responsible for the security and functionality of the cloud application. Instructing the vendor to conduct penetration testing, suspending the connection to the application in the firewall, and reporting the situation to the business owner of the application are all possible actions that may be taken as part of the incident response process, but they are not the best initial course of action.
Penetration testing may help to identify the root cause and the impact of the vulnerability, but it may also cause further damage or disruption to the cloud application. Suspending the connection to the application in the firewall may prevent unauthorized access or exploitation of the vulnerability, but it may also affect the availability and continuity of the cloud application. Reporting the situation to the business owner of the application is an important step to inform them of the risk and the potential business impact, but it is not sufficient to address the vulnerability and its consequences. Therefore, the information security manager should initiate the incident response process as the best course of

action, and then perform the other actions as appropriate based on the incident response plan and the risk assessment. References = CISM Review Manual 2023, page 211 1; CISM Practice Quiz 2

質問: **172**
組織が災害復旧プログラムの管理を支援するために、サービスとしての災害復旧(DRaaS)を利用する主な利点は次のうちどれですか？
A. クラウドインフラストラクチャを使用して、組織に柔軟な導入オプションを提供します。
B. 組織がコア業務を優先できるようにする。
C. 従来のデータバックアップアーキテクチャよりも安全です。
D. より低いコストでプロの対応チームを利用できます。
正解: **(**正解を表示します**)**
The primary advantage of an organization using Disaster Recovery as a Service (DRaaS) to help manage its disaster recovery program is B. It allows the organization to prioritize its core operations. This is because DRaaS is a cloud computing service model that allows an organization to back up its data and IT infrastructure in a third-party cloud computing environment and provide all the disaster recovery orchestration, all through a SaaS solution, to regain access and functionality to IT infrastructure after a disaster1. DRaaS can help the organization to prioritize its core operations by:
Reducing the need for provisioning and maintaining its own off-site disaster recovery environment, which can be costly, complex, and resource-intensive12 Enabling the organization to continue running its applications from the service provider's cloud or hybrid cloud environment instead of from the disaster-affected physical servers, which can minimize the downtime, data loss, and business disruption12 Providing the organization with flexible and scalable deployment options, such as on-demand, pay-per-use, or subscription-based models, that can meet its changing business needs and budget12 Leveraging the expertise, experience, and best practices of the service provider, who can handle the disaster recovery planning, testing, and execution, and ensure compliance with the relevant standards and regulations12 DRaaS is a cloud computing service model that allows an organization to back up its data and IT infrastructure in a third-party cloud computing environment and provide all the disaster recovery orchestration, all through a SaaS solution, to regain access and functionality to IT infrastructure after a disaster. DRaaS can help the organization to prioritize its core operations by reducing the need for provisioning and maintaining its own off-site disaster recovery environment, enabling the organization to continue running its applications from the service provider's cloud or hybrid cloud environment, providing the organization with flexible and scalable deployment options, and leveraging the expertise, experience, and best practices of the service provider. (From CISM Manual or related resources)

質問: **173**
組織のシステムへの侵入が成功したことを示す最も適切な指標は次のうちどれですか？
A. ログイン失敗回数の増加
B. 内部ネットワークトラフィックの減少
C. 不規則な申請件数の増加
D. 利用可能な収納スペースの減少
正解: **(正解を表示します)**

質問: **174**
情報セキュリティマネージャーは、セキュリティインシデント時のコミュニケーション計画にメディアコミュニケーション手順を組み込む作業を進めています。最も重要な項目は以下のとおりです。
A. 承認された地元メディア連絡先一覧
B. 事前に準備されたメディア声明
C. 法執行機関への連絡手順
D. 組織内の単一の連絡窓口
正解: **(正解を表示します)**
A single point of contact within the organization is the most important element to include when incorporating media communication procedures into the security incident communication plan because it helps to ensure a consistent and accurate message to the public and avoid confusion or misinformation. A single point of contact is a designated person who is authorized and trained to communicate with the media on behalf of the organization during a security incident. The single point of contact should coordinate with the incident response team, senior management, legal counsel, and public relations to prepare and deliver timely and appropriate statements to the media, as well as to respond to any inquiries or requests. A single point of contact also helps to prevent unauthorized or conflicting disclosures from other employees or stakeholders that may harm the organization's reputation or legal position. Therefore, a single point of contact within the organization is the correct answer.
References:
https://www.lifars.com/2020/09/communication-during-incident-response/
https://ifpo.org/resource-links/articles-and-reports/public-and-media-relations/planning-for-effective-media-relations-during-a-critical-incident/
https://www.techtarget.com/searchsecurity/tip/Incident-response-How-to-implement-a-communication-plan.

質問: **175**
情報セキュリティ監査の結果、ITスタッフがITシステムの構成および管理において定められた基準に従っていなかったことが判明しました。今後同様の事態を防ぐための最善の方法は次のうちどれでしょうか？

A. 情報セキュリティ意識向上トレーニングを毎年実施する
B. 定期的な脆弱性スキャンを実施する
C. 厳格な変更管理プロセスを実施する
D. 構成ベースラインの更新
正解**: C (**コメントを発表する**)**
A strict change control process (C) is the most effective preventive measure because it embeds compliance with standards into the system lifecycle and operational workflow. If staff are deviating from configuration
/management standards, the core issue is often lack of enforced process controls: undocumented changes, rushed fixes, inconsistent approvals, or missing validation. Formal change management ensures changes are requested, risk-assessed, approved by authorized parties, tested, implemented, and reviewed, with traceability and accountability. Annual awareness training (A) helps general understanding but is weaker than a control that prevents and detects unauthorized deviations. Vulnerability scanning (B) is detective and may identify weaknesses after the fact, but it does not ensure standards are followed. Updating configuration baselines (D) is valuable, but without change control, baselines can still be bypassed. In CISM program management, the best answer typically emphasizes repeatable, auditable processes that reduce human error and enforce governance.
References: ISACA CISM Review Manual (Program management-control implementation, change control governance, assurance and compliance); CISM Exam Content Outline (Domain 3).

質問**: 176**
組織のリスク管理へのアプローチを決定する際に、次のうちどれが最適な戦略でしょうか？
A. リスク許容度に基づいた既存管理の成熟度向上
B. 組織の最も重大なリスクを直接的に軽減する対策を優先する
C. すぐに効果が得られるリスク軽減策を実施する
D. 全ての組織単位に一律の統制を導入する
正解**: (**正解を表示します**)**
The best strategy for risk treatment is to prioritize controls that directly mitigate the organization's most critical risks. This aligns with a risk-based approach, where limited resources are directed toward areas with the highest business impact.
"Effective risk treatment involves prioritizing actions that address the most critical risks to the organization, considering impact and likelihood."
- CISM Review Manual 15th Edition, Chapter 2: Risk Response and Mitigation* Advancing maturity or applying quick wins may help, but they are not as strategic or impactful as targeting top-priority risks.

質問**: 177**

金融テクノロジー企業は、スコアリングと不正検出にAIモデルを使用しています。AIモデルの誤作動による悪影響を防ぐための最適な方法は次のうちどれでしょうか？
A. モデルの透明性が確保されていることを確認してください
B. モデル学習に使用するデータを暗号化する
C. 定期的な外部監査とバイアステストを実施する
D. AIモデルのプロセスと出力に対する人間の監視を義務付ける
正解: **(**正解を表示します**)**
The correct answer is D because human oversight is the best way to reduce negative business impacts from AI model hallucinations, especially in financial technology use cases such as scoring and fraud detection.
Hallucinations can produce inaccurate, unsupported, or misleading outputs that may affect customer decisions, fraud alerts, account actions, compliance obligations, or reputational trust. Human review provides a control point before AI outputs are used for significant decisions. Model transparency is useful because it helps explain how outputs are generated, but transparency alone does not prevent harmful decisions.
Encrypting training data protects confidentiality but does not address hallucinated or inaccurate model outputs. External audits and bias testing are valuable governance controls, but they are periodic and may not prevent incorrect outputs in operational decision-making. CISM risk management principles emphasize controls proportionate to business impact and risk. For AI-driven financial decisions, human oversight provides the most direct safeguard against harmful consequences from hallucinations.
Reference: CISM Information Risk Management; AI risk management, human oversight, model output validation, and financial technology control principles.

質問: **178**
情報セキュリティ管理者は、評価の結果、転送中のデータに必要な暗号化が実装されていないことが判明した場合、まず最初に次のうちどれを行うべきでしょうか？
A. 不遵守の理由を特定する
B. 事業影響分析を実施する
C. 上級管理職への報告
D. 補償制御を実施する
正解: **A (**コメントを発表する**)**
The correct answer is A because the information security manager should first determine why the required encryption control has not been implemented. Understanding the reason for noncompliance is necessary before selecting the appropriate corrective action. The issue may be caused by technical limitations, lack of awareness, cost constraints, legacy systems, misconfiguration, project delay, undocumented exception, or business requirements. Performing a business impact analysis is not the first step because BIA is used mainly for continuity planning and impact analysis, not immediate control noncompliance investigation. Reporting to senior management may be necessary if the issue creates significant risk or remains unresolved, but reporting before understanding the

cause may be premature. Implementing compensating controls may be appropriate if encryption cannot be implemented immediately, but the manager must first understand why the requirement was not met. CISM program management emphasizes control monitoring, exception management, root cause understanding, and risk-based remediation. Therefore, determining the reason for noncompliance is the correct first action.
Reference: CISM Information Security Program Development and Management; control compliance, exception management, remediation, and control monitoring principles.

質問: **179**
情報セキュリティ管理者は、組織のCEOになりすましたフィッシングメールを使って送金詐欺を企てる攻撃が増加しているという傾向を把握しました。この種の攻撃に伴うリスクを軽減するための最善策は次のうちどれですか？
A. 電信送金を担当するスタッフに意識向上トレーニングを実施する。
B. 組織の電信送金を一時的に停止します。
C. この種のフィッシング攻撃に対する認識向上トレーニングをCEOに提供する。
D. 電信送金を担当するスタッフのメールを無効にする。
正解: **A** (コメントを発表する)

質問: **180**
新規事業分野に関連するアプリケーションに必要なデータ分類レベルを決定する責任は誰が負うべきか？
A. データアナリスト
B. 情報セキュリティ責任者(ISO)
C. データ管理者
D. データ所有者
正解: **D** (コメントを発表する)
Data owners are responsible for determining the classification of data based on its sensitivity, value, and business impact. They understand the context in which the data is used and can best evaluate its importance and risk profile.
"Data owners are responsible for defining the classification and protection requirements of their data."
- CISM Review Manual 15th Edition, Chapter 2: Information Risk Management, Section: Data Classification Roles* The ISO may assist in developing the classification scheme, but the final responsibility lies with the data owner.

質問: **181**
組織文化をセキュリティガイドラインに沿わせるための最も効果的な方法は、次のうちどれですか？
A. 規制要件を遵守する

B. セキュリティ意識向上活動を実施する
C. セキュリティ手順書を作成し配布する
D. セキュリティポリシーを伝達し、実施する
正解: **(**正解を表示します**)**
Communicating and enforcing policies demonstrates leadership commitment and drives behavior across the organization, fostering a culture of security.
"Policies must be effectively communicated and enforced to influence culture and employee behavior."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Security Culture*

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu **1193**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、顧客データを危険にさらした可能性のある重大なセキュリティ侵害を規制当局に通知しなかったため、規制当局から罰則を受けました。今後同様の罰則を防ぐために、最も見直しと更新が必要なのは次のどれですか。
A. インシデントコミュニケーション計画
B. インシデント対応トレーニングプログラム
C. 事業継続計画 (BCP)
D. 情報セキュリティポリシーと手順
正解: **A (**コメントを発表する**)**

質問: **183**
効果的な情報セキュリティ戦略を策定する上で、最も重要な要素は次のうちどれですか？
A. リスクおよび事業影響評価
B. 明確に定義されたセキュリティポリシーと手順
C. 現在のセキュリティ状態と望ましいセキュリティ状態
D. ビジネスプロセスと要件
正解: **(**正解を表示します**)**

質問: **184**

情報セキュリティ管理者がインシデントを上級管理者にエスカレーションする必要性を判断する際に、最も役立つのは次のうちどれですか？
A. インシデント管理手順
B. インシデント管理ポリシー
C. システムリスク評価
D. 組織リスク登録簿
正解: **(**正解を表示します**)**
The organizational risk register is the most useful for an information security manager when determining the need to escalate an incident to senior management because it contains a list of identified risks to the organization, their likelihood and impact, and their predefined risk thresholds or targets, which can help the information security manager assess the severity and urgency of the incident and decide whether it requires senior management's attention or action. Incident management procedures are not very useful for this purpose because they do not provide any specific criteria or guidance on when to escalate an incident to senior management. Incident management policy is not very useful for this purpose because it does not provide any specific criteria or guidance on when to escalate an incident to senior management. System risk assessment is not very useful for this purpose because it does not reflect the current risk exposure or status of the organization as a whole. References: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6
/how-to-measure-the-effectiveness-of-information-security-using-iso-27004
https://www.isaca.org/resources
/isaca-journal/issues/2017/volume-5/incident-response-lessons-learned

質問: **185**
クラウド プロバイダーと連携してインシデント対応戦略を策定する際に、セキュリティに関する最も重要な考慮事項は次のどれですか。
A. エスカレーションプロセス
B. 技術的能力
C. 復旧時間目標（RTO）
D. セキュリティ監査レポート
正解: **(**正解を表示します**)**
Escalation processes ensure that the provider and the organization can coordinate quickly and effectively during incidents.
"A clearly defined escalation process ensures that incidents are handled swiftly and with the appropriate level of authority, particularly when working with cloud service providers." - CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Cloud and Outsourced Incident Response* ISACA practice questions reinforce that escalation processes are critical when collaborating with third parties in incident management.

質問: **186**

情報セキュリティ投資のための資金調達にビジネスケースを活用する場合、ビジネスケースが以下の条件を満たす場合に最も効果的です。
A. 情報セキュリティの目標を組織戦略に再調整する。
B. 経営陣の意図と情報セキュリティに関する指示を明確な言葉で表現する。
C. 投資を組織の戦略計画に関連付ける。
D. 情報セキュリティポリシーと標準をビジネス要件に変換する。
正解: **A** (コメントを発表する)

質問: **187**
以下のインシデント対応フェーズのうち、事業運営を維持しながら重要システムを保護するための措置が含まれるのはどれですか？
A. 回復
B. 識別
C. 準備
D. 封じ込め
正解: **D** (コメントを発表する)

質問: **188**
情報セキュリティ運営委員会の最も重要な機能は、次のうちどれですか？
A. 組織資産へのデータ分類の割り当て
B. 組織的リスク評価プロセスの開発
C. ビジネスから複数の視点を得る
D. 論理アクセス制御のセキュリティ標準の定義
正解: **C** (コメントを発表する)
An information security steering committee is a group of senior executives and managers from different business units and functions who provide strategic direction, oversight, and support for the information security program. The most important function of the committee is to obtain multiple perspectives from the business, as this helps to ensure that the information security program aligns with the business goals, needs, and culture, and that the security decisions reflect the interests and expectations of the stakeholders.
References = CISM Review Manual 2022, page 331; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.22; Improve Security Governance With a Security Steering Committee2; The Role of the Corporate Information Security Steering Committee3

質問: **189**
ある金融機関が、顧客データの取り扱いを必要とする新たなサービスを導入する計画を立てている。
情報セキュリティ管理者が判断すべき最も重要な事項は次のうちどれですか？
A. 情報セキュリティニーズを支援するためのプロジェクト資金の確保
B. 処理するデータの種類に関連する法的および規制上の要件

C. 取締役会に対するリスクおよびデータプライバシーに関する報告要件
D. 顧客情報を保護するためのインフラストラクチャと技術的制御の適切性
正解**: B (**コメントを発表する**)**
The correct answer is B because a financial institution handling customer data must first understand the legal and regulatory requirements associated with the data being processed. Financial services are highly regulated, and customer data may be subject to privacy, banking, consumer protection, reporting, retention, breach notification, and cross-border transfer requirements. These obligations directly influence security requirements, control design, risk treatment, vendor requirements, monitoring, and governance reporting.
Project funding is important, but funding decisions should be based on the security and compliance requirements that apply. Board reporting requirements may be relevant, but they depend on the regulatory and risk context. Infrastructure and technical controls are also important, but appropriate controls cannot be selected until the organization understands what legal and regulatory obligations apply to the customer data.
In CISM risk management, compliance requirements are critical inputs into risk assessment and control design. Therefore, determining applicable legal and regulatory requirements is the most important activity.
Reference: CISM Information Risk Management; regulatory compliance, customer data protection, financial services risk, and control requirement definition principles.

質問**: 190**
情報セキュリティプログラムの戦略を実行するためのロードマップを作成した後、情報セキュリティマネージャーは次に次のうちどれを行うべきでしょうか？
A. 取締役会から戦略に関する合意を得る。
B. 事業目標との整合性を確認する。
C. 組織のリスク許容度を定義する。
D. 戦略を実行するためのプロジェクト計画を作成する。
正解**: (**正解を表示します**)**
The next thing that an information security manager should do after creating a roadmap to execute the strategy for an information security program is D. Develop a project plan to implement the strategy. This is because a project plan is a detailed document that outlines the scope, objectives, deliverables, milestones, tasks, resources, roles, responsibilities, risks, and dependencies of the implementation process. A project plan can help the information security manager to organize, coordinate, monitor, and control the activities and resources required to execute the strategy and achieve the desired outcomes. A project plan can also facilitate communication, collaboration, and reporting among the project team, stakeholders, and sponsors.
A project plan is a detailed document that outlines the scope, objectives, deliverables, milestones, tasks, resources, roles, responsibilities, risks, and dependencies of the implementation process. (From CISM Manual or related resources) References = CISM

Review Manual 15th Edition, Chapter 3, Section 3.1.2, page 1281; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 74, page 19

質問: **191**
災害復旧におけるリカバリポイント目標(RPO)の貢献は以下のとおりです。
A. 停電期間を最小限に抑える。
B. 単一障害点を排除する。
C. バックアップ戦略を定義する
D. 平均故障間隔(MTBF)を短縮する。
正解: **C (**コメントを発表する**)**
The contribution of recovery point objective (RPO) to disaster recovery is to define backup strategy because it determines the maximum amount of data loss that is acceptable to an organization after a disruption, and guides the frequency and type of backups needed to restore the data to a usable format1. Minimize outage periods is not a contribution of RPO, but rather a contribution of recovery time objective (RTO), which defines the maximum amount of time that is acceptable to restore normal operations after a disruption2. Eliminate single points of failure is not a contribution of RPO, but rather a goal of high availability (HA), which ensures that systems or services are continuously operational and resilient3. Reduce mean time between failures (MTBF) is not a contribution of RPO, but rather a measure of reliability, which indicates the average time that a system or component operates without failure4. References: 1 https://www. druva.com/glossary/what-is-a-recovery-point-objective-definition-and-related-faqs 2 https://www.druva.com /glossary/what-is-a-recovery-time-objective-definition-and-related-faqs 3 https://www.fortinet.com/resources /cyberglossary/high-availability 4 https://www.fortinet.com/resources/cyberglossary/mean-time-between- failures

質問: **192**
インシデント対応計画の有効性を判断するための最良の方法は次のうちどれですか？
A. 過去の監査報告書のレビュー
B. 卓上演習の実施
C. 計画をベストプラクティスと比較評価する
D. 侵入テストの実施
正解: **(**正解を表示します**)**
A tabletop exercise is a simulation of a potential incident scenario that involves the key stakeholders and tests the roles, responsibilities, and procedures of the incident response plan. It is the best way to determine the effectiveness of the plan because it allows the participants to identify and address any gaps, weaknesses, or ambiguities in the plan, as well as to evaluate the communication, coordination, and decision-making processes. A

tabletop exercise can also help to raise awareness, enhance skills, and improve teamwork among the incident response team members and other relevant parties.

質問: **193**
リスクを認識する文化を構築するための最良の方法はどれですか?
A. セキュリティ制御への準拠を定期的にテストします。
B. 脅威が文書化され、タイムリーに伝達されるようにします。
C. リスク認識メッセージを定期的に変更します。
D. スタッフがリスクを報告するためのチャネルを確立します。
正解: **(**正解を表示します**)**

質問: **194**
内部脅威を防止するための最良の方法は次のうちどれですか？
A. 組織全体でセキュリティ意識向上トレーニングを実施する。
B. 厳格なセキュリティポリシーとパスワード管理を実施する。
C. すべてのアクセスアクティビティのログ記録を実装します。
D. 職務分掌と最小権限アクセスを徹底する。
正解: **(**正解を表示します**)**

質問: **195**
以下の役割のうち、データの保護に責任を負うのはどれですか？
A. CISO
B. データ管理者
C. データ所有者
D. データ管理者
正解: **C (**コメントを発表する**)**
Under CISM governance principles, the data owner is accountable for the protection of data. Accountability includes decisions regarding data classification, access authorization, acceptable use, retention, and risk acceptance. While the CISO (A) provides oversight and guidance, they are not accountable for individual data assets. Data custodians (B) and administrators (D) are responsible for implementing and operating controls but do not own the business risk associated with the data. CISM clearly distinguishes accountability (business) from responsibility (operational/technical). Assigning accountability to the data owner ensures that protection requirements align with business value, regulatory obligations, and risk appetite.
References: ISACA CISM Review Manual (Governance-roles and responsibilities, information asset ownership); CISM Exam Content Outline (Domain 2).

質問: **196**

新しく導入された情報セキュリティフレームワークの成功を最もよく示す指標は、次のうちどれでしょうか？
A. セキュリティポリシー例外の件数の減少
B. コンプライアンスに準拠した業務プロセスの増加
C. セキュリティ監査で指摘された事項の減少
D. 確認されたセキュリティインシデント数の増加
正解: **B** (コメントを発表する)

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu 「**193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **197**
リスクオーナーを割り当てる際に最も重要な考慮事項は、オーナーが以下の条件を満たしていることを確認することです。
A. リスク処理および関連する管理活動に関する十分な知識。
B. 意思決定権限とリスクに対する資源配分能力。
C. リスクを効果的に監視および管理するための十分な時間。
D. 意思決定を可能にするためのリスクコミュニケーションと報告のスキル。
正解: (正解を表示します)
Comprehensive and Detailed Explanation = The risk owner is the person or entity with the accountability and authority to manage a risk. The risk owner should have the decision-making authority and the ability to allocate resources for risk treatment and related control activities. The risk owner should also be responsible for monitoring and reporting on the risk, but these are not the most important considerations when assigning a risk owner. The risk owner may not have adequate knowledge of risk treatment and related control activities, but can delegate or consult with experts as needed. The risk owner should also have sufficient time for managing the risk effectively, but this is not a prerequisite for assigning a risk owner.
References =
CISM Review Manual 15th Edition, page 76
CISM Practice Quiz, question 4171

質問: **198**

BYOD(私物端末の業務利用)プログラムを導入する企業にとって、セキュリティ対策が施されていないモバイル端末に保存されている企業データを保護する上で、次のうちどれが最適なセキュリティ対策となるでしょうか？
A. 利用規約
B. コンテナ化ソリューション
C. データ損失防止
D. 機器認証プロセス
正解: **B** (コメントを発表する)
The correct answer is B because containerization separates corporate data and applications from personal data and applications on a mobile device. In a bring your own device environment, the organization does not fully control the endpoint because it is personally owned and may be used on untrusted networks or with unmanaged applications. A containerization solution helps protect enterprise information by enforcing encryption, access controls, remote wipe, data sharing restrictions, and policy controls within the corporate container. An acceptable use policy is important, but it is administrative and does not technically protect data stored on the device. Data loss prevention can help detect or block unauthorized data movement, but it may not provide the same direct separation and control over mobile data. A device certification process helps assess device suitability, but certification alone does not secure corporate data after deployment. In CISM, controls should be selected based on risk and effectiveness. Containerization is the strongest option for protecting corporate data on unsecured BYOD devices.
Reference: CISM Information Risk Management; mobile device risk, BYOD security, data protection, and compensating control principles.

質問: **199**
新しく開発された情報システムに対する最も包括的なセキュリティ要件を定義しているのは次のうちどれですか？
A. リスク評価結果
B. 監査結果
C. 主要リスク指標(KRI)
D. ベースラインコントロール
正解: **D** (コメントを発表する)
Baseline controls are the minimum set of security requirements that apply to all information systems in an organization, regardless of their specific functions or characteristics. They are derived from the organization's security policies, standards, and best practices, and they reflect the organization's risk appetite and tolerance.
Baseline controls provide a consistent and comprehensive foundation for the security of the information systems, and they can be tailored or supplemented by additional controls as needed for specific systems or situations. The other options are not as comprehensive as baseline controls, as they may only address certain aspects or aspects of the security

requirements, or they may vary depending on the system or the context. For example, risk assessment results are an important input for defining the security requirements, but they are not the requirements themselves. Audit findings are an output of evaluating the compliance and effectiveness of the security requirements, but they are not the requirements themselves. Key risk indicators (KRIs) are metrics that measure the level of risk exposure and performance of the security requirements, but they are not the requirements themselves. References = CISM Review Manual 15th Edition, page 113: "Baseline controls are the minimum security requirements that apply to all systems within the organization." CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, question 478:
"Baseline controls are the minimum security requirements that apply to all systems within the organization.
They are derived from the organization's security policies, standards, and best practices, and they reflect the organization's risk appetite and tolerance."

質問**: 200**
組織における新たなリスクを評価する上で、最も大きな課題は次のうちどれですか？
A. リスクフレームワークの欠如
B. セキュリティ対策が不十分
C. 既知の脆弱性の存在
D. 脅威の特定が不完全
正解**: (**正解を表示します**)**
The greatest challenge with assessing emerging risk in an organization is the incomplete identification of threats, as emerging risks are often new, unknown, or unfamiliar, and may not be fully understood or assessed. Incomplete identification of threats can lead to gaps in risk analysis and management, and expose the organization to unexpected or unprepared scenarios. The other options, such as lack of a risk framework, ineffective security controls, or presence of known vulnerabilities, are not specific to emerging risks, and may apply to any type of risk assessment. References:
https://committee.iso.org/sites/tc262/home/projects/ongoing/iso-31022-guidelines-for-impl-2.html
https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-6/emerging-risk-analysis
https://projectriskcoach.com/emerging-risks/

質問**: 201**
インシデント対応プロセスの復旧フェーズにおいて、影響を受けたシステムをオンラインに戻す前に完了しておくべき最も重要な項目は次のうちどれですか？
A. 影響を受けたシステムのフォレンジックイメージをキャプチャして保存します。
B. 上級管理職向け報告のための文書復旧手順。

C. 侵害されたシステムがクリーンであることをテストして検証します。
D. セキュリティインシデントチケットを記録し、クローズします。
正解: **C** (コメントを発表する)

質問: **202**
重要なセキュリティシステムの残存リスクを受け入れるかどうかを判断する上で、以下のうちどれが最も役立つでしょうか？
A. 利用可能な年間予算
B. 緩和策の費用便益分析
C. 復旧時間目標(RTO)
D. 最大許容停電時間(MTO)
正解: (正解を表示します)
Cost-benefit analysis of mitigating controls is the BEST way to assist in determining whether to accept residual risk of a critical security system, because it helps to compare the costs of implementing and maintaining the controls with the benefits of reducing the risk and the potential losses. Cost-benefit analysis can help to justify the investment in security controls and to optimize the level of residual risk that is acceptable for the organization.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 50: "Cost-benefit analysis is the process of comparing the costs of risk treatment options with the benefits of risk reduction and the potential losses from risk events." CISM Review Manual, 16th Edition, ISACA, 2020, p. 51: "Cost-benefit analysis can help to justify the investment in information security controls and to optimize the level of residual risk that is acceptable for the enterprise." CISM Domain 2: Information Risk Management (IRM) [2022 update]: "Cost-benefit analysis: This is a comparison of the costs of implementing and maintaining security controls with the benefits of reducing risk and potential losses. It helps to justify the investment in security controls and optimize the level of residual risk."

質問: **203**
従業員から、企業情報が保存された個人用モバイル端末の紛失が報告されました。情報セキュリティ管理者は、まず以下のどれを行うべきでしょうか？
A. インシデント対応を開始する。
B. リモコンを無効にする
C. デバイスのリセットを開始します。
D. リスク評価を実施する。
正解: (正解を表示します)
Initiating incident response is the first course of action for an information security manager when an employee reports the loss of a personal mobile device containing corporate

information. This will help to contain the incident, assess the impact, and take appropriate measures to prevent or mitigate further damage.
According to ISACA, incident management is one of the key processes for information security governance.
Initiating a device reset, disabling remote access, and conducting a risk assessment are possible subsequent actions, but they should be part of the incident response plan.
References: 1: Find, lock, or erase a lost Android device - Google Account Help 2: Find, lock, or erase a lost Android device - Android Help 3: Lost or Stolen Mobile Device Procedure - Information Security Office : CISM Practice Quiz | CISM Exam Prep | ISACA : 200 CISM Exam Prep Questions | Free Practice Test | Simplilearn : CISM practice questions to prep for the exam | TechTarget

質問**: 204**
情報セキュリティ プログラムに対する組織全体のサポートを得るための最良の方法はどれですか?
A. 定期的なセキュリティ意識向上トレーニングを義務付けます。
B. セキュリティ パフォーマンス メトリックを開発します。
C. セキュリティをビジネス促進要因として位置付けます。
D. IT 戦略に基づいてセキュリティ イニシアチブに優先順位を付けます。
正解**: C (**コメントを発表する**)**
Positioning security as a business enabler is the BEST way to obtain organization-wide support for an information security program, because it helps to demonstrate the value and benefits of security to the organization's strategic objectives, performance, and reputation. By aligning security with the business goals and needs, the information security manager can gain the buy-in and commitment of senior management and other stakeholders, and foster a positive security culture across the organization.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 37: "The information security manager should position information security as a business enabler that supports the achievement of the enterprise's business objectives and adds value to the enterprise."
CISM Review Manual, 16th Edition, ISACA, 2020, p. 39: "The information security manager should communicate the value and benefits of information security to senior management and other stakeholders to obtain their support and commitment for the information security program." CISM Review Manual, 16th Edition, ISACA, 2020, p. 40: "The information security manager should promote a positive security culture within the enterprise by influencing the behavior and attitude of employees and other parties toward information security."

質問**: 205**

イベント ログがインシデント調査に受け入れられるためには、証拠の連鎖を確立するために考慮すべき最も重要な事項は次のどれですか。
A. 集中ログ
B. 管理者ログアクセス
C. 利用可能なフォレンジックツール
D. タイムクロックの同期
正解: **(**正解を表示します**)**

質問: **206**
情報セキュリティガバナンスの望ましい成果として、次のうちどれが挙げられますか？
A. 貫通テスト
B. リスク管理の改善
C. ビジネスの俊敏性
D. 成熟度モデル
正解: **C (**コメントを発表する**)**
Business agility is a desired outcome of information security governance, as it enables the organization to respond quickly and effectively to changing business needs and opportunities, while maintaining a high level of security and risk management. Information security governance provides the strategic direction, policies, standards, and oversight for the information security program, ensuring that it aligns with the organization's business objectives and stakeholder expectations. Information security governance also facilitates the integration of security into the business processes and systems, enhancing the organization's ability to adapt to the dynamic and complex environment. By implementing information security governance, the organization can achieve business agility, as well as other benefits such as improved risk management, compliance, reputation, and value creation. References = CISM Review Manual 15th Edition, page 25.

質問: **207**
主要なITプロジェクトのライフサイクルにセキュリティリスク評価を確実に組み込むには、次のうちどれが最も効果的でしょうか？
A. 情報セキュリティマネージャーをプロジェクト運営委員会に参加させる
B. ITプロジェクトへのグローバルセキュリティ標準の適用
C. プロジェクトマネージャーへのリスク評価に関する研修
D. リスク評価を内部監査プログラムに統合する
正解: **(**正解を表示します**)**

質問: **208**
組織が新たな国へ事業を拡大する際、情報セキュリティマネージャーが最も重視すべき事項は次のうちどれでしょうか？
A. 現地規制の遵守

B. 顧客データを収集する能力
C. 新しい国での文化の違い
D. ITインフラの変化
正解: **A** (コメントを発表する)

質問: **209**
組織のインシデント検知および対応能力を向上させるための最良の方法は、次のうちどれですか？
A. セキュリティギャップ分析を実施する。
B. 事業影響分析(BIA)を実施する。
C. 定期的な意識向上トレーニングを実施する。
D. ネットワーク侵入テストを実施する。
正解: (正解を表示します)
The best way to improve an organization's ability to detect and respond to incidents is to conduct periodic awareness training (C). From a CISM incident management perspective, people are often the first line of detection. Employees, help desk staff, and operational personnel are frequently the first to notice unusual behavior, system anomalies, phishing attempts, or policy violations. Regular awareness training equips them with the knowledge to recognize indicators of compromise and escalate incidents promptly, which directly improves both detection and response times.
A security gap analysis (A) identifies deficiencies in controls but does not improve real-time detection or response capability. A business impact analysis (B) focuses on prioritizing recovery and resilience, not incident identification or handling. Network penetration testing (D) is a preventive and diagnostic activity that helps identify vulnerabilities but does not enhance operational response once an incident occurs.
CISM emphasizes that effective incident management depends on clear roles, defined escalation paths, and continuous awareness across the organization. Periodic training reinforces incident reporting criteria, response procedures, and accountability, thereby strengthening the organization's overall incident detection and response capability.
References:
ISACA CISM Review Manual, Information Security Incident Management - incident detection, response readiness, and awareness ISACA CISM Exam Content Outline, Domain 4: Information Security Incident Management

質問: **210**
情報セキュリティ対策の有効性を経営陣に示すために、最も適切な指標は次のうちどれですか？
A. マルウェア感染によるシステム停止
B. ネットワークスキャンで発見されたセキュリティ脆弱性の数
C. パッチ適用済みのサーバーの割合

D. セキュリティインシデントに起因する年間損失
正解: **(**正解を表示します**)**
Annualized loss resulting from security incidents is the most appropriate metric to demonstrate the effectiveness of information security controls to senior management, as it quantifies the financial impact of security breaches on the organization's assets, operations, and reputation. This metric helps to communicate the value of security investments, justify the security budget, and prioritize the security initiatives based on the potential loss reduction. Annualized loss resulting from security incidents can be calculated by multiplying the annualized rate of occurrence (ARO) of an incident by the single loss expectancy (SLE) of an incident. ARO is the estimated frequency of an incident occurring in a year, and SLE is the estimated cost of an incident. For example, if an organization estimates that a ransomware attack may occur once every two years, and that each attack may cost $100,000 to recover, then the annualized loss resulting from ransomware attacks is $50,000 ($100,000 / 2).
References = CISM Review Manual 2022, page 3171; CISM Exam Content Outline, Domain 4, Knowledge Statement 4.112; Key Performance Indicators for Security Governance, Part 1; Performance Measurement Guide for Information Security

質問: **211**
子会社が内乱が始まったばかりの国に所在していることを知った場合、組織はまず最初に次のうちどれを行うべきでしょうか？
A. インシデント対応計画を発動する。
B. セキュリティ意識向上トレーニングを実施する。
C. 災害復旧計画(DRP)を発動する。
D. リスクプロファイルの変化を評価する。
正解: **(**正解を表示します**)**

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu ↾**193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **212**
情報資産を適切に分類する主な理由は、次のことを決定することです。
A. リスクベースのアプローチを使用した適切な暗号化強度。
B. 資産が侵害された場合のビジネスへの影響。

C. 知る必要があるかどうかに基づいたユーザー アクセス レベル。
D. 機密性に基づいた適切な保護。
正解: **(**正解を表示します**)**

質問: **213**
ブラックボックス制御テストを実施することのホワイトボックス制御テストとの主な利点は、以下の点です。
A. 潜在的な生産上の問題を軽減します。
B. ITスタッフの準備が少なくて済む。
C. 現実世界の攻撃をシミュレートします。
D. より多くの脅威を特定する。
正解: **C (**コメントを発表する**)**
The primary advantage of performing black-box control tests as opposed to white-box control tests is that they simulate real-world attacks. Black-box control tests are a software testing methodology in which the tester analyzes the functionality of an application without a thorough knowledge of its internal design. Conversely, in white-box control tests, the tester is knowledgeable of the internal design of the application and analyzes it during testing. By performing black-box control tests, the tester can mimic the perspective and behavior of an external attacker who does not have access to the source code or the implementation details of the application.
This way, the tester can evaluate how the application responds to different inputs and scenarios, and identify any vulnerabilities or errors that may affect its functionality or security. The other options are not the primary advantage of performing black-box control tests, although they may be some benefits or drawbacks depending on the context. Causing fewer potential production issues is not necessarily true, as black-box control tests may still introduce errors or disruptions to the application if not performed carefully. Requiring less IT staff preparation is not always true, as black-box control tests may still require a lot of planning and documentation to ensure adequate test coverage and quality. Identifying more threats is not necessarily true, as black-box control tests may miss some threats that are hidden in the internal logic or structure of the application.

質問: **214**
セキュリティレポートにおいて、将来を見据えたトレンドを伝える上で最も効果的な方法はどれですか？
A. 主要管理指標(KCI)
B. 主要リスク指標(KRI)
C. 主要業績評価指標(KPI)
D. 主要目標指標(KGI)
正解: **(**正解を表示します**)**

= Security reporting is the process of providing relevant and timely information on the status and performance of the information security program to the stakeholders. Security reporting should be aligned with the business objectives and risk appetite of the organization, and should provide meaningful insights and recommendations for decision making and improvement. Security reporting should also include forward- looking trends, which are projections or predictions of future events or conditions based on historical data, current situation, and external factors. Forward-looking trends can help the organization anticipate and prepare for potential risks and opportunities, and adjust their strategies and plans accordingly.

One of the most effective ways to communicate forward-looking trends within security reporting is to use key risk indicators (KRIs). KRIs are metrics that measure the level of exposure or likelihood of a risk event occurring, and provide early warning signals of potential changes in the risk profile. KRIs can help the organization monitor and manage the key risks that may affect the achievement of their objectives, and take proactive actions to mitigate or avoid them. KRIs can also help the organization identify emerging risks and trends, and evaluate the effectiveness of their risk treatment options. KRIs should be aligned with the risk appetite and tolerance of the organization, and should be regularly reviewed and updated to reflect the changing risk environment.

The other options are not the most effective ways to communicate forward-looking trends within security reporting. Key control indicators (KCIs) are metrics that measure the effectiveness and efficiency of the security controls implemented to reduce the impact or likelihood of a risk event. KCIs can help the organization assess and improve the performance of their security processes and activities, and ensure compliance with the security policies and standards. However, KCIs do not directly measure the level of exposure or likelihood of a risk event, and may not provide sufficient information on the future trends and scenarios. Key performance indicators (KPIs) are metrics that measure the achievement of the security objectives and goals, and demonstrate the value and contribution of the information security program to the organization. KPIs can help the organization evaluate and communicate the results and outcomes of their security initiatives and projects, and align them with the business strategy and vision. However, KPIs do not directly measure the level of exposure or likelihood of a risk event, and may not provide sufficient information on the future trends and scenarios. Key goal indicators (KGIs) are metrics that measure the progress and completion of the security goals and targets, and indicate the degree of success and satisfaction of the information security program. KGIs can help the organization track and report the status and milestones of their security plans and actions, and ensure alignment with the stakeholder expectations and requirements.

However, KGIs do not directly measure the level of exposure or likelihood of a risk event, and may not provide sufficient information on the future trends and scenarios. References = CISM Review Manual, 16th Edition, ISACA, 2020, pp. 77-78, 81-821; CISM Online

Review Course, Domain 3: Information Security Program Development and Management, Module 4: Information Security Program Resources, ISACA2

質問: **215**
情報セキュリティ指標を導入する主な目的は以下のとおりです。
A. 継続的なセキュリティ予算要件をサポートする。
B. 技術的な作業が仕様を満たしていることを確認する。
C. 意思決定に必要な情報を提供する。
D. プログラムの効果をベンチマークと比較する。
正解: **(**正解を表示します**)**

質問: **216**
組織全体でセキュリティ意識向上プログラムを実施することの最大のメリットは次のうちどれですか？
A. セキュリティ戦略が推進されています。
B. セキュリティインシデントの報告件数が減少している。
C. セキュリティ動作が改善されました。
D. セキュリティインシデントがさらに検出されました。
正解: **(**正解を表示します**)**
The greatest benefit of conducting an organization-wide security awareness program is to improve the security behavior of the employees, contractors, partners, and other stakeholders who interact with the organization's information assets. Security behavior refers to the actions and decisions that affect the confidentiality, integrity, and availability of information, such as following the security policies and procedures, reporting security incidents, avoiding risky practices, and applying security controls. By improving the security behavior, the organization can reduce the human-related risks and vulnerabilities, enhance the security culture and awareness, and support the security strategy and objectives.
The other options are not as beneficial as improving the security behavior, although they may also be outcomes or objectives of a security awareness program. Promoting the security strategy is important to communicate the vision, mission, and goals of the security function, as well as to align the security activities with the business needs and expectations. However, promoting the security strategy alone is not enough to ensure its implementation and effectiveness, as it also requires the involvement and commitment of the stakeholders, especially the senior management. Reporting fewer security incidents may indicate a lower level of security breaches or threats, but it may also reflect a lack of detection, reporting, or awareness mechanisms.
Moreover, reporting fewer security incidents is not a reliable measure of the security performance or maturity, as it does not account for the impact, severity, or root causes of the incidents. Detecting more security incidents may indicate a higher level of security

monitoring, alerting, or awareness capabilities, but it may also reflect a higher level of security exposures or attacks. Moreover, detecting more security incidents is not a desirable goal of a security awareness program, as it also implies a higher level of security incidents that need to be responded to and resolved. References = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 201-202, 207-208.
CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1006.
The Benefits of Information Security and Privacy Awareness Training Programs, ISACA Journal, Volume 1,
2019, 1.

質問**: 217**
以下のうち、利用規約の主な目的はどれですか？
A. セキュリティ関連の手順を実行するための手順を提供する
B. セキュリティプロセスワークフローの実施を容易にするため
C. 組織の情報資産の不正使用を防ぐため
D. 情報資産に対する最低限のセキュリティ基準を提供する
正解**: C (**コメントを発表する**)**
The PRIMARY purpose of an acceptable use policy is to protect the organization from misuse of information assets, such as data, hardware, software, and network resources, by defining the rules and expectations for the authorized and appropriate use of these assets by the users. An acceptable use policy helps to prevent or reduce the risks of security breaches, legal liabilities, reputational damage, or loss of productivity that may result from unauthorized, inappropriate, or unethical use of information assets.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 74: "An acceptable use policy is a policy that establishes an agreement between users and the enterprise that defines, for all parties, the ranges of use that are approved before gaining access to a network or the Internet." The essentials of an acceptable use policy - Infosec Resources: "An Acceptable Use Policy (henceforward mentioned as " AUP ") is agreement between two or more parties to a computer network community, expressing in writing their intent to adhere to certain standards of behaviour with respect to the proper usage of specific hardware & software services." Acceptable use policy template - Workable: "This Acceptable Use Policy sets the minimum requirements for the use of our company's IT resources, including computers, networks, devices, software, and internet. It aims to protect our company and our employees from harm and liability, and to ensure that our IT resources are used appropriately, productively, and securely."

質問**: 218**
組織の災害復旧計画(DRP)を作成する際に、情報セキュリティ管理者が最初に行うべきことは次のうちどれですか？
A. 事業影響分析(BIA)を実施する

B. 応答と回復の学習を特定する。
C. コミュニケーションプランを見直してください。
D. 対応および復旧戦略を策定する。
正解: **A (**コメントを発表する**)**
Conducting a business impact analysis (BIA) is the first step when creating an organization's disaster recovery plan (DRP) because it helps to identify and prioritize the critical business functions or processes that need to be restored after a disruption, and determine their recovery time objectives (RTOs) and recovery point objectives (RPOs)2. Identifying the response and recovery teams is not the first step, but rather a subsequent step that involves assigning roles and responsibilities for executing the DRP. Reviewing the communications plan is not the first step, but rather a subsequent step that involves defining the communication channels and protocols for notifying and updating the stakeholders during and after a disruption. Developing response and recovery strategies is not the first step, but rather a subsequent step that involves selecting and implementing the appropriate solutions and procedures for restoring the critical business functions or processes.
References: 2 https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/business-impact-analysis- bia-and-disaster-recovery-planning-drp

質問: **219**
情報セキュリティ管理者は、義務付けられたセキュリティ基準が特定されたビジネス目標の達成を妨げる場合、まず最初に次のうちどれを行うべきでしょうか？
A. 事業目標を再検討する。
B. 上級管理職に報告する。
C. 費用対効果分析を実施する。
D. リスク受容を推奨します。
正解: **(**正解を表示します**)**
Escalate to senior management, because this could help the information security manager to inform the decision-makers of the situation, explain the implications and trade-offs, and seek their guidance and approval for the next steps2. However, this answer is not certain, and you might need to consider other factors as well.

質問: **220**
ある組織のマーケティング部門が、情報セキュリティポリシーに準拠していないオンラインコラボレーションサービスを利用したいと考えている。リスク評価が実施され、リスク受容の手続きが進められている。リスク受容の承認は、以下の者によって行われるべきである。
A. 最高リスク責任者(CRO)
B. 事業部門の上級管理職。

C. 情報セキュリティマネージャー。
D. コンプライアンス担当者
正解: **(**正解を表示します**)**
Risk acceptance is the decision to accept the level of residual risk after applying security controls, and to tolerate the potential impact and consequences of a security incident. Approval of risk acceptance should be provided by business senior management, as they are the owners and accountable parties of the business processes, activities, and assets that are exposed to the risk. Business senior management should also have the authority and responsibility to allocate the resources, personnel, and budget to implement and monitor the risk acceptance decision, and to report and escalate the risk acceptance status to the board of directors or the executive management.
The chief risk officer (CRO) (A) is a senior executive who oversees the organization's risk management function, and provides guidance, direction, and support for the identification, assessment, treatment, and monitoring of risks across the organization. The CRO may be involved in the risk acceptance process, such as by reviewing, endorsing, or advising the risk acceptance decision, but the CRO is not the ultimate approver of risk acceptance, as the CRO is not the owner or accountable party of the business processes, activities, and assets that are exposed to the risk.
The information security manager © is the manager who leads and coordinates the information security function, and provides guidance, direction, and support for the development, implementation, and maintenance of the information security program and activities. The information security manager may be involved in the risk acceptance process, such as by conducting the risk assessment, recommending the risk treatment options, or documenting the risk acceptance decision, but the information security manager is not the ultimate approver of risk acceptance, as the information security manager is not the owner or accountable party of the business processes, activities, and assets that are exposed to the risk.
The compliance officer (D) is the officer who oversees the organization's compliance function, and provides guidance, direction, and support for the identification, assessment, implementation, and monitoring of the compliance requirements and obligations across the organization. The compliance officer may be involved in the risk acceptance process, such as by verifying, validating, or advising the risk acceptance decision, but the compliance officer is not the ultimate approver of risk acceptance, as the compliance officer is not the owner or accountable party of the business processes, activities, and assets that are exposed to the risk.
References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Treatment, Subsection: Risk Acceptance, page 95-961

質問**: 221**
組織のインシデント管理能力を向上させるための最良の方法は、次のうちどれですか？
A. 事業影響分析を実施する

B. 業界のベストプラクティスとのベンチマーク
C. インシデント対応計画を事業計画と整合させる
D. 事後検証から得られた教訓を実践する
正解: **(**正解を表示します**)**
The correct answer is D because implementing lessons learned from post-incident reviews directly improves the organization's incident management capability. Post-incident reviews identify what worked, what failed, where delays occurred, whether escalation was effective, whether communication was timely, and whether containment and recovery procedures were adequate. The value comes from converting those findings into corrective actions, updated procedures, improved training, better tools, revised playbooks, and stronger controls. Performing a business impact analysis is useful for continuity planning and recovery priorities, but it does not directly enhance incident management unless linked to improvements. Benchmarking against best practices can identify improvement opportunities, but it does not improve capability unless changes are implemented. Aligning the incident response plan with the business plan is important for business relevance, but continuous improvement is best achieved through actual lessons learned. CISM incident management emphasizes post-incident review, root cause analysis, corrective action, and continuous improvement.
Reference: CISM Information Security Incident Management; lessons learned, post-incident review, corrective action, and incident response improvement principles.

質問: **222**
情報セキュリティインシデントの影響を受けた顧客への連絡において、以下のうちどれを最も重要に含めるべきでしょうか？
A. 漏洩したデータの種類の詳細
B. 攻撃者の身元
C. 組織にとってのインシデントによるコスト
D. 事件に関する技術情報
正解: **(**正解を表示します**)**
The most important information to include in communications to impacted customers is the details of the type of data exposed (A). From a CISM incident management and governance perspective, customer communications must focus on information that enables affected individuals to understand their personal risk and take appropriate protective actions. Knowing what type of data was exposed (e.g., personal identifiers, financial data, credentials, health information) allows customers to assess potential impact, such as identity theft or fraud, and to take timely mitigation steps.
Identities of attackers (B) are often unknown, sensitive, or irrelevant to customers' immediate needs. Costs to the organization (C) are internal matters and do not help customers protect themselves. Technical details (D) may cause confusion, expose additional security information, or create legal and reputational risk without providing practical value to customers.

CISM emphasizes that incident communications should be clear, accurate, relevant, and audience-focused, while also supporting legal, regulatory, and privacy obligations. Communicating the type of data exposed is central to transparency, trust, and compliance with breach notification requirements.
References:
ISACA CISM Review Manual, Information Security Incident Management - incident communication and stakeholder notification ISACA CISM Exam Content Outline, Domain 4: Information Security Incident Management

質問: **223**
ある組織が、カスタムソフトウェアの開発を第三者サービスプロバイダーに委託することを計画しています。以下のうち、ソフトウェアのセキュリティを最も確実に保証するのに役立つのはどれでしょうか？
A. サービスプロバイダーのソフトウェア開発スタッフ向けセキュリティ研修
B. 関連基準に対する独立した評価
C. 個々の開発者が保有する資格の検証
D. サービスプロバイダーのソフトウェア開発ポリシーのレビュー
正解: **(**正解を表示します**)**
An independent assessment against a relevant standard (B) provides the greatest assurance because it offers objective, third-party validation that security controls and development practices meet defined criteria.
Examples include assessments against secure development standards or recognized control frameworks.
Training (A), certifications (C), and policy reviews (D) are useful inputs, but they are indirect and do not confirm consistent, effective implementation. CISM emphasizes independent assurance for third-party risk management, especially when outsourcing high-risk activities such as custom software development.
Independent assessments reduce reliance on self-attestation and help validate governance, SDLC controls, and security testing practices.
References: ISACA CISM Review Manual (Third-party risk management, assurance, and program oversight); CISM Exam Content Outline (Domain 3).

質問: **224**
インシデント対応計画を策定する情報セキュリティ管理者は、以下の事項を必ず含める必要がある。
A. 重要なデータの目録。
B. エスカレーションの基準。
C. 事業影響分析(BIA)。
D. 重要インフラ図。
正解: **(**正解を表示します**)**

An incident response plan is a set of procedures and guidelines that define the roles and responsibilities of the incident response team, the steps to follow in the event of an incident, and the communication and escalation protocols to ensure timely and effective resolution of incidents. One of the essential components of an incident response plan is the criteria for escalation, which specify the conditions and thresholds that trigger the escalation of an incident to a higher level of authority or a different function within the organization. The criteria for escalation may depend on factors such as the severity, impact, duration, scope, and complexity of the incident, as well as the availability and capability of the incident response team. The criteria for escalation help to ensure that incidents are handled by the appropriate personnel, that management is kept informed and involved, and that the necessary resources and support are provided to resolve the incident. References = https://blog.exigence.io/a-practical-approach-to-incident-management-escalation
https://www.uc.edu/content/dam/uc/infosec/docs/Guidelines/Information_Security_Incident_Response_Escalation_Guideline.pdf

質問: **225**
情報セキュリティ管理者が、セキュリティポリシーを繰り返し遵守していない部署を特定した場合、次に取るべき行動は何でしょうか？
A. 政策遵守を強制するための追加的な管理策を導入する。
B. ポリシー違反を上級管理職に報告する。
C. 部門のユーザーにセキュリティ意識向上トレーニングを再度受講させる。
D. 部署内のシステムに対する脆弱性評価を実施する。
正解: **(**正解を表示します**)**

質問: **226**
インシデント対応チームにとって最も役立つツールは次のどれでしょうか?
A. 侵入検知システム（IDS）
B. エンドポイント検出および対応（EDR）ソリューション
C. ユーザーとエンティティの行動分析
D. 脆弱性スキャンツール
正解: **(**正解を表示します**)**
An endpoint detection and response (EDR) solution provides advanced visibility, detection, and response capabilities at the endpoint level, which are critical for investigating and responding to incidents.
"EDR solutions help identify, investigate, and respond to threats on endpoints quickly, making them vital for incident response teams."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Tools and Technologies for Incident Response* ISACA's practice questions highlight EDR as the most helpful tool for comprehensive incident analysis and response.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu ↾**193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **227**
組織のサイバー攻撃への対応能力を情報セキュリティ管理者に最も正確に示す指標は、次のうちどれですか？
A. インシデント対応計画の概要説明
B. ブラックボックス侵入テスト
C. 模擬フィッシング演習
D. レッドチーム演習
正解: **(**正解を表示します**)**
A red team exercise is a simulated cyber attack conducted by a group of ethical hackers or security experts (the red team) against an organization's network, systems, and staff (the blue team) to test the organization's ability to detect, respond, and recover from a real cyber attack. A red team exercise provides an information security manager with the most accurate indication of the organization's ability to respond to a cyber attack, because it mimics the tactics, techniques, and procedures of real threat actors, and challenges the organization' s security posture, incident response plan, and security awareness in a realistic and adversarial scenario12. A red team exercise can measure the following aspects of the organization's cyber attack response capability3:
The effectiveness and efficiency of the security controls and processes in preventing, detecting, and mitigating cyber attacks The readiness and performance of the incident response team and other stakeholders in following the incident response plan and procedures The communication and coordination among the internal and external parties involved in the incident response process The resilience and recovery of the critical assets and functions affected by the cyber attack The lessons learned and improvement opportunities identified from the cyber attack simulation The other options, such as a walk-through of the incident response plan, a black box penetration test, or a simulated phishing exercise, are not as accurate as a red team exercise in indicating the organization's ability to respond to a cyber attack, because they have the following limitations4 :
A walk-through of the incident response plan is a theoretical and hypothetical exercise that involves reviewing and discussing the incident response plan and procedures with the relevant stakeholders, without actually testing them in a live environment. A walk-through can help to familiarize the participants with the incident response roles and responsibilities,

and to identify any gaps or inconsistencies in the plan, but it cannot measure the actual performance and effectiveness of the incident response process under a real cyber attack scenario.
A black box penetration test is a technical and targeted exercise that involves testing the security of a specific system or application, without any prior knowledge or access to its internal details or configuration. A black box penetration test can help to identify the vulnerabilities and weaknesses of the system or application, and to simulate the perspective and behavior of an external attacker, but it cannot test the security of the entire network or organization, or the response of the incident response team and other stakeholders to a cyber attack.
A simulated phishing exercise is a social engineering and awareness exercise that involves sending fake emails or messages to the organization's staff, to test their ability to recognize and report phishing attempts. A simulated phishing exercise can help to measure the level of security awareness and training of the staff, and to simulate one of the most common cyber attack vectors, but it cannot test the security of the network or systems, or the response of the incident response team and other stakeholders to a cyber attack.
References = 1: What is a Red Team Exercise? | Redscan 2: Red Team vs Blue Team: How They Differ and Why You Need Both | CISA 3: Red Team Exercises: What They Are and How to Run Them | Rapid7 4: What is a Walkthrough Test? | Definition and Examples | ISACA : Penetration Testing Types: Black Box, White Box, and Gray Box | CISA

質問**: 228**
SaaS(Software as a Service)ベンダーを利用する際に伴うリスクを評価する最良の方法は、次のうちどれですか？
A. 契約書に情報セキュリティ要件が含まれていることを確認してください。
B. ベンダーに顧客紹介を依頼する。
C. ベンダーに情報セキュリティに関する質問票への記入を義務付ける。
D. ベンダーの独立管理報告書の結果をレビューする。
正解**: (**正解を表示します**)**
Reviewing the results of the vendor's independent control reports is the best way to assess the risk associated with using a SaaS vendor because it provides an objective and reliable evaluation of the vendor's security controls and practices. Independent control reports, such as SOC 2 or ISO 27001, are conducted by third-party auditors who verify the vendor's compliance with industry standards and best practices. These reports can help the customer identify any gaps or weaknesses in the vendor's security posture and determine the level of assurance and trust they can place on the vendor.
Verifying that information security requirements are included in the contract is a good practice, but it does not provide sufficient assurance that the vendor is actually meeting

those requirements. The contract may also have limitations or exclusions that reduce the customer's rights or remedies in case of a breach or incident.
Requesting customer references from the vendor is not a reliable way to assess the risk associated with using a SaaS vendor because the vendor may only provide positive or biased references that do not reflect the true experience or satisfaction of the customers. Customer references may also not have the same security needs or expectations as the customer who is conducting the assessment.
Requiring vendors to complete information security questionnaires is a useful way to gather information about the vendor's security policies and procedures, but it does not provide enough evidence or verification that the vendor is actually implementing and maintaining those policies and procedures. Information security questionnaires are also subject to the vendor's self-reporting and interpretation, which may not be accurate or consistent. References = CISM Review Manual 15th Edition, page 144 SaaS Security Risk and Challenges - ISACA1 SaaS Security Checklist & Assessment Questionnaire | LeanIX2 Risk Assessment Guide for Microsoft Cloud3

質問**: 229**
火災関連災害に対して実施された物理的および環境的セキュリティ対策の有効性を評価するための最良の方法は、次のうちどれですか？
A. 避難訓練を実施する
B. 災害復旧計画(DRP)を見直す
C. 啓発セッションを実施する
D. 緊急時対応チームの手順を確認する
正解**: (**正解を表示します**)**
Evacuation drills provide real-time validation of physical security measures, staff preparedness, and response time during fire-related scenarios. They test both people and systems.
"Simulated exercises are the most effective method to evaluate real-world preparedness and the adequacy of response procedures."
- CISM Review Manual 15th Edition, Chapter 3: Security Controls Testing* Paper reviews and awareness are useful, but only exercises reveal actual gaps in preparedness.

質問**: 230**
潜在的なシステム脆弱性に対処するための技術的解決策に関するビジネスケースを作成する上で、以下のうちどれが最適な情報源となるでしょうか？
A. リスク評価
B. 事業影響分析(BIA)
C. 貫通試験結果
D. 脆弱性スキャン結果
正解**: A (**コメントを発表する**)**

Risk assessment is the BEST input to a business case for a technical solution to address potential system vulnerabilities, because it helps to identify and prioritize the most critical risks that the solution should mitigate or reduce. Risk assessment also helps to evaluate the costs and benefits of the solution in terms of reducing the likelihood and impact of potential threats and incidents.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 47: "Risk assessment is the process of identifying and analyzing information security risks and determining their potential impact on the enterprise's business objectives." CISM Review Manual, 16th Edition, ISACA, 2020, p. 48: "Risk assessment provides input to the business case for information security investments by identifying and prioritizing the most critical risks that need to be addressed and evaluating the costs and benefits of the proposed solutions."

質問: **231**
組織の情報セキュリティに関するビジョンと戦略を策定する上で、最も優れた情報源は次のうちどれですか？
A. 能力成熟度モデル
B. ガバナンス方針
C. 指標ダッシュボード
D. エンタープライズ情報セキュリティアーキテクチャ
正解: **(正解を表示します)**

質問: **232**
サイバー攻撃が確認された場合、最初に行うべきことは次のうちどれですか？
A. 影響を受けたシステムを隔離します。
B. 上級管理職に報告する。
C. システムをシャットダウンします。
D. 法執行機関に連絡してください。
正解: **(正解を表示します)**
Isolating the affected system is the first step in the incident response process, as it helps to contain the attack, prevent further damage, and preserve the evidence for analysis. Isolating the system can be done by disconnecting it from the network, blocking the malicious traffic, or applying quarantine rules.
References = CISM Review Manual 2022, page 3121; CISM Exam Content Outline, Domain 4, Task 4.22; Cybersecurity Incident Response Exercise Guidance3

質問: **233**
情報セキュリティに対する経営陣の支持を得る上で最も重要な情報は以下のとおりです。
A. 事業戦略との整合性を示すデモンストレーション。
B. 脅威の全体像の把握。

C. 競合他社への攻撃が成功したという報告。
D. 組織リスクの特定。
正解: **A** (コメントを発表する)
The most important information for influencing management's support of information security is an demonstration of alignment with the business strategy because it shows how information security contributes to the achievement of the organization's goals and objectives, and adds value to the organization's performance and competitiveness. An identification of the overall threat landscape is not very important because it does not indicate how information security addresses or mitigates the threats or risks. A report of a successful attack on a competitor is not very important because it does not indicate how information security prevents or responds to such attacks. An identification of organizational risks is not very important because it does not indicate how information security manages or reduces the risks. References: https://www.isaca.org /resources/isaca-journal/issues/2016/volume-4/technical-security-standards-for-information-systems
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/how-to-align-security-initiatives-with-business-goals-and-objectives

質問: **234**
ITシステムに必要な保護レベルを決定する上で、以下のうちどれが最適な入力情報となるか？
A. 脆弱性評価
B. 内部監査結果
C. 資産分類
D. 脅威分析
正解: **C** (コメントを発表する)

質問: **235**
情報セキュリティ管理者は、ユーザーワークステーションに必要な最低限のセキュリティ対策を詳細に記述した要件を文書化したいと考えています。この目的に最も適したリソースは次のうちどれでしょうか？
A. ガイドライン
B. ポリシー
C. 手順
D. 規格
正解: **D** (コメントを発表する)
Standards are detailed statements of the minimum requirements for hardware, software, or security configurations. They are used to define the minimum security controls required for user workstations. References = CISM Review Manual, 16th Edition, page 69.

質問: **236**
ある組織が、新たな市場で優位に立つために、外国の企業を買収しました。情報セキュリティマネージャーが最初にとるべきステップは次のうちどれですか？
A. どの国の情報セキュリティ規制を使用するかを決定する。
B. 既存の2つの情報セキュリティプログラムを統合する。
C. 買収した企業に既存の情報セキュリティプログラムを適用する。
D. 買収した企業に適用される情報セキュリティ法を評価する。
正解: **(正解を表示します)**
The information security manager should first evaluate the information security laws that apply to the acquired company, as they may differ from the laws of the parent organization. This will help the information security manager to understand the legal and regulatory requirements, risks, and challenges that the acquired company faces in its operating environment. The information security manager can then determine the best approach to align the information security programs of the two entities, taking into account the different laws and regulations, as well as the business objectives and strategies of the acquisition. References = : CISM Review Manual 15th Edition, page 32.

質問: **237**
災害復旧計画(DRP)が策定された後、以下のどのタスクを実行すべきでしょうか？
A. テスト計画を作成する。
B. 事業への影響を分析する。
C. 対応チームの役割を定義する。
D. 復旧時間目標(RTO)を特定する。
正解: **A (コメントを発表する)**
= Developing the test plan is the task that should be performed once a disaster recovery plan (DRP) has been developed. The test plan is a document that describes the objectives, scope, methods, and procedures for testing the DRP. The test plan should also define the roles and responsibilities of the test team, the test scenarios and criteria, the test schedule and resources, and the test reporting and evaluation. The purpose of testing the DRP is to verify its effectiveness, identify any gaps or weaknesses, and improve its reliability and usability. Testing the DRP also helps to increase the awareness and readiness of the staff and stakeholders involved in the disaster recovery process. Analyzing the business impact, defining response team roles, and identifying recovery time objectives (RTOs) are all tasks that should be performed before developing the DRP, not after. These tasks are part of the business continuity planning (BCP) process, which aims to identify the critical business functions and assets, assess the potential threats and impacts, and determine the recovery strategies and requirements. The DRP is a subset of the BCP that focuses on restoring the IT systems and services after a disaster. Therefore, the DRP should be based on the results of the BCP process, and tested after it has been developed. References = CISM Review Manual 2023, page 218 1; CISM Practice Quiz 2

質問: **238**
サプライチェーン攻撃によって発生する可能性が最も高いリスクシナリオは次のうちどれですか？
A. 第三者のリソースを介した重要資産の侵害
B. サプライヤーが提供するサービスが利用できない
C. 製品の入手困難による顧客離れ
D. サプライヤーによるハードウェアおよびソフトウェアリソースの供給が不安定
正解: **(**正解を表示します**)**
= A supply chain attack is a type of cyberattack that targets the suppliers or service providers of an organization, rather than the organization itself. The attackers exploit the vulnerabilities or weaknesses in the supply chain to gain access to the organization's network, systems, or data. The attackers may then use the compromised third-party resources to launch further attacks, steal sensitive information, disrupt operations, or damage reputation. Therefore, the most likely risk scenario that emerges from a supply chain attack is the compromise of critical assets via third-party resources. This scenario poses a high threat to the confidentiality, integrity, and availability of the organization's assets, as well as its compliance and trustworthiness.
Unavailability of services provided by a supplier, loss of customers due to unavailability of products, and unreliable delivery of hardware and software resources by a supplier are all possible consequences of a supply chain attack, but they are not the most likely risk scenarios. These scenarios may affect the organization's productivity, profitability, and customer satisfaction, but they do not directly compromise the organization's critical assets. Moreover, these scenarios may be caused by other factors besides a supply chain attack, such as natural disasters, human errors, or market fluctuations. References = CISM Review Manual 2023, page
189 1; CISM Practice Quiz 2

質問: **239**
事前の承認なしに、研修部門が会社を無料のクラウドベースのコラボレーションサイトに登録し、従業員に利用を促しました。情報セキュリティマネージャーの最も適切な対応は次のうちどれですか？
A. サイトの一時的な利用を許可し、データ漏洩を監視します。
B. 活動内容を上級管理職に報告する
C. リスク評価を実施し、影響分析を作成する
D. リスクレジスターを更新し、情報セキュリティ戦略を見直す
正解: **(**正解を表示します**)**
The best response is to conduct a risk assessment and develop an impact analysis. The situation represents shadow IT and possible unauthorized cloud service use, but CISM emphasizes that the security manager should first understand the risk before deciding

whether to allow, restrict, escalate, or formalize the service. A risk assessment identifies what data is being shared, who has access, what contractual protections exist, what privacy or regulatory obligations apply, and what threats may affect the service. An impact analysis helps determine potential business, legal, operational, and reputational consequences. Allowing temporary use and monitoring for leakage may expose the organization before risk is understood. Reporting immediately to senior management may be premature unless the risk is clearly severe. Updating the risk register is appropriate after the risk has been assessed and characterized. Therefore, conducting a risk assessment and impact analysis is the best response because it enables informed, risk-based decision-making about the unauthorized cloud collaboration service.
References:
ISACA CISM Review Manual, Information Risk Management - shadow IT, cloud risk, and risk assessment ISACA CISM Exam Content Outline, Domain 1: Information Risk Management

質問**: 240**
組織内でリスクオーナーを任命する主な理由は次のうちどれですか？
A. 残存リスクを是正するため
B. 責任範囲を明確にする
C. 説明責任を確保するため
D. 新たなリスクを特定する
正解**: C (**コメントを発表する**)**
The primary reason to assign a risk owner in an organization is to ensure accountability for the risk and its treatment. A risk owner is a person or entity that has the authority and responsibility to manage a specific risk and to implement the appropriate risk response actions. By assigning a risk owner, the organization can ensure that the risk is monitored, reported, and controlled in accordance with the organization's risk appetite and tolerance.
References: The CISM Review Manual 2023 defines risk owner as "the person or entity with the accountability and authority to manage a risk" and states that "the risk owner is responsible for ensuring that the risk is treated in a manner consistent with the enterprise's risk appetite and tolerance" (p. 93). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "To ensure accountability is the correct answer because it is the primary reason to assign a risk owner in an organization, as it ensures that the risk and its treatment are managed by a person or entity that has the authority and responsibility to do so" (p. 29). Additionally, the article Risk Ownership: The First Step of Effective Risk Management from the ISACA Journal 2019 states that "risk ownership is the first and most important step of effective risk management" and that "risk ownership ensures that there is clear accountability and responsibility for each risk and that risk owners are empowered to make risk decisions and implement risk responses" (p. 1)

質問: **241**
資産分類プログラムを開発する際、以下の手順のうち、最初に完了すべきものはどれですか？
A. 各資産を分類する。
B. 在庫を作成します。
C. デジタル著作権管理ツールのビジネスケースを作成する。
D. データ損失防止(OLP)システムを導入する。
正解: **(正解を表示します)**
Creating an inventory is the FIRST step in developing an asset classification program because it helps to identify and list all the information systems assets of the organization that need to be protected and classified.
An inventory should include the asset name, description, owner, custodian, location, type, value, and other relevant attributes. Creating an inventory also enables the establishment of the ownership and custody of the assets, which are essential for defining the roles and responsibilities for asset protection and classification12.
Categorizing each asset (A) is a subsequent step in developing an asset classification program, after creating an inventory. Categorizing each asset involves assigning a security level or category to each asset based on its value, sensitivity, and criticality to the organization. The security level or category determines the protection level and controls required for each asset12. Creating a business case for a digital rights management tool © is not a step in developing an asset classification program, but rather a possible outcome or recommendation based on the asset classification results. A digital rights management tool is a type of control that can help to enforce the security policies and objectives for the classified assets, such as preventing unauthorized access, copying, or distribution of the assets3. Implementing a data loss prevention (DLP) system (D) is also not a step in developing an asset classification program, but rather a possible outcome or recommendation based on the asset classification results. A DLP system is a type of control that can help to monitor, detect, and prevent the loss or leakage of the classified assets, such as through email, web, or removable media4. References = 1:
CISM Review Manual 15th Edition, page 77-781; 2: IT Asset Valuation, Risk Assessment and Control Implementation Model - ISACA2; 3: What is Digital Rights Management? - Definition from Techopedia3; 4:
What is Data Loss Prevention (DLP)? - Definition from Techopedia4

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu ｶ193問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **242**
頻繁に発生するインシデントをユーザーセキュリティ意識向上トレーニングプログラムに反映させるための最善の方法は、以下を含めることです。
A. 退職面接の結果。
B. 過去のトレーニングセッション。
C. ヘルプデスクへの問い合わせ例。
D. セキュリティに関する質問への回答。
正解: **C** (コメントを発表する)
The best way to ensure that frequently encountered incidents are reflected in the user security awareness training program is to include examples of help desk requests. Help desk requests are requests for assistance or support from users who encounter problems or issues related to information security, such as password resets, malware infections, phishing emails, unauthorized access, data loss, or system errors. Help desk requests can provide valuable insights into the types, frequencies, and impacts of the incidents that affect the users, as well as the users' knowledge, skills, and behaviors regarding information security. By including examples of help desk requests in the user security awareness training program, the information security manager can achieve the following benefits12:
Increase the relevance and effectiveness of the training content: By using real-life scenarios and cases that the users have experienced or witnessed, the information security manager can make the training content more relevant, engaging, and applicable to the users' needs and situations. The information security manager can also use the examples of help desk requests to illustrate the consequences and costs of the incidents, and to highlight the best practices and solutions to prevent or resolve them. This can help the users to understand the importance and value of information security, and to improve their knowledge, skills, and attitudes accordingly.
Identify and address the gaps and weaknesses in the training program: By analyzing the patterns and trends of the help desk requests, the information security manager can identify and address the gaps and weaknesses in the existing training program, such as outdated or inaccurate information, insufficient or ineffective coverage of topics, or lack of feedback or evaluation. The information security manager can also use the examples of help desk requests to measure and monitor the impact and outcomes of the training program, such as changes in the number, type, or severity of the incidents, or changes in the users' satisfaction, performance, or behavior.
Enhance the communication and collaboration with the users and the help desk staff: By including examples of help desk requests in the user security awareness training program, the information security manager can enhance the communication and collaboration with

the users and the help desk staff, who are the key stakeholders and partners in information security. The information security manager can use the examples of help desk requests to solicit feedback, suggestions, or questions from the users and the help desk staff, and to provide them with timely and relevant information, guidance, or support. The information security manager can also use the examples of help desk requests to recognize and appreciate the efforts and contributions of the users and the help desk staff in reporting, responding, or resolving the incidents, and to encourage and motivate them to continue their involvement and participation in information security.
The other options are not the best way to ensure that frequently encountered incidents are reflected in the user security awareness training program, as they are less reliable, relevant, or effective sources of information.
Results of exit interviews are feedback from employees who are leaving the organization, and they may not reflect the current or future incidents that the remaining or new employees may face. Previous training sessions are records of the past training activities, and they may not capture the changes or updates in the information security environment, threats, or requirements. Responses to security questionnaires are answers to predefined questions or surveys, and they may not cover all the possible or emerging incidents that the users may encounter or experience12. References = Information Security Awareness Training: Best Practices
- Infosec Resources, How to Create an Effective Security Awareness Training Program - Infosec Resources, Security Awareness Training: How to Build a Successful Program - ISACA, Security Awareness Training: How to Educate Your Employees - ISACA

質問: **243**
次のうち、インシデントトリアージの主な目的はどれですか？
A. コミュニケーションの調整
B. 脆弱性の軽減
C. イベントの分類
D. 脅威の封じ込め
正解: **(**正解を表示します**)**
The primary objective of incident triage is to categorize events based on their severity, impact, urgency, and priority. Incident triage helps the security operations center (SOC) to allocate the appropriate resources, assign the relevant roles and responsibilities, and determine the best course of action for each event. Incident triage also helps to filter out false positives, reduce noise, and focus on the most critical events that pose a threat to the organization's information security.
Coordination of communications, mitigation of vulnerabilities, and containment of threats are important tasks that are performed during the incident response process, but they are not the primary objective of incident triage. Coordination of communications ensures that the relevant stakeholders are informed and updated about the incident status, roles, actions, and outcomes. Mitigation of vulnerabilities addresses the root causes of the

incident and prevents or reduces the likelihood of recurrence. Containment of threats isolates and stops the spread of the incident and minimizes the damage to the organization's assets and operations. These tasks are dependent on the outcome of the incident triage, which determines the scope, severity, and priority of the incident.
References = CISM Certified Information Security Manager Study Guide, Chapter 8: Security Operations and Incident Management, page 2691; CISM Foundations: Module 4 Course, Part One: Security Operations and Incident Management2; Critical Incident Stress Management - National Interagency Fire Center3; Critical Incident Stress Management - US Forest Service4

質問: **244**
クラウド技術環境において、セキュリティインシデントの調査において、以下のうちどれが最大の課題となるでしょうか？
A. 非標準イベントログ
B. データ暗号化
C. ハードウェアへのアクセス
D. 圧縮された顧客データ
正解: **(**正解を表示します**)**

質問: **245**
サイバーセキュリティインシデントへの対応が成功した後に実施される教訓抽出演習において、以下のうちどれを最優先事項とすべきでしょうか？
A. 事件の根本原因の特定
B. 事件で使用された攻撃ベクトルの特定
C. 事件後、事業運営が再開されたとき
D. インシデント管理プロセスはどのように実行されたか
正解: **(**正解を表示します**)**
The primary focus of a lessons learned exercise following a successful response to a cybersecurity incident is to evaluate how the incident management processes were executed, and to identify the strengths, weaknesses, best practices, and improvement opportunities for future incidents. A lessons learned exercise is not meant to determine the root cause, the attack vectors, or the recovery time of the incident, but rather to assess the performance and effectiveness of the incident response team and the incident response plan.
References: The CISM Review Manual 2023 states that "post-incident reviews are an essential part of the incident response process" and that "they provide an opportunity to assess the performance of the incident response team, identify areas for improvement, and document lessons learned and best practices" (p. 191).
The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "How incident management processes were executed is the correct answer because it is the primary focus of a lessons learned exercise, which

aims to evaluate the incident response capability and to implement corrective actions and improvement plans" (p. 97). Additionally, the Cybersecurity Incident Response Exercise Guidance article from the ISACA Journal 2022 states that "The AAR [after-action review] should include the date and time of the exercise, a list of participants, scenario descriptions, findings (generic and specific), observations with recommendations, lessons learned and an evaluation of the exercise (strengths, weaknesses, lessons learned)" (p. 3)1

質問: **246**
情報セキュリティポリシーは、主に以下の点との整合性を反映するべきである。
A. 業界のベストプラクティス。
B. データセキュリティ基準。
C. 経営陣の意図。
D. 情報セキュリティフレームワーク。
正解: **(**正解を表示します**)**

質問: **247**
組織のインシデント対応プロセスのテスト中に検証すべき最も重要な項目は次のうちどれですか？
A. ユーザーが通話ツリーでどの番号に電話をかけるべきかを知っているかどうか
B. インシデント対応チームのメンバーが自身の責任を認識しているか
C. インシデント対応チームのメンバーが複数の分野で訓練を受けているかどうか
D. 経営陣がインシデント対応プロセスを承認しているかどうか
正解: **B (**コメントを発表する**)**
The most important item to verify during an incident response test is whether incident response team members know their responsibilities. CISM incident management emphasizes that effective response depends on clearly defined and understood roles, responsibilities, escalation paths, and decision authority. During a real incident, confusion about who must contain, investigate, communicate, approve, or recover systems can cause delays and increase business impact. Users knowing call-tree numbers is useful, but the response team's execution responsibilities are more central to incident handling. Cross-training is valuable for resilience, but it is secondary to each team member understanding their assigned role. Senior management endorsement is important for governance and support, but it is not what an operational test primarily validates. Incident response testing should determine whether the process works in practice, including coordination, communication, containment, escalation, and recovery. Therefore, verifying that response team members understand their responsibilities is the most important objective of the test.
References:

ISACA CISM Review Manual, Information Security Incident Management - incident response testing, roles, and responsibilities ISACA CISM Exam Content Outline, Domain 4: Information Security Incident Management

質問: **248**
組織全体で報告された情報セキュリティインシデントを文書化する最も重要な理由は次のうちどれですか？
A. 事件の再発を防止する。
B. 組織のセキュリティ体制を評価する。
C. セキュリティへの企業投資を支援する。
D. 未解決のリスクを特定する。
正解: **(**正解を表示します**)**

質問: **249**
組織がインシデント対応チームの適切な準備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. 第三者鑑識会社による研修の提供
B. 対応チームの業界認定資格の取得
C. 組織に適した机上演習を実施する
D. 組織と対応手順に関する複数のシナリオを文書化する
正解: **C (**コメントを発表する**)**
The BEST way for an organization to ensure that incident response teams are properly prepared is by conducting tabletop exercises appropriate for the organization.
Tabletop exercises are an effective way to test and validate an organization ' s incident response plan (IRP) and the readiness of the incident response team. These exercises simulate different scenarios in a controlled environment and allow the team to practice their response procedures, identify gaps, and make improvements to the plan. By conducting regular tabletop exercises, the incident response team can stay current with changes in the threat landscape and ensure that they are prepared to respond to incidents effectively.
According to the Certified Information Security Manager (CISM) Study Manual, " Tabletop exercises are a valuable tool for testing and validating the effectiveness of the IRP and the readiness of the incident response team. These exercises simulate different scenarios in a controlled environment and allow the team to practice their response procedures, identify gaps, and make improvements to the plan. " While providing training from third-party forensics firms, obtaining industry certifications, and documenting multiple scenarios for the organization and response steps can all be useful in preparing incident response teams, they are not as effective as conducting tabletop exercises appropriate for the organization.
Reference:
Certified Information Security Manager (CISM) Study Manual, 15th Edition, Page 324.

質問: **250**
新型ランサムウェアが組織のネットワークに感染しました。この状況を組織が最も効果的に検知できたのは、次のうちどれでしょうか？
A. システム動作の異常監視
B. 脅威状況の定期的な見直し
C. エンドユーザー向けの定期的な情報セキュリティ研修
D. 統合パッチ展開ツールの使用
正解: **(正解を表示します)**

質問: **251**
組織に影響を与える可能性のある情報リスクの概要を上級管理職に伝える上で、次のうちどれが最も役立ちますか？
A. 第三者リスク評価
B. 事業影響分析
C. 内部監査報告書
D. リスク登録簿
正解: **(正解を表示します)**
The correct answer is D because a risk register provides a consolidated overview of identified risks, owners, likelihood, impact, treatment plans, residual risk, status, and priorities. Senior management needs an enterprise-level view of information risk to support oversight, resource allocation, risk acceptance, and strategic decision-making. A third-party risk assessment is useful, but it focuses only on vendor or external provider risk and does not provide a complete organizational risk overview. A business impact analysis identifies the impact of disruptions on business processes and supports continuity planning, but it is not a full inventory of information risks. Internal audit reports provide independent assurance and identify control issues, but they are periodic and may not include all current risks. In CISM risk management, the risk register is a key tool for tracking, communicating, and managing information risk across the organization. Therefore, it is the most useful source for giving senior management an overview of information risk that may affect the organization.
Reference: CISM Information Risk Management; risk register, enterprise risk reporting, risk ownership, and senior management oversight.

質問: **252**
インシデント対応計画のどの段階で根本原因が特定されるのか？
A. 回復
B. 学んだ教訓
C. 封じ込め
D. 根絶

正解: **D** (コメントを発表する)
The eradication phase of an incident response plan is where the root cause of the incident is determined and eliminated. This phase involves identifying and removing all traces of the malicious activity from the affected systems and restoring them to a secure state. References = NIST SP 800-61 Revision 2, CISM Review Manual 15th Edition

質問: **253**
システムが侵害を検出できないリスクに最もよく対処できるのは次のどれですか?
A. ユーザーアクセスレビュー
B. ログ監視
C. 脆弱性スキャン
D. セキュリティ管理テスト
正解: (正解を表示します)
Log monitoring (B) directly addresses the risk of a system failing to detect a breach by enabling continuous visibility into system activity, anomalies, and indicators of compromise. CISM emphasizes detection as a critical component of incident management, with log review and monitoring serving as primary detective controls. User access reviews (A) are preventive and periodic, not real-time. Vulnerability scanning (C) identifies weaknesses but does not detect active breaches. Security control testing (D) validates control design and effectiveness but does not provide ongoing breach detection. Effective log monitoring reduces mean time to detect incidents and limits business impact. References: ISACA CISM Review Manual (Incident management-detection and monitoring); CISM Exam Content Outline (Domain 4).

質問: **254**
最小権限の原則を実施するには、主に以下の事項を特定する必要があります。
A. 職務内容
B. データ所有者
C. 主要な危険因子。
D. 認証制御
正解: (正解を表示します)
Implementing the principle of least privilege primarily requires the identification of job duties. Job duties are the specific tasks and responsibilities that an individual performs as part of their role in the organization. By identifying the job duties, the organization can determine the minimum access privileges necessary for each individual to perform their assigned function, and nothing more. This helps to reduce the risk of unauthorized access, misuse, or compromise of information and resources. The principle of least privilege is a key security principle that states that every module (such as a user, a process, or a program) must be able to access only the information and resources that are necessary for its legitimate purpose12.

The other options are not the primary factors that require identification for implementing the principle of least privilege. Data owners are the individuals or entities that have the authority and responsibility to define the classification, usage, and protection of data. Data owners may be involved in granting or revoking access privileges to data, but they are not the ones who identify the job duties of the data users. Primary risk factors are the sources or causes of potential harm or loss to the organization. Primary risk factors may influence the level of access privileges granted to users, but they are not the ones who define the job duties of the users.
Authentication controls are the mechanisms that verify the identity of users or systems before granting access to resources. Authentication controls may enforce the principle of least privilege, but they are not the ones who determine the job duties of the users.
References = Principle of least privilege What Is the Principle of Least Privilege and Why is it Important? - F5 1
4

質問: **255**
既知の脆弱性があるWebアプリケーションを使用する場合、次のうちどれが最善の対処法ですか？
A. ホストベースの侵入検知を導入する。
B. アプリケーションファイアウォールを導入します。
C. アプリケーションレベルのログを監視します。
D. スパイウェア対策ソフトウェアをインストールしてください。
正解: **(正解を表示します)**

質問: **256**
組織にとって、脆弱性スキャンツールの主な利点は次のうちどれですか？
A. ネットワーク上のデバイスがもたらす潜在的なリスクを特定する
B. 組織プロセスにおける脆弱性の特定
C. 複雑な脆弱性を見逃さないようにする
D. 情報セキュリティリスク分析プログラムの自動化
正解: **(正解を表示します)**
The primary benefit of a vulnerability scanning tool is identifying potential risks posed by devices on the network. Vulnerability scanning detects known technical weaknesses in systems, applications, services, and configurations. These weaknesses may expose the organization to threats and therefore represent potential sources of risk. CISM distinguishes vulnerability identification from full risk analysis: scanning provides technical input, but risk analysis also requires evaluating likelihood, impact, asset value, and business context.
A vulnerability scanner does not identify weaknesses in organizational processes, which usually require audits, assessments, or process reviews. It also cannot ensure that

complex vulnerabilities are never missed, since scanning tools depend on coverage, signatures, configuration, and scope. Finally, it does not automate the complete risk analysis program; it only supplies data for risk evaluation. CISM risk management guidance emphasizes that vulnerability information must be interpreted in relation to business impact and threat exposure. Therefore, the best answer is identifying potential risks associated with networked devices.
References:
ISACA CISM Review Manual, Information Risk Management - vulnerability identification and risk analysis inputs ISACA CISM Exam Content Outline, Domain 1: Information Risk Management

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu **1193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **257**
特権アカウントに関連するリスクを軽減するための主要な予防策は、次のうちどれですか？
A. 必要なユーザーにのみ特権アカウントへのアクセスを提供します。
B. 特権アカウントの活動を頻繁に監視する。
C. 特権アカウントへのアクセスについて定期的な認証を実施する。
D. 特権アカウントを削除します。
正解: **(**正解を表示します**)**

質問: **258**
インシデント対応計画のエスカレーション手順を策定する際に、最も重要な事項は次のうちどれですか？
A. 各プロセスには責任者が割り当てられます。
B. 連絡先リストは定期的に更新されます。
C. 最低限の規制要件が維持されています。
D. 上級管理職の承認が文書化されています。
正解: **B (**コメントを発表する**)**
= The contact list is the most important element of the escalation procedures for an incident response plan, as it ensures that the appropriate stakeholders are notified and involved in the incident management process. A contact list should include the names,

roles, responsibilities, phone numbers, email addresses, and backup contacts of the key personnel involved in the incident response, such as the incident response team, senior management, legal counsel, public relations, law enforcement, and external service providers. The contact list should be regularly updated and tested to ensure its accuracy and availability123. References =
1: Information Security Incident Response Escalation Guideline2, page 4
2: A Practical Approach to Incident Management Escalation1, section "Step 2: Log the escalation and record the related incident problems that occurred"
3: Computer Security Incident Handling Guide4, page 18

質問: **259**
情報セキュリティプログラムへの継続的な投資を最も正当化する要因は次のうちどれでしょうか？
A. 残存リスクの低減
B. セキュリティフレームワークとの整合性
C. 実装のスピード
D. 業界における同業他社とのベンチマーク
正解: **(**正解を表示します**)**
Residual risk is the risk that remains after implementing controls to mitigate the inherent risk. A reduction in residual risk indicates that the information security program is effective in managing the risks to an acceptable level. This would best justify the continued investment in the program, as it demonstrates the value and benefits of the security activities. Security framework alignment, speed of implementation, and industry peer benchmarking are not direct measures of the effectiveness or value of the information security program. They may be useful for comparison or compliance purposes, but they do not necessarily reflect the impact of the program on the risk profile of the organization. References = CISM Review Manual, 16th Edition, page 431; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 622 Residual risk is the remaining risk after all security controls have been implemented. It is important to measure the residual risk of an organization in order to determine the effectiveness of the security program and to justify continued investment in the program. A reduction in residual risk is an indication that the security program is effective and that continued investment is warranted.

質問: **260**
情報セキュリティガバナンスとコーポレートガバナンスが統合されていることを最もよく示しているのは、次のうちどれですか？
A. 情報セキュリティチームはビジネス目標を認識しています。
B. 取締役会は情報セキュリティの主要業績評価指標(KPI)について定期的に報告を受けています。
C. 情報セキュリティ運営委員会は、ビジネスリーダーで構成されています。

D. すべての情報セキュリティ対策について費用対効果分析を実施します。
正解: **(**正解を表示します**)**
The information security steering committee is composed of business leaders is the best indicator that information security governance and corporate governance are integrated, as this shows that the information security program is aligned with the business objectives and strategies, and that the information security manager has the support and involvement of the senior management. The information security steering committee is responsible for overseeing the information security program, setting the direction and scope, approving policies and standards, allocating resources, and monitoring performance and compliance. The information security steering committee also ensures that the information security risks are communicated and addressed at the board level, and that the information security program is consistent with the corporate governance framework and culture. The information security team is aware of business goals, the board is regularly informed of information security key performance indicators (KPIs), and a cost-benefit analysis is conducted on all information security initiatives are also important, but not as important as the information security steering committee is composed of business leaders, as they do not necessarily imply that the information security governance and corporate governance are integrated, and that the information security program has the authority and accountability to achieve its goals. References = CISM Review Manual 2023, page 271; CISM Review Questions, Answers & Explanations Manual 2023, page 342; ISACA CISM - iSecPrep, page 193

質問: **261**
医療機関が、第三者ベンダーにおける情報漏洩の報告を受けました。医療機関の情報セキュリティ管理者は、まず最初に次のうちどれを行うべきでしょうか？
A. 関係規制機関に通知する
B. 関連する契約条項を確認する
C. 影響を評価する
D. 上級管理職に通知する
正解: **(**正解を表示します**)**
The correct answer is C because the first step after being informed of a third-party vendor breach is to assess the impact on the organization. The information security manager must determine whether organizational data, patient information, regulated records, systems, services, or business processes were affected. This assessment helps determine incident severity, legal notification obligations, regulatory reporting requirements, contractual rights, business impact, and required containment actions. Notifying regulatory bodies may be required in a health care context, but notification should be based on confirmed facts such as affected data types, number of individuals impacted, jurisdiction, and reporting thresholds. Reviewing contract clauses is important to understand vendor obligations, breach notification timelines, audit rights, and liability, but the organization first needs to understand the impact. Notifying senior management may be necessary for significant

incidents, but meaningful notification depends on initial impact assessment. CISM incident management and third-party risk principles emphasize timely assessment, classification, escalation, and response. Therefore, assessing impact is the correct first action.
Reference: CISM Information Security Incident Management; third-party breach response, impact assessment, health care data protection, and incident escalation principles.

質問: **262**
サイバーインシデントの影響度に基づいて優先順位を付け、解決するまで追跡するのに最も効果的なシステムはどれですか？
A. セキュリティ情報およびイベント管理(SIEM)
B. 拡張型検出 ･対応(XDR)
C. エンドポイント検出 ･対応(EDR)
D. ネットワーク侵入検知システム(NIDS)
正解: **(**正解を表示します**)**
A SIEM system provides the ability to collect, correlate, and analyze security events, enabling effective prioritization of incidents based on risk and impact. SIEM solutions also support tracking incidents from detection through resolution, as stated in the CISM Review Manual under incident management and monitoring.
Reference:ISACA CISM Review Manual, 16th Edition, Page 303-304, " SIEM and Incident Prioritization " .

質問: **263**
組織の情報セキュリティポリシーを策定する際に、最も重要な考慮事項は次のうちどれでしょうか？
A. 職務内容には、セキュリティポリシーを読むことが求められます。
B. ポリシーは毎年更新されます。
C. 経営陣はこれらの方針を支持しています。
D. これらのポリシーは業界のベストプラクティスに準拠しています。
正解: **C (**コメントを発表する**)**
The most important consideration when establishing information security policies for an organization is to ensure that senior management supports the policies. Senior management support is essential for the successful implementation and enforcement of information security policies, as it demonstrates the commitment and accountability of the organization's leadership to information security. Senior management support also helps to allocate adequate resources, establish clear roles and responsibilities, and promote a security-aware culture within the organization. Without senior management support, information security policies may not be aligned with the organization's goals and objectives, may not be communicated and disseminated effectively, and may not be followed or enforced consistently.

Job descriptions that include requirements to read security policies are a way of ensuring that employees are aware of their security obligations, but they are not the most important consideration when establishing information security policies. The policies should be relevant and applicable to the employees' roles and functions, and should be reinforced by regular training and awareness programs.
The policies should be updated periodically to reflect the changes in the organization's environment, risks, and requirements, but updating them annually may not be sufficient or necessary. The frequency of updating the policies should depend on the nature and impact of the changes, and should be determined by a defined policy review process.
The policies should be aligned with industry best practices, standards, and frameworks, but this is not the most important consideration when establishing information security policies. The policies should also be customized and tailored to the organization's specific context, needs, and expectations, and should be consistent with the organization's vision, mission, and values. References = ISACA, CISM Review Manual, 16th Edition, 2020, pages 37-38.
ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1009.

質問: **264**
コールセンターにおいて、ソーシャルエンジニアリングを行う最大の理由は以下のとおりです。
A. 追加のセキュリティ研修を受ける候補者を特定する。
B. 攻撃が成功する可能性を最小限に抑える。
C. 情報セキュリティ対策のための資金を獲得する。
D. パスワードポリシーを改善する。
正解: **A (**コメントを発表する**)**
The best reason to conduct a social engineering test in a call center is to identify candidates for additional security training because it helps to assess the level of awareness and skills of the call center staff in recognizing and resisting social engineering attacks, and provide them with the necessary training or education to improve their security posture. Minimizing the likelihood of successful attacks is not a reason to conduct a social engineering test, but rather a possible outcome or benefit of conducting such a test.
Gaining funding for information security initiatives is not a reason to conduct a social engineering test, but rather a possible outcome or benefit of conducting such a test.
Improving password policy is not a reason to conduct a social engineering test, but rather a possible outcome or benefit of conducting such a test. References:
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-6/the-value-of-penetration-testing
https://www.isaca.org/resources/isaca-journal/issues/2016/volume-5/security-scanning-versus-penetration-testing

質問: **265**
ある組織が、使用されていないと思われる大量の古いデータを発見しました。情報セキュリティマネージャーは次に、次のうちどれを行うべきでしょうか？
A. 記録保存ポリシーを参照してください。
B. 意識向上および研修プログラムを更新する。
C. メディアのサニタイズ手順を実施する。
D. バックアップおよび復旧ポリシーを参照してください。
正解: **(正解を表示します)**
The next thing that the information security manager should do after identifying a large volume of old data that appears to be unused is to consult the record retention policy. The record retention policy is a document that defines the types, formats, and retention periods of data that the organization needs to keep for legal, regulatory, operational, or historical purposes. By consulting the record retention policy, the information security manager can determine if the old data is still required to be stored, archived, or disposed of, and how to do so in a secure and compliant manner.
References: The CISM Review Manual 2023 states that "the information security manager is responsible for ensuring that the data lifecycle management process is in alignment with the organization's record retention policy" and that "the record retention policy defines the types, formats, and retention periods of data that the organization needs to keep for legal, regulatory, operational, or historical purposes" (p. 140). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Consult the record retention policy is the correct answer because it is the next logical step to take after identifying a large volume of old data that appears to be unused, as it will help the information security manager to decide on the appropriate data lifecycle management actions for the old data, such as storage, archiving, or disposal" (p. 64). Additionally, the article Data Retention Policy: What It Is and How to Create One from the ISACA Journal 2019 states that "a data retention policy is a document that outlines the types, formats, and retention periods of data that an organization needs to keep for various purposes, such as legal compliance, business operations, or historical records" and that "a data retention policy can help an organization to manage its data lifecycle, optimize its storage capacity, reduce its costs, and enhance its security and privacy" (p. 1)1.

質問: **266**
インシデント対応計画を成功裏に実施するために、以下のうち最も重要なものはどれですか？
A. 対応スタッフの機能に関するRACIチャートの作成
B. 対応要員が適切な訓練を受けていることを確認する
C. ヘルプデスクのエスカレーションプロセスを確立する
D. インシデント対応報告のための指標の開発

正解: **(**正解を表示します**)**

質問: **267**
組織が混乱時にも、許容可能な時間枠内で、かつ事前に定義された能力で製品やサービスの提供を維持できる能力を最も効果的に実現できるのは、次のうちどれですか？
A. サービスレベル契約(SLA)
B. 事業継続計画(BCP)
C. 災害復旧計画(DRP)
D. 事業影響分析(BIA)
正解: **(**正解を表示します**)**
The best option to enable the capability of an organization to sustain the delivery of products and services within acceptable time frames and at predefined capacity during a disruption is B. Business continuity plan (BCP). This is because a BCP is a documented collection of procedures and information that guides the organization to prepare for, respond to, and recover from a disruption, such as a natural disaster, a cyberattack, or a pandemic. A BCP aims to ensure the continuity of the critical business functions and processes that support the delivery of products and services to the customers and stakeholders. A BCP also defines the roles, responsibilities, resources, and actions required to maintain the operational resilience of the organization in the face of a disruption.
References = CISM Review Manual 15th Edition, Chapter 4, Section 4.2.3, page 2141; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 6, page 3

質問: **268**
情報セキュリティ侵害が発生した後、以下のうち測定が最も難しいものはどれですか？
A. 評判の低下
B. 人件費
C. 規制上の制裁
D. 代替策
正解: **(**正解を表示します**)**
Reputational damage is often intangible, subjective, and hard to quantify, making it the most challenging aspect to measure.
"Reputation impact is difficult to quantify and may have long-term effects that are not immediately apparent."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Post-incident Analysis* ISACA practice questions highlight that reputational damage is uniquely challenging to measure accurately.

質問: **269**

CI/CDパイプラインにおけるセキュリティインシデントを封じ込めるための最善の対策は、次のうちどれですか？
A. 直ちにすべての開発者アカウントを無効化してください
B. 最後に確認された安全なビルドに戻す
C. 本番環境を無効にする
D. ビルドを変更せずにログ記録を増やす
正解: **(**正解を表示します**)**
The correct answer is B because reverting to the last known secure build is the most appropriate containment action when a security incident affects a continuous integration and continuous delivery pipeline. A compromised or insecure build can introduce malicious code, vulnerable components, configuration weaknesses, or unauthorized changes into downstream environments. Reverting to a known secure build helps stop propagation of the compromised version while preserving business continuity as much as possible. Disabling all developer accounts is excessive unless there is evidence that all accounts are compromised, and it could unnecessarily disrupt operations. Disabling the production environment may create significant business impact and may not be necessary for containment. Increasing logging can support investigation, but it does not contain the incident. CISM incident management emphasizes selecting containment actions that limit damage while considering business impact. In a CI/CD pipeline incident, restoring or reverting to a trusted build is the best containment action among the options.
Reference: CISM Information Security Incident Management; incident containment, secure DevOps, CI/CD pipeline security, and business impact reduction.

質問: **270**
組織が災害復旧サービス(DRaaS)を利用する最も適切な理由は次のうちどれですか？
A. 企業の年間コストを削減します。
B. 企業がテストを実施する必要がなくなります。
C. これは、復旧に伴うリスクを第三者に移転するものです。
D. オフサイト施設の維持管理が不要になります。
正解: **A (**コメントを発表する**)**

質問: **271**
情報セキュリティマネージャーが、ビジネス情報システムのリスク評価を完了しました。以下のうち、リスク軽減策の実施を決定するのに最も適任なのは誰でしょうか？
A. システム管理者
B. システムオーナー
C. 最高情報責任者
D. リスクマネージャー
正解: **(**正解を表示します**)**

The correct answer is B because the system owner is best positioned to decide on the implementation of mitigating controls for a business information system. The system owner is accountable for the system's business purpose, data, operational impact, and associated risk. After a risk assessment identifies threats, vulnerabilities, likelihood, impact, and recommended controls, the system owner must decide which risk treatment actions are appropriate based on business needs, risk appetite, cost, and operational requirements. A system administrator may implement technical controls, but does not normally own the business risk. The chief information officer may provide technology oversight, but may not be the accountable owner of the specific business system. The risk manager facilitates the risk management process and provides guidance, but risk treatment decisions belong to the risk or system owner. In CISM, business ownership and accountability are central principles. Information security managers advise and recommend, but accountable business or system owners decide on mitigation.
Reference: CISM Information Risk Management; risk ownership, system ownership, risk treatment, and control implementation accountability principles.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu 「**193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **272**
情報資産の固有リスクに最も大きな影響を与えるのは、次のうちどれですか？
A. リスク許容度
B. 正味現在価値(NPV)
C. 投資収益率(ROI)
D. ビジネス上の重要度
正解: **(**正解を表示します**)**
Inherent risk is the risk that exists before any controls are applied. It is influenced by factors such as the nature, value, sensitivity, and exposure of the information asset. Business criticality is one of the most important factors that affect the inherent risk of an information asset, as it reflects how essential the asset is for the organization's operations and objectives. The higher the business criticality, the higher the inherent risk. Risk tolerance, NPV, and ROI are not directly related to the inherent risk of an information asset, as they are more relevant for the risk assessment and risk treatment processes.
References = CISM Review Manual,
16th Edition, page 971

Business criticality is the degree to which an asset is essential to the success of the business and the extent to which its loss or compromise could have a significant impact on the business. Business criticality is one of the main factors that help to determine the inherent risk of an asset, as assets that are more critical to the business tend to have a higher inherent risk.

質問: **273**
ある金融機関が新しいモバイルアプリケーションの開発を計画しています。アプリケーションのセキュリティコンプライアンスの評価を開始するのに最適な時期は次のうちどれですか？
A. 設計段階において
B. 規制当局による審査中
C. ユーザー受け入れテスト(UAT)中
D. 静的コード解析中
正解: **(正解を表示します)**

質問: **274**
行動分析ツールは、主に組織内のリスク管理に使用されます。
A. 機密データの流出防止
B. 外部ユーザーからの通信を分析し、マルウェアを検出する
C. エンドポイントにおけるセキュリティ基準の確立
D. 異常なユーザーアクティビティの検出
正解: **(正解を表示します)**
The correct answer is D because behavioral analytics tools are primarily used to detect activities that deviate from normal user or entity behavior. These tools analyze patterns such as login times, access locations, data usage, application activity, privilege use, file access, and network behavior to identify anomalies that may indicate insider threats, compromised accounts, credential misuse, or advanced attacks. Preventing data exfiltration is normally associated with data loss prevention controls, although behavioral analytics may help detect suspicious activity related to exfiltration. Analyzing external communications for malware is more closely associated with email security gateways, web gateways, sandboxing, or malware detection tools.
Establishing security baselines on endpoints is more related to configuration management or endpoint protection. In CISM risk management, behavioral analytics supports monitoring, detection, and risk reduction by identifying unusual activity that may require investigation. Since its primary value is identifying behavior that differs from expected patterns, detecting anomalous user activities is the best answer.
Reference: CISM Information Risk Management; user behavior analytics, monitoring controls, anomaly detection, insider threat, and risk detection principles.

質問: **275**

次のうち、インシデント対応チームの主要な機能はどれですか？
A. 重大な事案に対する単一の連絡窓口を提供する
B. ゼロデイ脆弱性に対するリスク評価を提供する
C. 効果的なインシデント軽減策を提供する
D. 事業影響分析(BIA)を提供する
正解: **(**正解を表示します**)**

質問: **276**
組織のセキュリティ体制の有効性に最も大きな影響を与えるのは、次のうちどれですか？
A. インシデント指標は、業界ベンチマークと比較されることが多い。
B. 新規採用者はセキュリティ研修への参加が義務付けられています
C. セキュリティは組織文化に根付いている
D. 経営陣はセキュリティ対策を承認し、支持しています
正解: **C (**コメントを発表する**)**
When security is embedded in organizational culture, it becomes a shared responsibility, increasing adherence and effectiveness.
"A security-aware culture is a key component of an effective security program because it encourages responsible behavior and supports ongoing risk management."
- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Security Culture ISACA's practice questions identify security culture as the foundational element impacting the organization's entire security posture.

質問: **277**
ビジネスに支障をきたす可能性のある重大なセキュリティインシデントに対応する際、情報セキュリティマネージャーが取るべき最も重要な行動は次のうちどれですか？
A. エスカレーションの手順に従ってください。
B. 妥協の兆候を特定する。
C. 法執行機関に通報する。
D. 鑑識捜査官に連絡してください。
正解: **(**正解を表示します**)**
When responding to a major security incident that could disrupt the business, the information security manager's most important course of action is to follow the escalation process. The escalation process is a predefined set of steps and procedures that define who should be notified, when, how, and with what information in the event of a security incident. The escalation process helps to ensure that the appropriate stakeholders, such as senior management, business units, legal counsel, public relations, and external parties, are informed and involved in the incident response process. The escalation process also helps to coordinate the actions and decisions of the incident response team and the business continuity team, and to align the incident response objectives with the

business priorities and goals. The escalation process should be documented and communicated as part of the incident response plan, and should be reviewed and updated regularly to reflect the changes in the organization's structure, roles, and responsibilities. References =
CISM Review Manual 15th Edition, page 1631
CISM 2020: Incident Management and Response, video 32
Incident Response Models3

質問: **278**
鑑識捜査を行う際に最も重要なのは次のうちどれですか？
A. システムメモリの解析
B. 分析手順の文書化
C. システム全体のイメージをキャプチャします
D. 保管管理の連鎖を維持する
正解: **D (**コメントを発表する**)**
Maintaining a chain of custody is the most important step when conducting a forensic investigation, as this ensures that the evidence is preserved, protected, and documented from the time of collection to the time of presentation in court. A chain of custody provides a record of who handled the evidence, when, where, why, and how, and prevents any tampering, alteration, or loss of the evidence. A chain of custody also establishes the authenticity, reliability, and admissibility of the evidence in legal proceedings. Analyzing system memory, documenting analysis steps, and capturing full system images are also important, but not as important as maintaining a chain of custody, as they do not guarantee the integrity and validity of the evidence. References = CISM Review Manual 2023, page 1701; CISM Review Questions, Answers & Explanations Manual 2023, page 332; ISACA CISM - iSecPrep, page 183

質問: **279**
組織の情報セキュリティ戦略の包括性を判断する上で、情報セキュリティ管理者にとって最も有効な方法はどれですか？
A. 内部セキュリティ監査
B. 外部セキュリティ監査
C. 組織のリスク許容度
D. 事業影響分析(BIA)
正解: **C (**コメントを発表する**)**
The organizational risk appetite is the best indicator of the comprehensiveness of an information security strategy. The risk appetite defines the level of risk that the organization is willing to accept in pursuit of its objectives. The information security strategy should align with the risk appetite and provide a framework for managing the risks that the organization faces. An internal or external security audit can assess the effectiveness of the information security strategy, but not its comprehensiveness. A business impact analysis (BIA) can

identify the critical business processes and assets that need to be protected, but not the overall scope and direction of the information security strategy. References = CISM Review Manual 2023, page 36 1; CISM Practice Quiz 2

質問: **280**
情報セキュリティマネージャーがセキュリティ目標とビジネス目標を整合させるための最善の行動方針は、次のうちどれですか？
A. 事業影響分析(BIA)の実施
B. 事業戦略の見直し
C. 主要業績評価指標(KPI)の定義
D. ステークホルダーとの積極的な関わり
正解: **(**正解を表示します**)**
= According to the CISM Review Manual, the information security manager should actively engage with stakeholders to align security and business goals. This means understanding the business needs, expectations, and risk appetite of the stakeholders, and communicating the value and benefits of security initiatives to them.
By engaging with stakeholders, the information security manager can also gain their support and commitment for security programs and projects, and ensure that security objectives are aligned with business strategy and priorities. References = CISM Review Manual, 16th Edition, ISACA, 2020, page 23.

質問: **281**
セキュリティ対策の戦略的な整合性を効果的に促進する上で、最も有効なのは次のうちどれですか？
A. 事業戦略は定期的に更新されます
B. 手順と基準は部門長によって承認されます。
C. 第三者機関による定期的なセキュリティ監査が実施されます。
D. 組織単位が優先事項に貢献し、合意する
正解: **(**正解を表示します**)**
Organizational units contribute to and agree on priorities is the best way to facilitate effective strategic alignment of security initiatives because it ensures that the security initiatives are aligned with the business goals and objectives, supported by relevant stakeholders, and prioritized based on risk and value. The business strategy is periodically updated is not sufficient to facilitate effective strategic alignment of security initiatives because it does not involve collaboration or communication between different organizational units.
Procedures and standards are approved by department heads is not sufficient to facilitate effective strategic alignment of security initiatives because it does not reflect the strategic direction or vision of the organization.

Periodic security audits are conducted by a third-party is not sufficient to facilitate effective strategic alignment of security initiatives because it does not address the planning or implementation of security initiatives. References: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-2/how-to-align- security-initiatives-with-business-goals-and-objectives https://www.isaca.org/resources/isaca-journal/issues /2015/volume-1/how-to-measure-the-effectiveness-of-information-security-governance

質問**: 282**
ビジネスインパクト分析(BIA)BESTは、組織が以下のことを確立することを可能にします。
A. 総所有コスト(TCO)。
B. 復旧の優先順位。
C. 年間損失期待値(ALE)。
D. 復旧方法。
正解**: (**正解を表示します**)**
A business impact analysis (BIA) best enables an organization to establish restoration priorities (B). In CISM, the primary purpose of a BIA is to identify critical business processes, assess the impact of disruptions over time, and determine which functions must be restored first to minimize business impact. Restoration priorities are derived from factors such as maximum tolerable downtime, recovery time objectives (RTOs), and recovery point objectives (RPOs), all of which are key BIA outputs.
Total cost of ownership (A) is a financial analysis concept unrelated to continuity planning. Annualized loss expectancy (C) is an output of quantitative risk analysis, not a BIA. Recovery methods (D) are defined after restoration priorities are established and are part of business continuity and disaster recovery planning. CISM emphasizes that the BIA provides the business-driven foundation upon which recovery strategies and methods are later selected.
By clearly defining restoration priorities, the BIA ensures that continuity planning aligns with business objectives, risk appetite, and operational resilience requirements.
References:
ISACA CISM Review Manual, Information Security Program Development and Management - Business Impact Analysis (BIA) purpose and outcomes ISACA CISM Exam Content Outline, Domain 3: Information Security Program Development and Management

質問**: 283**
重要システムの情報セキュリティリスク評価の結果、いくつかの重大な問題が特定されました。情報セキュリティマネージャーが確認すべき最も重要な事項は次のうちどれですか？
A. リスクは組織のリスク登録簿に記録されます。
B. リスクは事業部門の上級管理職に報告されます。
C. リスクはIT部門にエスカレーションされ、是正措置が取られます。

D. リスクは中央リスク管理部門に伝達されます。
正解: **(**正解を表示します**)**
Entering identified risks into the organization ' s risk register ensures that they are documented, tracked, assigned, and addressed. Without recording in the risk register, there's no formal mechanism to manage, treat, or monitor the risk.
"The risk register is the central repository for tracking all known risks, their status, and treatment plans."
- CISM Review Manual 15th Edition, Chapter 2: Information Risk Management, Section: Risk Response and Risk Register*

質問: **284**
組織の災害復旧計画(DRP)の効果的な実行を確実にするために、次のうちどれが最も役立ちますか？
A. この計画は、上級管理職およびIT運用管理職によってレビューされます。
B. この計画は業界のベストプラクティスに基づいています。
C. プロセス手順は災害復旧チームによって文書化されています。
D. 手順はプライマリおよびフェイルオーバーの場所で利用可能です。
正解: **(**正解を表示します**)**
The best way to ensure the effective execution of a disaster recovery plan (DRP) is to make sure that the procedures are available at both the primary and the failover location, so that the staff can access them in case of a disaster. The procedures should be clear, concise, and updated regularly to reflect the current situation and requirements. Having the procedures available at both locations also helps to avoid confusion and delays in the recovery process.
References = CISM Review Manual, 16th Edition eBook1, Chapter 9: Business Continuity and Disaster Recovery, Section: Disaster Recovery Planning, Subsection: Disaster Recovery Plan Development, Page 373.

質問: **285**
セキュリティインシデントを効果的に封じ込めるためのアプローチを策定する際に、最も重要な考慮事項は次のうちどれですか？
A. インシデントの影響を受けたシステムを本番環境から隔離する
B. 事業に影響を与える可能性のある評判の損害を軽減する
C. 停電によって生じる可能性のある経済的損失を最小限に抑える
D. インシデント封じ込めに対する上級管理職の責任の割り当て
正解: **A (**コメントを発表する**)**
Isolating impacted systems (A) is the most critical consideration for effective incident containment because it directly limits spread, escalation, and additional damage. CISM incident management guidance prioritizes technical containment actions that preserve evidence and protect unaffected systems. Reputational (B) and financial (C) concerns are

important but are outcomes of how well containment is executed. Assigning accountability (D) supports governance but does not directly contain an incident. Rapid isolation is essential to reduce overall impact and enable effective eradication and recovery. References: ISACA CISM Review Manual (Incident management-containment strategies); CISM Exam Content Outline (Domain 4).

質問: **286**
情報セキュリティマネージャーが変更要求に対して必ず実行しなければならない活動は次のうちどれですか？
A. 影響を受けるシステムに対して侵入テストを実施する。
B. ITシステムをスキャンして、オペレーティングシステムの脆弱性を調べます。
C. 情報セキュリティリスクへの影響を評価する。
D. 情報セキュリティに関する業務要件の変更点を確認する。
正解: **(**正解を表示します**)**

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu 今**193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **287**
組織の災害復旧計画(DRP)を策定する際に、情報セキュリティ管理者が最初に行うべきことは次のうちどれですか？
A. ビジネス要件を特定する
B. 災害復旧手順書の作成
C. リスク評価を実施する
D. 事業影響分析(BIA)を実施する
正解: **D (**コメントを発表する**)**
The Business Impact Analysis (BIA) is the first step in developing a disaster recovery plan because it identifies critical business processes, dependencies, and acceptable downtime. " A BIA provides the foundation for disaster recovery planning by identifying business functions and their criticality. "
- CISM Review Manual 15th Edition, Chapter 3: Program Development, Section: Disaster Recovery Planning* Risk assessments follow the BIA and inform recovery strategies, but the BIA must come first.

質問: **288**
インシデントの影響を最小限に抑えようとするインシデント対応チームにとって、最も重要な考慮事項は次のうちどれですか？
A. 経営陣のリスク許容度に関する理解
B. インシデント対応訓練の修了状況に関する年ごとの分析
C. 組織の業務要件の理解
D. インシデント管理機能に割り当てられた資金の配分
正解: **(**正解を表示します**)**
The correct answer is C because an incident response team can limit impact most effectively when it understands the organization's operational requirements, including critical systems, business priorities, dependencies, acceptable downtime, data sensitivity, and service restoration needs. Incident response decisions often require balancing containment with business continuity. For example, disconnecting a system may stop an attack but could also interrupt critical operations. Understanding operational requirements enables the team to choose response actions that reduce security impact while minimizing disruption to essential business activities. Senior management's understanding of risk appetite is important for governance, but the response team needs practical operational knowledge during incidents. Training completion trends are useful for program monitoring, but they do not directly guide impact-limiting decisions during an event.
Funding supports capability, but it is not the most immediate consideration during response. CISM incident management emphasizes business impact reduction, coordinated response, prioritization, and restoration of critical services. Therefore, understanding operational requirements is the most important consideration for limiting incident impact.
Reference: CISM Information Security Incident Management; incident response prioritization, business impact, operational requirements, and impact limitation principles.

質問: **289**
サイバーセキュリティインシデント対応において使用される事前決定済みの封じ込め方法は、主に以下の点に基づいているべきである。
A. 影響を受けたユーザー数。
B. インシデントハンドラーの能力。
C. 確認された事件の種類。
D. 予測される事象の継続時間。
正解: **C (**コメントを発表する**)**
According to the NIST SP 800-61 Computer Security Incident Handling Guide, the type of confirmed incident is one of the most important criteria for choosing a containment strategy, as different types of incidents may require different levels of urgency, scope, and impact1. For example, a denial-of-service attack may require a different containment strategy than a ransomware attack or a data breach.
References = 1: NIST SP 800-61: 3.1. Choosing a Containment Strategy2

質問: **290**
データ探索プロジェクトで、機密指定されていないプロセス文書が発見されました。以下のうち、その文書の機密区分を判断するのに最も適任なのは誰ですか？
A. セキュリティポリシー作成者
B. 文書の作成者
C. データ管理者
D. 情報セキュリティマネージャー
正解: **(正解を表示します)**

質問: **291**
組織内で情報セキュリティ文化を確立するために最も貢献するのは、次のうちどれですか？
A. 定期的な情報セキュリティ意識向上活動を実施する
B. 情報セキュリティポリシーの経営陣の承認を得る
C. 情報セキュリティに関する業界のベストプラクティスに従う
D. ソフトウェア開発ライフサイクルに情報セキュリティ要件を組み込む
正解: **(正解を表示します)**
The correct answer is A because a security culture is built through continuous reinforcement of expected behaviors across the organization. Regular information security awareness initiatives help employees understand threats, responsibilities, acceptable behavior, and how their daily actions affect organizational security. Executive approval of policy is important, but a policy alone does not create culture unless it is communicated, understood, and practiced. Following industry best practices may improve the security program, but it does not directly influence employee behavior throughout the organization. Incorporating security requirements into the software development life cycle is important for secure systems development, but it targets a specific process area rather than the entire organization. A strong information security culture requires awareness, communication, leadership support, and repeated behavioral reinforcement. From a CISM perspective, governance promotes a culture where information security is recognized as a business responsibility, not just a technical function. Regular awareness initiatives are therefore the best direct contributor among the options.
Reference: CISM Information Security Governance; security awareness, culture, and organizational behavior principles.

質問: **292**
サイバーセキュリティインシデント発生時に、組織がシステム上で発生した活動や変更を把握するのに最も適した方法はどれですか？
A. 根本原因分析
B. 継続的なログ監視

C. 侵入テスト
D. コンピュータフォレンジック
正解**: (**正解を表示します**)**
Computer forensics (D) best enables an organization to determine what activities occurred and what changes were made to a system during a cybersecurity incident. In CISM incident management, computer forensics focuses on the systematic collection, preservation, analysis, and reconstruction of digital evidence to establish a detailed timeline of events, attacker actions, data access, and system modifications. This capability is essential for understanding the scope and impact of an incident, supporting legal or regulatory requirements, and preventing recurrence.
Continuous log monitoring (B) supports detection and early awareness of suspicious activity, but logs alone may be incomplete, altered, or insufficient to fully reconstruct attacker behavior. Root cause analysis (A) is performed after facts are established and focuses on why an incident occurred, not what exactly happened.
Penetration testing (C) is a proactive security testing activity and is unrelated to incident investigation.
CISM emphasizes that once an incident has occurred, forensic analysis is critical to ensure accurate incident handling, evidence integrity, accountability, and informed remediation decisions.
References:
ISACA CISM Review Manual, Information Security Incident Management - incident investigation and forensics ISACA CISM Exam Content Outline, Domain 4: Information Security Incident Management

質問**: 293**
セキュリティ分類に基づくラベル情報：
A. 人々が情報を安全に取り扱う可能性を高めます。
B. 必要な対策の数と種類を削減します。
C. 各分類のベースラインコントロールを特定する必要性を軽減します。
D. 情報が安全に取り扱われなかった場合の結果に影響します。
正解**: (**正解を表示します**)**
Labeling information according to its security classification enhances the likelihood of people handling information securely. Security classification is a process of categoriz-ing information based on its level of sensitivity and importance, and applying appropri-ate security controls based on the level of risk associated with that infor-mation1. Labeling is a process of marking the information with the appropriate classifi-cation level, such as public, internal, confidential, secret, or top secret2. The purpose of labeling is to inform the users of the information about its value and protection re-quirements, and to guide them on how to handle it securely. Labeling can help users to:
*Identify the information they are dealing with and its classification level
*Understand their roles and responsibilities regarding the information

*Follow the security policies and procedures for the information
*Avoid unauthorized access, disclosure, modification, or destruction of the information
*Report any security incidents or breaches involving the information
Labeling can also help organizations to:
*Track and monitor the information and its usage
*Enforce access controls and encryption for the information
*Audit and review the compliance with security standards and regulations for the information
*Educate and train employees and stakeholders on information security awareness and best practices Therefore, labeling information according to its security classification enhances the likelihood of people handling information securely, as it increases their awareness and accountability, and supports the implementation of security measures. The other op-tions are not the primary benefits of labeling information according to its security clas-sification. Reducing the number and type of countermeasures required is not a benefit, but rather a consequence of applying security controls based on the classification lev-el. Reducing the need to identify baseline controls for each classification is not a benefit, but rather a prerequisite for labeling information according to its security classifica-tion. Affecting the consequences if information is handled insecurely is not a benefit, but rather a risk that needs to be managed by implementing appropriate security con-trols and incident response procedures. References: 1: Information Classification - Ad-visera 2: Information Classification in Information Security - GeeksforGeeks : Infor-mation Security Policy - NIST :
Information Security Classification Framework - Queensland Government

質問**: 294**
組織の情報セキュリティ戦略を策定する際、どこに注力すべきかを理解するために最も役立つのは次のうちどれですか？
A. ギャップ分析
B. プロジェクト計画
C. 脆弱性評価
D. 事業影響分析(BIA)
正解**: A (**コメントを発表する**)**
Gap analysis is the MOST helpful tool for understanding where to focus efforts when developing an information security strategy for an organization, because it helps to identify the current state and the desired state of the information security governance, and the gaps between them. Gap analysis also helps to prioritize the actions and resources needed to close the gaps and achieve the information security objectives.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 36: "Gap analysis is the process of comparing the current state and the desired state of information security governance and identifying the gaps that need to be addressed." CISM Review Manual, 16th Edition,

ISACA, 2020, p. 37: "Gap analysis should be performed periodically to assess the effectiveness and efficiency of the information security strategy and program and to identify the areas for improvement." CISM domain 1: Information security governance [Updated 2022] - Infosec Resources: "Gap analysis: This is a comparison of the current state of security with the desired state. It helps to identify the gaps in security and prioritize the actions required to close them."

質問: **295**
効果的なインシデント対応テストを最も促進するのは、次のうちどれですか？
A. すべての事業部門をテスト対象に含める
B. 現実的なテストシナリオのシミュレーション
C. 検査結果を四半期ごとに見直す
D. 大規模な事業変更後のテスト
正解: **B (**コメントを発表する**)**
Effective incident response testing is a process of verifying and validating the incident response plan, procedures, roles, and resources that are designed to respond to and recover from information security incidents. The purpose of testing is to ensure that the incident response team and the organization are prepared, capable, and confident to handle any potential or actual incidents that could affect the business continuity, reputation, and value. The best way to facilitate effective testing is to simulate realistic test scenarios that reflect the most likely or critical threats and vulnerabilities that could cause an incident, and the most relevant or significant impacts and consequences that could result from an incident. Simulating realistic test scenarios can help to evaluate the adequacy, accuracy, and applicability of the incident response plan, procedures, roles, and resources, as well as to identify and address any gaps, weaknesses, or errors that could hinder or compromise the incident response process. Simulating realistic test scenarios can also help to enhance the skills, knowledge, and experience of the incident response team and the organization, as well as to improve the communication, coordination, and collaboration among the stakeholders involved in the incident response process. Simulating realistic test scenarios can also help to measure and report the effectiveness and efficiency of the incident response process, and to provide feedback and recommendations for improvement and optimization. References = CISM Review Manual 15th Edition, page 2401; CISM Practice Quiz, question 1362

質問: **296**
組織の新しい情報セキュリティ戦略を支援するために、情報セキュリティポリシーが最近改訂されました。情報セキュリティマネージャーが次に取るべき行動は次のうちどれでしょうか？
A. 基準と手順を更新する。
B. 技術的管理をレビューする。

C. 事業戦略との整合性を評価する。
D. セキュリティ研修プログラムを更新する。
正解: **A** (コメントを発表する)

質問: **297**
情報セキュリティガバナンスフレームワークの主要目標として、次のうちどれが適切でしょうか？
A. 組織のセキュリティプロファイルを最適化するための基準値を提供する。
B. 経営陣のコミットメントを示す。
C. 外部の利害関係者に対し、業界のベストプラクティスへの準拠を示す。
D. ユーザーが組織の情報セキュリティポリシーを遵守していることを確認する。
正解: **A** (コメントを発表する)
According to the Certified Information Security Manager (CISM) Study Manual, " The primary objective of information security governance is to provide a framework for managing and controlling information security practices and technologies at an enterprise level. Its goal is to manage and reduce risk through a process of identification, assessment, and management of those risks. " While demonstrating senior management commitment, compliance with industry best practices, and ensuring user compliance with policies are all important aspects of information security governance, they are not the primary objective. The primary objective is to manage and reduce risk by establishing a framework for managing and controlling information security practices and technologies at an enterprise level.
Reference:
Certified Information Security Manager (CISM) Study Manual, 15th Edition, Page 60.

質問: **298**
情報セキュリティマネージャーは、事業部門のリーダーたちが顧客へのアプローチ手段としてソーシャルメディアプラットフォームの利用拡大を奨励していることを知りました。従業員によるソーシャルメディア上での機密情報漏洩のリスクを軽減するために、まず最初に行うべきことはどれでしょうか？
A. 組織全体でソーシャルメディアポリシーを策定する。
B. ソーシャルメディアサイトの悪用に対する制裁措置を策定する。
C. 従業員が閲覧したソーシャルメディアサイトを監視する。
D. 企業所有のデバイスでのソーシャルメディアへのアクセスを制限する。
正解: (正解を表示します)
An organization-wide social media policy is a document that defines the rules and guidelines for using social media platforms within the organization. It covers topics such as who can use social media, what they can post, how they should protect confidential information, and what are the consequences for violating the policy. An organization-wide social media policy helps to mitigate the risk of confidential information being disclosed by

employees on social media by providing a clear and consistent framework for managing social media activities12.
References = 1: CISM Review Manual (Digital Version), page 271 2: CISM Review Manual (Print Version), page 271

質問: **299**
組織の災害復旧計画(DRP)を策定する際に、情報セキュリティ管理者が最初に行うべきことは次のうちどれですか？
A. リスク評価を実施する。
B. 災害復旧手順を文書化する。
C. ビジネス要件を特定する。
D. 事業影響分析(BIA)を実施する。
正解: **(正解を表示します)**
The business impact analysis (BIA) is the foundational step in disaster recovery planning. The CISM Review Manual states that BIA should be performed first to determine critical business functions, recovery priorities, and the impact of disruptions. Risk assessments and documentation follow after the BIA.
Reference:ISACA CISM Review Manual, 16th Edition, Page 237-238, " Business Impact Analysis (BIA) in DRP Development " .

質問: **300**
情報セキュリティ管理者は、エンドポイントデバイスが侵害されたことを通知されました。さらなる被害を防ぐための最善の対策は次のうちどれですか？
A. エンドポイントデバイスを消去してリセットします。
B. エンドポイントデバイスを隔離します。
C. エンドポイントデバイスの電源を切ります。
D. エンドポイントデバイスでウイルススキャンを実行します。
正解: **(正解を表示します)**
A compromised endpoint device is a potential threat to the security of the network and the data stored on it.
The best course of action to prevent further damage is to isolate the endpoint device from the network and other devices, so that the attacker cannot access or spread to other systems. Isolating the endpoint device also allows the information security manager to investigate the incident and determine the root cause, the extent of the compromise, and the appropriate remediation steps. Wiping and resetting the endpoint device may not be feasible or desirable, as it may result in data loss or evidence destruction. Powering off the endpoint device may not stop the attack, as the attacker may have installed persistent malware or backdoors that can resume once the device is powered on again. Running a virus scan on the endpoint device may not be effective, as the attacker may have used sophisticated techniques to evade detection or disable the antivirus software. References

= CISM Review Manual, 15th Edition, page 1741; CISM Review Questions, Answers & Explanations Database, question ID 2112; Using EDR to Address Unmanaged Devices - ISACA3; Boosting Cyberresilience for Critical Enterprise IT Systems With COBIT and NIST Cybersecurity Frameworks - ISACA; Endpoint Security: On the Frontline of Cyber Risk.
The best way to reduce the risk associated with a bring your own device (BYOD) program is to implement a mobile device policy and standard. This policy should include guidelines and rules regarding the use of mobile devices, such as acceptable use guidelines and restrictions on the types of data that can be stored or accessed on the device. Additionally, it should also include requirements for secure mobile device practices, such as the use of strong passwords, encryption, and regular patching. A mobile device management (MDM) solution can also be implemented to help ensure mobile devices meet the organizational security requirements. However, it is not enough to simply implement the policy and MDM solution; employees must also be trained on the secure mobile device practices to ensure the policy is followed.

質問: **301**
技術的なセキュリティ対策が不十分なまま、新しいアプリケーションが本番環境に導入されました。以下のうち、最も可能性の高い根本原因はどれですか？
A. 不十分なインシデント対応管理
B. 法的審査の欠如
C. 不十分な変更管理
D. 品質管理の欠如
正解: **C** (コメントを発表する)
Change control is the process of ensuring that changes to an information system are authorized, tested, documented and implemented in a controlled manner. Inadequate change control can result in deficient technical security controls, such as missing patches, misconfigurations, vulnerabilities or errors in the new application.
References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.3.2, page 2291

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu 問**193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **302**
情報セキュリティプログラムの有効性に関する有用な情報の報告を最も容易にするのは、次のうちどれですか？

A. リスクヒートマップ。
B. セキュリティベンチマークレポート。
C. セキュリティ指標ダッシュボード。
D. 主要リスク指標(KRI)。
正解: **(**正解を表示します**)**
A security metrics dashboard is a graphical representation of key performance indicators (KPIs) and key risk indicators (KRIs) that provide useful information about the effectiveness of the information security program.
A security metrics dashboard can help communicate the value and performance of the information security program to senior management and other stakeholders, as well as identify areas for improvement and alignment with business objectives. A security metrics dashboard should be concise, relevant, timely, accurate, and actionable.
References = CISM Review Manual 16th Edition, page 163; CISM Review Questions, Answers & Explanations Manual 9th Edition, page 419.

質問: **303**
リスク対応計画がタイムリーに策定 実行されることを最も確実にするために役立つのは、次のうちどれですか？
A. リスク指標の設定
B. リスク管理手順に関する研修
C. 文書化された不備に関する報告
D. リスクオーナーの割り当て
正解: **(**正解を表示します**)**
Assigning a risk owner is the best way to ensure a risk response plan will be developed and executed in a timely manner, because a risk owner is responsible for monitoring, controlling, and reporting on the risk, as well as implementing the appropriate risk response actions. A risk owner should have the authority, accountability, and resources to manage the risk effectively. Establishing risk metrics, training on risk management procedures, and reporting on documented deficiencies are all important aspects of risk management, but they do not guarantee that a risk response plan will be executed promptly and properly. Risk metrics help to measure and communicate the risk level and performance, but they do not assign any responsibility or action. Training on risk management procedures helps to increase the awareness and competence of the staff involved in risk management, but it does not ensure that they will follow the procedures or have the authority to do so. Reporting on documented deficiencies helps to identify and communicate the gaps and weaknesses in the risk management process, but it does not provide any solutions or corrective actions. References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 125-126, 136-
137.

質問: **304**
ランサムウェア攻撃への対応において最も重要な考慮事項は、以下の点を確実にすることです。
A. バックアップが利用可能です。
B. 最新のパッチが適用されました。
C. ランサムウェア攻撃は封じ込められました
D. 事業は運営できます
正解: **D (**コメントを発表する**)**
Ensuring the business can operate is the primary consideration when responding to a ransomware attack because it helps to minimize the disruption and impact of the attack on the organization's mission-critical functions and services. Ransomware is a type of malware that encrypts the files or systems of the victims and demands payment for their decryption. Ransomware attacks can cause significant operational, financial, and reputational damage to organizations, especially if they affect their core business processes or customer data.
Therefore, ensuring the business can operate is the primary consideration when responding to a ransomware attack.
References:
https://www.cisa.gov/stopransomware/ransomware-guide
https://csrc.nist.gov/Projects/ransomware-protection-and-response
https://learn.microsoft.com/en-us/azure/security/fundamentals/ransomware-detect-respond

質問: **305**
組織が重要な業務プロセスにサードパーティのクラウドコンピューティングサービスを利用することを計画している場合、情報セキュリティマネージャーはまず何をすべきでしょうか？
A. リスク評価を実施する。
B. ホストするデータを特定します。
C. ギャップ分析を実施する。
D. ビジネス要件を分析します。
正解: **(**正解を表示します**)**

質問: **306**
攻撃が成功した後、情報セキュリティ管理者は、どのインシデント対応フェーズの完了時にマルウェアが拡散し続けていることを確信できるでしょうか？
A. 封じ込め
B. 回復
C. 根絶
D. 識別
正解: **(**正解を表示します**)**

According to the CISM Review Manual (Digital Version), page 212, the incident response process consists of six phases: preparation, identification, containment, eradication, recovery, and lessons learned. Containment is the phase where the incident response team isolates the affected systems or networks to prevent further damage or spread of the malware. Eradication is the phase where the incident response team removes the malware and any traces of its activity from the affected systems or networks. Recovery is the phase where the incident response team restores the normal operations of the systems or networks. Identification is the phase where the incident response team detects and analyzes the signs of the incident. Therefore, the information security manager should be confident tha t the malware has not continued to spread at the completion of the containment phase, which is the earliest phase where the incident response team can stop the propagation of the malware. References = 1: CISM Review Manual (Digital Version), page 212

質問: **307**
組織の業務機能の重要性を判断する上で、次のうちどれが最も役立ちますか？
A. 災害復旧計画(DRP)
B. 事業影響分析(BIA)
C. 事業継続計画(BCP)
D. セキュリティ評価報告書(SAR)
正解: **(**正解を表示します**)**
Business impact analysis (BIA) is the most helpful in determining the criticality of an organization's business functions because it is a process of identifying and evaluating the potential effects of disruptions or interruptions to those functions. BIA helps to prioritize the recovery of the most critical functions and to estimate the resources and time needed for the recovery. Therefore, business impact analysis (BIA) is the correct answer.
References:
https://www.linkedin.com/pulse/business-continuity-critical-functions-tino-marquez
https://www.techtarget.com/searchitchannel/feature/Business-impact-analysis-for-business-continuity-Understanding-impact-criticality

質問: **308**
情報システムの機密性と可用性を確保するための適切な管理体制が整っていることを保証する責任は誰にあるのでしょうか？
A. 情報セキュリティマネージャー
B. 情報所有者
C. ビジネスマネージャー
D. 上級管理職
正解: **D (**コメントを発表する**)**

質問: **309**

新たな情報セキュリティ報告要件がまもなく発効します。情報セキュリティ管理者が最初に行うべき行動は次のうちどれですか？
A. 新しい要件への非準拠に関連する費用便益分析を実施します。
B. 新しい要件に対するギャップ評価を実行します。
C. 新しい要件がビジネスに適用されるかどうかを調査します。
D. 新しい要件を上級管理職に通知します。
正解: **C** (コメントを発表する)
Before taking any compliance steps, the information security manager must first assess whether the regulation is applicable to the organization. This ensures resources are not spent unnecessarily.
"The applicability of legal, regulatory, and contractual requirements must be determined before initiating compliance activities."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Legal and Regulatory Compliance*

質問: **310**
情報セキュリティ状況報告書を上級管理職に提出する際に、最も重要な項目は次のうちどれですか？
A. 主要リスク指標(KRI)
B. 情報セキュリティポリシーの見直し
C. 情報セキュリティ予算要求
D. 最近のセキュリティイベント一覧
正解: (正解を表示します)
According to the CISM Review Manual, key risk indicators (KRIs) are the most important information to include in an information security status report to senior management, as they provide a measure of the current level of risk exposure and the effectiveness of the risk management activities. KRIs also help to identify trends, patterns and emerging risks that may require management attention or action.
References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.3.2, page 209

質問: **311**
情報セキュリティガバナンスフレームワークを導入する際に、最初に確立すべき事項は次のうちどれですか？
A. セキュリティアーキテクチャ
B. セキュリティポリシー
C. セキュリティインシデント管理チーム
D. セキュリティ意識向上トレーニングプログラム
正解: (正解を表示します)

This is the most urgent and effective action to prevent further damage or compromise of the organization's network and data. The other options are less important or irrelevant in this situation.
According to How to identify suspicious insider activity using Active Directory, one of the steps to detect and respond to suspicious activity is to isolate the affected device from the network. This can be done by disabling the network adapter, unplugging the network cable, or blocking the device's IP address on the firewall1. This will prevent the device from communicating with any malicious actors or spreading malware to other devices on the network.
`

質問: **312**
ヘルプデスクが情報セキュリティインシデントを認識するために最も役立つのは、次のうちどれでしょうか？
A. ヘルプデスク担当者に通話ログを確認するよう指導する。
B. ヘルプデスクにインシデント後の検証に参加することを義務付ける。
C. セキュリティインシデントの基準をヘルプデスクに提供する。
D. セキュリティインシデント対応チームにヘルプデスクのメンバーを含める。
正解: **(正解を表示します)**
Providing the help desk with clear criteria for what constitutes a security incident (C) is the most effective way to enable early recognition. In CISM incident management, frontline functions such as the help desk are critical for early detection and escalation, but only if they understand what events require security attention.
Reviewing call logs (A) or participating in post-incident reviews (B) improves awareness after the fact, not recognition in real time. Including help desk staff on the response team (D) is unnecessary and impractical for incident identification. Clearly defined criteria and escalation thresholds empower the help desk to act quickly and consistently.
References: ISACA CISM Review Manual (Incident management-incident identification and escalation); CISM Exam Content Outline (Domain 4).

質問: **313**
ネットワークスニッフィングは、以下のような方法で実行できるため、検出が困難です。
A. 受動的に。
B. 継続的に。
C. 積極的に。
D. 遠隔で。
正解: **(正解を表示します)**
Network sniffing is difficult to detect primarily because it can be performed passively. In CISM terms, a passive attack is one in which the attacker monitors or intercepts data without altering system resources or network traffic patterns. Because passive sniffing

does not generate abnormal traffic, modify packets, or interact directly with target systems, it often leaves no observable indicators that traditional security monitoring tools can easily detect.
CISM distinguishes between passive and active attacks, emphasizing that passive techniques such as packet sniffing, eavesdropping, and traffic analysis are inherently harder to identify than active attacks, which disrupt operations or modify data. Continuous operation (B) does not explain detectability, active sniffing (C) would generate detectable anomalies, and remote execution (D) does not inherently make detection more difficult. From an incident management and detection perspective, this highlights the importance of preventive controls, such as encryption, secure network design, and segmentation, rather than relying solely on detection mechanisms. Because passive sniffing exploits visibility rather than system weakness, prevention is the primary risk mitigation strategy.
References:
ISACA CISM Review Manual, Information Security Incident Management - attack types and detection challenges ISACA CISM Exam Content Outline, Domain 4: Information Security Incident Management

質問**: 314**
重大な情報セキュリティインシデントが発生した後、情報セキュリティマネージャーが是正措置を決定する上で最も役立つのは次のうちどれですか？
A. 事件の費用を計算する
B. 死後評価の実施
C. 影響分析の実施
D. 証拠の保全
正解**: (**正解を表示します**)**
The best way to determine corrective actions after a major information security incident is to conduct a postmortem assessment, which is a systematic and structured review of the incident, its causes, its impacts, and its lessons learned. A postmortem assessment can help to identify the root causes of the incident, the strengths and weaknesses of the incident response process, the gaps and deficiencies in the security controls, and the opportunities for improvement and remediation. A postmortem assessment can also help to document the recommendations and action plans for preventing or minimizing the recurrence of similar incidents in the future.
References = CISM Review Manual, 16th Edition eBook1, Chapter 4: Information Security Incident Management, Section: Incident Response, Subsection: Postincident Activities, Page 211.

質問**: 315**
情報資産の分類を最も適切に決定するのは、次のうちどれですか？
A. 市場における情報資産の価値
B. ビジネスプロセスにおける重要性

C. データ所有者によるリスク評価
D. 情報資産の生産コスト
正解**: B (**コメントを発表する**)**
According to the CISM Review Manual, 15th Edition1, information asset classification is the process of assigning a level of sensitivity to information assets based on their importance to the organization and the potential impact of unauthorized disclosure, modification or destruction. The criticality of an information asset to a business process is one of the key factors that determines its classification level.
References = 1: CISM Review Manual, 15th Edition, ISACA, 2016, Chapter 2, page 61.

質問**: 316**
組織が実施すべき情報セキュリティポリシーを決定する上で、以下のうちどれが最も役立ちますか？
A. リスク評価
B. 事業影響分析(BIA)
C. 脆弱性評価
D. 業界のベストプラクティス
正解**: A (**コメントを発表する**)**
Information security policies are high-level statements or rules that define the goals and objectives of information security in an organization, and provide the framework and direction for implementing and enforcing security controls and processes1. Information security policies should be aligned with the organization's business goals and objectives, and reflect the organization's risk appetite and tolerance2.
Therefore, the most helpful activity for determining which information security policies should be implemented by an organization is a risk assessment.
A risk assessment is a systematic process of identifying, analyzing, and evaluating the risks that an organization faces, and determining the appropriate risk responses3. A risk assessment helps to determine the following aspects of information security policies:
The scope and applicability of the policies, based on the assets, threats, and vulnerabilities that affect the organization's security objectives and requirements.
The level and type of security controls and processes that are needed to mitigate the risks, based on the likelihood and impact of the risk scenarios and the cost-benefit analysis of the risk responses.
The roles and responsibilities of the stakeholders involved in the implementation and enforcement of the policies, based on the risk ownership and accountability.
The metrics and indicators that are used to measure and monitor the effectiveness and compliance of the policies, based on the risk appetite and tolerance.
The other options, such as a business impact analysis (BIA), a vulnerability assessment, or industry best practices, are not as helpful as a risk assessment for determining which information security policies should be implemented by an organization, because they have the following limitations:

A business impact analysis (BIA) is a process of identifying and evaluating the potential effects of disruptions or incidents on the organization's critical business functions and processes, and determining the recovery priorities and objectives. A BIA can help to support the risk assessment by providing information on the impact and criticality of the assets and processes, but it cannot identify or analyze the threats and vulnerabilities that pose risks to the organization, or determine the appropriate risk responses or controls.
A vulnerability assessment is a process of identifying and measuring the weaknesses or flaws in the organization's systems, networks, or applications that could be exploited by threat actors. A vulnerability assessment can help to support the risk assessment by providing information on the vulnerabilities and exposures that affect the organization's security posture, but it cannot identify or analyze the threats or likelihood that could exploit the vulnerabilities, or determine the appropriate risk responses or controls.
Industry best practices are the standards or guidelines that are widely accepted and followed by the information security community or the organization's industry sector, based on the experience and knowledge of the experts and practitioners. Industry best practices can help to inform and guide the development and implementation of information security policies, but they cannot replace or substitute the risk assessment, as they may not reflect the organization's specific context, needs, and objectives, or address the organization's unique risks and challenges.
References = 1: CISM Review Manual 15th Edition, page 29 2: CISM Review Manual 15th Edition, page
30 3: CISM Review Manual 15th Edition, page 121 : CISM Review Manual 15th Edition, page 122 : CISM Review Manual 15th Edition, page 123 : CISM Review Manual 15th Edition, page 124 : CISM Review Manual 15th Edition, page 125 : CISM Review Manual 15th Edition, page 126

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu 「**193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **317**
情報セキュリティ プロジェクトのサポートを得るためのビジネス ケース開発の主な根拠となるのは次のどれですか。
A. 予算要件
B. 実現可能性調査
C. エンタープライズアーキテクチャ (EA)

D. リスク許容レベル
正解**: D (**コメントを発表する**)**
Risk tolerance levels (D) should be the primary basis for an information security business case because security investments are justified by their ability to reduce risk to levels acceptable to the organization. CISM stresses that security exists to manage risk in alignment with business objectives and appetite. Budget (A), feasibility (B), and EA alignment (C) are important considerations, but they are secondary to demonstrating how a proposed initiative addresses risks that exceed tolerance. A strong business case clearly articulates the current risk exposure, the residual risk after implementation, and how the investment aligns with executive- defined tolerance thresholds. This approach directly supports informed decision-making by senior management.
References: ISACA CISM Review Manual (Program management-business cases, risk-based decision making); CISM Exam Content Outline (Domain 3).

質問**: 318**
組織のホスティング型給与計算サービスプロバイダーでデータ漏洩が発生したことをマスメディアを通じて知った場合、情報セキュリティ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. プロバイダとのデータ交換を一時停止する
B. 違反について適切な規制当局に通知する。
C. 事業継続計画(BCP)を開始する
D. プロバイダーと連携して違反を確認する
正解**: (**正解を表示します**)**
The first thing an information security manager should do after learning through mass media of a data breach at the organization's hosted payroll service provider is to validate the breach with the provider, which means contacting the provider directly and confirming the details and scope of the breach, such as when it occurred, what data was compromised, and what actions the provider is taking to mitigate the impact. Validating the breach with the provider can help the information security manager assess the situation accurately and plan the next steps accordingly. The other options, such as suspending the data exchange, notifying regulatory authorities, or initiating the business continuity plan, may be premature or unnecessary before validating the breach with the provider.
References:
https://www.wired.com/story/sequoia-hr-data-breach/
https://cybernews.com/news/kronos-major-hr-and-payroll-service-provider-hit-with-ransomware-warns-of-a-long-outage/
https://www.afr.com/work-and-careers/workplace/pay-in-crisis-as-major-payroll-company-hacked-20211117-p599mr

質問**: 319**

組織の品質プロセスは、以下の点を提供することでセキュリティ管理を最適にサポートできます。
A. セキュリティ構成制御。
B. セキュリティ要件が満たされていることの保証。
C. セキュリティ戦略に関するガイダンス。
D. セキュリティシステムドキュメントのリポジトリ。
正解: **(**正解を表示します**)**
= A quality process is a set of activities that ensures that the products or services delivered by an organization meet the customer's expectations and comply with the applicable standards and regulations. A quality process can support security management by providing assurance that security requirements are met throughout the development, implementation and maintenance of information systems and processes. A quality process can also help to identify and correct security defects, measure security performance and effectiveness, and improve security practices and procedures. References = CISM Review Manual, 15th Edition, page 671; CISM Review Questions, Answers & Explanations Database, question ID 2092.
An organization ' s quality process can BEST support security management by providing assurance that security requirements are met. This means that the quality process can be used to ensure that security controls are being implemented as intended and that they are achieving the desired results. This helps to ensure that the organization is properly protected and that it is in compliance with security regulations and standards.

質問: **320**
インシデント管理チームのリーダーが、組織がサイバー攻撃から正常に復旧したことを通知しました。次に実行すべきことは次のうちどれですか？
A. 上級管理職向けに要約を作成する
B. ビジネスへの影響に関するフィードバックを収集する
C. 会議を開催し、得られた教訓を記録する。
D. 分析のためにデジタル証拠を安全に保管する。
正解: **C (**コメントを発表する**)**
Conducting a meeting to capture lessons learned is the next step after an incident management team leader sends out a notification that the organization has successfully recovered from a cyberattack because it helps to identify the strengths and weaknesses of the current incident response plan, capture the feedback and recommendations from the incident responders and stakeholders, and implement the necessary improvements and corrective actions for future incidents. Preparing an executive summary for senior management is not the next step, but rather a subsequent step that involves reporting the incident details, impact, and resolution to the senior management. Gathering feedback on business impact is not the next step, but rather a concurrent step that involves assessing the extent and severity of the damage or disruption caused by the incident.

Securing and preserving digital evidence for analysis is not the next step, but rather a previous step that involves collecting and documenting the relevant data or artifacts related to the incident. References:
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-5/incident-response-lessons-learned
https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/incident-response-lessons-learned

質問: **321**
情報セキュリティ活動をチェンジマネジメントプロセスに統合する主なメリットは以下のとおりです。
A. 共謀やコンプライアンス違反の脅威から事業を守る。
B. 必要な制御が変更に含まれていることを確認する。
C. 事業におけるセキュリティ関連の変更に対する説明責任を強化する。
D. 組織を不正な変更から保護します。
正解: **(**正解を表示します**)**

質問: **322**
情報セキュリティ投資に対するリターンを最も的確に示す指標はどれですか？
A. 年間損失期待値(ALE)の増加
B. 報告された事件数の増加
C. 年間損失期待値(ALE)の低減
D. 報告された事件数の減少
正解: **(**正解を表示します**)**
A reduction in annualized loss expectancy (ALE) demonstrates that implemented controls have effectively reduced the organization's exposure to risk.
"ALE reduction is a key indicator of the cost-effectiveness of security investments and the improvement of the risk posture."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Cost-Benefit Analysis*

質問: **323**
組織のセキュリティ体制を改善するための取り組みに最も大きな影響を与えるのは、次のうちどれですか？
A. 上級管理職への定期的な報告
B. セキュリティに関するトップの支持的な姿勢
C. セキュリティ制御の自動化
D. 十分に文書化されたセキュリティポリシーと手順
正解: **(**正解を表示します**)**

The supportive tone at the top regarding security is the greatest impact on efforts to improve an organization's security posture. This means that senior management should demonstrate their commitment and leadership to information security by setting clear goals, allocating adequate resources, communicating effectively, and rewarding good practices. A supportive tone at the top can also influence the culture and behavior of the organization, as well as foster trust and collaboration among stakeholders12. References = CISM Review Manual 15th Edition, page 1261; CISM Item Development Guide, page 82

質問: **324**
事業部門の情報システム上でクレジットカードデータを扱うためのセキュリティプロセスを策定する際、情報セキュリティマネージャーはまず最初に以下の点に留意すべきである。
A. クレジットカードデータを扱うシステムがセグメント化されていることを確認する。
B. 安全な決済処理に関する業界のベストプラクティスを確認する。
C. クレジットカード情報に関する企業方針を確認する。
D. 業界の暗号化標準に準拠していることを確認してください。
正解: **C** (コメントを発表する)

質問: **325**
機密性の高いデータを保存する重要なシステムの開発において、情報セキュリティマネージャーが最も重視すべき事項は次のうちどれでしょうか？
A. 検出される脆弱性の数を減らす
B. 残存リスクの量が許容範囲内であることを確認する
C. 特定されたシステム脅威を回避する
D. 規制要件の遵守
正解: (正解を表示します)
The information security manager's primary focus during the development of a critical system storing highly confidential data should be ensuring the amount of residual risk is acceptable. Residual risk is the level of cyber risk remaining after all the security controls are accounted for, any threats have been addressed and the organization is meeting security standards. It's the risk that slips through the cracks of the system. For a critical system storing highly confidential data, the residual risk should be as low as possible, and within the organization's risk appetite and tolerance. The information security manager should monitor and review the residual risk throughout the system development life cycle, and ensure that it is communicated and approved by the appropriate stakeholders. The other options are not the primary focus, although they may be part of the security objectives and activities. Reducing the number of vulnerabilities detected is a desirable outcome, but it does not necessarily mean that the residual risk is acceptable, as some vulnerabilities may have a higher impact or likelihood than others. Avoiding identified system threats is a preventive measure, but it does not account for unknown or emerging

threats that may pose a residual risk to the system. Complying with regulatory requirements is a mandatory obligation, but it does not guarantee that the residual risk is acceptable, as regulations may not cover all aspects of security or reflect the specific context and needs of the organization.

質問: **326**
クラウド環境への移行時にクラウドアクセスセキュリティブローカーを使用する最も重要な利点は次のうちどれですか？
A. 強化されたデータガバナンス
B. 第三者保証の強化
C. インシデント管理の改善
D. 総所有コスト(TCO)の削減
正解: **(正解を表示します)**
According to the web search results, a cloud access security broker (CASB) is a software solution that stands between the cloud service provider and the cloud service user to enforce security controls. One of the most important benefits of using a CASB when migrating to a cloud environment is enhanced data governance, as it helps to protect sensitive information from unauthorized access, sharing, or loss. A CASB can also provide data classification, encryption, data loss prevention (DLP), and other features that enable organizations to manage and secure their data in the cloud.
References = What Is a Cloud Access Security Broker (CASB)?, A beginner's guide to cloud access security brokers

質問: **327**
以下のうち、補償対照群への支出を最も正当化できるのはどれですか？
A. 根本原因分析
B. 脆弱性評価
C. 新たなリスク動向
D. リスク分析
正解: **(正解を表示します)**
A risk analysis (D) best justifies spending on a compensating control because it quantifies or qualifies risk exposure and residual risk, providing a business-based rationale for investment. CISM stresses that control decisions must be driven by risk, not by the existence of vulnerabilities alone. Root cause analysis (A) explains why an issue occurred, vulnerability assessments (B) identify weaknesses, and emerging trends (C) provide context-but only risk analysis connects threats, vulnerabilities, impact, and likelihood to justify expenditure.
References: ISACA CISM Review Manual (Risk management-risk evaluation and treatment); CISM Exam Content Outline (Domain 1).

質問: **328**

組織のセキュリティ目標が業務運営に確実に組み込まれるようにするための最善の方法は、次のうちどれですか？
A. 採用した情報セキュリティ基準を公開する。
B. 情報セキュリティコンプライアンスに関する年次レビューを実施する。
C. 情報セキュリティガバナンスフレームワークを導入する。
D. 情報セキュリティ違反に対する罰則を定義する。
正解: **(**正解を表示します**)**
The best way to ensure the organization's security objectives are embedded in business operations is to implement an information security governance framework. An information security governance framework is a set of policies, procedures, standards, guidelines, roles, and responsibilities that define and direct how the organization manages and measures its information security activities. An information security governance framework helps to align the information security strategy with the business strategy and the organizational culture, and to ensure that the information security objectives are consistent with the business objectives and the stakeholder expectations. An information security governance framework also helps to establish the authority, accountability, and communication channels for the information security function, and to provide the necessary resources, tools, and controls to implement and monitor the information security program. By implementing an information security governance framework, the organization can embed the information security objectives in business operations, and ensure that the information security function supports and enables the business processes and functions, rather than hinders or restricts them.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:
Information Security Governance Framework, page 181; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 75, page 702.

質問: **329**
社内の重要なアプリケーション、データベース、またはサーバーの復旧時間目標(RTO)を決定する際に、以下のうちどれを最も重視すべきでしょうか？
A. 回復目標点(RPO)の決定
B. 上級管理職からの指示
C. サービス中断の影響
D. 回復試験の結果
正解: **C (**コメントを発表する**)**

質問: **330**
事業継続計画(BCP)を最新の状態に保つための最良の方法は、次のうちどれですか？
A. 業務プロセスの変更を管理する。
B. 事業影響分析(BIA)を定期的に更新する。

C. 定期的な検査を実施する。
D. 緊急連絡先リストを確認し、更新する。
正解: **C** (コメントを発表する)
Conducting periodic testing is the best way to ensure the BCP is current because it can validate the effectiveness and efficiency of the BCP, identify any gaps or weaknesses, and provide feedback and recommendations for improvement. Testing can also verify that the BCP reflects the current business environment, processes, and requirements, and that the BCP team members are familiar with their roles and responsibilities.
References: The CISM Review Manual 2023 states that "testing is a critical component of the BCP process" and that "testing can help ensure that the BCP is current, effective, and efficient, and that it meets the business objectives and expectations" (p. 195). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Conducting periodic testing is the correct answer because it is the best way to ensure the BCP is current, as it can evaluate the BCP against the current business environment, processes, and requirements, and identify any areas for improvement or update" (p. 98).
Additionally, the article Business Continuity Planning: Testing an Organization's Plan from the ISACA Journal 2019 states that "testing is essential to ensure that the BCP is current and effective" and that "testing can provide assurance that the BCP is aligned with the business needs and expectations, and that the BCP team members are competent and confident in executing their tasks" (p. 1)

質問: **331**
セキュリティインシデントからの効果的な復旧を可能にするために、以下のうちどれが最も重要ですか？
A. 対応チームのクロス -トレーニング
B. ネットワークアーキテクチャレビュー
C. 侵入テスト
D. オフサイトデータバックアップ
正解: **D** (コメントを発表する)
The correct answer is D because effective recovery from many security incidents depends on the ability to restore reliable data and systems. Offsite backups are especially important when primary systems or data are corrupted, encrypted, destroyed, or otherwise unavailable. Security incidents such as ransomware, destructive malware, insider misuse, or system compromise may require restoration from clean backups. Response team cross-training improves operational flexibility, but it does not directly restore lost or damaged data. Network architecture reviews may improve security design and reduce future exposure, but they are not the most important recovery enabler. Penetration testing helps identify weaknesses before an incident occurs, but it does not support restoration after an incident. CISM incident management includes recovery as a key phase, and recovery

requires tested, available, and protected backup capabilities aligned with recovery objectives.
Offsite backups reduce dependence on compromised local infrastructure and support business resilience.
Therefore, offsite data backups are the most important recovery enabler.
Reference: CISM Information Security Incident Management; recovery, backup strategy, resilience, disaster recovery, and restoration principles.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu ↾**193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **332**
アプリケーション開発部門の責任者は、最近の評価で特定されたリスクを受け入れることを決定しました。規制当局の監督下では勧告事項の実施が義務付けられているにもかかわらず、勧告事項は一切実施されません。情報セキュリティマネージャーは次に何をすべきでしょうか？
A. リスク監視計画を見直してください。
B. 決定を正式に文書化する。
C. 規則を確認してください。
D. リスク管理チームに助言する。
正解: **(**正解を表示します**)**
Since the identified risks are subject to regulatory requirements, and cannot simply be accepted without oversight, the information security manager should escalate the issue to the risk management team or higher authority to ensure proper governance.
"When risk acceptance contradicts regulatory requirements, it must be escalated to senior management or the risk function for resolution."
- CISM Review Manual 15th Edition, Chapter 1: Governance Responsibilities, Section: Risk Governance and Oversight*

質問: **333**
組織のデータを保護する戦略を策定する際に、最初に考慮すべき事項は次のうちどれですか?
A. 暗号化
B. アクセス監視

C. 分類
D. アクセス権
正解: **(**正解を表示します**)**

質問: **334**
バッファオーバーフローを最も適切に説明しているのは次のうちどれですか？
A. 関数が処理できるデータ量を超えるデータで関数が実行される
B. プログラムに、セキュリティリスクをもたらす隠れた意図しない機能が含まれている。
C. 通常の動作を妨害するように設計された悪意のあるコード
D. データを傍受する一種の隠蔽チャネル
正解: **(**正解を表示します**)**
A buffer overflow is a software coding error or vulnerability that occurs when a function is carried out with more data than the function can handle, resulting in adjacent memory locations being overwritten or corrupted by the excess data1. A program contains a hidden and unintended function that presents a security risk is not a buffer overflow, but rather a backdoor2. Malicious code designed to interfere with normal operations is not a buffer overflow, but rather malware3. A type of covert channel that captures data is not a buffer overflow, but rather a keylogger. References: 1 https://www.fortinet.com/resources/cyberglossary/buffer- overflow 2 https://www.fortinet.com/resources/cyberglossary/backdoor 3 https://www.fortinet.com/resources /cyberglossary/malware https://www.fortinet.com/resources/cyberglossary/keylogger

質問: **335**
情報セキュリティガバナンスにおいて、規制遵守を確保する主要な責任を負っているのは次のうちどれですか？
A. 上級管理職
B. 企業リスクマネジメント
C. 所有者を管理する
D. 法律顧問
正解: **(**正解を表示します**)**
The correct answer is A because senior management has primary responsibility for ensuring that the organization complies with applicable laws, regulations, contractual obligations, and governance requirements. While compliance tasks may be delegated to legal, risk, compliance, IT, and control owners, accountability remains with senior management. Enterprise risk management may help identify and manage regulatory risk, but it does not replace management accountability. Control owners are responsible for operating specific controls, but they are not accountable for overall regulatory compliance. Legal counsel advises on legal interpretation and obligations, but does not own enterprise compliance accountability. In CISM governance, senior management provides direction, resources, oversight, and accountability for information security and compliance. The

information security manager supports this by implementing security programs, reporting risks, and advising on controls. However, the responsibility for ensuring regulatory compliance rests with senior leadership because compliance failures can affect the entire organization, including legal exposure, financial penalties, operational restrictions, and reputational harm.
Reference: CISM Information Security Governance; senior management accountability, regulatory compliance, governance oversight, and enterprise responsibility principles.

質問: **336**
詳細な事業継続計画(BCP)は、主に以下の点に基づいて策定されるべきである。
A. すべてのアプリケーションを網羅する戦略。
B. 上級管理職によって承認された戦略。
C. 実行に必要なコストとリソース。
D. 利用可能な現地ベンダーの能力。
正解: **(**正解を表示します**)**

質問: **337**
リスクの所有権はどの時点で割り当てるべきか？
A. リスク対策計画が実行されるとき
B. 資産の所有権が割り当てられる場合
C. リスクが特定された場合
D. 関連する脆弱性が特定された場合
正解: **C (**コメントを発表する**)**
Risk ownership should be assigned when the risk is identified (C). CISM emphasizes early assignment of ownership to ensure accountability for analysis, treatment decisions, and monitoring throughout the risk lifecycle. Waiting until treatment execution (A) delays accountability, while asset ownership (B) or vulnerability identification (D) alone does not ensure ownership of the broader business risk. Early ownership ensures risks are properly evaluated, escalated, and managed in line with risk appetite.
References: ISACA CISM Review Manual (Risk management-risk lifecycle and accountability); CISM Exam Content Outline (Domain 1).

質問: **338**
第三者プロバイダーが組織の情報セキュリティ要件を遵守していることを確認するために、最も重要なことは以下の点を確認することです。
A. セキュリティ指標はサービスレベル契約(SLA)に含まれています。
B. 契約条項は組織の情報セキュリティポリシーに準拠している。
C. 第三者サービスプロバイダーの情報セキュリティポリシーをレビューします。
D. 監査権はサービスレベル契約(SLA)に含まれています。
正解: **(**正解を表示します**)**

= To confirm that a third-party provider complies with an organization's information security requirements, it is most important to ensure that the right to audit is included in the service level agreement (SLA), which is a contract that defines the scope, quality, and terms of the services that the third-party provider delivers to the organization. The right to audit is a clause that grants the organization the authority and opportunity to inspect and verify the third-party provider's security policies, procedures, controls, and performance, either by itself or by an independent auditor, at any time during the contract period or after a security incident. The right to audit can help to ensure that the third-party provider adheres to the organization's information security requirements, as well as to the legal and regulatory standards and obligations, and that the organization can monitor and measure the security risks and issues that arise from the outsourcing relationship. The right to audit can also help to identify and address any gaps, weaknesses, or errors that could compromise the security of the information assets and systems that are shared, stored, or processed by the third-party provider, and to provide feedback and recommendations for improvement and optimization of the security posture and performance.
Security metrics, contract clauses, and the information security policy of the third-party provider are all important elements of ensuring the compliance of the third-party provider with the organization's information security requirements, but they are not the most important ones. Security metrics are quantitative and qualitative measures that indicate the effectiveness and efficiency of the security controls and processes that the third-party provider implements and reports to the organization, such as the number of security incidents, the time to resolve them, the level of customer satisfaction, or the compliance rate. Security metrics can help to evaluate and compare the security performance and outcomes of the third-party provider, as well as to identify and address any deviations or discrepancies from the expected or agreed levels. Contract clauses are legal and contractual terms and conditions that bind the third-party provider to the organization's information security requirements, such as the confidentiality, integrity, and availability of the information assets and systems, the roles and responsibilities of the parties, the liabilities and penalties for breach or violation, or the dispute resolution mechanisms. Contract clauses can help to enforce and protect the organization's information security interests and rights, as well as to prevent or resolve any conflicts or issues that arise from the outsourcing relationship. The information security policy of the third-party provider is a document that defines and communicates the third-party provider's security vision, mission, objectives, and principles, as well as the security roles, responsibilities, and rules that apply to the third-party provider's staff, customers, and partners. The information security policy of the third-party provider can help to ensure that the third-party provider has a clear and consistent security direction and guidance, as well as to align and integrate the third- party provider's security practices and culture with the organization's security expectations and requirements. References = CISM Review Manual 15th Edition, pages 57-581; CISM Practice Quiz, question
1662

質問: **339**
脅威と脆弱性の評価が重要な主な理由は以下のとおりです。
A. セキュリティ投資を確立するために使用される
B. 管理目標を設定するための基礎。
C. 組織のセキュリティ態勢の要素。
D. リスクを推定するために必要。
正解: **(正解を表示します)**
Threat and vulnerability assessments are important primarily because they are the basis for setting control objectives. Control objectives are the desired outcomes of implementing security controls, and they should be aligned with the organization's risk appetite and business objectives. Threat and vulnerability assessments help to identify the potential sources and impacts of security incidents, and to prioritize the mitigation actions based on the likelihood and severity of the risks. By conducting threat and vulnerability assessments, the organization can establish the appropriate level and type of security controls to protect its information assets and reduce the residual risk to an acceptable level. References = CISM Review Manual (Digital Version), Chapter 3: Information Security Risk Management, Section 3.1: Risk Identification, p. 115-1161. CISM Review Manual (Print Version), Chapter 3: Information Security Risk Management, Section 3.1: Risk Identification, p. 115-1162. CISM ITEM DEVELOPMENT GUIDE, Domain 3: Information Security Program Development and Management, Task Statement 3.1, p. 193.
Threat and vulnerability assessments are important PRIMARILY because they are the basis for setting control objectives. Control objectives are the desired outcomes or goals of implementing security controls in an information system. They are derived from the risk assessment process, which identifies and evaluates the threats and vulnerabilities that could affect the system's confidentiality, integrity and availability. By conducting threat and vulnerability assessments, an organization can determine the level of risk it faces and establish the appropriate control objectives to mitigate those risks.

質問: **340**
情報セキュリティ管理者が組織の電子通信および電子メール データをアーカイブして保持する最も重要な理由は次のうちどれですか。
A. ユーザーによる電子通信の個人的な使用を追跡するため
B. 必要に応じて法的手続きで証拠として提出する
C. グローバルセキュリティ標準の要件を満たす
D. 添付ファイルを識別してマルウェアをスキャンする
正解: **(正解を表示します)**
Retaining communications ensures the organization can produce evidence for litigation or regulatory investigations, which is often a legal obligation.

"Organizations must retain electronic communications to support legal discovery, compliance audits, and investigative needs."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Legal and Regulatory Requirements*

質問: **341**
情報セキュリティ管理者が、完全な機能継続性テストを実施する前に確認すべき最も重要な事項は次のうちどれですか？
A. 企業によるリスク受容は文書化されている
B. 復旧を担当するチームと個人が特定されました
C. 復旧計画およびインシデント対応計画のコピーはオフサイトに保管されています
D. インシデント対応および復旧計画は、平易な言葉で文書化されています。
正解: **(正解を表示します)**
Before conducting full-functional continuity testing, an information security manager should verify that teams and individuals responsible for recovery have been identified and trained on their roles and responsibilities.
This will ensure that the testing can be executed effectively and efficiently, as well as identify any gaps or issues in the recovery process. Risk acceptance by the business, copies of plans kept offsite and plans documented in simple language are all good practices for continuity management, but they are not as important as having clear roles and responsibilities defined before testing.

質問: **342**
情報セキュリティ戦略を策定する文脈において、次のうちどれが、またはを決定するために最も有用な入力を提供しますか？
A. セキュリティ予算
B. リスク登録簿
C. リスクスコア
D. 法律および規制
正解: **D (コメントを発表する)**
Laws and regulations provide the most useful input to determine the organization's information security strategy because they define the legal and compliance requirements and obligations that the organization must adhere to, and guide the development and implementation of the security policies and controls that support them. Security budget is not a useful input to determine the organization's information security strategy because it does not reflect the organization's security needs or goals, but rather a resource to enable the security activities and initiatives. Risk register is not a useful input to determine the organization's information security strategy because it does not reflect the organization's security vision or mission, but rather a tool to identify and manage the security risks. Risk score is not a useful input to determine the organization's information security strategy

because it does not reflect the organization's security priorities or objectives, but rather a measure of the level of risk exposure or performance. References: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/technical-security-standards-for-information-systems
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/how-to-align-security-initiatives-with-business-goals-and-objectives

質問: **343**
証拠能力のある証拠を収集する際に、以下のうち最も重要な要件はどれですか？
A. 知っておくべきこと
B. 監査ログの保存
C. デューデリジェンス
D. 保管管理記録
正解: **(正解を表示します)**
Chain of custody is the MOST important requirement when collecting admissible evidence, because it ensures the integrity and authenticity of the evidence by documenting its history, handling, and storage. Chain of custody records who, what, when, where, why, and how the evidence was collected, analyzed, and preserved.
Without a proper chain of custody, the evidence may be challenged or rejected in a court of law. Need to know, preserving audit logs, and due diligence are important aspects of evidence collection, but they are not as critical as chain of custody. References = CISM Review Manual, 16th Edition, page 3031; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1492 The most important requirement when collecting admissible evidence is the chain of custody. The chain of custody is a documented record of who had control of the evidence at any given time, from the point of collection until the evidence is presented in court. This is important in order to ensure the evidence can be authenticated and is not subject to tampering or any other form of interference. Other important considerations include need to know, preserving audit logs, and due diligence.

質問: **344**
組織のインシデント検出能力と対応能力を向上させるための最良の方法は次のうちどれですか?
A. ビジネス影響分析 (BIA) を実施します。
B. ネットワーク侵入テストを実行します。
C. 定期的な意識啓発トレーニングを実施します。
D. セキュリティギャップ分析を実行します。
正解: **(正解を表示します)**

質問: **345**

ある組織は、市場環境の変化に対応するため、会計年度の途中で事業目標を更新しました。新しい目標をサポートするために、情報セキュリティマネージャーが更新すべき最も重要な項目は次のうちどれですか？
A. 情報セキュリティポリシー
B. 情報セキュリティ戦略
C. 情報セキュリティ脅威プロファイル
D. 情報セキュリティの目標
正解: **B** (コメントを発表する)

質問: **346**
情報セキュリティプログラムを更新する際に、情報セキュリティマネージャーが最初にとるべきステップは何でしょうか？
A. コストを見直し、業界標準と比較する
B. 組織の事業上の期待と目標を再評価する
C. 事業目標に合致しないプログラム構成要素を特定する
D. 事業部門のマネージャーと主要な関係者へのインタビュー
正解: **B** (コメントを発表する)
The first step when updating an information security program is to re-evaluate the organization's business expectations and objectives. CISM emphasizes that the information security program must be aligned with business goals, risk appetite, and enterprise priorities. Before identifying misaligned components or interviewing stakeholders, the security manager must first understand the current business direction and expectations that the program must support. Benchmarking costs against industry norms may be useful later, but cost comparison does not define the program's required direction. Identifying misaligned components is only possible after current business objectives are understood. Interviewing business unit managers and stakeholders is a method that may support re-evaluation, but the primary first step is determining what the organization expects the updated program to achieve. Business objectives may change due to digital transformation, mergers, regulatory shifts, new products, or changing threat conditions. Therefore, re- evaluating business expectations and objectives is the correct starting point for updating the program.
References:
ISACA CISM Review Manual, Information Security Governance - business alignment and security program direction ISACA CISM Exam Content Outline, Domain 2: Information Security Governance

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu 1193問、３０%ディスカウント、特別な割引コード: JPNshiken」

質問: **347**
組織が新たなサイバーリスクを効果的に管理するために、最も適した方法はどれですか？
A. 定期的な内部監査および外部監査
B. 明確な責任体制
C. 十分なサイバー予算の配分
D. サイバーセキュリティポリシー
正解: **(正解を表示します)**
Cybersecurity policies are the high-level statements that define the organization's objectives, principles, and expectations for protecting its information assets from cyber threats. Cybersecurity policies provide the foundation for developing and implementing cybersecurity strategies, plans, procedures, standards, and guidelines. However, cybersecurity policies alone are not enough to ensure effective cybersecurity. The organization also needs to allocate sufficient budget resources to support the implementation and maintenance of cybersecurity controls, such as hardware, software, personnel, training, testing, auditing, and incident response. Sufficient cyber budget allocation demonstrates the organization's commitment to cybersecurity and enables it to achieve its cybersecurity goals. References: https://www.isaca.org/credentialing/cism https://www.wiley.com/en-us/CISM+Certified+Information+Security+Manager+Study+Guide-p-9781119801948

質問: **348**
次のうち、新たに出現する高度な持続的脅威(APT)攻撃者から最も効果的に保護できるのはどれですか？
A. ハニーポット環境
B. セキュリティ意識向上資料の更新
C. 継続的なインシデント対応訓練
D. プロアクティブなモニタリング
正解: **(正解を表示します)**
Proactive monitoring (e.g., threat hunting, real-time log analysis, anomaly detection) is the most effective defense against Advanced Persistent Threats (APTs), which are stealthy, well-resourced, and long-term attacks.
APT actors:
Use zero-day exploits
Maintain long-term unauthorized access
Avoid detection

Traditional controls often fail. Proactive monitoring detects anomalies early, allowing for faster mitigation.
"Ongoing monitoring and detection programs are essential for identifying and responding to persistent and evolving threats."
- CISM Review Manual 15th Edition, Chapter 4: Threat Management, Section: APT Detection Techniques*

質問: **349**
情報セキュリティ管理者が、システムが新たな脅威に対して脆弱であると判断した場合、次のうちどれが最善の対応策でしょうか？
A. システムを頻繁に更新し、脅威の状況を監視する。
B. 影響を受けるシステムを含むネットワークを監視し、悪意のあるトラフィックを検出します。
C. システムを扱う従業員の間で脅威に対する意識を高める。
D. 経営陣および主要な関係者に脅威を通知する。
正解: **(**正解を表示します**)**
The best course of action when an information security manager identifies that systems are vulnerable to emerging threats is to frequently update systems and monitor the threat landscape, as this will help to reduce the exposure and impact of the threats, and enable timely detection and response. Updating systems involves applying patches, fixing vulnerabilities, and implementing security controls. Monitoring the threat landscape involves collecting and analyzing threat intelligence, identifying new attack vectors and techniques, and assessing the risk and impact of the threats.
References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.2.1, page 2211; State of Cybersecurity 2023: Navigating Current and Emerging Threats2; CISM Online Review Course, Module 4, Lesson 2, Topic 13

質問: **350**
規制の厳しい市場で事業を展開している組織にとって、ビジネスに大きな影響を与える新しい規制要件を実装する必要がある場合、最も重要な考慮事項は何ですか?
A. ギャップ分析の実施
B. 補償制御の確立
C. 外部監査の実施
D. 強力な監視制御の実施
正解: **A (**コメントを発表する**)**

質問: **351**
情報セキュリティガバナンスフレームワークを設計する際に、以下のうち最も重要なものはどれですか？
A. 情報セキュリティの現状評価

B. 情報セキュリティリソースの可用性の評価
C. 情報セキュリティ戦略との整合性
D. 業界のベストプラクティスフレームワークに準拠する
正解: **C** (コメントを発表する)

質問: **352**
ランサムウェア攻撃後の重要システムおよびデータの復旧において、最も大きな課題となるのは次のうちどれですか？
A. 転送中のバックアップデータの暗号化が欠如している
B. 未定義または文書化されていないバックアップ保持ポリシー
C. バックアップ操作に対するアラート設定が効果的でない
D. データバックアップが利用できないか、破損しています
正解: (正解を表示します)
A ransomware incident is a type of cyberattack that encrypts the victim's data and demands a ransom for its decryption. Ransomware can cause significant disruption and damage to critical systems and data, as well as financial losses and reputational harm. To recover from a ransomware incident, the organization needs to have reliable and accessible backups of its data, preferably in an encrypted format. However, if the backups are unavailable or corrupt, the organization will face a major challenge in restoring its data and operations. Therefore, option D is the most challenging factor for the recovery of critical systems and data following a ransomware incident. References = CISA MS-ISAC Ransomware Guide1, page 9; How to Write an Incident Response Plan for Ransomware Recovery2.

質問: **353**
以下のうち、情報セキュリティプログラムに対する経営陣の支持を最もよく示しているのはどれですか？
A. トップダウンコミュニケーション
B. 定期的なセキュリティ意識向上トレーニング
C. 運営委員会の関与
D. 認定プログラムへの参加
正解: (正解を表示します)
The correct answer is C because active involvement in an information security steering committee demonstrates senior management's ongoing participation in governance, prioritization, decision-making, and oversight. Senior management support is not shown only by words or occasional communication; it is demonstrated through active engagement, resource allocation, risk decisions, and accountability. Top-down communication is useful and may show support, but it is less meaningful than direct participation in a governance body. Regular security awareness training is important for employees, but it does not necessarily prove senior management support. Participation in

a certification program may improve professional skills or demonstrate individual commitment, but it is not the best indicator of organizational leadership support. In CISM, information security governance requires senior management direction and oversight to ensure that security objectives align with business objectives. A steering committee provides a formal mechanism for that oversight and involvement. Therefore, steering committee involvement is the best indicator of senior management support.
Reference: CISM Information Security Governance; senior management commitment, steering committee oversight, and governance accountability principles.

質問**: 354**
セキュリティ管理のパフォーマンスが向上したことを経営陣に最も的確に示す証拠は、次のうちどれでしょうか？
A. セキュリティ投資に対する実績
B. 固有リスクの低減
C. 新たな脅威分析の結果
D. セキュリティ指標の動向レビュー
正解**: (**正解を表示します**)**
Review of security metrics trends is the best evidence to senior management that security control performance has improved because it helps to measure and demonstrate the effectiveness and efficiency of the security controls over time. Security metrics are quantitative or qualitative indicators that provide information about the security status or performance of an organization, system, process, or activity. Security metrics can be used to evaluate the implementation, operation, and outcome of security controls, such as the number of vulnerabilities detected and remediated, the time to respond and recover from incidents, the compliance level with security policies and standards, or the return on security investment. Review of security metrics trends helps to identify and communicate the progress, achievements, and challenges of the security program, as well as to support decision making and continuous improvement. Therefore, review of security metrics trends is the correct answer.
References:
https://www.bitsight.com/blog/importance-continuous-improvement-security-performance-management
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-2
https://www.nist.gov/news-events/news/2021/09/dhs-nist-coordinate-releasing-preliminary-cybersecurity-performance-goals.

質問**: 355**
サイバーインシデントをその影響に基づいて監視し、解決するまで追跡するのに最も効果的なシステムの種類はどれですか?
A. エンドポイント検出と応答 (EDR)

B. ネットワーク侵入検知システム（NIDS）
C. 拡張検出および応答 (XDR)
D. セキュリティ情報イベント管理 (SIEM)
正解: **D** (コメントを発表する)
SIEM systems collect and analyze log data from across the organization, allowing for real-time monitoring, incident correlation, and end-to-end tracking of response activities - including severity classification and closure.
"SIEM tools enable centralized management, prioritization, and documentation of incidents, making them essential for impact tracking and incident lifecycle management." - CISM Review Manual 15th Edition, Chapter 4: Incident Management Systems* While EDR and XDR help detect threats, SIEMs offer the full scope for impact-based tracking.

質問: **356**
悪意のある内部関係者による機密情報の漏洩を防ぐための最も効果的な防御策は、次のうちどれですか？
A. アクセス制御の定期監査
B. スタッフ採用時の厳格な身元調査
C. 迅速な解約手続き
D. 役割ベースアクセス制御(RBAC)
正解: **D** (コメントを発表する)
role-based access control (RBAC) is the most effective defense against malicious insiders compromising confidential information, as it helps to limit the access of users to the information and resources that are necessary for their roles and responsibilities. RBAC also helps to enforce the principle of least privilege, which reduces the risk of unauthorized or inappropriate access, disclosure, modification, or destruction of information by insiders. RBAC also facilitates the monitoring and auditing of user activities and access rights. References = Malicious insiders | Cyber.gov.au, Insider Threat Mitigation Guide - CISA, Malicious Insiders:
Types, Indicators & Common Techniques - Ekran System

質問: **357**
ある組織が、BYOD(私物端末の業務利用)環境で使用するモバイルデバイス管理ソフトウェアを評価しています。モバイルデバイス管理ソフトウェアの最も重要な機能は、以下のとおりです。
A. ネットワークアクセスをブロックします
B. デバイスの位置を追跡
C. リモートワイプを有効にする
D. テキストメッセージを保持する
正解: (正解を表示します)

The correct answer is C because remote wipe is one of the most important mobile device management features in a bring your own device environment. BYOD devices may be lost, stolen, compromised, or used after an employee leaves the organization. Remote wipe allows the organization to remove corporate data from a device to reduce the risk of unauthorized disclosure. This is especially important because the device is personally owned and may not be fully controlled by the organization. Blocking network access can help prevent future connectivity, but it does not remove sensitive data already stored on the device. Tracking device location may raise privacy concerns and does not directly protect organizational information. Retaining text messages is generally not a primary security requirement and may create privacy or legal concerns. In CISM risk management, mobile controls should protect information while balancing user privacy and business needs. Remote wipe best addresses the risk of corporate data exposure on BYOD devices.
Reference: CISM Information Risk Management; BYOD risk, mobile device management, data protection, remote wipe, and endpoint security principles.

質問: **358**
制御目標を定義する際に最も重要な考慮事項は次のどれですか?
A. 上級管理職のサポート
B. リスク選好度
C. 脅威環境
D. 予算配分
正解: **B (**コメントを発表する**)**
Risk appetite reflects how much risk the organization is willing to tolerate. It is the primary driver when defining control objectives, ensuring alignment with overall business strategy.
"Risk appetite should be used to guide the selection and design of control objectives to ensure risk is managed within acceptable boundaries."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management Strategy* Support, budget, and threats matter, but without alignment to risk appetite, controls may be misaligned.

質問: **359**
分散型サービス拒否(DDoS)攻撃に対する有効な封じ込め戦略として、次のうちどれが適切でしょうか?
A. 攻撃者が使用するIPアドレスをブロックする
B. 攻撃者のトラフィックをリダイレクトする
C. 攻撃者が悪用したファイアウォールポートを無効にします。
D. 影響を受けるサーバーの電源を切る
正解: **(**正解を表示します**)**
Redirecting the attacker's traffic is a viable containment strategy for a distributed denial of service (DDoS) attack because it helps to divert the malicious traffic away from the target

server and reduce the impact of the attack. A DDoS attack is an attempt by attackers to overwhelm a server or a network with a large volume of requests or packets, preventing legitimate users from accessing the service or resource. Redirecting the attacker's traffic is a technique that involves changing the DNS settings or routing tables to send the attacker's traffic to another destination, such as a sinkhole, a honeypot, or a scrubbing center. A sinkhole is a server that absorbs and discards the malicious traffic. A honeypot is a decoy server that mimics the target server and collects information about the attacker's behavior and techniques. A scrubbing center is a service that filters out the malicious traffic and forwards only the legitimate traffic to the target server. Redirecting the attacker's traffic helps to contain the DDoS attack by reducing the load on the target server and preserving its availability and performance. Therefore, redirecting the attacker's traffic is the correct answer.
References:
https://www.fortinet.com/resources/cyberglossary/implement-ddos-mitigation-strategy
https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-response-strategy
https://www.cloudflare.com/learning/ddos/glossary/sinkholing/.

質問**: 360**
新たに任命された情報セキュリティマネージャーは、5年以上変更されていないセキュリティ関連のポリシーと手順をすべて更新するよう求められました。次に何をすべきでしょうか？
A. 最良のビジネス慣行に従って更新します。
B. 現在のIT環境のリスク評価を実施する。
C. 現在の事業の方向性を理解する。
D. 現在のセキュリティポリシーを一覧し、見直します。
正解**: (**正解を表示します**)**
The next step for the information security manager should be to inventory and review the current security policies to understand the existing security requirements, controls, and gaps. This will help to identify the areas that need to be updated, revised, or replaced to align with the current business needs and objectives, as well as the legal and regulatory requirements. Updating the policies in accordance with the best business practices, performing a risk assessment of the current IT environment, or gaining an understanding of the current business direction are important activities, but they should be done after reviewing the current security policies.
References = CISM Review Manual, 16th Edition eBook1, Chapter 1: Information Security Governance, Section: Information Security Policies, Standards, Procedures and Guidelines, Subsection: Information Security Policies, Page 28.

質問**: 361**

クラウドサービスプロバイダーの倒産によって発生する情報損失のリスクを最も効果的に軽減できるのは、次のうちどれですか？
A. 監査権に関する契約条項
B. データ返還に関する契約条項
C. 効果的なデータ損失防止(DLP)対策
D. サイバーセキュリティ保険の購入
正解: **(**正解を表示します**)**
The best mitigation for information loss caused by a cloud service provider becoming insolvent is contractual provisions for data repatriation. In CISM third-party and cloud governance, organizations must ensure they can retrieve their data in a usable format if a provider fails, terminates service, or becomes financially insolvent. Data repatriation clauses define how data will be returned, in what format, within what timeframe, and how securely it will be transferred or deleted from the provider environment. Right-to-audit clauses help assess controls but do not ensure data recovery if the provider fails. Data loss prevention controls reduce unauthorized data leakage, but they do not address provider insolvency or service termination. Cybersecurity insurance may offset some financial loss, but it does not restore access to critical information. Because data availability and portability are central cloud exit strategy requirements, contractual repatriation rights are the strongest control to mitigate the risk of losing access to information due to provider insolvency.
References:
ISACA CISM Review Manual, Information Security Governance - cloud service governance, exit strategy, and third-party contracts ISACA CISM Exam Content Outline, Domain 2: Information Security Governance

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu **193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **362**
情報セキュリティインシデント発生後のレビューにおいて、以下のうちどれを最優先事項とすべきでしょうか？
A. 実施した措置を十分に詳細に記録する
B. 主要リスク指標(KRI)の更新
C. インシデント対応チームメンバーのパフォーマンス評価
D. インシデント対応の有効性の評価

正解: **(**正解を表示します**)**
An information security post-incident review is a process that aims to identify the root causes, impacts, lessons learned, and improvement actions of a security incident. The highest priority during a post-incident review should be evaluating the effectiveness of the incident response, which means assessing how well the incident response plan, procedures, roles, resources, and communication were executed and aligned with the business objectives and requirements. Evaluating the incident response effectiveness can help to identify the gaps, weaknesses, strengths, and opportunities for improvement in the incident response process and capabilities. Documenting actions taken in sufficient detail, updating key risk indicators (KRIs), and evaluating the performance of incident response team members are also important activities during a post- incident review, but they are not as critical as evaluating the incident response effectiveness, which can provide a holistic and strategic view of the incident response maturity and value.
References =
ISACA, CISM Review Manual, 16th Edition, 2020, page 2411
ISACA, CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, 2020, question ID 2192 During post-incident reviews, the highest priority should be given to evaluating the effectiveness of the incident response effort. This includes assessing the accuracy of the response to the incident, the timeliness of the response, and the efficiency of the response. It is important to assess the effectiveness of the response in order to identify areas for improvement and ensure that future responses can be more effective. Documenting the actions taken in sufficient detail, updating key risk indicators (KRIs), and evaluating the performance of incident response team members are all important components of a post-incident review, but evaluating incident response effectiveness should be given the highest priority.

質問: **363**
事件対応担当者の有効性を高める上で、以下のうち最も重要なものはどれですか？
A. 経営陣とのコミュニケーション
B. IT部門とスタッフの連携
C. テスト応答シナリオ
D. インシデント対応計画を毎年見直す
正解: **(**正解を表示します**)**
= Testing response scenarios is the most important factor in increasing the effectiveness of incident responders, as it allows them to practice their skills, identify gaps and weaknesses, evaluate the adequacy and feasibility of the incident response plan, and improve their coordination and communication. Testing response scenarios can also help to enhance the confidence and readiness of the incident responders, as well as to measure their performance and compliance with the policies and procedures. Testing response scenarios can be done through various methods, such as tabletop exercises,

simulations, drills, or full-scale exercises, depending on the scope, objectives, and complexity of the scenarios.
The other options are not as important as testing response scenarios, although they may also contribute to the effectiveness of incident responders. Communicating with the management team is important to ensure that the incident responders have the necessary support, resources, and authority to carry out their tasks, as well as to report the status and outcomes of the incident response. However, communication alone is not sufficient to increase the effectiveness of incident responders, as they also need to have the relevant knowledge, skills, and experience to handle the incidents. Integrating staff with the IT department may help to facilitate the collaboration and information sharing between the incident responders and the IT staff, who may have the technical expertise and access to the systems and data involved in the incidents. However, integration alone is not enough to increase the effectiveness of incident responders, as they also need to have the appropriate roles, responsibilities, and processes to manage the incidents. Reviewing the incident response plan annually is important to ensure that the plan is updated and aligned with the current risks, threats, and business requirements, as well as to incorporate the lessons learned and best practices from previous incidents.
However, reviewing the plan alone is not enough to increase the effectiveness of incident responders, as they also need to test and validate the plan in realistic scenarios and conditions. References = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 223-225, 230-231.
CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1004.

質問: **364**
インシデント管理計画が効果的に実行されることを確実にするために、以下のうちどれが最も重要ですか？
A. インシデント対応成熟度評価が実施されました。
B. インシデント対応チームは適切な訓練を受けている。
C. 評判の良いマネージドセキュリティサービスプロバイダーと契約しました。
D. 経営陣の支持と承認を得ました。
正解: **(**正解を表示します**)**

質問: **365**
インシデント通知プロセスを評価する上で、以下の指標のうちどれが最も適切ですか？
A. 報告されたインシデント1件あたりのダウンタイムの平均総コスト
B. 応答から解決までの経過時間
C. 報告期間あたりの平均インシデント数
D. 検出、報告、対応までの経過時間
正解: **D (**コメントを発表する**)**

Elapsed time between detection, reporting, and response is the most appropriate metric for evaluating the incident notification process because it measures how quickly and effectively the organization identifies, communicates, and responds to security incidents. The incident notification process is a critical part of the incident response plan that defines the roles and responsibilities, procedures, and channels for reporting and escalating security incidents to the relevant stakeholders. Elapsed time between detection, reporting, and response helps to assess the performance and efficiency of the incident notification process, as well as to identify any bottlenecks or delays that may affect the incident resolution and recovery. Therefore, elapsed time between detection, reporting, and response is the correct answer.
References:
https://www.atlassian.com/incident-management/kpis/common-metrics
https://securityscorecard.com/blog/how-to-use-incident-response-metrics/
https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf

質問: **366**
情報セキュリティ環境の変化を特定する最も効果的な方法は、次のうちどれですか？
A. 事業影響分析(BIA)
B. 年間リスク評価
C. 定期的な侵入テスト
D. 継続的なモニタリング
正解: **(正解を表示します)**
Continuous monitoring is the most effective way to identify changes in an information security environment, as it provides ongoing awareness of the security status, vulnerabilities, and threats that may affect the organization's information assets and risk posture. Continuous monitoring also helps to evaluate the performance and effectiveness of the security controls and processes, and to detect and respond to any deviations or incidents in a timely manner. (From CISM Review Manual 15th Edition and NIST Special Publication 800-1371) References: CISM Review Manual 15th Edition, page 181, section 4.3.2.4; NIST Special Publication 800-
1371, page 1, section 1.1.

質問: **367**
次のうち、リスク軽減策の例はどれですか？
A. 保険の購入
B. リスクに関連する活動を中止する
C. セキュリティ管理の改善
D. 費用便益分析の実施
正解: **(正解を表示します)**

Improving security controls is an example of risk mitigation, which is the process of reducing the likelihood or impact of a risk. Risk mitigation can be achieved by implementing various strategies, such as purchasing insurance, discontinuing the activity associated with the risk, or improving security controls. Purchasing insurance is a form of risk transfer, which is the process of shifting the responsibility or burden of a risk to another party. Discontinuing the activity associated with the risk is a form of risk avoidance, which is the process of eliminating or avoiding a potential source of harm. Performing a cost-benefit analysis is a form of risk evaluation, which is the process of assessing the costs and benefits of different options to manage a risk. References = CISM Review Manual, 16th Edition, page 1741; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 802

質問**: 368**
組織のリスク許容度がリスク対策プロセスの一部として考慮されるようにするための最善の方法は、次のうちどれですか？
A. 主要リスク指標(KRI)を確立する。
B. 定量的リスク評価手法を用いる。
C. リスク対策に関する定期的な報告を上級管理職に提供する。
D. リスク対策計画には運営委員会の承認が必要である。
正解**: (**正解を表示します**)**
= Requiring steering committee approval of risk treatment plans is the best way to help ensure an organization's risk appetite will be considered as part of the risk treatment process because the steering committee is composed of senior management and key stakeholders who are responsible for defining and communicating the risk appetite and ensuring that it is aligned with the business objectives and strategy. The steering committee can review and approve the risk treatment plans proposed by the information security manager and ensure that they are consistent with the risk appetite and the risk tolerance levels. The steering committee can also monitor and evaluate the effectiveness of the risk treatment plans and provide feedback and guidance to the information security manager. Establishing key risk indicators (KRIs), using quantitative risk assessment methods, and providing regular reporting on risk treatment to senior management are not the best ways to help ensure an organization's risk appetite will be considered as part of the risk treatment process, although they may be useful tools and techniques to support the risk management process. KRIs are metrics that measure the level of risk exposure and the performance of risk controls. Quantitative risk assessment methods are techniques that use numerical values and probabilities to estimate the likelihood and impact of risk events. Regular reporting on risk treatment to senior management is a way to communicate the status and results of the risk treatment process and to obtain feedback and support from senior management.

However, none of these methods can ensure that the risk treatment plans are approved and aligned with the risk appetite, which is the role of the steering committee. References = CISM Review Manual 2023, Chapter
2, Section 2.4.3, page 76; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 121.

質問: **369**
経営陣が巨額の罰金を回避するために、現在遵守されている規制よりもはるかに厳格な新しい個人データ規制を遵守することを決定した場合、次に取るべき行動は次のうちどれでしょうか？
A. 転送中および保存中のデータを暗号化します。
B. 投資収益率(ROI)分析を実施する。
C. データ最小化計画を作成し、実施する。
D. ギャップ分析を実施する。
正解: **D** (コメントを発表する)
A gap analysis is a tool that helps to identify the current state of compliance and the desired state of compliance, as well as the actions needed to achieve the desired state. A gap analysis should be done before implementing any specific controls or solutions, such as encryption, data minimization, or ROI analysis.
References = CISM Review Manual 15th Edition, page 65; Information Security Architecture: Gap Assessment and Prioritization, ISACA Journal, volume 2, 2018.

質問: **370**
組織の契約管理プロセスにおいて、最も効果的なセキュリティ対策となるのは、次のうちどれでしょうか？
A. 提案依頼書(RFP)段階でベンダーのセキュリティベンチマーク分析を実施する
B. セキュリティ要件が提案依頼書(RFP)の段階で定義されていることを確認する
C. 契約終了時の資産処分を対象とするセキュリティ評価の拡大
D. セキュリティ評価を拡張し、ランダム侵入テストを含める
正解: **B** (コメントを発表する)
Ensuring security requirements are defined at the request-for-proposal (RFP) stage is the most effective security outcome in an organization's contract management process because it establishes and communicates the security expectations and obligations for both parties, and enables the organization to evaluate and select the most suitable and secure vendor or service provider. Performing vendor security benchmark analyses at the RFP stage is not an effective security outcome, but rather a possible security activity that involves comparing and ranking different vendors or service providers based on their security capabilities or performance. Extending security assessment to cover asset disposal on contract termination is not an effective security outcome, but rather a possible security activity that involves verifying and validating that any assets or data belonging to

the organization are securely disposed of by the vendor or service provider at the end of the contract. Extending security assessment to include random penetration testing is not an effective security outcome, but rather a possible security activity that involves testing and auditing the vendor's or service provider's security controls or systems at random intervals during the contract. References: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-1/data-ownership-and-custodianship-in-the-cloud
https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/integrating-assurance-functions

質問: **371**
セキュリティ制御を設計する際に最も重要なことは以下のとおりです。
A. リスクベースのアプローチを適用する
B. 機密データに対する技術的制御の適用
C. 事業影響分析(BIA)の結果を考慮する
D. 予防的管理に重点を置く
正解: **(**正解を表示します**)**
A risk-based approach (A) is fundamental to control design in CISM. Controls must be proportionate to risk, aligned with business objectives, and consistent with risk appetite. Focusing solely on technical controls (B), BIA results (C), or preventive controls (D) limits effectiveness. A risk-based approach ensures balanced use of preventive, detective, and corrective controls.
References: ISACA CISM Review Manual (Risk management-control selection); CISM Exam Content Outline (Domain 1).

質問: **372**
アプリケーションセキュリティ制御の実装コストを削減するための最適な選択肢は次のうちどれですか？
A. 開発環境でセキュリティテストを実施します。
B. 開発プロセスにセキュリティ活動を統合する
C. プロジェクト完了後にリスク分析を実施する。
D. 標準的なアプリケーションセキュリティ要件を含める
正解: **B (**コメントを発表する**)**
Integrating security activities within the development process is the best option to lower the cost to implement application security controls because it ensures that security is considered and addressed throughout the software development life cycle (SDLC), from design to deployment, and reduces the likelihood and impact of security flaws or vulnerabilities that may require costly fixes or patches later on. Performing security tests in the development environment is not the best option because it may not detect or prevent all security issues that may arise in different environments or scenarios. Performing a risk analysis after project completion is not a good option because it may be too late to identify

or mitigate security risks that may have been introduced during the project. Including standard application security requirements is not a good option because it may not account for specific or unique security needs or challenges of different applications or projects. References: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/secure-software- development-lifecycle https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/technical-security- standards-for-information-systems

質問: **373**
情報セキュリティ投資を正当化するためのビジネスケースを作成する際、経営陣が十分な情報に基づいた意思決定を行うために最も役立つのは次のうちどれでしょうか？
A. 情報セキュリティ戦略
B. セキュリティインシデントによる損失
C. リスク評価の結果
D. 業界におけるセキュリティ投資の動向
正解: **C** (コメントを発表する)
The results of a risk assessment would best enable an informed decision by senior management when developing a business case to justify an information security investment. A risk assessment will help to identify and prioritize the threats and vulnerabilities that affect the organization's assets and processes, as well as the potential impact and likelihood of occurrence. A risk assessment will also provide a basis for selecting and evaluating the effectiveness of controls to mitigate the risks. According to CISA, developing a business case for security will be based on an in-depth understanding of organizational vulnerabilities, operational priorities, and return on investment1. The information security strategy, losses due to security incidents, and security investment trends in the industry are possible inputs or outputs of a risk assessment, but they are not sufficient to enable an informed decision by senior management. References: 1: The Business Case for Security - CISA 2: The Business Case for Security | CISA 3: #HowTo: Build a Business Case for Cybersecurity Investment 4: Making the Business Case for Information Security

質問: **374**
アプリケーション開発における情報セキュリティマネージャーの主な役割は、次のうちどれですか？
A. セキュリティがシステム開発ライフサイクル(SDLC)に確実に統合されるようにする
B. 業界のベストプラクティスへの準拠を確保するため
C. 企業セキュリティ管理が確実に実施されるようにする
D. 管理手順がビジネスリスクに対応していることを確認する
正解: (正解を表示します)
According to the CISM Review Manual, one of the primary roles of the information security manager in application development is to ensure that security is integrated into the SDLC. This means that security requirements, design, testing, deployment, and maintenance are

all considered and addressed throughout the application development process. By doing so, the information security manager can help to prevent or mitigate security risks, ensure compliance with standards and regulations, and improve the quality and reliability of the application1 The other options are not as accurate as ensuring security is integrated into the SDLC. Ensuring compliance with industry best practices is a secondary role of the information security manager in application development, as it involves following established guidelines and frameworks for secure application development. However, compliance alone does not guarantee that security is actually implemented in the application. Ensuring enterprise security controls are implemented is a tertiary role of the information security manager in application development, as it involves applying existing policies and procedures for managing and monitoring security activities across the organization. However, enterprise controls alone do not ensure that security is tailored to the specific needs and context of each application. Ensuring control procedures address business risk is a quaternary role of the information security manager in application development, as it involves identifying and assessing potential threats and vulnerabilities that could affect the business objectives and operations of each application. However, business risk alone does not ensure that security measures are aligned with the value proposition and benefits of each application1 References = 1: CISM Review Manual, 16th Edition, ISACA, 2020, pp. 30-31...

質問**: 375**
リスクを許容可能なレベルまで軽減するための最適な対策を選択する際、情報セキュリティ管理者の意思決定は主に以下の点に基づいて行われるべきである。
A. ベストプラクティス。
B. 制御フレームワーク
C. 規制要件。
D. 費用便益分析、
正解**: (**正解を表示します**)**
Cost-benefit analysis (CBA) is a method of comparing the costs and benefits of different alternatives for achieving a desired outcome. CBA can help information security managers to choose the best controls to mitigate risk to acceptable levels by providing a rational and objective basis for decision making. CBA can also help information security managers to justify their choices to senior management, stakeholders, and auditors by demonstrating the value and return on investment of the selected controls. CBA can also help information security managers to prioritize and allocate resources for implementing and maintaining the controls12.
CBA involves the following steps12:
Identify the objectives and scope of the analysis
Identify the alternatives and options for achieving the objectives
Identify and quantify the costs and benefits of each alternative

Compare the costs and benefits of each alternative using a common metric or criteria Select the alternative that maximizes the net benefit or minimizes the net cost Perform a sensitivity analysis to test the robustness and validity of the results Document and communicate the results and recommendations CBA is mainly driven by the information security manager's decision, but it can also take into account other factors such as best practices, control frameworks, and regulatory requirements. However, these factors are not the primary drivers of CBA, as they may not always reflect the specific needs and context of the organization. Best practices are general guidelines or recommendations that may not suit every situation or environment. Control frameworks are standardized models or methodologies that may not cover all aspects or dimensions of information security. Regulatory requirements are mandatory rules or obligations that may not address all risks or threats faced by the organization. Therefore, CBA is the best method to choose the most appropriate and effective controls to mitigate risk to acceptable levels, as it considers the costs and benefits of each control in relation to the organization's objectives, resources, and environment12. References = CISM Domain 2: Information Risk Management (IRM) [2022 update], Five Key Considerations When Developing Information Security Risk Treatment Plans

質問: **376**
組織のインシデント対応能力を評価する上で、最も費用対効果の高い方法は次のうちどれですか？
A. テーブルトップエクササイズ
B. 上級管理職面接
C. 侵入テスト
D. 第三者評価
正解: **(**正解を表示します**)**
The correct answer is A because a tabletop exercise is a low-cost and effective way to assess incident response capabilities. It allows participants to walk through a simulated incident scenario and evaluate roles, responsibilities, escalation paths, communication procedures, decision-making, and coordination without disrupting production systems. A tabletop exercise can identify weaknesses in the incident response plan, improve readiness, and increase participant familiarity with response procedures. Senior management interviews may provide insight into governance awareness, but they do not test operational response capability. Penetration testing can identify vulnerabilities and may trigger response processes, but it is more expensive and focused on technical exposure rather than full incident response capability. A third-party assessment can be valuable, but it is usually more costly than an internal tabletop exercise. CISM incident management emphasizes regular testing, lessons learned, and continuous improvement. Because tabletop exercises provide practical assessment value with relatively low cost and low operational risk, they are the most cost-effective method.

Reference: CISM Information Security Incident Management; incident response testing, tabletop exercises, preparedness, and continuous improvement principles.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu **193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **377**
システム開発プロジェクトに情報セキュリティを確実に組み込むために、最初に行うべきことはどれですか？
A. セキュリティ要件を定義する
B. 事業への影響に基づいてリソースを割り当てる
C. セキュリティポリシーを確認する
D. 各プロジェクトチームにセキュリティ担当者を配置する
正解: **(**正解を表示します**)**
The correct answer is A because security must be defined as a requirement early in system development projects. Security requirements translate business, regulatory, privacy, risk, and control expectations into specific project deliverables. When requirements are defined early, security can be built into architecture, design, development, testing, and deployment. If requirements are not defined at the beginning, security may be added later as a costly or incomplete afterthought. Assigning resources based on business impact is useful, but resource planning should follow a clear understanding of the required security outcomes. Reviewing the security policy may provide guidance, but it does not by itself integrate security into the project. Embedding a security representative can support integration, but the representative still needs defined requirements to guide the project team. CISM program management emphasizes integrating information security into life cycle processes and business initiatives as early as possible. Therefore, defining security requirements is the first and most important step to ensure security is built into system development projects.
Reference: CISM Information Security Program Development and Management; SDLC security, security requirements, project integration, and secure development principles.

質問: **378**
組織の情報セキュリティ基準をサードパーティのバックアップサイトが引き続き満たすことを確実にするために、次のうちどれが最も役立ちますか？
A. サービスレベル契約(SLA)

B. 覚書(MoU)
C. 事業継続計画(BCP)
D. 災害復旧計画(DRP)
正解: **(**正解を表示します**)**
A Service Level Agreement (SLA) is a legally binding document that defines the performance and compliance expectations for third-party services, including information security requirements. It is the best mechanism to ensure that the third-party backup site meets ongoing security standards.
"SLAs should include security, availability, and performance expectations to align third-party services with organizational policies."
- CISM Review Manual 15th Edition, Chapter 3: Program Development, Section: Third-Party Relationships*

質問: **379**
機密性、完全性、可用性(CIA)の三要素の中で、以下の活動のうち、機密性の概念を最もよくサポートするのはどれですか？
A. 管理者認証情報のハッシュ化を確実に行う
B. サービスレベル契約(SLA)の履行
C. 転送中のデータの暗号化を確保する
D. 正式な変更管理プロセスを活用する
正解: **(**正解を表示します**)**
Ensuring encryption for data in transit is the best activity that supports the concept of confidentiality within the CIA triad, as it protects the data from unauthorized access or interception while it is being transmitted over a network. Encryption is a technique that transforms data into an unreadable form using a secret key, so that only authorized parties who have the key can decrypt and access the data. Encryption standards include AES (Advanced Encryption Standard) and DES (Data Encryption Standard).
References = CISM Review Manual 2022, page 321; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.12; The CIA triad: Definition, components and examples3; CIA Triad - GeeksforGeeks4

質問: **380**
ビジネスアプリケーションへのサイバー攻撃の増加を受けて、経営陣がセキュリティを組織のあらゆるプロセスに統合するために最も効果的な方法はどれでしょうか？
A. 組織戦略に合わせてプロセス図を更新する
B. 開発者に対し、安全なアプリケーション開発に関するカスタマイズされた研修への参加を義務付ける。
C. 各事業分野内の主要関係者に対し、セキュリティ研修を提供する。
D. 事業目標に沿ったセキュリティポリシーの策定
正解: **(**正解を表示します**)**

The correct answer is D because senior management integrates security into organizational processes by establishing security policies that are aligned with business objectives. Policies communicate management's intent, define required behavior, and provide the foundation for standards, procedures, controls, and accountability across the enterprise. When policies align with business objectives, security becomes part of how the organization operates rather than a separate technical activity. Updating process diagrams may help document processes, but documentation alone does not integrate security. Developer training is useful for application security, but it applies mainly to development teams and not all organizational processes. Training key stakeholders is valuable, but training alone does not establish mandatory enterprise-wide requirements.
CISM governance principles emphasize that information security must support business goals, be directed by senior management, and be embedded into organizational structures and processes. Therefore, establishing business-aligned security policies is the best mechanism for integrating security into all organizational processes.
Reference: CISM Information Security Governance; policy alignment, senior management direction, business integration, and governance principles.

質問**: 381**
情報セキュリティガバナンスフレームワークを維持する組織にとって、最も重要なメリットは何ですか？
A. 投資収益率(ROI)を最大化するために、リソースの優先順位付けを行います。
B. 情報セキュリティガイドラインは企業全体に周知されている。
C. 組織は規制要件を遵守しています。
D. 事業リスクは許容できるレベルに管理されている。
正解**: (**正解を表示します**)**
According to the Certified Information Security Manager (CISM) Study Manual, a mature information security culture is one in which staff members regularly consider risk in their decisions. This means that they are aware of the risks associated with their actions and take preventative steps to reduce the likelihood of negative outcomes. Other indicators of a mature information security culture include mandatory information security training for all staff, documented and communicated information security policies, and regular interaction between the CISO and the board.
Maintaining an information security governance framework enables an organization to identify, assess, and manage its information security risks. By establishing policies, procedures, and controls that are aligned with the organization ' s objectives and risk tolerance, an information security governance framework helps ensure that information security risks are managed to an acceptable level.
According to the Certified Information Security Manager (CISM) Study Manual, "
Information security governance provides a framework for managing and controlling information security practices and technologies at an enterprise level. Its primary objective

is to manage and reduce risk through a process of identification, assessment, and management of those risks. " While the other options listed (prioritizing resources, communicating guidelines, and remaining compliant with regulations) are also important benefits of maintaining an information security governance framework, they are all secondary to the primary benefit of managing business risks to an acceptable level.
Reference:
Certified Information Security Manager (CISM) Study Manual, 15th Edition, Pages 60-63.

質問: **382**
公開ウェブサイトの企業プライバシーポリシーを作成する際、次のうちどれを必ず含める必要がありますか？
A. 責任限定条項
B. 情報利用の説明
C. 情報暗号化要件
D. アクセス制御要件
正解: **(**正解を表示します**)**
A privacy statement should inform the users of the website how their personal information will be collected, used, shared, and protected by the organization. References = CISM Review Manual, 16th Edition, Chapter 4, Section 4.2.1.11

質問: **383**
フィッシングメールが悪質かどうかを判断するのに最も役立つのは次のどれですか?
A. リバースエンジニアリング
B. セキュリティ意識向上トレーニング
C. 脅威情報
D. サンドボックス
正解: **(**正解を表示します**)**

質問: **384**
ある組織が使用しているセキュリティ基準は、認証機関によって大幅に改訂されました。認証を維持したい組織は、旧バージョンの基準を使用できなくなります。
以下のうちどれが最初にすべきか
取るべき行動は？
A. 認証維持にかかる費用を評価する。
B. 新しい基準が事業に適用可能かどうかを検討する。
C. 新たな要件が確実に満たされるよう、ポリシーを修正する。
D. 新しい基準を上級幹部に伝える。
正解: **(**正解を表示します**)**
Reviewing the new standard for applicability to the business is the first course of action, as it helps to understand the changes, gaps, and impacts of the revision on the organization's

security posture, compliance status, and business objectives. Evaluating the cost of maintaining the certification, modifying policies to ensure new requirements are covered, and communicating the new standard to senior leadership are important steps, but they should be done after reviewing the new standard for applicability to the business. References = CISM Review Manual 2022, page 361; CISM Exam Content Outline, Domain 1, Task 1.2

質問: **385**
情報資産を保護するためのポリシー、基準、手順を策定する上で、最も重要なインプットは次のうちどれですか？
A. 脆弱性評価
B. 規制要件
C. 業界のベストプラクティス
D. 企業目標
正解: **D** (コメントを発表する)
Enterprise goals are the most critical input because security policies must align with and support the organization's objectives and mission. Policies that do not align with enterprise goals are less likely to gain management support and may not effectively protect key assets.
"Information security must support enterprise goals and objectives to ensure alignment with the broader business strategy."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Alignment with Business Goals and Objectives ISACA's CISM questions reiterate that alignment with enterprise goals is essential for policy effectiveness.

質問: **386**
組織の新たな業界規制への対応に最も大きな影響を与えるのは、次のうちどれでしょうか？
A. 組織の統制目標
B. 組織のリスク管理フレームワーク
C. 組織のリスク許容度
D. 組織のリスク管理基準
正解: (正解を表示します)
The most influential factor on an organization's response to a new industry regulation is the organization's risk appetite. This is because the risk appetite defines the level of risk that the organization is willing to accept in pursuit of its objectives, and it guides the decision-making process for managing risks. The risk appetite also determines the extent to which the organization needs to comply with the new regulation, and the resources and actions required to achieve compliance. The risk appetite should be aligned with the organization's strategy, culture, and values, and it should be communicated and monitored throughout the organization.

質問: **387**
組織の情報セキュリティプログラムへの投資を正当化する提案書に含めるべき最も重要な項目は次のうちどれでしょうか？
A. 脆弱性スキャン結果
B. 競合他社ベンチマーク分析
C. 以前のセキュリティ予算
D. ビジネス要件
正解: **(正解を表示します)**
Comprehensive and Detailed Step-by-Step Explanation:
Justifying investments in information security requires aligning proposals with business objectives to gain management approval.
A). Vulnerability scan results: These provide technical insights but are insufficient for high-level justification.
B). Competitor benchmark analysis: While useful, this is less relevant than demonstrating direct alignment with organizational needs.
C). Previous security budget: Historical data may provide context but does not justify future needs.
D). Business requirements: This is the BEST answer because aligning security investments with business objectives demonstrates the value and necessity of the program to stakeholders.
Reference: CISM Job Practice Area 1 (Information Security Governance) focuses on aligning security initiatives with business goals to secure buy-in.

質問: **388**
侵入が検知され、封じ込められました。復旧したシステムの完全性を確保するための最善策は、以下のどの手順でしょうか？
A. OS、パッチ、およびアプリケーションを元のソースからインストールします。
B. バックアップからOS、パッチ、およびアプリケーションを復元します。
C. フォレンジックコピーからアプリケーションとデータを復元します。
D. OSとアプリケーションから侵入の痕跡をすべて削除します。
正解: **(正解を表示します)**
After an intrusion has been detected and contained, the system should be recovered to a known and trusted state. The best practice for ensuring the integrity of the recovered system is to install the OS, patches, and application from the original source, such as the vendor's website or media. This way, any malicious code or backdoors that may have been inserted by the intruder can be eliminated. Restoring the OS, patches, and application from a backup may not guarantee the integrity of the system, as the backup may have been compromised or outdated. Restoring the application and data from a forensic copy may preserve the evidence of the intrusion, but it may also reintroduce the

vulnerability or malware that allowed the intrusion in the first place. Removing all signs of the intrusion from the OS and application may not be sufficient or feasible, as the intruder may have made subtle or hidden changes that are difficult to detect or undo.
References =
ISACA, CISM Review Manual, 16th Edition, 2020, page 2401
ISACA, CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, 2020, question ID 2132 The BEST practice for ensuring the integrity of the recovered system after an intrusion is to restore the OS, patches, and application from a backup. This will ensure that the system is in a known good state, without any potential residual malicious code or changes from the intrusion. Restoring from a backup also enables the organization to revert to a previous configuration that has been tested and known to be secure. This step should be taken prior to conducting a thorough investigation and forensic analysis to determine the cause and extent of the intrusion.

質問**: 389**
情報セキュリティプログラムとビジネス戦略との整合性を判断する上で、最も効果的な方法は次のうちどれですか？
A. 事業継続性テストの結果を評価する。
B. 主要業績評価指標(KPI)を確認する。
C. インシデントのビジネスへの影響を評価する。
D. ビジネスプロセスの責任者を巻き込む。
正解**: D (**コメントを発表する**)**
The most effective way to determine the alignment of an information security program with the business strategy is D. Engage business process owners. This is because business process owners are the key stakeholders who are responsible for defining, executing, and monitoring the business processes that support the organization's mission, vision, and goals. By engaging them, the information security manager can understand their needs, expectations, and challenges, and ensure that the information security program is aligned with their requirements and objectives. Engaging business process owners can also help to establish trust, collaboration, and communication between the information security function and the business units, and foster a culture of security awareness and accountability.
Business process owners are the key stakeholders who are responsible for defining, executing, and monitoring the business processes that support the organization's mission, vision, and goals. By engaging them, the information security manager can understand their needs, expectations, and challenges, and ensure that the information security program is aligned with their requirements and objectives. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 1, Section 1.2.2, page 201; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 78, page 20

質問: **390**
経営陣は新会社の買収を発表しました。親会社の情報セキュリティマネージャーは、アクセス権限の競合により、2社の統合中に重要な情報が漏洩する可能性があることを懸念しています。この懸念に最も適切に対処するために、情報セキュリティマネージャーは次のことを行うべきです。
A. 買収統合が進むにつれて、アクセス権限を見直します。
B. アクセス権限のリスク評価を実施する。
C. アクセス権限の競合に関する懸念を経営陣に報告する。
D. 一貫したアクセス制御基準を導入する。
正解: **B (**コメントを発表する**)**
Performing a risk assessment of the access rights is the best way to address the concern of conflicting access rights during the integration of two companies. A risk assessment will help to identify and prioritize the threats and vulnerabilities that affect the access rights of both companies, as well as the potential impact and likelihood of information exposure. A risk assessment will also provide a basis for selecting and evaluating the controls to mitigate the risks. According to NIST, a risk assessment is an essential component of risk management and should be performed before implementing any security controls1. The other options are not the best ways to address the concern of conflicting access rights during the integration of two companies, but rather possible subsequent actions based on the risk assessment. Reviewing access rights as the acquisition integration occurs may be too late or too slow to prevent information exposure. Escalating concerns for conflicting access rights to management may not be effective without evidence or recommendations from a risk assessment. Implementing consistent access control standards may not be feasible or desirable for different systems or business units. References: 1: NIST SP 800-30 Rev. 1 Guide for Conducting Risk Assessments 2: M & A integration strategy is crucial for deal success but remains difficult: PwC 3: The 10 steps to successful M & A integration | Bain & Company : Cracking the code to successful post-merger integration

質問: **391**
組織が適切なセキュリティ管理環境を維持する上で、最も効果的なのは次のうちどれですか？
A. 業界セキュリティフレームワークへの準拠
B. 治安対策のための予算支援
C. 定期的な従業員セキュリティ研修
D. 脅威状況の監視
正解: **(**正解を表示します**)**
Alignment to an industry security framework ensures that the organization adopts best practices and standards for security control implementation and maintenance. References = CISM Review Manual, 16th Edition, Domain 1: Information Security Governance,

Chapter 1: Establish and Maintain an Information Security Strategy, Section: Information Security Frameworks

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu **193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **392**
情報セキュリティプログラムにおいて、最も重要な要素は次のうちどれですか？
A. プログラムの関連性をグローバルスタンダードと比較評価する
B. 利用可能なリソースに基づいてプログラムの成果物の優先順位付けを行う
C. プログラム開発に機能別マネージャーを参加させる
D. 企業が採用しているプロジェクト管理手法を適用する
正解: **(正解を表示します)**
Involving functional managers in program development is the most essential element of an information security program, because they are responsible for ensuring that the information security policies, standards, and procedures are implemented and enforced within their respective business units. They also provide input and feedback on the information security requirements, risks, and controls that affect their operations and objectives.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 37: "Functional managers are responsible for ensuring that the information security policies, standards, and procedures are implemented and enforced within their respective business units." CISM Review Manual, 16th Edition, ISACA, 2020, p. 38: "Functional managers should be involved in the development of the information security program to provide input and feedback on the information security requirements, risks, and controls that affect their operations and objectives."

質問: **393**
アプリケーションで発見されたリスクを管理するのに最も適しているのは、次の誰ですか?
A. システム所有者
B. 上級管理職
C. コントロールの所有者
D. 情報セキュリティ管理者

正解: **(**正解を表示します**)**

質問: **394**
組織が混乱事象に見舞われた場合、事業継続計画(BCP)は主に以下の点に基づいて発動されるべきである。
A. 停電の予想期間。
B. 経営方針
C. セキュリティインシデントの種類。
D. 事件の根本原因。
正解: **(**正解を表示します**)**
The expected duration of outage is the primary factor that should trigger the BCP because it indicates how long the organization can tolerate the disruption of its critical business processes and functions before it causes unacceptable consequences. The expected duration of outage is determined by the recovery time objectives (RTOs) that are defined for each critical business process and function based on the business impact analysis (BIA). The BCP should be triggered when the expected duration of outage exceeds or is likely to exceed the RTOs.
References: The CISM Review Manual 2023 defines RTO as "the maximum acceptable time that a service can be unavailable or disrupted before it causes unacceptable consequences" and states that "the RTO is determined based on the impact of service interruption on the enterprise's business processes, reputation, customers, and stakeholders" (p. 189). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Expected duration of outage is the correct answer because it is the primary factor that should trigger the BCP, as it reflects the maximum time that the organization can afford to lose its critical business processes and functions without causing unacceptable consequences" (p. 96).
Additionally, the article Invoking your business continuity plan: five triggers, six decision points from the ITWeb website states that "the expected duration of outage is the most important consideration when deciding to invoke the BCP, as it indicates how long the organization can sustain the disruption before it impacts its business objectives, operations, reputation, and legal obligations" (p. 2)

質問: **395**
ある組織が情報セキュリティガバナンスフレームワークを導入している。ステークホルダーにプログラムの有効性を伝えるために最も重要なことは、以下の点を確立することである。
A. 自己評価(CSA)プロセス。
B. 利害関係者への自動報告。
C. セキュリティポリシーの監視プロセス。
D. 各マイルストーンの指標。

正解: **D** (コメントを発表する)
= Establishing metrics for each milestone is the best way to communicate the program's effectiveness to stakeholders, as it provides a clear and measurable way to track the progress, performance, and outcomes of the information security governance framework. Metrics are quantifiable indicators that can be used to evaluate the achievement of specific objectives, goals, or standards. Metrics can also help to demonstrate the value, benefits, and return on investment of the information security program, as well as to identify and address the gaps, issues, or risks. Metrics for each milestone should be aligned with the organization's strategy, vision, and mission, as well as with the expectations and needs of the stakeholders. Metrics for each milestone should also be SMART (specific, measurable, achievable, relevant, and time-bound), as well as consistent, reliable, and transparent.
The other options are not as important as establishing metrics for each milestone, as they do not provide a comprehensive and holistic way to communicate the program's effectiveness to stakeholders. A control self- assessment (CSA) process is a technique to involve the staff in assessing the design, implementation, and effectiveness of the information security controls. It can help to increase the awareness, ownership, and accountability of the staff, as well as to identify and mitigate the risks. However, a CSA process alone is not enough to communicate the program's effectiveness to stakeholders, as it does not measure the overall performance or maturity of the information security program. Automated reporting to stakeholders is a method to provide timely, accurate, and consistent information to the stakeholders about the status, results, and issues of the information security program. It can help to facilitate the communication, collaboration, and decision making among the stakeholders, as well as to ensure the compliance and transparency of the information security program. However, automated reporting alone is not enough to communicate the program's effectiveness to stakeholders, as it does not evaluate the achievement or impact of the information security program. A monitoring process for the security policy is a process to ensure that the security policy is implemented, enforced, and reviewed in accordance with the organization's objectives, standards, and regulations. It can help to maintain the relevance, adequacy, and effectiveness of the security policy, as well as to incorporate the feedback, changes, and improvements. However, a monitoring process alone is not enough to communicate the program's effectiveness to stakeholders, as it does not cover the other aspects of the information security program, such as governance, risk management, incident management, or business continuity. References = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 211-212, 215-216, 233-234, 237-238.
CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1018.
CISM domain 1: Information security governance [Updated 2022], Infosec, 1.
Key Performance Indicators for Security Governance, Part 1, ISACA Journal, Volume 6, 2020, 2.

質問: **396**

インシデント後の検証における最優先目標は以下のとおりである。
A. 事件が企業に与えるコストを算定する。
B. 再発防止のための政策変更を特定する。
C. インシデント処理プロセスを改善する方法を決定する。
D. 事件が発生した理由を特定する。
正解: **(**正解を表示します**)**

質問: **397**
情報セキュリティポリシーが遵守されているかどうかを判断する上で、以下のうちどれが最も役立ちますか？
A. 探偵の操作
B. 指令制御
C. 予防的管理
D. 是正措置
正解: **A (**コメントを発表する**)**

質問: **398**
ある組織が、自社開発のアプリケーションを、Platform as a Service(PaaS)モデルを使用するサードパーティのクラウドホスティングプロバイダーに移行したいと考えています。クラウドプロバイダーを選定する前に、組織にとって最も重要な確認事項は何でしょうか？
A. クラウドプロバイダーは、復旧目標時点(RPO)を満たすことができます。
B. クラウドプロバイダーは適用される規制を遵守します。
C. クラウドプロバイダーのサービスレベル契約(SLA)には可用性要件が含まれます。
D. ホスティング契約には解約条項があります。
正解: **B (**コメントを発表する**)**
When outsourcing to a cloud provider, regulatory compliance is paramount-especially with sensitive or proprietary applications. Non-compliance could result in legal penalties, fines, or reputational damage.
While RPOs, SLAs, and contract clauses are critical components of vendor risk management, ensuring adherence to relevant laws and industry regulations (such as GDPR, HIPAA, PCI DSS) is the first priority in cloud migration decisions.
"Prior to selecting a cloud provider, legal, regulatory, and contractual requirements must be reviewed to ensure alignment."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Compliance Considerations in Cloud Computing*

質問: **399**
退職した従業員のシステムアクセス権を削除する際に、最も重要な機能は次のうちどれですか？
A. 法律

B. 情報セキュリティ
C. ヘルプデスク
D. 人事部(HR)
正解: **(**正解を表示します**)**
Information security is the most critical function when initiating the removal of system access for terminated employees, as it is responsible for ensuring that the access rights of the employees are revoked in a timely and effective manner, and that the security of the organization's data and systems is maintained. Information security should coordinate with other functions, such as HR, legal, and help desk, to implement the access removal process, but it is the primary function that has the authority and capability to disable or delete the access credentials of the terminated employees. The other options are not as critical as information security, as they may have different roles or responsibilities in the access removal process, or they may not have direct access to the systems or tools that control the access rights of the employees. References = CISM Review Manual 15th Edition, page 114: "Information security is responsible for ensuring that access rights are revoked in a timely and effective manner." SOC 2 Controls: Access Removal for Terminated or Transferred Users, snippets: "Systems access that is no longer required for terminated or transferred users is removed within one business day. For terminated employees, access to key IT systems is revoked in a timely manner. A termination checklist and ticket are completed, and access is revoked for employees as a component of the employee termination process." IT Involvement in Employee Termination, A Checklist, snippets: "Disable all network access. If your company uses a master access list of active passwords, tell the system to deny any passcodes associated with the user being terminated. If your system doesn't have a deny function, delete the user and their associated passwords. Monitor employee access." Human resources (HR) is the most critical function when initiating the removal of system access for terminated employees because it is responsible for notifying the relevant parties, such as information security, help desk, and legal, of the employee's termination status and date. HR also ensures that the employee's exit process is completed and documented, and that the employee returns any company-owned devices or assets.
HR also coordinates with the employee's manager and team to ensure a smooth transition of work and responsibilities.

質問: **400**
組織内のセキュリティ文化に最も大きな影響を与えることができる役割は、次のうちどれですか？
A. 最高情報セキュリティ責任者(CISO)
B. 最高情報責任者(CIO)
C. 最高経営責任者(CEO)
D. 最高執行責任者(COO)
正解: **C (**コメントを発表する**)**

The CEO is the best able to influence the security culture within an organization because the CEO sets the tone and direction for the organization and has the authority and responsibility to ensure that the organization' s objectives are aligned with its strategy. The CEO can also communicate the importance and value of information security to all stakeholders and foster a culture of security awareness and accountability. The CISO, CIO and COO are important roles in information security management, but they do not have the same level of influence and authority as the CEO. References = CISM Review Manual, 16th Edition, page 221; CISM Exam Content Outline, Domain 1, Task 12 The Chief Information Security Officer (CISO) is responsible for leading and coordinating an organization ' s information security program, and as such, is in a prime position to influence the security culture within the organization. The CISO is responsible for setting policies and standards, educating employees about security risks and best practices, and ensuring that the organization is taking appropriate measures to mitigate security risks. By demonstrating a strong commitment to information security, the CISO can help to create a security- aware culture within the organization.

質問**: 401**
インシデント対応計画のテストを実施することで得られる最も有益な結果は、次のうちどれですか？
A. 対応策には上級管理職へのエスカレーションが含まれます
B. インシデント対応時間が改善されました
C. 試験結果を反映させるため、計画が強化されました。
D. テスト計画の結果が文書化されている
正解**: C (**コメントを発表する**)**
The correct answer is C because the most beneficial outcome of testing an incident response plan is using the findings to improve the plan. Testing is not performed only to confirm that a plan exists; it is performed to identify weaknesses, validate assumptions, clarify roles, improve communication, and strengthen response capability. When the plan is enhanced based on test findings, the organization gains lasting value and improves preparedness for future incidents. Improved response time is a valuable result, but it usually occurs because the plan, procedures, training, or coordination have been improved after testing. Escalation to senior management may be appropriate for certain incidents, but it is not always required and is not the main benefit of testing. Documenting test results is necessary for accountability and lessons learned, but documentation alone does not improve response capability unless corrective actions are taken. CISM incident management emphasizes testing, lessons learned, continuous improvement, and plan maintenance. Therefore, enhancing the plan based on test findings is the best answer. Reference: CISM Information Security Incident Management; incident response testing, lessons learned, plan maintenance, and continuous improvement principles.

質問**: 402**

組織がソーシャルメディアポリシーを策定する最も重要な理由は以下のとおりです。
A. 企業ブランドを保護する
B. 従業員の生産性を向上させる
C. 従業員のインターネット活動を監視する
D. マルウェアの拡散を防ぐ
正解: **A** (コメントを発表する)
The correct answer is A because a social media policy is primarily intended to protect the organization from reputational, legal, confidentiality, and brand-related risks arising from employee or corporate use of social media. Social media can quickly expose the organization to public criticism, unauthorized disclosures, inappropriate statements, misinformation, privacy violations, and brand damage. While productivity may be affected by social media use, productivity is not usually the most important information security or governance concern. Monitoring employee internet activity may be one method of enforcement, but it is not the main reason for having the policy. Preventing malware is important, but malware risk is normally addressed through technical controls such as web filtering, endpoint protection, and awareness training. A social media policy defines acceptable use, responsibilities, restrictions, approval requirements, and consequences. In CISM terms, policies should address business risk and protect organizational value. Since social media misuse can significantly harm public trust and reputation, protecting the company brand is the best answer.
Reference: CISM Information Security Governance; policy development, acceptable use, reputation risk, communication risk, and organizational governance principles.

質問: **403**
インシデント対応チームの有効性が最も高まるのは、以下の場合です。
A. 得られた教訓に基づいて、インシデント対応プロセスが更新されます。
B. セキュリティ情報およびイベント監視(SIEM)システムを使用してインシデントを特定します。
C. インシデント対応チームは定期的に会合を開き、ログファイルをレビューします。
D. インシデント対応チームのメンバーは、訓練を受けた警備員です。
正解: (正解を表示します)

質問: **404**
インシデント対応チームは、事業影響度分析(BIA)の結果をどのように最大限に活用できるでしょうか？
A. インシデント発生時の復旧優先順位の設定
B. 総所有コスト(TCO)の算出
C. 事業回復に不可欠なベンダーの評価
D. インシデント復旧フェーズ後の残存リスクの計算
正解: (正解を表示します)

The incident response team can best leverage the results of a business impact analysis (BIA) by assigning restoration priority during incidents. A BIA is a process that identifies and evaluates the criticality and dependency of the organization's business functions, processes, and resources, and the potential impacts and consequences of their disruption or loss. The BIA results provide the basis for determining the recovery objectives, strategies, and plans for the organization's business continuity and disaster recovery. By using the BIA results, the incident response team can prioritize the restoration of the most critical and time-sensitive business functions, processes, and resources, and allocate the appropriate resources, personnel, and time to minimize the impact and duration of the incident.
Determining total cost of ownership (TCO) (B) is not a relevant way to leverage the results of a BIA, as it is not directly related to incident response. TCO is a financial metric that estimates the total direct and indirect costs of owning and operating an asset or a system over its lifecycle. TCO may be useful for evaluating the cost-effectiveness and return on investment of different security solutions or alternatives, but it does not help the incident response team to respond to or recover from an incident.
Evaluating vendors critical to business recovery © is also not a relevant way to leverage the results of a BIA, as it is not a primary responsibility of the incident response team. Evaluating vendors critical to business recovery is a part of the vendor management process, which involves selecting, contracting, monitoring, and reviewing the vendors that provide essential products or services to support the organization's business continuity and disaster recovery. Evaluating vendors critical to business recovery may be done before or after an incident, but not during an incident, as it does not contribute to the incident response or restoration activities.
Calculating residual risk after the incident recovery phase (D) is also not a relevant way to leverage the results of a BIA, as it is not a timely or effective use of the BIA results. Residual risk is the risk that remains after the implementation of risk treatment or mitigation measures. Calculating residual risk after the incident recovery phase may be done as a part of the incident review or improvement process, but not during the incident response or restoration phase, as it does not help the incident response team to resolve or contain the incident.
References = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Plan, Subsection: Business Impact Analysis, page 182-1831

質問**: 405**
ビジネスの観点から見ると、インシデント対応計画の最大の利点は次のとおりである。
A. 事前定義された応答手順を提供することで効率性を向上させます
B. 破壊的な事象に対するセキュリティ対応能力を向上させる
C. 破壊的な出来事の悪影響を制限する
D. 規制要件への準拠を保証します

正解: **(**正解を表示します**)**
The greatest business benefit of an incident response plan is minimizing the negative impact of disruptive incidents on operations and reputation.
"The primary business objective of an incident response plan is to minimize the impact of incidents on business operations and assets."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Incident Response Plan Objectives* ISACA practice questions reinforce that limiting impact is the key outcome from a business perspective.

質問: **406**
医療機関がAI開発の要件収集段階で取り組むべき最も重要な事項は次のうちどれですか？
A. アルゴリズム選択の課題
B. データプライバシーに関する懸念
C. 計算リソースが不足している
D. データラベリングの非効率性
正解: **B (**コメントを発表する**)**
The most important consideration during the requirements gathering phase of AI development in a healthcare organization is data privacy concerns (B). From a CISM governance and risk management perspective, healthcare organizations handle highly sensitive personal and regulated data, such as protected health information (PHI), which is subject to strict privacy, confidentiality, and regulatory requirements. During requirements gathering, it is critical to ensure that legal, regulatory, and ethical obligations related to data use, retention, consent, access controls, and cross-border processing are fully understood and incorporated into system requirements.
Algorithm selection (A), computational resources (C), and data labeling efficiencies (D) are important technical and operational considerations, but they are secondary and should be addressed only after privacy requirements are clearly defined. CISM emphasizes that security and privacy must be built in by design, not retrofitted later in development. Failure to address privacy requirements early can result in regulatory noncompliance, reputational damage, and unacceptable risk exposure.
In healthcare, governance-driven requirements-especially privacy, data minimization, and lawful processing-must guide AI system design to ensure alignment with organizational risk appetite and compliance obligations.
References:
ISACA CISM Review Manual, Information Security Governance - privacy, regulatory compliance, and emerging technology risk ISACA CISM Exam Content Outline, Domain 2: Information Security Governance

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu ↾**193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **407**
あるソフトウェアベンダーが、組織の重要な業務システムを危険にさらすゼロデイ脆弱性を発表しました。ベンダーは緊急パッチをリリースしました。情報セキュリティマネージャーが最も懸念すべき事項は次のうちどれでしょうか？
A. インシデント対応計画の妥当性
B. 制御を実施するためのリソースの可用性
C. パッチ適用手順の文書化
D. 展開前にパッチをテストできる機能
正解: **(**正解を表示します**)**

質問: **408**
新しい規制に対応するために情報セキュリティポリシーを更新する場合、情報セキュリティマネージャーはまず最初に次のことを行う必要があります。
A. 主要リスク指標(KRI)のレビュー
B. ギャップ分析を実施する
C. プロセスオーナーに相談する
D. 主要業績評価指標(KPI)を更新する
正解: **(**正解を表示します**)**
A gap analysis identifies the differences between current practices and the new regulatory requirements, ensuring targeted and effective policy updates.
"Performing a gap analysis is critical to identify the areas where the current policy falls short of new regulatory requirements."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Compliance* ISACA practice questions confirm that a gap analysis is the foundational step before engaging stakeholders or updating policies.

質問: **409**
シートホスティング組織のデータセンターには、サーバー、アプリケーション、
組織の物理アクセス制御ポリシーを策定するための最善のアプローチは？
A. 顧客のセキュリティポリシーを確認してください。
B. セキュリティリスクと軽減策を特定するためにリスク評価を実施する。
C. 各システムおよびアプリケーションに対するアクセス制御要件を策定する。

D. シングルサインオン(SSO)またはフェデレーションアクセスを設計します。
正解: **B (**コメントを発表する**)**
= The best approach for developing a physical access control policy for the organization is to conduct a risk assessment to determine the security risks and mitigating controls that are relevant and appropriate for the organization's data center. A risk assessment is a process of identifying, analyzing, and evaluating the information security risks that could affect the availability, integrity, or confidentiality of the servers, applications, and data that are hosted in the data center. A risk assessment can help to determine the likelihood and impact of the unauthorized or inappropriate physical access to the data center, such as theft, damage, sabotage, or espionage, and the potential consequences for the organization and its customers, such as service disruption, data loss, data breach, or legal liability. A risk assessment can also help to identify and prioritize the appropriate risk treatment options, such as implementing technical, administrative, or physical controls to prevent, detect, or respond to the physical access incidents, such as locks, alarms, cameras, guards, badges, or logs. A risk assessment can also help to communicate and report the risk level and status to the senior management and the relevant stakeholders, and to provide feedback and recommendations for improvement and optimization of the physical access control policy and the risk management process.
Reviewing customers' security policies, developing access control requirements for each system and application, and designing single sign-on (SSO) or federated access are all possible steps that the organization can take after conducting the risk assessment, but they are not the best ones. Reviewing customers' security policies is a process of understanding and complying with the customers' expectations and requirements for the security of their servers, applications, and data that are hosted in the data center, and ensuring that the organization's physical access control policy is consistent and compatible with them. Developing access control requirements for each system and application is a process of defining and implementing the specific rules and criteria for granting or denying the physical access to the servers and applications that are hosted in the data center, based on the roles, responsibilities, and privileges of the users, and the sensitivity and criticality of the systems and applications. Designing single sign-on (SSO) or federated access is a process of enabling and facilitating the authentication and authorization of the users who need to access the servers and applications that are hosted in the data center, by using a single or shared identity and credential across multiple systems and domains.
References = CISM Review Manual 15th Edition, pages 51-531; CISM Practice Quiz, question 1542

質問: **410**
情報セキュリティ プログラムと組織戦略の整合性を確保するために最も重要なのは次のうちどれですか。
A. ビジネス固有のリスク要因の特定
B. 業界で認められたフレームワークの採用

C. 上級管理職からの承認
D. 業界の同業他社とのベンチマーク
正解: **C** (コメントを発表する)

質問: **411**
セキュリティ対策の実施優先順位を決定する際に、情報セキュリティ管理者が最も重視すべき事項は次のうちどれでしょうか？
A. 業界ベンチマークとの整合性
B. 事業影響分析(BIA)の結果
C. 事件発生による評判低下の可能性
D. セキュリティ予算の確保
正解: (正解を表示します)
The priority for implementing security controls should be based on the results of BIAs, which identify the criticality and recovery requirements of business processes and the supporting information assets. BIAs help to align security controls with business needs and objectives, and to optimize the allocation of security resources. Alignment with industry benchmarks, possibility of reputational loss due to incidents, and availability of security budget are important factors, but they are not the most important consideration for determining the priority for implementing security controls. References = CISM Review Manual, 16th Edition, page 971; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 2672

質問: **412**
予告なしに実施される災害復旧訓練の主な目的は何ですか？
A. サービスレベル契約を評価する
B. 上級管理職に指標を提供する
C. 回復時間の目標を推定する
D. 職員が状況にどのように反応するかを評価する
正解: **D** (コメントを発表する)
The correct answer is D because an unannounced disaster recovery exercise is primarily intended to evaluate how personnel respond under realistic and unexpected conditions. Unlike scheduled exercises, unannounced tests help determine whether staff understand their roles, follow procedures, communicate effectively, and make appropriate decisions when there is no advance preparation. This type of exercise can reveal weaknesses in readiness, escalation, coordination, and practical response behavior. Assessing service level agreements may be a secondary benefit, but it is not the main purpose of an unannounced exercise. Providing metrics to senior management is useful for reporting, but metrics are an output of the exercise, not the primary objective.
Estimating the recovery time objective is incorrect because the RTO should already be established through business impact analysis and business requirements; testing helps validate whether the RTO can be met. In CISM practice, disaster recovery and incident

exercises are used to validate preparedness, response capability, and organizational resilience.
Reference: CISM Information Security Incident Management; disaster recovery testing, response preparedness, business continuity, and exercise management principles.

質問: **413**
インシデントエスカレーションプロセスを策定する際、最適なアプローチは、インシデントを以下の基準に基づいて分類することです。
A. 回復までの推定時間。
B. 影響を受ける情報資産。
C. リカバリポイント目標(RPO)。
D. それらの根本原因。
正解: **B (**コメントを発表する**)**
The best approach to developing an incident escalation process is to classify incidents based on the information assets affected, because this will help to determine the impact and severity of the incidents, as well as the appropriate response and recovery actions. The information assets affected by an incident can indicate the potential loss of confidentiality, integrity, or availability of the information, as well as the legal, regulatory, contractual, or reputational implications. By classifying incidents based on the information assets affected, the organization can prioritize the incidents and escalate them to the relevant stakeholders and authorities.
References = CISM Review Manual, 16th Edition, page 2901; A Practical Approach to Incident Management Escalation2

質問: **414**
経営陣は情報セキュリティマネージャーに対し、シャドウITが組織にとってリスクとなる可能性があるとの懸念を表明しました。情報セキュリティマネージャーが最初にとるべきステップは何でしょうか？
A. シャドウITの使用状況を把握する
B. シャドウITに対処するため、セキュリティポリシーを更新する。
C. エンドユーザーによるシャドウITの使用をブロックする
D. シャドウITプロジェクトの価値を判断する
正解: **(**正解を表示します**)**
The first step is to determine the extent of shadow IT usage (A). CISM emphasizes understanding the current state before implementing controls or policy changes. Without knowing where and how shadow IT exists, actions such as blocking usage (C) or updating policy (B) may disrupt business operations unnecessarily.
Evaluating value (D) is secondary. Identifying scope enables informed risk assessment and proportionate response.

References: ISACA CISM Review Manual (Governance-risk identification and assessment); CISM Exam Content Outline (Domain 2).

質問: **415**
買収のデューデリジェンス段階において、情報セキュリティマネージャーにとって最も重要な行動は以下のとおりです。
A. リスク評価を実施する
B. ギャップ分析を実施する
C. 情報セキュリティポリシーの見直し
D. セキュリティ意識の現状を確認する
正解: **A (**コメントを発表する**)**
During due diligence, performing a risk assessment is critical to understanding the potential impact of integrating the new organization into the acquiring company. This includes evaluating inherited risks, compliance gaps, and technical vulnerabilities.
"As part of due diligence during mergers and acquisitions, it is crucial to assess risks associated with the target organization to ensure proper integration and continuity."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Due Diligence
ISACA's CISM practice database reinforces that identifying and quantifying risks early helps ensure appropriate controls are in place before the integration, making risk assessment the most critical activity.

質問: **416**
ある組織がIT業務を外部委託することを決定しました。情報セキュリティマネージャーは、次のうちどれを最優先事項とすべきでしょうか？
A. セキュリティ要件はベンダー契約に含まれています
B. 外部セキュリティ監査の結果を確認します。
C. サービスレベル契約(SLA)は運用基準を満たしています。
D. 事業継続のための緊急時対応計画が提供されます
正解: **(**正解を表示します**)**
Security requirements are included in the vendor contract is the primary focus of the information security manager when outsourcing IT operations because it ensures that the vendor is legally bound to comply with the client's security policies and standards, as well as any external regulations or laws. This also helps to define the roles and responsibilities of both parties, the security metrics and controls to be used, and the penalties for non-compliance or breach. Therefore, security requirements are included in the vendor contract is the correct answer.
References:
https://www.techtarget.com/searchsecurity/tip/15-benefits-of-outsourcing-your-cybersecurity-operations
https://www.sciencedirect.com/science/article/pii/S0378720616302166

質問: **417**
サイバーセキュリティインシデントの結果として失われたデータの復旧を最も容易にするのは、次のうちどれですか？
A. 取り外し可能なストレージメディア
B. 災害復旧計画(DRP)
C. オフサイトデータバックアップ
D. 暗号化データドライブ
正解: **(正解を表示します)**
The best option to facilitate recovery of data lost as a result of a cybersecurity incident is offsite data backups.
This is because offsite data backups provide a secure and reliable way to restore data that may have been corrupted, deleted, or encrypted by malicious actors. Offsite data backups also reduce the risk of data loss due to physical damage, theft, or natural disasters that may affect the primary data storage location. Offsite data backups should be part of a comprehensive disaster recovery plan (DRP) that defines the roles, responsibilities, procedures, and resources for restoring normal operations after a cyber incident.

質問: **418**
事件の分類は、以下のうちどれを評価する上で最も重要ですか？
A. 適切なコミュニケーションチャネル
B. 必要な資源の配分
C. リスクの深刻度とインシデントの優先度
D. 対応および封じ込めに関する要件
正解: **(正解を表示します)**
The categorization of incidents is most important for evaluating the risk severity and incident priority, as these factors determine the impact and urgency of the incident, and the appropriate level of response and escalation.
The categorization of incidents helps to classify the incidents based on their type, source, cause, scope, and affected assets or services. By categorizing incidents, the information security manager can assess the potential or actual harm to the organization, its stakeholders, and its objectives, and assign a priority level that reflects the need for immediate action and resolution. The risk severity and incident priority also influence the allocation of resources, the response and containment requirements, and the communication channels, but they are not the primary purpose of categorization.
References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.4.1, page 2371; CISM Online Review Course, Module 4, Lesson 4, Topic 12; CIRT Case Classification (Draft) - FIRST3

質問: **419**
インシデント管理への備えを確実にするために、以下のうちどれが最も重要ですか？

A. この計画は業界標準に準拠しています。
B. この計画は定期的にテストされています。
C. この計画は毎年更新されます。
D. この計画は簡潔で、チェックリストが含まれています。
正解: **(**正解を表示します**)**
Regular testing ensures that the incident management plan is practical and effective in real-world scenarios.
"Regular testing of the incident response plan is essential to verify that it can be executed effectively and that staff understand their roles."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Testing and Evaluation*

質問: **420**
効果的な災害復旧計画プロセスを示す最良の指標は、次のうちどれですか？
A. 災害復旧プロセス全体を通して、保管管理の連鎖が維持されます。
B. 災害宣言が出された場合は、ホットスポットが必要です。
C. 事後検証は各事案の後に実施されます。
D. リカバリ時間目標(RTO)はリカバリポイント目標(RPO)よりも短い。
正解: **C (**コメントを発表する**)**

質問: **421**
重要な業務システムで潜在的な業務侵害が発見された場合、情報セキュリティマネージャーが最初にとるべき行動は次のうちどれでしょうか？
A. 直ちに緩和策を実施する。
B. インシデント対応計画を発動する。
C. 上級管理職に情報漏洩を報告する。
D. 違反を検証する。
正解: **D (**コメントを発表する**)**
The first step when a potential breach is discovered is to validate the breach. According to the CISM Review Manual, Domain 4, the information security manager must confirm the event to avoid unnecessary escalation or resource allocation. This validation ensures that the incident is real and justifies further response actions.
Invoking the incident response plan or informing management comes after the breach is validated.
Reference:ISACA CISM Review Manual, 16th Edition, Page 280, " Incident Detection and Validation " .

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu ↾**193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **422**
ある組織が新しい会社を買収する過程にある場合、統合前に新たに取得したデータ資産を保護する方法を決定するための最適なアプローチは次のうちどれでしょうか？
A. 契約書にセキュリティ要件を含める
B. セキュリティ対策を評価する。
C. リスク評価を実施する
D. データアーキテクチャをレビューする。
正解: **C** (コメントを発表する)
Performing a risk assessment is the best approach to determine how to protect newly acquired data assets prior to integration, as it will help to identify the threats, vulnerabilities, impacts, and likelihoods of the data assets, and to prioritize the appropriate risk treatment options. Including security requirements in the contract is a good practice, but it may not be sufficient to address the specific risks of the data assets. Assessing security controls and reviewing data architecture are also important steps, but they should be done after performing a risk assessment, as they will depend on the risk level and the risk app The best approach to determine how to protect newly acquired data assets prior to integration is to perform a risk assessment. A risk assessment will identify the various threats and vulnerabilities associated with the data assets and help the organization develop an appropriate security strategy. This risk assessment should include an assessment of the security controls in place to protect the data, a review of the data architecture, and a review of any contractual requirements related to security.

質問: **423**
エンドユーザーを事業継続計画に関与させる主な利点は、エンドユーザーが以下の点を享受できることです。
A. 具体的なビジネスニーズをより深く理解する。
B. 情報セキュリティ管理よりも客観的である。
C. 事業全体への影響を把握できます。
D. 技術的リスクとビジネス上のリスクのバランスを取ることができます。
正解: **A** (コメントを発表する)
= End users are the primary stakeholders of the business processes and functions that need to be protected and recovered in the event of a disruption. They have the most

knowledge and experience of the specific business needs, requirements, and dependencies that affect the continuity planning. Involving them in the planning process can help to ensure that the continuity plan is aligned with the business objectives and expectations, and that the critical activities and resources are prioritized and protected accordingly. End users can also provide valuable feedback and suggestions to improve the plan and its implementation. References = CISM Review Manual 15th Edition, page 2291; CISM Practice Quiz, question 1182

質問: **424**
ソーシャルメディアに関する明確なポリシーを持つ組織において、個人を特定できる情報の漏洩に伴う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. 従業員に対し、ソーシャルメディアの利用に関する定期的な研修を実施する。
B. 従業員のソーシャルメディア利用状況を監視し、機密情報が含まれていないか確認する
C. 社内ネットワーク上でのソーシャルメディアサイトのブロック
D. 組織内における個人識別情報へのアクセス制御
正解: **D** (コメントを発表する)
The correct answer is D because the most effective way to reduce disclosure risk is to limit access to personally identifiable information to only those individuals who have a legitimate business need. If employees do not have unnecessary access to PII, the likelihood of accidental or intentional disclosure through social media is reduced at the source. Training is important and supports awareness, but it does not prevent inappropriate access to sensitive information. Monitoring social media may detect some disclosures after they occur, but it is reactive and may also raise privacy and legal concerns. Blocking social media sites on the corporate network is limited because employees may still use personal devices or external networks.
CISM emphasizes risk-based controls, including access management, data protection, and least privilege.
Since the risk involves disclosure of PII, the best preventive control is restricting and controlling access to that information within the organization.
Reference: CISM Information Risk Management; privacy risk, data protection, access control, and least privilege principles.

質問: **425**
インシデント対応計画をタイムリーに実行するために最も適しているのは、次のうちどれですか？
A. 意思決定支援ツールの導入
B. トリガーイベントの定義
C. 明確に定義されたデータ分類プロセス
D. 集中サービスデスク
正解: **B** (コメントを発表する)

Definition of trigger events is the best way to enable the timely execution of an incident response plan because it helps to specify the conditions or criteria that initiate the incident response process. Trigger events are predefined scenarios or indicators that signal the occurrence or potential occurrence of a security incident, such as a ransomware attack, a data breach, a denial-of-service attack, or an unauthorized access attempt.
Definition of trigger events helps to ensure that the incident response team is alerted and activated as soon as possible, as well as to determine the appropriate level and scope of response based on the severity and impact of the incident. Therefore, definition of trigger events is the correct answer.
References:
https://www.atlassian.com/incident-management/kpis/common-metrics
https://www.varonis.com/blog/incident-response-plan/
https://holierthantao.com/2023/05/03/minimizing-disruptions-a-comprehensive-guide-to-incident-response-planning-and-execution/

質問: **426**
インシデントへの対応を優先するために、以下のうちどれを最初に行うべきですか？
A. 分析
B. エスカレーション
C. 封じ込め
D. トリアージ
正解: **(正解を表示します)**

質問: **427**
情報セキュリティプログラムの有効性を監視するための指標を選択する際、情報セキュリティマネージャーにとって最も重要なことは以下のとおりです。
A. プログラムのリスクと補償制御を特定する。
B. 組織の事業戦略を検討する。
C. 業界ベンチマークを活用する。
D. プログラムの戦略目標を検討する。
正解: **(正解を表示します)**

質問: **428**
セキュリティプログラムについて経営陣に報告する際に、最も効果的なアプローチは次のうちどれですか？
A. 包括的なセキュリティ統計情報を提供します
B. 業界セキュリティベンチマークに関するレポート
C. 事業部門別のセキュリティ監査結果の概要
D. セキュリティとビジネス戦略の連携
正解: **(正解を表示します)**

The correct answer is D because business leadership needs security reporting that explains how the security program supports business objectives, risk management, compliance, resilience, and value delivery. Linking security to business strategy enables leadership to understand whether security investments and initiatives are helping the organization achieve its goals. Comprehensive security statistics may be too technical or operational unless translated into business impact. Industry benchmarks can provide useful context, but they do not necessarily reflect the organization's specific strategy, risk appetite, or priorities. Security audit results by line of business may help with accountability, but they are still only one source of assurance. CISM governance principles emphasize that security must be aligned with enterprise objectives and communicated in business-relevant terms. Effective reporting should support informed decision-making, prioritization, funding, and oversight. Therefore, the most effective approach is to connect the security program directly to business strategy.
Reference: CISM Information Security Governance; strategic alignment, business-focused reporting, governance metrics, and value delivery principles.

質問**: 429**
情報セキュリティガバナンスフレームワークの承認責任者は誰ですか？
A. 取締役会
B. 最高情報セキュリティ責任者(CISO)
C. 企業リスク委員会
D. 最高情報責任者(CIO)
正解**: A (**コメントを発表する**)**
The board of directors is ultimately responsible for the governance of the organization, including the approval of the information security governance framework and the oversight of its implementation and performance. References = CISM Review Manual, 16th Edition, Domain 1: Information Security Governance, Chapter 2: Establish and Maintain an Information Security Governance Framework, Section:
Roles and Responsibilities of Senior Management and the Board of Directors1

質問**: 430**
新しいサイバーセキュリティ規制が導入された後、情報セキュリティ管理者が最初に行うべきことは次のうちどれですか？
A. 費用対効果分析を実施する。
B. 企業法務顧問に相談する
C. 情報セキュリティポリシーを更新する。
D. ギャップ分析を実施する。
正解**: (**正解を表示します**)**
When a new cybersecurity regulation has been introduced, an information security manager should first consult corporate legal counsel to understand the scope, applicability,

and implications of the regulation for the organization. Legal counsel can also advise on the compliance obligations and deadlines, as well as the potential penalties or sanctions for non-compliance. Based on this information, the information security manager can then perform a gap analysis to assess the current state of compliance and identify any areas that need improvement. The information security policy can then be updated accordingly to reflect the new regulatory requirements. References: https://www.isaca.org/credentialing/cism https://www.wiley.com/en-us/CISM+Certified+Information+Security+Manager+Study+Guide-p-9781119801948

質問: **431**
情報セキュリティマネージャーは、既存のサプライヤーが最近開発した生成AI技術を同じサービス範囲で導入する予定であることを知りました。3か月前にサプライヤーに対してリスク評価を実施しましたが、特筆すべき点はありませんでした。関連するリスクに対処するための最適な対策は、次のうちどれですか？
A. AI技術のリスク評価が完了するまでサプライヤーの使用を一時停止する
B. リスクの変化を上級管理職に報告する
C. 前回のリスク評価の結果を確認する
D. 更新段階で契約書に補償条項を追加する
正解: **A (**コメントを発表する**)**
Generative AI introduces new risks (e.g., data leakage, model poisoning). These risks were not part of the original assessment, so a fresh risk assessment must be conducted before continuing service.
"When a significant change in third-party operations occurs, it necessitates a reassessment of risk before continuing operations."
- CISM Review Manual 15th Edition, Chapter 3: Third-Party Risk Management* This ensures security, compliance, and operational continuity.

質問: **432**
クラウドベースのソリューションに移行する組織にとって、インシデント対応における最適なアプローチは次のうちどれですか？
A. クラウドプロバイダーのインシデント対応手順を採用してください。
B. インシデント対応の責任をクラウドプロバイダーに移管する。
C. 既存のインシデント対応手順を引き続き使用する。
D. クラウド環境を包含するようにインシデント対応手順を改訂する。
正解: **(**正解を表示します**)**
The best approach to incident response for an organization migrating to a cloud-based solution is to revise the existing incident response procedures to encompass the cloud environment. This is because the cloud environment introduces new challenges and risks that may not be adequately addressed by the current procedures. For example, the cloud provider may have different roles and responsibilities, service level agreements,

notification and escalation processes, data protection and privacy requirements, and legal and regulatory obligations than the organization. Therefore, the organization should review and update its incident response procedures to align with the cloud provider's policies and practices, as well as the organization's business objectives and risk appetite. The organization should also ensure that the incident response team members are trained and aware of the changes in the procedures and the cloud environment.
The other options are not the best approaches because they do not consider the specific characteristics and implications of the cloud environment. Adopting the cloud provider's incident response procedures may not be feasible or desirable, as the organization may have different needs and expectations than the cloud provider. Transferring responsibility for incident response to the cloud provider may not be possible or advisable, as the organization may still retain some accountability and liability for the security and availability of its data and services in the cloud. Continuing to use the existing incident response procedures may not be effective or efficient, as the procedures may not cover the scenarios and issues that may arise in the cloud environment. References = CISM Review Manual (Digital Version) 1, Chapter 4: Information Security Incident Management, pages 191-
192, 195-196, 199-200.
Cloud Incident Response Framework - A Quick Guide 2, pages 3-4, 6-7, 9-10.
CISM ITEM DEVELOPMENT GUIDE 3, page 18, Question 1.

質問: **433**
インシデント対応計画の準備フェーズで確立されるのは次のどれですか?
A. 保管手順
B. 復旧時間目標（RTO）
C. 平均応答時間（MTTR）
D. ステークホルダーコミュニケーション計画
正解: **(**正解を表示します**)**

質問: **434**
ある企業は、業務遂行のために旧バージョンのアプリケーションを必要としているが、そのアプリケーションにはパッチを適用できない。企業へのリスクを軽減するため、旧バージョンのアプリケーションの前にファイアウォールを導入した。これは、どのリスク対策オプションが適用されたかを示すものである。
A. 緩和する
B. 承認
C. 転送
D. 避ける
正解: **(**正解を表示します**)**

Mitigate is the risk treatment option that has been applied by implementing a firewall in front of the legacy application because it helps to reduce the impact or probability of a risk. Mitigate is a process of taking actions to lessen the negative effects of a risk, such as implementing security controls, policies, or procedures.
A firewall is a security device that monitors and filters the network traffic between the legacy application and the external network, blocking or allowing packets based on predefined rules. A firewall helps to mitigate the risk of unauthorized access, exploitation, or attack on the legacy application that cannot be patched.
Therefore, mitigate is the correct answer.
References:
https://simplicable.com/risk/risk-treatment
https://resources.infosecinstitute.com/topic/risk-treatment-options-planning-prevention/
https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-process/risk-treatment.

質問: **435**
ある事業部門が最近、組織の新しい強力なパスワードポリシーを業務アプリケーションに統合しました。このポリシーでは、ユーザーは30日ごとにパスワードをリセットする必要があります。現在、ヘルプデスクにはパスワードリセットのリクエストが殺到しています。この状況に対処するために、情報セキュリティマネージャーが取るべき最善の行動は次のうちどれでしょうか？
A. 引き続き政策を実施する。
B. エンドユーザー向けのトレーニングを提供します。
C. 上級管理職に報告する。
D. 事業影響分析(BIA)を実施する。
正解: **(正解を表示します)**

質問: **436**
新しく任命された情報セキュリティ マネージャーに、組織の既存のセキュリティ体制を最もよく把握させるタスクは次のどれですか。
A. ポリシーと手順の見直し
B. リスク評価の実行
C. 経営者と従業員へのインタビュー
D. ビジネス影響分析 (BIA) の実行
正解: **B (コメントを発表する)**
Performing a risk assessment gives a holistic and objective understanding of the threats, vulnerabilities, and controls across the organization. It reveals actual risk exposures and the effectiveness of current controls, which directly reflect the organization's security posture.

"Risk assessments identify and evaluate risk and provide the basis for determining how those risks should be managed and mitigated."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Assessment According to ISACA's CISM Practice Question Database, performing a risk assessment is prioritized over reviewing documents or conducting interviews because it offers direct insight into current exposures and control effectiveness.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu **1193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **437**
サイバーレジリエンス戦略の主要目的は次のうちどれですか？
A. 従業員の意識
B. 事業継続
C. 経営陣のサポート
D. 規制遵守
正解: **B** (コメントを発表する)
The primary objective of a cyber resilience strategy is business continuity (B). In CISM, cyber resilience is defined as the organization's ability to prepare for, respond to, recover from, and adapt to adverse cyber events while continuing to deliver critical business services. The focus is not on preventing all incidents- which is unrealistic-but on ensuring that essential operations can continue or be restored within acceptable timeframes despite cyber disruptions.
Employee awareness (A) and executive support (C) are important enablers of resilience, but they are means, not the ultimate objective. Regulatory compliance (D) is a governance requirement, but compliance alone does not guarantee operational resilience. CISM emphasizes that resilience strategies are driven by business impact analysis (BIA) results, recovery objectives, and tolerance for disruption, all of which directly support continuity of critical services.
A cyber resilience strategy integrates incident response, disaster recovery, backup, redundancy, and crisis management to minimize operational impact. Therefore, ensuring business continuity and operational resilience is the core objective against which cyber resilience effectiveness is measured.
References:

ISACA CISM Review Manual, Information Security Program Development and Management - cyber resilience and business continuity ISACA CISM Exam Content Outline, Domain 3: Information Security Program Development and Management

質問: **438**
組織の情報資産を一貫して保護するために必要なものは、次のうちどれですか？
A. 分類モデル
B. 管理評価
C. データ所有権
D. 規制要件
正解: **(**正解を表示します**)**
The answer to the question is A. Classification model. This is because a classification model is a system of assigning labels or categories to information assets based on their value, sensitivity, and criticality to the organization. A classification model helps to ensure consistent protection for the organization's information assets by:
Providing a common language and criteria for defining and communicating the security requirements and expectations for the information assets Enabling the identification and prioritization of the information assets that need the most protection and resources Facilitating the implementation and enforcement of the appropriate level of security controls and measures for the information assets, based on their classification Supporting the compliance with the legal, regulatory, and contractual obligations regarding the information assets, such as the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA) A classification model is a system of assigning labels or categories to information assets based on their value, sensitivity, and criticality to the organization. A classification model helps to ensure consistent protection for the organization's information assets by providing a common language and criteria for defining and communicating the security requirements and expectations for the information assets, enabling the identification and prioritization of the information assets that need the most protection and resources, facilitating the implementation and enforcement of the appropriate level of security controls and measures for the information assets, based on their classification, and supporting the compliance with the legal, regulatory, and contractual obligations regarding the information assets. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 2, Section 2.2.1, page 751; CISA Domain 5 - Protection of Information Assets2; CISM domain 3: Information security program development and management [2022 update]3; CISM Domain 2: Information Risk Management (IRM) [2022 update] 4

質問: **439**
ファイアウォールのアクティビティをログに記録する最も重要な理由はどれですか?
A. ファイアウォールの調整
B. メトリクスレポート

C. 事件調査
D. 侵入防止
正解: **(**正解を表示します**)**

質問: **440**
情報セキュリティマネージャーが複数年計画を策定する際に、最も重要な考慮事項は何でしょうか？
A. 潜在的な情報セキュリティリスクに対する緊急時対応計画が策定されていることを確認する
B. 他の事業部門の計画との整合性を確保する
C. 情報セキュリティプログラムの機能拡張を可能にする
D. 予算が年々増加する見込みであることを示す
正解: **B (**コメントを発表する**)**
= The most important consideration when developing a multi-year plan for information security is to ensure alignment with the plans of other business units. Alignment means that the information security plan supports and enables the achievement of the business objectives, strategies, and priorities of the organization and its various units. Alignment also means that the information security plan is consistent and compatible with the plans of other business units, and that it addresses the needs, expectations, and requirements of the relevant stakeholders1 .
By ensuring alignment with the plans of other business units, the information security manager can achieve the following benefits1 :
Increase the value and effectiveness of information security: By aligning the information security plan with the business goals and drivers, the information security manager can demonstrate the value and contribution of information security to the organization's performance, growth, and competitiveness. The information security manager can also ensure that the information security plan addresses the most critical and relevant risks and opportunities for the organization and its units, and that it provides adequate and appropriate protection and support for the organization's assets, processes, and activities.
Enhance the communication and collaboration with other business units: By aligning the information security plan with the plans of other business units, the information security manager can enhance the communication and collaboration with the other business unit leaders and managers, who are the key stakeholders and partners in information security. The information security manager can also solicit and incorporate their input, feedback, and suggestions into the information security plan, and provide them with timely and relevant information, guidance, and support. The information security manager can also foster a culture of trust, respect, and cooperation among the different business units, and promote a shared vision and commitment to information security.
Optimize the use and allocation of resources for information security: By aligning the information security plan with the plans of other business units, the information security manager can optimize the use and allocation of resources for information security, such as

budget, staff, time, or technology. The information security manager can also avoid duplication, conflict, or waste of resources among the different business units, and ensure that the information security plan is feasible, realistic, and sustainable. The information security manager can also leverage the resources and capabilities of other business units to enhance the information security plan, and provide them with the necessary resources and capabilities to implement and maintain the information security plan.
The other options are not the most important consideration when developing a multi-year plan for information security, as they are less strategic, comprehensive, or impactful than ensuring alignment with the plans of other business units. Ensuring contingency plans are in place for potential information security risks is an important component of the information security plan, but it is not the most important consideration, as it focuses on the reactive and preventive aspects of information security, rather than the proactive and enabling aspects. Allowing the information security program to expand its capabilities is an important objective of the information security plan, but it is not the most important consideration, as it depends on the availability and suitability of the resources, technologies, and opportunities for information security, and it may not align with the organization's needs, priorities, or constraints. Demonstrating projected budget increases year after year is an important outcome of the information security plan, but it is not the most important consideration, as it reflects the cost and demand of information security, rather than the value and benefit of information security, and it may not be justified or supported by the organization's financial situation or expectations1 . References = CISM Domain 1: Information Security Governance (ISG) [2022 update], CISM Domain 2: Information Risk Management (IRM) [2022 update] , Aligning Information Security with Business Strategy - ISACA, [Aligning Information Security with Business Objectives - ISACA]

質問**: 441**
情報セキュリティ管理者は、セキュリティリスクがタイムリーに対処されていないことを指摘した。
次のどれか
A. リスクの現状について定期的に最新情報を提供する。
B. 定期的にリスク分析を再実施する。
C. 各リスクにリスクオーナーを割り当てる
D. リスクを管理するための緩和策を作成する。
正解**: (**正解を表示します**)**
An email digital signature will verify to recipient the integrity of an email message because it ensures that the message has not been altered or tampered with during transit, and confirms that the message originated from the sender and not an imposter. An email digital signature will not protect the confidentiality of an email message because it does not encrypt or hide the message content from unauthorized parties. An email digital signature

will not automatically correct unauthorized modification of an email message because it does not change or restore the message content if it has been altered or tampered with. An email digital signature will not prevent unauthorized modification of an email message because it does not block or stop any attempts to alter or tamper with the message content. References: https://support.microsoft.com/en-us/office/secure- messages-by-using-a-digital-signature-549ca2f1-a68f-4366-85fa-b3f4b5856fc6 https://www.techtarget.com /searchsecurity/definition/digital-signature

質問: **442**
組織内でセキュリティインシデントが報告されました。情報セキュリティマネージャーはいつ情報所有者に連絡すべきでしょうか？
A. 事件が収束した後
B. 事件が収束した後
C. 事件が確認された後
D. 潜在的なインシデントが記録された後
正解: **(**正解を表示します**)**
The information owner is the person who has the authority and responsibility for the information asset and its protection. The information security manager should contact the information owner as soon as possible after the incident has been confirmed, to inform them of the incident, its impact, and the actions taken or planned to resolve it. The information owner may also need to be involved in the decision-making process regarding the incident response and recovery. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 191, section 4.3.4.1.

質問: **443**
インシデント対応プログラムを計画する際に、最も重要な目標は次のうちどれですか？
A. 事業への影響を最小限に抑える
B. ITシステムの回復力の確保
C. 災害からの復興
D. リソースの管理
正解: **A (**コメントを発表する**)**

質問: **444**
情報セキュリティガバナンスを企業ガバナンスに統合する上で、最も効果的な方法はどれでしょうか？
A. リスク評価に基づいた情報セキュリティポリシーの策定
B. 情報セキュリティ運営委員会の設置
C. 情報セキュリティガバナンスフレームワークの文書化
D. 情報セキュリティ意識向上プログラムの実施

正解: (正解を表示します)
Establishing an information security steering committee is the best way to facilitate the integration of information security governance into enterprise governance. The information security steering committee is a cross-functional group of senior managers who provide strategic direction, oversight, and support for the information security program. The committee ensures that the information security strategy is aligned with the enterprise strategy, objectives, and risk appetite. The committee also fosters collaboration and communication among various stakeholders and promotes a culture of security awareness and accountability. Developing an information security policy, documenting the information security governance framework, and implementing an information security awareness program are all important activities for implementing and maintaining information security governance, but they do not necessarily facilitate its integration into enterprise governance. These activities may be initiated or endorsed by the information security steering committee, but they are not sufficient to ensure that information security governance is embedded into the enterprise governance structure and processes. References = CISM Review Manual 2023, page 34 1; CISM Practice Quiz 2

質問: **445**
フェイルオーバーサイトの種類を決定する際に、最も重要な考慮事項は次のうちどれですか？
A. 相互協定
B. 災害復旧テスト結果
C. 復旧時間目標(RTO)
D. データ保持要件
正解: (正解を表示します)
The most important consideration when determining which type of failover site to employ is the recovery time objectives (RTOs). A failover site is a backup site that can be used to restore the functionality and operations of an organization's primary site in the event of a disaster or disruption. There are different types of failover sites, such as hot sites, warm sites, and cold sites, that vary in terms of availability, cost, and complexity. A recovery time objective (RTO) is a metric that defines the maximum acceptable amount of time that an organization can tolerate to restore a system or an application after a disaster or disruption. By determining the RTOs for each system or application, the organization can choose the most suitable type of failover site that can meet its recovery needs and expectations. For example, if the RTO for a critical system is very low, the organization may opt for a hot site that can provide immediate failover and minimal downtime. However, if the RTO for a non-critical system is high, the organization may choose a cold site that requires manual setup and activation, but has lower cost and maintenance. The other options are not the most important consideration when determining which type of failover site to employ, although they may be some factors or constraints that affect the decision. Reciprocal agreements are arrangements between two or more organizations that agree to

provide backup facilities or resources to each other in case of a disaster or disruption. Reciprocal agreements can help reduce the cost and complexity of setting up and maintaining a failover site, but they may not guarantee the availability or compatibility of the backup facilities or resources.
Disaster recovery test results are outcomes of testing and validating the functionality and performance of a failover site. Disaster recovery test results can help evaluate and improve the effectiveness and efficiency of a failover site, but they do not determine which type of failover site to employ. Data retention requirements are policies and regulations that define how long and in what format an organization must store its data. Data retention requirements can affect the design and configuration of a failover site, but they do not dictate which type of failover site to employ

質問: **446**
情報セキュリティ管理者がゼロデイ脆弱性を知るための最良の方法は次のうちどれですか？
A. シグネチャベースのマルウェア検出ツール
B. サイバーセキュリティ脅威インテリジェンスグループ
C. 侵入テストの結果
D. 最新の脆弱性スキャンツール
正解: **B** (コメントを発表する)
The correct answer is B because cybersecurity threat intelligence groups provide the most effective source of information about zero-day vulnerabilities. Zero-day vulnerabilities are newly discovered or previously unknown weaknesses that may not yet have patches, signatures, or standard scanner checks. Threat intelligence sources can provide early warnings, exploit details, indicators of compromise, affected technologies, attacker tactics, and recommended mitigations. Signature-based malware detection tools are limited because they depend on known malicious patterns and may not detect new threats. Penetration testing can identify weaknesses, but it is periodic and limited to the scope of the test. Vulnerability scanning tools are useful for identifying known vulnerabilities, but they may not detect zero-day vulnerabilities until detection logic is available. In CISM risk management, organizations should maintain awareness of emerging threats and adapt controls as the threat environment changes. Therefore, cybersecurity threat intelligence groups are the best source for learning of zero-day vulnerabilities.
Reference: CISM Information Risk Management; threat intelligence, emerging threats, zero-day vulnerabilities, and risk monitoring principles.

質問: **447**
ある組織は、市場での競争力を維持するために、モノのインターネット（IoT）ソリューションの導入を決定しました。情報セキュリティ対策として、まず最初に取り組むべきものは何でしょうか？
A. リスクプロファイルを再計算する

B. 補償制御を実装する
C. リスク許容度を再評価する
D. セキュリティアーキテクチャを更新する
正解: **A** (コメントを発表する)
When introducing new technologies, the first step is to recalculate the risk profile to identify any new or changed risks.
"The implementation of new technologies should trigger a review of the risk profile to identify and address new exposures."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Assessment and Analysis*

質問: **448**
情報セキュリティ管理者は、情報が不適切に分類されている、つまり情報漏洩のリスクがあると判断しました。情報セキュリティ管理者が取るべき最善の行動は次のうちどれですか？
A. この問題を内部監査部門に照会し、勧告を求めてください。
B. ビジネスリスクに対応するため、データを再分類し、セキュリティレベルを引き上げる。
C. 関係するシステム所有者にデータを再分類するよう指示する。
D. リスク評価を実施し、その結果をデータ所有者に報告する。
正解: (正解を表示します)
= Information classification is the process of assigning appropriate labels to information assets based on their sensitivity and value to the organization. Information classification should be aligned with the business objectives and risk appetite of the organization, and should be reviewed periodically to ensure its accuracy and relevance. The information security manager is responsible for establishing and maintaining the information classification policy and procedures, as well as providing guidance and oversight to the data owners and custodians. Data owners are the individuals who have the authority and accountability for the information assets within their business unit or function. Data owners are responsible for determining the appropriate classification level and security controls for their information assets, as well as ensuring compliance with the information classification policy and procedures. Data custodians are the individuals who have the operational responsibility for implementing and maintaining the security controls for the information assets assigned to them by the data owners.
If the information security manager believes that information has been classified inappropriately, increasing the risk of a breach, the best action is to complete a risk assessment and refer the results to the data owners. A risk assessment is a systematic process of identifying, analyzing, and evaluating the risks associated with the information assets, and recommending appropriate risk treatment options. By conducting a risk assessment, the information security manager can provide objective and evidence-based information to the data owners, highlighting the potential impact and likelihood of a breach,

as well as the cost and benefit of implementing additional security controls. This will enable the data owners to make informed decisions about the appropriate classification level and security controls for their information assets, and to justify and document any deviations from the information classification policy and procedures.
The other options are not the best actions for the information security manager. Refering the issue to internal audit for a recommendation is not the best action, because internal audit is an independent and objective assurance function that provides assurance on the effectiveness of governance, risk management, and control processes. Internal audit is not responsible for providing recommendations on information classification, which is a management responsibility. Re-classifying the data and increasing the security level to meet business risk is not the best action, because the information security manager does not have the authority or accountability for the information assets, and may not have the full understanding of the business context and objectives of the data owners. Instructing the relevant system owners to reclassify the data is not the best action, because system owners are not the same as data owners, and may not have the authority or accountability for the information assets either. System owners are the individuals who have the authority and accountability for the information systems that process, store, or transmit the information assets. System owners are responsible for ensuring that the information systems comply with the security requirements and controls defined by the data owners and the information security manager. References = CISM Review Manual, 16th Edition, ISACA, 2020, pp. 49-51, 63-64, 69-701; CISM Online Review Course, Domain 3: Information Security Program Development and Management, Module 2: Information Security Program Framework, ISACA2

質問**: 449**
情報セキュリティ管理者が、サイバー犯罪者が悪用している新たな手法を発見しました。管理者が特定したのは次のうちどれでしょうか？
A. リスク
B. 脅威
C. 事件
D. イベント
正解**: B (**コメントを発表する**)**
A new technique exploited by cybercriminals represents a threat (B). In CISM terminology, a threat is any circumstance or event with the potential to adversely impact an asset by exploiting a vulnerability. A risk (A) requires both a threat and a vulnerability with associated impact. An incident (C) is a realized event that compromises security, and an event (D) is an observable occurrence that may or may not lead to an incident.
Identifying new threat techniques is a key part of proactive risk management and threat intelligence activities emphasized in CISM.
References: ISACA CISM Review Manual (Risk management-threats, vulnerabilities, and risk definitions); CISM Exam Content Outline (Domain 1).

質問: **450**
ランサムウェア インシデントが正常に封じ込められた後、最初に実行する必要があるのは次のうちどれですか。
A. 影響を受けたシステムを復元します。
B. 関係する関係者に通知します。
C. フォレンジック分析を実施します。
D. 学んだ教訓を実行します。
正解: **B** (コメントを発表する)

質問: **451**
多国籍企業の情報セキュリティマネージャーは、各地域拠点の情報セキュリティポリシーを統合するよう依頼されました。以下のうち、最も懸念されるのはどれでしょうか？
A. 多様な脅威環境
B. 報告系統の相違
C. 法的要件の矛盾
D. 職場文化の違い
正解: (正解を表示します)
Conflicting legal requirements would be of greatest concern when consolidating the information security policies of regional locations, as they may pose significant challenges and risks for the organization's compliance, privacy, and data protection obligations. Different jurisdictions may have different laws and regulations regarding information security, 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. These laws and regulations may have different definitions, scopes, standards, and enforcement mechanisms for information security, which may create conflicts or inconsistencies when applying a unified policy across the organization.
Therefore, the information security manager should conduct a thorough analysis of the legal requirements of each location, and ensure that the consolidated policy meets the highest level of compliance and avoids any violations or penalties.
References = CISM Review Manual 2022, page 361; CISM Exam Content Outline, Domain 1, Task
1.22; CISM 2020: IT Security Policies; Information Security Due Diligence Questionnaire

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu 1193問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **452**
第三者との契約交渉において、組織のセキュリティ上の懸念に対処する最も効果的な方法は次のうちどれですか？
A. 調達プロセスにセキュリティが関与していることを確認してください。
B. サードパーティベンダーとセキュリティポリシーについて話し合う。
C. 組織の法務部門と第三者との契約内容を確認する。
D. 第三者ベンダーの情報セキュリティ監査を実施する。
正解: **(**正解を表示します**)**

質問: **453**
アプリケーションの耐障害性要件は、以下の方法で最適に決定できます。
A. リスク評価
B. 事業影響分析(BIA)
C. 費用便益分析
D. 脅威評価
正解: **B (**コメントを発表する**)**
A business impact analysis (BIA) (B) best determines application resilience requirements because it identifies criticality, maximum tolerable downtime, recovery time objectives (RTOs), and recovery point objectives (RPOs) based on business impact. Resilience is fundamentally about the organization's ability to continue or rapidly restore critical business functions. Risk assessments (A) and threat assessments (D) identify risks and threat sources but do not define acceptable downtime or recovery priorities. Cost-benefit analysis (C) helps evaluate investment decisions but is secondary to understanding business impact. CISM clearly positions the BIA as the foundation for continuity, resilience, and recovery planning decisions, ensuring security and availability controls align with business priorities.
References: ISACA CISM Review Manual (Risk management-BIA, resilience, continuity planning); CISM Exam Content Outline (Domain 1).

質問: **454**
以下の文書のうち、サービス復旧の初期優先順位を記載すべきものはどれですか？
A. ITリスク分析
B. 脅威評価
C. 事業影響分析(BIA)
D. ビジネスプロセスマップ
正解: **(**正解を表示します**)**

A business impact analysis (BIA) is the document that should contain the initial prioritization of recovery of services. A BIA is a process of identifying and analyzing the potential effects of disruptions to critical business functions and processes. A BIA typi-cally includes the following steps1:
*Identifying the critical business functions and processes that support the organization's mission and objectives.
*Estimating the maximum tolerable downtime (MTD) for each function or process, which is the longest time that the organization can afford to be without that function or process before suffering unacceptable consequences.
*Assessing the potential impacts of disruptions to each function or process, such as financial losses, reputational damage, legal liabilities, regulatory penalties, customer dissatisfaction, etc.
*Prioritizing the recovery of functions or processes based on their MTDs and impacts, and assigning recovery time objectives (RTOs) and recovery point objectives (RPOs) for each function or process. RTOs are the target times for restoring functions or processes after a disruption, while RPOs are the acceptable amounts of data loss in case of a disruption.
*Identifying the resources and dependencies required for each function or process, such as staff, equipment, software, data, suppliers, customers, etc.
A BIA provides the basis for developing a business continuity plan (BCP), which is a document that outlines the strategies and procedures for ensuring the continuity or recovery of critical business functions and processes in the event of a disruption2. The other options are not documents that should contain the initial prioritization of recov-ery of services. An IT risk analysis is a process of identifying and evaluating the threats and vulnerabilities that affect the IT systems and assets of an organization. It helps to determine the likelihood and impact of potential IT incidents, and to select and imple-ment appropriate controls to mitigate the risks3.
A threat assessment is a process of identifying and analyzing the sources and capabilities of adversaries that may pose a threat to an organization's security. It helps to determine the level of threat posed by different actors, and to develop countermeasures to prevent or respond to attacks. A business process map is a visual representation of the activities, inputs, outputs, roles, and resources involved in a business process. It helps to understand how a process works, how it can be improved, and how it relates to other processes.
References: 1:
Business impact analysis (BIA) - Wikipedia 2: Business continuity plan - Wikipedia 3: IT risk management - Wikipedia : Threat assessment - Wikipedia : Business process mapping - Wikipedia

質問**: 455**
組織のポリシーに沿って、最低限の情報セキュリティ要件を最も適切に伝えているのは次のうちどれですか？
A. 規格

B. 手順
C. 規制
D. ベースライン
正解: **A (**コメントを発表する**)**
Standards (A) best convey minimum information security requirements in alignment with organizational policies. In CISM governance, policies define management's intent and direction at a high level, while standards translate that intent into mandatory, enforceable minimum requirements that must be met across the organization. Standards ensure consistency and provide a clear benchmark against which compliance can be measured.
Procedures (B) describe how to perform specific tasks and are operational in nature; they are derived from standards and policies, not used to define minimum requirements.
Regulations (C) are external mandates imposed by laws or regulatory bodies and are not internally defined mechanisms for conveying organizational security requirements.
Baselines (D) typically represent a starting configuration or reference point for systems, often derived from standards, but they do not formally communicate organizational requirements on their own.
CISM clearly defines the hierarchy as policy # standards # procedures/guidelines, where standards play the critical role of establishing the minimum acceptable level of security needed to support governance objectives and ensure policy enforcement throughout the enterprise.
References:
ISACA CISM Review Manual, Information Security Governance - policy, standards, and procedures hierarchy ISACA CISM Exam Content Outline, Domain 2: Information Security Governance

質問: **456**
リスク評価の一環として、セキュリティ対策が不十分であることが判明しました。リスクオーナーを任命する際に、以下の属性のうち、最も重要な考慮事項はどれですか？
A. リスク所有者は、是正措置後にリスクを再評価することができます。
B. リスク所有者は、リスクに対して行動を起こす権限を有します。
C. リスク所有者は、リスク登録簿を適時に更新することができます。
D. リスク所有者は、失敗した関連する制御も所有しています。
正解: **(**正解を表示します**)**
The most important attribute when assigning a risk owner is that the risk owner has the authority to take action on the risk (B). In CISM, risk ownership is fundamentally about accountability and decision-making authority. The risk owner must be empowered to decide on risk treatment options-such as mitigation, transfer, acceptance, or avoidance-and to allocate resources or approve changes necessary to address the risk.

While reassessing risk after remediation (A) and updating the risk register (C) are important responsibilities, they are administrative and follow-on activities that do not, by themselves, ensure effective risk management.
Ownership of the failed control (D) is not required; in fact, CISM distinguishes between risk ownership (business accountability) and control ownership (operational responsibility). The risk owner is typically a business role accountable for the impact of the risk, not necessarily the individual responsible for implementing or operating the control.
CISM guidance consistently stresses that risk owners must have sufficient authority, accountability, and understanding of business impact to make informed decisions aligned with the organization's risk appetite.
Without authority, risk ownership becomes ineffective and purely symbolic.
References:
ISACA CISM Review Manual, Information Risk Management - risk ownership, accountability, and risk response ISACA CISM Exam Content Outline, Domain 1: Information Risk Management

質問**: 457**
ある部署から、セキュリティ対策がもはや有効ではないとの報告がありました。情報セキュリティマネージャーにとって、次のうちどれが最善の対応策でしょうか？
A. コントロールを交換します
B. 多層防御を確認する
C. 制御状態を評価する
D. 管理者に不具合を報告する
正解**: (**正解を表示します**)**
The best first step is to assess the control state to determine why it is ineffective and whether adjustments, replacements, or compensating controls are needed.
"Regularly assess the effectiveness of security controls to ensure they are providing the intended level of protection."
- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Control Monitoring and Assessment* ISACA practice questions stress that assessing the control state comes before taking further action.

質問**: 458**
情報セキュリティ管理者が組織に対する新たなリスクを特定するための最良の方法は、次のうちどれですか？
A. 上級関係者との定期的なリスク会議を開催する
B. 管理目標を満たしていることを確認するため、管理策の定期的なテストを実施する。
C. 責任ある所有者とともに、最新のリスク登録簿を維持する
D. 外部の脅威インテリジェンスソースを購読する

正解: (正解を表示します)
The correct answer is D because external threat intelligence sources provide timely information about emerging threats, vulnerabilities, attack methods, threat actors, malware campaigns, and industry-specific risk trends. Emerging risks often arise from changes outside the organization, such as new vulnerabilities, geopolitical activity, supply chain attacks, regulatory changes, or new adversary techniques. Regular risk meetings with senior stakeholders can help discuss business risk, but senior stakeholders may not have early visibility into technical or external threat developments. Periodic testing of controls helps validate existing control effectiveness, but it may not identify newly emerging risks until after exposure exists. Maintaining a risk register is essential for documenting and tracking known risks, but it does not by itself identify new external threats. CISM risk management emphasizes continuous risk monitoring and awareness of changes in the threat environment. Therefore, subscribing to external threat intelligence sources is the best way to identify emerging risks.
Reference: CISM Information Risk Management; emerging risk identification, threat intelligence, continuous risk monitoring, and external threat awareness.

質問: **459**
効果的な情報セキュリティガバナンスの重要な利点は次のとおりです。
A. 情報セキュリティプロジェクトの優先順位付け
B. 情報セキュリティコンプライアンス要件との整合性
C. 情報に基づいた情報セキュリティ意思決定
D. 情報セキュリティリスクの回避
正解: (正解を表示します)
The correct answer is C because effective information security governance enables management to make informed decisions about risk, resources, priorities, investments, and control requirements. Governance establishes accountability, reporting structures, policies, metrics, risk oversight, and alignment with enterprise objectives. Prioritization of security projects is a benefit, but it is only one outcome of informed governance.
Alignment with compliance requirements is also important, but governance is broader than compliance alone.
Information security risk avoidance is not generally the objective because not all risk can or should be avoided; risk may be mitigated, transferred, accepted, or avoided depending on business context. CISM emphasizes that governance ensures information security supports business objectives and provides value through risk-informed decision-making. Senior management needs accurate, relevant, and timely information to decide how much risk to accept and where to allocate resources. Therefore, the key benefit of effective information security governance is improved and informed decision-making.
Reference: CISM Information Security Governance; governance outcomes, decision-making, risk oversight, and business alignment principles.

質問: **460**
離職率の高い組織でインシデント通知およびエスカレーション プロセスを実装する上で、最も大きな障害となるのは次のどれでしょうか。
A. コミュニケーションプロセスの欠如
B. 知識のある人材の不足
C. 組織目標との整合性の欠如
D. プロセスのドキュメント不足
正解: **(正解を表示します)**

質問: **461**
以下のセキュリティ目標のうち、どれを満たすことが、情報の不正開示からの保護を最も確実に保証するでしょうか？
A. 誠実さ
B. 真正性
C. 機密保持
D. 否認禁止
正解: **(正解を表示します)**
Confidentiality is the security objective that best ensures that information is protected against unauthorized disclosure. Confidentiality means that only authorized parties can access or view sensitive or classified information. Integrity means that information is accurate and consistent and has not been tampered with or modified by unauthorized parties. Authenticity means that information is genuine and trustworthy and has not been forged or misrepresented by unauthorized parties. Nonrepudiation means that information can be verified and proven to be sent or received by a specific party without any possibility of denial. References:
https://www.csoonline.com/article/3513899/the-cia-triad-definition-components-and-examples.html

質問: **462**
高価値資産の保護、または信頼性に関する懸念のある環境への対応において、最も優れた多層防御の実装方法は次のうちどれですか？
A. 区画化
B. 重複冗長性
C. 継続的なモニタリング
D. 多要素認証
正解: **(正解を表示します)**
Compartmentalization is the best defense-in-depth implementation for protecting high value assets or for handling environments that have trust concerns because it is a strategy that divides the network or system into smaller segments or compartments, each with its own security policies, controls, and access rules.

Compartmentalization helps to isolate and protect the most sensitive or critical data and functions from unauthorized or malicious access, as well as to limit the damage or impact of a breach or compromise.
Compartmentalization also helps to enforce the principle of least privilege, which grants users or processes only the minimum access rights they need to perform their tasks.
Therefore, compartmentalization is the correct answer.
References:
https://www.csoonline.com/article/3667476/defense-in-depth-explained-layering-tools-and-processes-for-better-security.html
https://www.fortinet.com/resources/cyberglossary/defense-in-depth
https://sciencepublishinggroup.com/journal/paperinfo?journalid=542 & doi=10.11648/j.ajai.20190302.11

質問: **463**
情報セキュリティ管理者がセキュリティ投資計画を見直す際に考慮すべき最も重要なことは次のうちどれですか?
A. この計画は、業界のベストプラクティスと業界標準を満たすことに重点を置いています。
B. 計画では実装に関する IT コストがまとめられています。
C. この計画は、ビジネス プロセスに対する潜在的な脅威をすべて解決します。
D. 計画は脅威と脆弱性のレビューに基づいています。
正解: **(**正解を表示します**)**

質問: **464**
侵入検知システム(IDS)が外部ネットワークベースの攻撃を報告した場合、ファイアウォールのログを確認する主な理由は次のうちどれですか？
A. インシデント対応戦略を策定する
B. ペイロード署名を検証する
C. 事件を検証するために
D. ネットワーク構成を確認する
正解: **(**正解を表示します**)**

質問: **465**
組織の人事部は、政府の規制を遵守するため、従業員の退職後3日以内にすべての企業ITシステムから従業員アカウントの権限を削除することを要求しています。しかし、システムごとにユーザーディレクトリが異なり、現在権限の削除には最大4週間かかります。規制遵守を最も容易にするのは何でしょうか？
A. 多要素認証(MFA)システム
B. IDおよびアクセス管理(IAM)システム
C. 特権アクセス管理(PAM)システム

D. ガバナンス、リスク、コンプライアンス(GRC)システム
正解: **(**正解を表示します**)**
= An identity and access management (IAM) system is a set of processes, policies, and technologies that enable an organization to manage the identities and access rights of its users across different systems and applications1. An IAM system can help an organization to comply with the government regulation by automating the provisioning and deprovisioning of user accounts, enforcing consistent access policies, and integrating different user directories2. An IAM system can also provide audit trails and reports to demonstrate compliance with the regulation3. A multi-factor authentication (MFA) system is a method of verifying the identity of a user by requiring two or more factors, such as something the user knows, has, or is4. An MFA system can enhance the security of user authentication, but it does not address the issue of removing user privileges from different systems within three days of termination. A privileged access management (PAM) system is a solution that manages and monitors the access of privileged users, such as administrators, to critical systems and resources. A PAM system can reduce the risk of unauthorized or malicious use of privileged accounts, but it does not solve the problem of managing the access of regular users across different systems. A governance, risk, and compliance (GRC) system is a software platform that integrates the functions of governance, risk management, and compliance management. A GRC system can help an organization to align its objectives, policies, and processes with the relevant regulations, standards, and best practices, but it does not directly enable the removal of user privileges from different systems within three days of termination. References = 1: CISM Review Manual (Digital Version), page 24 2: 1 3: 2 4: CISM Review Manual (Digital Version), page 25 : CISM Review Manual (Digital Version), page 26 : CISM Review Manual (Digital Version), page 27

質問: **466**
次の望ましい結果のうち、新しいセキュリティ対策への投資を決定する上で最も適切なものはどれですか？
A. セキュリティ監視とレポート機能の強化
B. 制御の複雑さの軽減
C. 強化された脅威検出機能
D. 組織リスクの低減
正解: **D (**コメントを発表する**)**
The reduction of organizational risk is the desired outcome that best supports a decision to invest in a new security initiative. The organizational risk is the level of exposure or uncertainty that the organization faces in achieving its objectives. The organizational risk is influenced by various factors, such as the threat landscape, the vulnerability of the assets, the impact of the incidents, and the effectiveness of the controls. The information security manager should evaluate the organizational risk and propose security initiatives that can reduce the risk to an acceptable level. The security initiatives should be aligned with the

business goals, the risk appetite, and the available resources of the organization. The security initiatives should also provide a positive return on investment (ROI) or value for money (VFM) for the organization. The reduction of organizational risk is the ultimate goal and benefit of any security initiative, as it enhances the security posture, performance, and resilience of the organization. Enhanced security monitoring and reporting, reduced control complexity, and enhanced threat detection capability are all possible outcomes of security initiatives, but they are not the best ones to support a decision to invest in a new security initiative. These outcomes are more specific and technical, and they may not directly relate to the business objectives or the risk appetite of the organization. These outcomes are also intermediate or enabling, rather than final or ultimate, as they may not necessarily lead to the reduction of organizational risk. For example, enhanced security monitoring and reporting may improve the visibility and awareness of the security status, but it may not prevent or mitigate the incidents. Reduced control complexity may simplify the security management and maintenance, but it may not address the emerging or evolving threats. Enhanced threat detection capability may increase the speed and accuracy of identifying the attacks, but it may not reduce the impact or the likelihood of the attacks. Therefore, the reduction of organizational risk is the best outcome to support a decision to invest in a new security initiative, as it demonstrates the value and effectiveness of the security initiative for the organization. References = CISM Review Manual 2023, page 40 1; CISM Practice Quiz 2

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu **193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **467**
BYOD(Bring Your Own Device)プログラムを導入する前に、最も重要なことは以下のとおりです。
A. モバイルデバイス管理(MDM)ソフトウェアを選択します。
B. 応募を希望する従業員を対象にアンケート調査を実施する。
C. 許容使用ポリシーを策定する。
D. 現在利用中のアプリケーションをレビューする。
正解: **(**正解を表示します**)**
Before implementing a BYOD program, it is most important to develop an acceptable use policy that defines the roles and responsibilities of the organization and the employees, the

security requirements and controls for the devices, the acceptable and unacceptable behaviors and activities, and the consequences of non- compliance. This policy will help to establish a clear and consistent framework for managing the risks and benefits of BYOD.
References = CISM Review Manual, 16th Edition, page 197

質問: **468**
情報セキュリティポリシーの第一の目的は何であるべきか？
A. 業界のベストプラクティスとの整合性を確保するため
B. 経営陣の期待事項を概説する
C. 規制要件を遵守するため
D. セキュリティ手順の詳細
正解: **B (**コメントを発表する**)**
The primary objective of an information security policy is to outline management expectations (B). In CISM governance, policies serve as high-level statements that define direction, intent, and accountability for information security. While alignment with best practices (A) and regulatory compliance (C) are important considerations, they are secondary to clearly communicating what management expects from the organization. Detailing procedures (D) is not the role of policy; procedures translate policy into actionable steps. Clear policies establish authority and provide the foundation for standards, procedures, and enforcement.
References: ISACA CISM Review Manual (Governance-policy purpose and hierarchy); CISM Exam Content Outline (Domain 2).

質問: **469**
情報セキュリティプログラムが適切な範囲をカバーしていることを証明するのに、以下のどの方法が最も効果的ですか？
A. セキュリティリスク分析
B. ギャップ評価
C. 成熟度評価
D. 脆弱性スキャンレポート
正解: **(**正解を表示します**)**
A gap assessment is the best way to demonstrate that an information security program provides appropriate coverage, as it compares the current state of the information security program with the desired state based on the organization's objectives, policies, standards, and regulations. A gap assessment can identify the strengths and weaknesses of the information security program, as well as the areas that need improvement or alignment. A gap assessment can also provide recommendations and action plans to close the gaps and achieve the desired level of information security coverage.
The other options are not as good as a gap assessment, as they do not provide a comprehensive and holistic view of the information security coverage. Security risk analysis is a process to identify and evaluate the risks to the information assets and the

impact of potential threats and vulnerabilities. It can help to prioritize and mitigate the risks, but it does not measure the compliance or performance of the information security program.
Maturity assessment is a process to measure the level of maturity of the information security program based on a predefined model or framework. It can help to benchmark and improve the information security program, but it does not account for the specific needs and expectations of the organization. Vulnerability scan report is a document that shows the results of a scan on the network or system to identify the existing or potential vulnerabilities. It can help to validate and improve the technical security, but it does not assess the non- technical aspects of information security, such as governance, policies, or awareness. References = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 211-212, 215-216, 233-234, 237-238.
CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1015.
CISM domain 3: Information security program development and management [2022 update], Infosec Certifications, 2.

質問**: 470**
なりすましは、以下のような目的で悪用される可能性があるため、防止する必要があります。
A. 送信者のアドレスを偽装して安全なシステムに不正侵入する、
B. オプションが提示されたときにプログラムがどちらの方向に分岐するかを予測する
C. 情報を収集し、トラフィックを追跡し、ネットワークの脆弱性を特定する。
D. ネットワークを介して送信されるパスワードなどの情報を傍受する
正解**: A (**コメントを発表する**)**
Gaining illegal entry to a secure system by faking the sender's address is one of the reasons why spoofing should be prevented. Spoofing is a technique that involves impersonating someone or something else to deceive or manipulate the recipient or target. Spoofing can be applied to various communication channels, such as emails, websites, phone calls, IP addresses, or DNS servers. One of the common goals of spoofing is to gain unauthorized access to a secure system by faking the sender's address, such as an email address or an IP address. For example, an attacker may spoof an email address of a trusted person or organization and send a phishing email that contains a malicious link or attachment. If the recipient clicks on the link or opens the attachment, they may be redirected to a fake website that asks for their credentials or downloads malware onto their device. Alternatively, an attacker may spoof an IP address of a trusted source and send packets to a secure system that contains malicious code or commands. If the system accepts the packets as legitimate, it may execute the code or commands and compromise its security. Therefore, gaining illegal entry to a secure system by faking the sender's address is one of the reasons why spoofing should be prevented.
References:
https://www.kaspersky.com/resource-center/definitions/spoofing

https://www.cisa.gov/resources-tools/resources/business-case-security
https://www.avast.com/c-spoofing

質問: **471**
大規模な多国籍企業の情報セキュリティ管理者が、データ処理をクラウドサービスプロバイダーにアウトソーシングする際に、最も懸念すべき点は何でしょうか？
A. ベンダーサービスレベル契約(SLA)
B. ベンダーの独立したレビュー
C. 現地の法律および規制
D. データのバックアップと復元
正解: **(**正解を表示します**)**
he greatest concern for an information security manager of a large multinational organization when outsourcing data processing to a cloud service provider is the local laws and regulations that may apply to the data and the cloud service provider. Local laws and regulations may vary significantly across different jurisdictions and may impose different requirements or restrictions on the data protection, privacy, security, sovereignty, retention, disclosure, transfer, or access. These laws and regulations may also create potential conflicts or inconsistencies with the organization's own policies, standards, or contractual obligations.
Therefore, an information security manager should conduct a thorough legal and regulatory analysis before outsourcing data processing to a cloud service provider and ensure that the cloud service provider complies with all the applicable laws and regulations in the relevant jurisdictions.
References = CISM Manual1, Chapter 3: Information Security Program Development (ISPD), Section 3.1:
Outsourcing2
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles 2: 1
Outsourcing data processing to a cloud service provider may expose the organization to different legal and regulatory requirements depending on the location of the data and the vendor. This could affect the organization's compliance and liability in case of a breach or dispute. Therefore, the information security manager should be most concerned about the local laws and regulations that apply to the outsourcing arrangement.

質問: **472**
情報セキュリティ管理者が、外部委託先の第三者との契約期間を通じて定期的に実施すべき最も重要な活動は次のうちどれですか？
A. 参加型災害復旧テスト
B. 包括的なリスク評価
C. サービスレベル契約(SLA)の更新
D. 財務整合性レビュー
正解: **(**正解を表示します**)**

Performing comprehensive risk assessments (B) throughout the life of a third-party contract is the most critical activity because risk posture changes over time due to evolving threats, business changes, or control degradation. CISM emphasizes that third-party risk is not static and must be continuously assessed to ensure ongoing alignment with risk appetite. Disaster recovery testing (A) and SLA updates (C) are important but limited in scope. Financial reviews (D) focus on cost rather than security risk. Periodic risk assessments enable timely identification of new risks and ensure appropriate mitigation or escalation.
References: ISACA CISM Review Manual (Governance-third-party risk lifecycle management); CISM Exam Content Outline (Domain 2).

質問: **473**
情報セキュリティインシデントを分類することによる最大のメリットは次のうちどれですか？
A. レポート機能
B. 保管管理体制の改善
C. 包括的なドキュメント
D. 優先復旧
正解: **(**正解を表示します**)**
Incident classification helps determine severity, which allows security teams to prioritize recovery efforts.
This ensures critical business functions are restored first.
" Incident classification is essential for establishing severity levels and response priorities. " - CISM Review Manual 15th Edition, Chapter 4: Incident Response Lifecycle, Section: Incident Classification* Reporting and documentation are important, but prioritized recovery is the greatest business-impact-driven benefit.

質問: **474**
経営幹部に対し、情報セキュリティプログラムの現状について説明する際に、最も重要な考慮事項は次のうちどれですか？
A. 状況予測を含む
B. 対象読者に適した言葉遣いをする
C. 指標のトレンドチャートを含む
D. 評価システムを用いてプログラムの効果を実証する
正解: **D (**コメントを発表する**)**
= When briefing executives about the current state of the information security program, the most important consideration is to use appropriate language for the target audience. This means avoiding technical jargon, acronyms, and details that may confuse or bore the executives, and instead focusing on the business value, risks, and benefits of the information security program. The other options are not as important or relevant as using appropriate language, although they may also be useful to include in the briefing. For

example, a situational forecast may be helpful to show the future trends and challenges, but it is not as essential as communicating the current state clearly and concisely. Similarly, trend charts for metrics and a rating system to demonstrate program effectiveness may be useful to support the briefing, but they are not as critical as using language that the executives can understand and relate to. References = Information Security Guide for Government Executives, page 7: "Reminding employees of their responsibilities and demonstrating management's commitment to the security program are key to maintaining effective security within the constantly changing information security environment." Information security guide for government executives - NIST, page 3: "The executive should communicate the importance of information security to the organization and its staff, using language that is meaningful to the target audience." Information Security Committee Charter - SecurityStudio, page 1: "The committee also coordinates and communicates the direction, current state, and oversight of the information security program."

質問**: 475**
複数の重要システムがマルウェアに感染しました。この事態を根絶するための最善の戦略は次のうちどれですか？
A. マルウェアスキャンを実行する
B. システムを再イメージングする
C. 影響を受けるシステムへのアクセスをブロックする
D. 脆弱性評価を実施する
正解**: (**正解を表示します**)**
Reimaging the systems (B) is the most reliable method to eradicate malware because it ensures complete removal of malicious code, including hidden persistence mechanisms. Malware scanning (A) may miss advanced threats, while blocking access (C) is a containment action, not eradication. Vulnerability assessments (D) help identify weaknesses but do not remove existing malware. CISM incident management guidance prioritizes thorough eradication to prevent reinfection and restore system integrity. References: ISACA CISM Review Manual (Incident management-eradication strategies); CISM Exam Content Outline (Domain 4).

質問**: 476**
次のうち、インシデント対応チームの主要な機能はどれですか？
A. 事業影響分析を提供する
B. ゼロデイ脆弱性に対するリスク評価を提供する
C. 効果的なインシデント軽減策を提供する
D. 重大な事案に対する単一の連絡窓口を提供する
正解**: C (**コメントを発表する**)**
The correct answer is C because the primary purpose of an incident response team is to respond to security incidents and reduce their impact through effective mitigation. Incident

response teams investigate incidents, classify severity, contain threats, coordinate response actions, support eradication, assist recovery, and help prevent recurrence through lessons learned. A business impact analysis is generally part of business continuity planning, not the primary responsibility of the incident response team. A risk assessment for zero-day vulnerabilities is part of risk management and vulnerability management, not the core incident response function. Acting as a single point of contact for critical incidents may be one responsibility of the team or incident coordinator, but it is not the primary function. CISM incident management emphasizes timely detection, response, containment, communication, recovery, and post-incident improvement. The team exists mainly to reduce business harm from incidents. Therefore, providing effective incident mitigation is the best answer.
Reference: CISM Information Security Incident Management; incident response team responsibilities, mitigation, containment, and impact reduction principles.

質問**: 477**
事業活動における残存リスクが許容リスクレベルを下回る場合、次のうちどれが最善の行動方針でしょうか？
A. 管理策の有効性を監視する
B. リスク評価フレームワークの更新
C. 固有のリスクレベルを確認する
D. リスクの発生確率と影響を検証する
正解**: A (**コメントを発表する**)**
If the residual risk of the business activity is lower than the acceptable risk level, it means that the existing controls are effectively mitigating the identified risks. In this case, the best course of action is to monitor the effectiveness of the controls and ensure they remain effective. The information security manager should review and test the controls periodically to ensure that they continue to provide adequate protection. It is also essential to update the risk assessment framework to reflect changes in the business environment or risk landscape.

質問**: 478**
セキュリティポリシーが事業運営全体に確実に適用されることを最もよく保証できるのは、次のうちどれですか？
A. 組織基準は意識向上トレーニングに含まれています。
B. 組織基準は技術的な管理によって強制されます。
C. 組織基準は正式に承認される必要がある。
D. 組織の基準は、業務手順書に文書化されています。
正解**: D (**コメントを発表する**)**
= The best assurance that security policies are applied across business operations is that organizational standards are documented in operational procedures. Operational

procedures are the specific steps and actions that need to be taken to implement and comply with the security policies and standards. They provide clear and consistent guidance for the staff members who are responsible for performing the security tasks and functions. They also help to ensure that the security policies and standards are aligned with the business objectives and processes, and that they are measurable and auditable. Documenting the organizational standards in operational procedures can help to improve the security awareness, accountability, and performance of the staff members, and to reduce the risks of errors, deviations, and violations. The other options are not the best assurance because they are either too general or too specific. Organizational standards are included in awareness training (A) is a good practice to educate the staff members about the security policies and standards, but it does not guarantee that they will follow them or understand how to apply them in their daily operations. Organizational standards are enforced by technical controls (B) is a way to automate and monitor the compliance with the security policies and standards, but it does not cover all the aspects of security that may require human intervention or judgment. Organizational standards are required to be formally accepted © is a way to obtain the commitment and support from the staff members for the security policies and standards, but it does not ensure that they will adhere to them or know how to execute them in their work activities. References = CISM Review Manual 2022, pages 24-25, 28-29; CISM Item Development Guide 2022, page 9; Policies, Procedures, Standards, Baselines, and Guidelines | CISSP Security-Management Practices | Pearson IT Certification

質問: **479**
サービス契約の以下の要素のうち、組織がクラウドサービスプロバイダーに関連する情報セキュリティリスクを監視するのに最も適しているのはどれですか？
A. 補償条項
B. 侵害検知および通知
C. コンプライアンス状況報告
D. サービス提供者の施設への物理的なアクセス
正解: **(**正解を表示します**)**
Compliance status reporting is the best element of a service contract that would enable an organization to monitor the information security risk associated with a cloud service provider, as it provides the organization with regular and timely information on the cloud service provider's compliance with the agreed-upon security requirements, standards, and regulations. Compliance status reporting also helps the organization to identify any gaps or issues that need to be addressed or resolved, and to verify the effectiveness of the cloud service provider's controls. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 184, section 4.3.3.2.

質問: **480**

アウトソーシングされたITサービスの情報セキュリティを確保するために、以下のうち最も重要なデューデリジェンス活動はどれですか？
A. サービスプロバイダーのセキュリティ意識レベルを評価する。
B. サービスプロバイダーからのサービスレベルレポートのサンプルを確認する。
C. サービスプロバイダーに情報セキュリティポリシーを遵守するよう要請する。
D. サービス提供者の最近の独立監査報告書を確認する。
正解: **(**正解を表示します**)**

質問: **481**
情報セキュリティプログラムの有効性を測定する指標を設定する際の主要な基準として、次のうちどれを用いるべきでしょうか？
A. 残存リスク
B. 規制要件
C. リスク許容度
D. 制御目標
正解: **(**正解を表示します**)**
The primary basis for establishing metrics that measure the effectiveness of an information security program should be the risk tolerance of the organization, which is the degree of risk that the organization is willing to accept or avoid in pursuit of its objectives. Metrics based on risk tolerance can help to evaluate whether the information security program is aligned with the business strategy, supports the risk management process, and delivers value to the organization. Residual risk, regulatory requirements, and control objectives are also important factors to consider when developing metrics, but they are not as fundamental as the risk tolerance.
References = CISM Review Manual, 16th Edition, page 69

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu 「**193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **482**
インシデント対応チームは、エンドユーザーのワークステーションと、感染の可能性のある外部サーバーとの間で不審な通信が発生していることを検知しました。次に取るべき行動は次のうちどれですか？

A. エンドユーザーのワークステーションのオペレーティングシステムを再インストールします。
B. イベントの分析と検証
C. IPアドレスブロックを要求する
D. エンドユーザーのワークステーションと外部サーバーを分離する
正解: **B** (コメントを発表する)
The correct answer is B because the next step after receiving an alert is to analyze and validate the event to determine whether it is a true incident, a false positive, or benign activity. Incident response should follow a structured process: detection, validation, classification, prioritization, containment, eradication, recovery, and lessons learned. Reinstalling the operating system is premature and may destroy evidence needed for analysis.
Requesting an IP address block may be appropriate later if the external server is confirmed to be malicious, but blocking without validation can disrupt legitimate business communication. Isolating the workstation may become necessary if compromise is confirmed or strongly suspected, but the question asks what should be done next after an alert. CISM incident management principles require events to be validated before full incident response actions are taken. Proper analysis ensures that response actions are proportionate, evidence is preserved, and business disruption is minimized. Therefore, analyzing and validating the event is the best next step.
Reference: CISM Information Security Incident Management; event validation, incident identification, analysis, classification, and response process principles.

質問: **483**
組織の情報セキュリティ戦略に最も大きな影響を与えるのは、次のうちどれですか？
A. 組織のリスク許容度
B. 組織構造
C. 業界セキュリティ基準
D. 情報セキュリティ意識
正解: **A** (コメントを発表する)
An organization ' s information security strategy should be aligned with its risk tolerance, which is the level of risk that an organization is willing to accept in pursuit of its objectives. The strategy should aim to balance the cost of security controls with the potential impact of security incidents on the organization ' s objectives.
Therefore, an organization ' s risk tolerance has the greatest influence on its information security strategy.
The organization's risk tolerance has the greatest influence on its information security strategy because it determines how much risk the organization is willing to accept and how much resources it will allocate to mitigate or transfer risk. The organizational structure, industry security standards, and information security awareness are important factors that

affect the implementation and effectiveness of an information security strategy but not as much as the organization's risk tolerance.
An information security strategy is a high-level plan that defines how an organization will achieve its information security objectives and address its information security risks. An information security strategy should align with the organization's business strategy and reflect its mission, vision, values, and culture. An information security strategy should also consider the external and internal factors that influence the organization's information security environment such as laws, regulations, competitors, customers, suppliers, partners, stakeholders, employees etc.

質問: **484**
情報セキュリティプログラムの有効性に関する主要関係者への報告書に含めるべき最も重要な項目は次のうちどれですか？
A. セキュリティ指標
B. セキュリティ基準
C. セキュリティインシデントの詳細
D. セキュリティリスクへの曝露
正解: **(**正解を表示します**)**
Security metrics are the most important to include in a report to key stakeholders regarding the effectiveness of an information security program because they provide objective and measurable evidence of security performance and progress. Security metrics can include measures such as the number and severity of security incidents, the level of compliance with security policies and standards, the effectiveness of security controls, and the return on investment (ROI) of security initiatives. The other choices may also be included in a security report, but security metrics are the most important.
An information security program is a set of policies, procedures, standards, guidelines, and tools that aim to protect an organization's information assets from threats and ensure compliance with laws and regulations.
The effectiveness of an information security program depends on various factors, such as the organization's risk appetite, business objectives, resources, culture, and external environment. Regular reporting to key stakeholders, such as senior management, the board of directors, and business partners, is critical to maintaining their support and buy-in for the program. The report should provide clear and concise information on the program's status, achievements, challenges, and future plans, and it should be tailored to the audience's needs and expectations.

質問: **485**
セキュリティ基準への不遵守に対処するための最適なアプローチは次のうちどれですか？
A. 新たなセキュリティ基準を策定する。
B. セキュリティ例外処理プロセスを維持する。
C. セキュリティ要件が満たされるまで、影響を受ける活動を中止してください。

D. 影響を受ける資産に対して、追加のログ記録と監視を適用します。
正解: **(**正解を表示します**)**
A security exceptions process is the most effective governance mechanism for handling noncompliance with standards because it creates a controlled, risk-based method to manage deviations while maintaining accountability. In CISM terms, standards define minimum acceptable baselines, but real-world constraints (legacy systems, third-party limitations, business urgency) sometimes require temporary or conditional deviations. A formal exception process ensures: the business documents the justification, identifies the risk owner, evaluates risk impact, defines compensating controls, sets an expiration date, and tracks remediation to closure. Creating new standards (A) does not fix noncompliance and can increase confusion. Stopping activities (C) may be necessary for extreme/unacceptable risk, but it is not the "best approach" in general because it can unnecessarily disrupt business operations. Extra monitoring (D) can be a compensating control, but without a formal exception workflow it lacks governance, approval, and traceability.
References: ISACA CISM Review Manual (Governance-policy/standards, exception handling, risk acceptance and accountability); CISM Exam Content Outline (Domain 2).

質問: **486**
事業継続計画および災害復旧計画に関する文書を定期的に更新する主な理由は次のうちどれですか？
A. セキュリティポリシー要件を強制するため
B. 事業資産の在庫管理
C. 監査およびコンプライアンス要件を満たすことを保証する
D. 事業運営の可用性を確保するため
正解: **D (**コメントを発表する**)**
The primary reason to regularly update business continuity and disaster recovery documents is to ensure that the plans and procedures are aligned with the current business needs and objectives, and that they can effectively support the availability of business operations in the event of a disaster. Updating the documents also helps to enforce security policy requirements, maintain business asset inventories, and ensure audit and compliance requirements are met, but these are secondary benefits.
References = CISM Review Manual, 16th Edition eBook1, Chapter 9: Business Continuity and Disaster Recovery, Section: Business Continuity Planning, Subsection: Business Continuity Plan Maintenance, Page
378.

質問: **487**
以下のうち、力ずくの攻撃に対する最善の防御策はどれですか？
A. 任意アクセス制御
B. 強制アクセス制御

C. 多要素認証(MFA)
D. 時間帯制限
正解: **C** (コメントを発表する)

質問: **488**
情報セキュリティプログラムの成熟度を判断するのに最も適した方法はどれですか？
A. セキュリティ予算配分
B. 組織のリスク許容度
C. リスク評価結果
D. セキュリティ指標
正解: **D** (コメントを発表する)
Security metrics are the best way to determine the maturity of an information security program because they are quantifiable indicators of the performance and effectiveness of the security controls and processes.
Security metrics help to evaluate the current state of security, identify gaps and weaknesses, measure progress and improvement, and communicate the value and impact of security to stakeholders. Therefore, security metrics are the correct answer.
References:
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-1
https://www.gartner.com/en/publications/protect-your-business-assets-with-roadmap-for-maturing-information-security

質問: **489**
情報セキュリティポリシーを策定する際に、様々な事業部門の利害関係者を関与させる主な理由は次のうちどれですか？
A. 政策策定の全体コストを削減するため
B. セキュリティ侵害への対応責任を共有する
C. IT部門の業務負担を軽減するため
D. 組織全体で方針の承認を得る
正解: (正解を表示します)
The main reason to involve stakeholders from various business units is to gain their acceptance and buy-in for the information security policy. The CISM Review Manual underlines that policies are more effective and enforceable when stakeholders understand and agree with them, which also aids in smooth policy implementation across the organization.
Reference:ISACA CISM Review Manual, 16th Edition, Page 45, " Stakeholder Involvement in Policy Development " .

質問: **490**

リスク対策オプションについて上級管理職の支持を得るために、以下のうちどれを伝えるのが最も効果的でしょうか？
A. 量的損失
B. 業界ベンチマーク
C. 脅威分析
D. 根本原因分析
正解: **A** (コメントを発表する)
communicating the quantitative loss associated with the risk scenarios and the risk treatment options would be the most helpful to gain senior management support, as it helps to demonstrate the value and effectiveness of the risk treatment options in terms of reducing the likelihood and impact of the risk. Quantitative loss also helps to compare the cost and benefit of the risk treatment options and to prioritize the most critical risks. Industry benchmarks, threat analysis, and root cause analysis may be useful for understanding and assessing the risk, but they do not directly measure the performance of the risk treatment options.
References = Five Key Considerations When Developing Information Security Risk Treatment Plans, CISM Domain 2: Information Risk Management (IRM) [2022 update]

質問: **491**
情報セキュリティに関する従業員の責任を理解させるための最も効果的な方法は、次のうちどれですか？
A. 規則違反に対する懲戒手続きについて周知徹底する。
B. スタッフに情報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。
C. 従業員に機密保持契約書への署名を義務付ける。
D. 職務記述書に情報セキュリティに関する責任を含める。
正解: (正解を表示します)
The most effective way to help staff members understand their responsibilities for information security is to require them to participate in information security awareness training. Information security awareness training is a program that educates and motivates the staff members about the importance, benefits, and principles of information security, and the roles and responsibilities that they have in protecting the information assets and resources of the organization. Information security awareness training also provides the staff members with the necessary knowledge, skills, and tools to comply with the information security policies, procedures, and standards of the organization, and to prevent, detect, and report any information security incidents or issues.
Information security awareness training also helps to create and maintain a positive and proactive information security culture among the staff members, and to increase their confidence and competence in performing their information security duties.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:

Information Security Culture, page 281; CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Information Security Awareness, Training and Education, pages 197-1982.

質問: **492**
情報セキュリティマネージャーが新しい侵入検知システム(IDS)ソリューションのビジネスケースを作成する際に、最初にとるべきステップは何でしょうか？
A. 対処すべき課題を明確にする。
B. 費用対効果分析を実施する。
C. 総所有コスト(TCO)を計算します。
D. 実現可能性調査を実施する。
正解: **(**正解を表示します**)**
The first step when developing a business case for a new intrusion detection system (IDS) solution is to define the issues to be addressed. A business case is a document that provides the rationale and justification for initiating a project or investment. It typically includes information such as the problem statement, the objectives, the alternatives, the costs and benefits, the risks and assumptions, and the expected outcomes. The first step in developing a business case is to define the issues to be addressed, which means identifying and describing the current situation, the problems or challenges faced by the organization, and the needs or opportunities for improvement. By defining the issues to be addressed, the information security manager can establish the scope and purpose of the business case, and provide a clear and compelling problem statement that explains why a new IDS solution is needed. The other options are not the first step when developing a business case for a new IDS solution, although they may be part of the subsequent steps. Performing a cost- benefit analysis is a step that involves comparing the costs and benefits of different alternatives, including the new IDS solution and the status quo. A cost-benefit analysis can help evaluate and justify the feasibility and desirability of each alternative, and support the decision-making process. Calculating the total cost of ownership (TCO) is a step that involves estimating the direct and indirect costs associated with acquiring, operating, maintaining, and disposing of an asset or a system over its entire life cycle. A TCO calculation can help determine the long-term financial implications of investing in a new IDS solution, and compare it with other alternatives. Conducting a feasibility study is a step that involves assessing the technical, operational, legal, and economic aspects of implementing a project or an investment. A feasibility study can help identify and mitigate any potential issues or risks that may affect the success of the project or investment, and provide recommendations for improvement

質問: **493**
電子商取引企業の情報セキュリティマネージャーが、事業継続計画の見直し結果を検討しています。以下の所見のうち、最も緊急に対処すべき事項はどれでしょうか？

A. 事業継続計画は最近テストされていません
B. 最近の回復テストの費用が予算の予想を上回った
C. 年次事業影響分析が延期されました
D. 事業継続計画は最近監査を受けていません
正解: **(**正解を表示します**)**
The correct answer is A because an untested business continuity plan creates immediate uncertainty about whether the organization can continue or recover critical operations during a disruption. For an e-commerce business, downtime can quickly affect revenue, customer trust, regulatory obligations, and service availability. Testing validates whether recovery procedures, people, technologies, communications, dependencies, and recovery objectives are realistic and achievable. A recovery test exceeding budget expectations is a concern, but it does not necessarily mean the organization cannot recover. A delayed business impact analysis is important because BIA supports continuity planning, but the immediate operational concern is that the plan has not been validated. A lack of recent audit may reduce assurance, but an audit is not a substitute for testing. In CISM, continuity and recovery capabilities must be tested to confirm readiness and identify weaknesses before a real incident occurs. Therefore, the absence of recent BCP testing is the most immediate concern.
Reference: CISM Information Security Incident Management; business continuity, disaster recovery, plan testing, and operational resilience principles.

質問: **494**
情報セキュリティマネージャーが組織のインシデント対応計画を更新しています。IT部門と事業部門が提供するプロセスと手順が完全かつ正確であり、すべての担当チームに周知されていることを検証する最良の方法は次のうちどれですか？
A. 関係者とテストの目的を確認する。
B. データ侵害事件の机上演習を実施する。
C. インシデント対応計画の調査を実施する。
D. データ漏洩事故のトリアージ手順を確認する。
正解: **(**正解を表示します**)**
Conducting a tabletop exercise is the best method to validate the completeness, accuracy, and awareness of incident response procedures. The CISM Review Manual details that tabletop exercises simulate scenarios, allowing teams to test responses, clarify responsibilities, and reveal gaps in the process in a controlled environment.
Reference:ISACA CISM Review Manual, 16th Edition, Page 295, " Testing and Validating Incident Response Plans " .

質問: **495**
パスワードポリシーを改訂する最も適切な理由は次のうちどれですか？
A. ベンダーのおすすめ

B. 監査勧告
C. リスク評価
D. 業界のベストプラクティス
正解: **(**正解を表示します**)**
The best justification for making a revision to a password policy is a risk assessment. A risk assessment is a process of identifying, analyzing, and evaluating the potential threats and vulnerabilities that may affect the confidentiality, integrity, and availability of information assets and systems. By conducting a risk assessment, the organization can determine the appropriate level of security controls and measures to protect its information assets and systems, including password policies. A risk assessment can also help identify any gaps or weaknesses in the existing password policy, and provide recommendations for improvement based on the organization's risk appetite and tolerance. The other options are not the best justification for making a revision to a password policy, although they may be some inputs or outputs of the risk assessment process. A vendor recommendation is an external source of advice or guidance that may or may not be relevant or applicable to the organization's specific context and needs. A vendor recommendation should not be followed blindly without conducting a risk assessment to evaluate its suitability and effectiveness. An audit recommendation is an internal source of feedback or suggestion that may or may not be accurate or complete.
An audit recommendation should not be implemented without conducting a risk assessment to verify its validity and feasibility. An industry best practice is a general standard or guideline that may or may not reflect the organization's unique characteristics and requirements. An industry best practice should not be adopted without conducting a risk assessment to customize it according to the organization's goals and priorities

質問: **496**
ある組織が、規制の厳しい市場で新たなeコマース事業を展開する計画を立てています。リスク管理戦略を更新する際に、最も重要な検討事項は次のうちどれでしょうか？
A. 同業他社の戦略
B. アウトソーシングのニーズ
C. 企業文化
D. コンプライアンス要件
正解: **(**正解を表示します**)**
When operating in a highly regulated market, compliance requirements become paramount, as failure to comply can lead to severe legal penalties, financial losses, and reputational harm. According to the CISM Review Manual, 16th Edition, Domain 2: Information Risk Management, Task 2, understanding and addressing legal, regulatory, and contractual requirements is critical in risk management, especially in regulated environments. This ensures that the risk management strategy is aligned with mandatory regulations and industry standards. Other factors (such as outsourcing and business culture) are important, but compliance is the primary driver in highly regulated markets.

Reference:ISACA CISM Review Manual, 16th Edition, Page 120-122, " Legal, Regulatory and Contractual Requirements " .

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu **193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **497**
情報セキュリティチームは、攻撃者がアプリケーション内の新たに発表された重大な脆弱性を悪用していることを確認しました。最初に行うべきことは次のうちどれですか？
A. 追加のアプリケーション制御をインストールします。
B. 上級管理職に報告する。
C. インシデント対応計画を発動する。
D. アプリケーションへのアクセスを防止します。
正解: **(**正解を表示します**)**
According to the NIST SP 800-61 Computer Security Incident Handling Guide1, the first step in responding to a cybersecurity incident is to invoke the incident response plan (IRP), which is a written document that defines the roles, responsibilities, and procedures for dealing with a confirmed or suspected security breach1. The IRP helps the organization to prepare for, detect, analyze, contain, eradicate, recover from, and learn from incidents1. Invoking the IRP ensures that the right personnel and resources are mobilized to effectively deal with the threat and minimize the impact.
References = 1: NIST SP 800-61: 1. Introduction1

質問: **498**
情報セキュリティ管理者が現在実施されている管理策の適切性を評価するために、以下のうちどれが必ず定義されていなければならないか？
A. セキュリティポリシー
B. リスク管理フレームワーク
C. リスク許容度
D. セキュリティ基準
正解: **(**正解を表示します**)**
= Risk appetite is the amount and type of risk that an organization is willing to accept in pursuit of its objectives. It is a key factor that influences the information security strategy and objectives, as well as the selection and implementation of security controls. Risk

appetite must be defined in order for an information security manager to evaluate the appropriateness of controls currently in place, as it provides the basis for determining whether the controls are sufficient, excessive, or inadequate to address the risks faced by the organization. The information security manager should align the controls with the risk appetite of the organization, ensuring that the controls are effective, efficient, and economical. References = CISM Review Manual 15th Edition, page 29, page 31.

質問: **499**
組織が新しい規制要件に準拠しないリスクを受け入れる可能性が最も高いのは、次の場合です。
A. 従業員は新しい規制で要求される管理に抵抗しています。
B. 規制要件がビジネス要件と矛盾しています。
C. コンプライアンス違反のリスクが組織のリスク許容度を超えています。
D. 規制を遵守するためのコストが、潜在的な罰金を上回ります。
正解: **(正解を表示します)**
An organization is most likely to accept the risk of noncompliance with a new regulatory requirement when the cost of complying with the regulation exceeds the potential penalties. In such cases, from a cost-benefit perspective, the organization might find it more economical to absorb potential fines or penalties rather than implementing costly controls or processes to comply with the regulation.
"Risk acceptance occurs when the cost of mitigating or transferring the risk exceeds the benefit of the mitigation. This also applies to regulatory noncompliance if the penalties are less than the costs of compliance."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Treatment Options* ISACA's practice questions highlight that risk acceptance is a legitimate treatment when costs outweigh potential penalties or impact.

質問: **500**
効果的な情報セキュリティ戦略を策定する際に、最も重要なのはどれを特定することでしょうか？
A. セキュリティ意識向上トレーニングの必要性
B. セキュリティガバナンスによって得られる潜在的なコスト削減効果
C. 事業資産の保全
D. 残存リスクレベル
正解: **C (コメントを発表する)**
Business assets are the resources that enable the organization to achieve its objectives and create value.
Identifying the business assets to be secured is the most important step in developing an effective information security strategy, as it helps to align the security goals with the

business goals, prioritize the security efforts and resources, and define the scope and boundaries of the security program. (From CISM Review Manual
15th Edition)
References: CISM Review Manual 15th Edition, page 27, section 1.2.1.

質問: **501**
次のうち、システムレベルのリスクを計算するために使用される入力項目はどれですか？
A. 主要リスク指標
B. 事業影響分析
C. システムのリスク許容度
D. システムの脆弱性
正解: **(**正解を表示します**)**
The correct answer is D because system-level risk is calculated or assessed by considering threats, vulnerabilities, likelihood, impact, and existing controls related to a specific system. Vulnerabilities are weaknesses that may be exploited by threats and are therefore direct inputs into determining risk. Key risk indicators are useful for monitoring changes in risk exposure over time, but they are generally reporting or monitoring measures rather than primary calculation inputs. A business impact analysis helps determine the effect of disruption on business processes and may support impact evaluation, but it is not by itself a system- level risk input. System risk appetite defines how much risk may be acceptable, but it does not calculate the risk itself; it is used to evaluate whether calculated or assessed risk is acceptable. In CISM risk management, risk assessment requires identifying assets, threats, vulnerabilities, likelihood, impact, and controls. Since vulnerabilities directly influence the likelihood and potential success of exploitation, system vulnerabilities are the best answer.
Reference: CISM Information Risk Management; risk assessment, vulnerabilities, likelihood, impact, system- level risk, and control evaluation principles.

質問: **502**
以下のリスク対応のうち、リスク移転の例はどれですか？
A. サードパーティ製アプリケーションの活用
B. サイバーセキュリティ保険の購入
C. リスク責任を別の部署に移管する
D. オフサイトバックアップの実施
正解: **(**正解を表示します**)**
Risk transfer involves shifting the impact or financial consequences of a risk to a third party. Purchasing cybersecurity insurance is the most common example, where the organization pays a premium to a provider who assumes certain financial responsibilities in the event of a security incident.
Other options listed do not transfer risk:
A). Using third-party applications may introduce new risks, not transfer existing ones.

C). Moving ownership within the organization is reassignment, not transfer.
D). Off-site backups are a form of risk mitigation, not transfer.
"Risk transfer shifts the financial consequences of a risk to another entity, typically through insurance or contractual arrangements."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Treatment Options* Example: "An organization may transfer the financial impact of a potential data breach through the purchase of cyber insurance."

質問: **503**
アプリケーションサーバー上のセキュリティ制御のギャップを特定するために、最も有用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. 脅威モデル
C. 侵入テスト
D. 内部監査報告書
正解: **(**正解を表示します**)**
Penetration testing is the most useful method for identifying security control gaps on an application server because it simulates real-world attacks and exploits the vulnerabilities and weaknesses of the application server. Penetration testing can reveal the actual impact and risk of the security control gaps, and provide recommendations for remediation and improvement.
References: The CISM Review Manual 2023 defines penetration testing as "a method of evaluating the security of an information system or network by simulating an attack from a malicious source" and states that
"penetration testing can help identify security control gaps and provide evidence of the potential impact and risk of the gaps" (p. 185). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer:
"Penetration testing is the correct answer because it is the most useful method for identifying security control gaps on an application server, as it simulates real-world attacks and exploits the vulnerabilities and weaknesses of the application server, and provides recommendations for remediation and improvement" (p. 95). Additionally, the web search result 4 states that "penetration testing is a valuable tool for discovering security gaps in your application server and network infrastructure" and that
"penetration testing can help you assess the effectiveness and efficiency of your security controls, and identify the areas that need improvement or enhancement" (p. 1).

質問: **504**
ある組織が、規制当局の監視対象となっている金融アプリケーションの監視とサポートを第三者ベンダーに委託することになった。組織にとって最も効果的なリスク管理策は次のうちどれだろうか？
A. 主要リスク指標(KRI)のモニタリング

B. システムとデータ間の職務分掌の実施
C. ベンダーアクセスを無効にし、アクセスが必要な場合にのみ再度有効にする
D. ベンダー契約に不履行に対する違約条項を含める
正解: **(**正解を表示します**)**

質問: **505**
企業内でBYOD(Bring Your Own Device)モバイルプログラムを導入する際に、情報セキュリティマネージャーにとって最も重要な課題は次のうちどれでしょうか？
A. モバイルアプリケーション制御
B. デバイスのセキュリティに一貫性がない
C. 構成管理
D. エンドユーザーの受容性
正解: **(**正解を表示します**)**
Inconsistent device security is the primary challenge for an information security manager when deploying a bring your own device (BYOD) mobile program in an enterprise because it increases the risk of data breaches and compromises. A BYOD mobile program allows employees to use their personal devices, such as smartphones, tablets, or laptops, to access the organization's network, applications, and data. However, personal devices may have different operating systems, versions, configurations, and security settings than the organization's standard devices. Moreover, personal devices may not be updated regularly, may have unauthorized or malicious apps installed, or may not have adequate protection against malware or theft.
Inconsistent device security makes it difficult for the information security manager to enforce and monitor the security policies and controls across all devices, as well as to ensure compliance with the regulatory requirements for data privacy and security.
Therefore, inconsistent device security is the correct answer.
References:
https://simplemdm.com/blog/challenges-of-bring-your-own-device-byod-policy/
https://www.timedoctor.com/blog/byod-pros-and-cons/
https://www.ncsc.gov.uk/files/NCSC-Vendor-Security-Assessment.pdf

質問: **506**
ある組織の主要製品は、SaaS(Software as a Service)を使用して提供される顧客向けアプリケーションです。主任セキュリティエンジニアが、主要クラウドプロバイダーで重大なセキュリティ脆弱性を発見しました。組織内で、この関連タスクの主たる責任者は誰でしょうか？
A. 情報セキュリティマネージャー
B. データ所有者
C. アプリケーションの所有者
D. セキュリティエンジニア

正解: **(**正解を表示します**)**
= The application owner is primarily accountable for the associated task because they are responsible for ensuring that the application meets the business requirements and objectives, as well as the security and compliance standards. The application owner is also the one who defines the roles and responsibilities of the application team, including the security engineer, and oversees the development, testing, deployment, and maintenance of the application. The application owner should work with the cloud provider to address the security vulnerability and mitigate the risk. The information security manager, the data owner, and the security engineer are not primarily accountable for the associated task, although they may have some roles and responsibilities in supporting the application owner. The information security manager is responsible for establishing and maintaining the information security program and aligning it with the business objectives and strategy. The data owner is responsible for defining the classification, usage, and protection requirements of the data. The security engineer is responsible for implementing and testing the security controls and features of the application. References = CISM Review Manual 2023, Chapter 1, Section 1.2.2, page 18; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 115.

質問: **507**
事業影響分析(BIA)は、主に以下の目的で定期的に実施されるべきである。
A. 環境変化に対する脆弱性を検証する。
B. 資産の重要性を分析する。
C. 規制への準拠を確認する。
D. 制御の有効性を検証する。
正解: **D (**コメントを発表する**)**
A business impact analysis (BIA) is a process that helps identify and evaluate the potential effects of disruptions or incidents on the organization's mission, objectives, and operations. A BIA should be periodically executed to verify the effectiveness of the controls that are implemented to prevent, mitigate, or recover from such disruptions or incidents12. According to the CISM Manual, a BIA should be performed at least annually for critical systems and processes, and more frequently for non-critical ones3. A BIA should also be updated whenever there are significant changes in the organization's environment, such as new regulations, technologies, business models, or stakeholder expectations3. A BIA should not be used to validate vulnerabilities on environmental changes (A), analyze the importance of assets (B), or check compliance with regulations ©, as these are not the primary purposes of a BIA.
References: 1: IR 8286D, Using Business Impact Analysis to Inform Risk Prioritization and Response | CSRC NIST 2: CISM Domain 4 Preview | BCP - Business Impact Analysis (BIA) - YouTube 3: CISM ITEM DEVELOPMENT GUIDE - ISACA

質問: **508**
主要リスク指標 (KRI) を開発する際に最も大きな課題となるのは次のうちどれですか?
A. KRIの数を制限する
B. KRIに関する包括的なレポート
C. 共通KRIの集約
D. KRIを特定のリスクにリンクする
正解: **D (**コメントを発表する**)**
The biggest challenge is linking KRIs to specific risks to ensure that they accurately measure and signal potential exposures. If KRIs aren't directly connected to real risks, they won't effectively support risk management efforts.
"A key challenge in developing KRIs is ensuring that they are directly linked to specific risks to provide meaningful and actionable insights."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Key Risk Indicators (KRIs)* ISACA's practice questions highlight the importance of clear linkage for effective risk measurement.

質問: **509**
新たに買収したビジネスアプリケーションのセキュリティ制御を設計する際に、情報セキュリティマネージャーが最も重視すべき事項は次のうちどれでしょうか?
A. 組織に対する規制要件
B. ビジネスアプリケーションのアクセス管理
C. アプリケーションによってサポートされるビジネスプロセス
D. ITセキュリティアーキテクチャフレームワーク
正解: **(**正解を表示します**)**
The correct answer is A because regulatory requirements establish mandatory obligations that must be addressed when designing security controls. A newly acquired business application may introduce legal, regulatory, privacy, financial, or industry-specific compliance requirements. Failure to meet these requirements can expose the organization to penalties, legal action, reputational damage, and unacceptable risk. Access management is important, but it is only one area of control design. Business processes supported by the application are also important for understanding risk and impact, but mandatory regulatory requirements must be identified and satisfied. The IT security architecture framework helps guide consistent control implementation, but it cannot override external compliance obligations. In CISM practice, control design must align with business objectives, risk appetite, and legal and regulatory requirements. When acquiring or integrating a business application, the information security manager must first ensure that required controls address applicable laws, regulations, contractual obligations, and compliance expectations.
Reference: CISM Information Risk Management; compliance requirements, control design, and risk treatment principles.

質問: **510**
災害発生時に組織が業務を継続するために、以下のどの計画を実行すべきでしょうか？
A. 災害復旧計画(DRP)
B. インシデント対応計画
C. 事業継続計画(BCP)
D. 事業継続計画
正解: **C (**コメントを発表する**)**
= A business continuity plan (BCP) is the plan that should be invoked by an organization in an effort to remain operational during a disaster. A disaster is a sudden, unexpected, or disruptive event that causes significant damage, loss, or interruption to the organization's normal operations, assets, or resources.
Examples of disasters are natural disasters, such as earthquakes, floods, or fires, or human-made disasters, such as cyberattacks, sabotage, or terrorism. A BCP is a document that describes the procedures, strategies, and actions that the organization will take to ensure the continuity of its critical business functions, processes, and services in the event of a disaster. A BCP also defines the roles and responsibilities of the staff, management, and other stakeholders involved in the business continuity management, and the resources, tools, and systems that will support the business continuity activities. A BCP helps the organization to:
Minimize the impact and duration of the disaster on the organization's operations, assets, and reputation.
Restore the essential functions and services as quickly and efficiently as possible.
Protect the health, safety, and welfare of the staff, customers, and partners.
Meet the legal, regulatory, contractual, and ethical obligations of the organization.
Learn from the disaster and improve the business continuity capabilities and readiness of the organization.
References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Business Continuity Plan (BCP), page 1771; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 83, page 772.

質問: **511**
セキュリティ重視の文化を構築しようとする際に、最も重要な考慮事項は次のうちどれですか？
A. 同業他社と比較した現在のセキュリティ戦略のベンチマーク
B. 情報セキュリティに関する地域的な規則および法令
C. 従業員の現在のセキュリティ意識レベル
D. 組織の既存のセキュリティポリシー、手順、およびフレームワーク
正解: **(**正解を表示します**)**

The most important consideration is the current security awareness level of employees (C). CISM emphasizes that culture change must start from an understanding of current behaviors, attitudes, and knowledge gaps.
Benchmarking (A), regulations (B), and formal frameworks (D) provide structure, but culture is driven by people. Tailoring initiatives to the existing awareness level increases adoption and effectiveness, leading to sustainable risk reduction.
References: ISACA CISM Review Manual (Program management-security culture development); CISM Exam Content Outline (Domain 3).

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu **1193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **512**
組織全体に一般的な情報セキュリティ責任を伝えるための最も効果的な方法は、次のうちどれですか？
A. 定期的なセキュリティ意識向上トレーニングを実施する
B. 従業員に機密保持契約書への署名を義務付ける
C. 社内イントラネットに情報セキュリティポリシーを公開する
D. 組織のRACIマトリックスを作成する
正解: **(**正解を表示します**)**
The correct answer is A because regular security awareness training is the most effective method for communicating general information security responsibilities to all personnel. Awareness training reinforces expected behaviors, reporting obligations, policy requirements, and individual accountability in a way that employees can understand and apply in daily work. Requiring staff to sign confidentiality agreements is important, but it mainly creates legal acknowledgment and does not ensure understanding of broader security responsibilities. Publishing the information security policy on the intranet makes the policy available, but passive publication is not enough to confirm communication or understanding. A RACI matrix is useful for defining roles and responsibilities for specific processes or functions, but it is generally too detailed and role- specific to communicate broad responsibilities across the entire organization. CISM emphasizes that security awareness, communication, and training are essential to building a security-aware culture and ensuring that all individuals understand their responsibilities for protecting information assets.

Reference: CISM Information Security Governance; security awareness, communication, accountability, and security culture principles.

質問: **513**
ゼロトラストを正常に実装する上で最も重要な要素は次のどれですか?
A. 侵入テストを実施したネットワークを優先する
B. ユーザー行動のログ記録と監視に重点を置く
C. アーキテクチャの戦略的なポイントの認証と承認
D. ネットワークの各コンポーネントを理解する
正解: **(**正解を表示します**)**
Zero Trust requires granular authentication and authorization at every critical juncture. It assumes no implicit trust within the network and enforces strict access control.
"Zero Trust is based on continuous authentication and authorization at all strategic control points."
- CISM Review Manual 15th Edition, Chapter 3: Security Architecture, Section: Zero Trust Principles*

質問: **514**
情報セキュリティガバナンスフレームワークを構築する際に、最初に実施すべきことはどれですか？
A. 第三者機関に委託して、プログラムの独立したレビューを実施する。
B. 環境に関連する情報セキュリティツールとスキルを評価する。
C. フレームワークの費用対効果分析を実施する。
D. ビジネスと文化の特性を理解する。
正解: **(**正解を表示します**)**

質問: **515**
重要なシステム間の関係は、
A. 主要業績評価指標(KPI)の評価
B. 事業影響分析(BIA)の実施
C. システム分類スキームの開発
D. 復旧時間目標(RTO)の評価
正解: **B (**コメントを発表する**)**
The explanation given is: "A BIA is a process that identifies and evaluates the potential effects of natural and man-made events on business operations. It helps to understand how critical systems are interrelated and what their dependencies are. A BIA also helps to determine the RTOs for each system. The other options are not directly related to understanding the relationships between critical systems."

質問: **516**

ビジネス目標と組織のリスク許容度は、情報セキュリティの開発に最も役立つ入力です。
A. 標準。
B. 戦略。
C. リスク評価。
D. 主要業績評価指標 (KPI)。
正解: **(**正解を表示します**)**

質問: **517**
以下の事業部門のうち、ID管理システムにデータを格納する権利を保有すべきなのはどれですか？
A. 人事部(HR)
B. 情報セキュリティ
C. 法律
D. 情報技術
正解: **A (**コメントを発表する**)**

質問: **518**
組織がセキュリティインシデントが発生したことを関係者に伝える最も重要な理由は次のうちどれですか？
A. 情報セキュリティに対する意識を高める
B. 事件の根本原因を明らかにする
C. 組織に対する好感度を高める
D. 通知に関する規制を遵守するため
正解: **D (**コメントを発表する**)**
Complying with regulations regarding notification is the most important reason for an organization to communicate to affected parties that a security incident has occurred, as it helps to avoid legal penalties, fines, or sanctions that may result from failing to notify the relevant authorities, customers, or other stakeholders in a timely and appropriate manner. Additionally, complying with regulations regarding notification may also help to preserve the trust and reputation of the organization, as well as to facilitate the investigation and resolution of the incident.
References = CISM Review Manual 2022, page 3151; CISM Exam Content Outline, Domain 4, Task 4.5

質問: **519**
インシデント後レビューを実施する主な目的は以下のとおりです。
A. 事件の影響を再評価する。
B. 脆弱性を特定する。
C. 管理改善点を特定する。
D. 根本原因を特定する。

正解: **(**正解を表示します**)**
= The primary objective of performing a post-incident review is to identify the root cause of the incident, which is the underlying factor or condition that enabled or facilitated the occurrence of the incident.
Identifying the root cause helps to understand the nature and origin of the incident, and to prevent or mitigate similar incidents in the future. A post-incident review also aims to evaluate the effectiveness and efficiency of the incident response process, identify lessons learned and best practices, and recommend improvements for the incident management policies, procedures, controls, and tools. However, these are secondary objectives that depend on the identification of the root cause as the first step.
Re-evaluating the impact of incidents is not the primary objective of performing a post-incident review, as it is already done during the incident response process. The impact of incidents is the extent and severity of the damage or harm caused by the incident to the organization's assets, operations, reputation, or stakeholders. Re- evaluating the impact of incidents may be part of the post-incident review, but it is not the main goal.
Identifying vulnerabilities is not the primary objective of performing a post-incident review, as it is also done during the incident response process. Vulnerabilities are weaknesses or flaws in the system or network that can be exploited by attackers to compromise the confidentiality, integrity, or availability of the information or resources. Identifying vulnerabilities may be part of the post-incident review, but it is not the main goal.
Identifying control improvements is not the primary objective of performing a post-incident review, as it is a result of the root cause analysis. Controls are measures or mechanisms that are implemented to protect the system or network from threats, reduce risks, or ensure compliance with policies and standards. Identifying control improvements is an important outcome of the post-incident review, but it is not the main goal. References = ISACA CISM: PRIMARY goal of a post-incident review should be to?
CISM Exam Overview - Vinsys
CISM Review Manual, Chapter 4, page 176
CISM Exam Content Outline | CISM Certification | ISACA, Domain 4, Task 4.3

質問: **520**
情報セキュリティインシデントを調査する際には、インシデントの詳細を共有する必要があります。
A. 広く肯定的な意図を示す。
B. 管理のみ。
C. 必要に応じてのみ、
D. 内部監査のみ。
正解: **(**正解を表示します**)**
When investigating an information security incident, details of the incident should be shared only as needed, according to the principle of least privilege and the need-to-know

basis. This means that only the authorized and relevant parties who have a legitimate purpose and role in the incident response process should have access to the incident information, and only to the extent that is necessary for them to perform their duties.
Sharing incident details only as needed helps to protect the confidentiality, integrity, and availability of the incident information, as well as the privacy and reputation of the affected individuals and the organization.
Sharing incident details only as needed also helps to prevent unauthorized disclosure, modification, deletion, or misuse of the incident information, which could compromise the investigation, evidence, remediation, or legal actions.
References = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Process, page 2311; CISM Review Questions, Answers & Explanations Manual,
10th Edition, Question 49, page 462.

質問: **521**
セキュリティインシデントを検出する最も効果的な方法はどれですか？
A. 最近のセキュリティリスク評価を分析する。
B. セキュリティ上の異常を分析する。
C. 侵入テストの結果を分析する。
D. 脆弱性評価を分析する。
正解: **(**正解を表示します**)**
Analyzing security anomalies is the most effective way to detect security incidents, as it involves comparing the current state of the information system and network with the expected or normal state, and identifying any deviations or irregularities that may indicate a security breach or compromise. Security anomalies can be detected by using various tools and techniques, such as security information and event management (SIEM) systems, intrusion detection and prevention systems (IDS/IPS), log analysis, network traffic analysis, and behavioral analysis. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 181, section 4.3.2.4; CISM: Information Security Incident Management Part 11, section recognize security anomalies.

質問: **522**
サイバーインシデント対応の封じ込めフェーズで最も適切なアクションは次のどれですか?
A. インシデントの最終的な根本原因を特定します。
B. ネットワークからインシデントのすべてのインスタンスを削除します。
C. 悪用された脆弱性を軽減して、将来のインシデントを防止します。
D. 被害の拡大を防ぐため、影響を受けたシステムを隔離します。
正解: **(**正解を表示します**)**

Isolating affected systems limits the damage and prevents the incident from impacting other parts of the organization.
"During containment, the primary objective is to isolate affected systems to prevent further damage."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Incident Response Process*

質問: **523**
情報セキュリティ状況報告管理において、最も重要な項目は次のうちどれですか？
A. 最近のセキュリティ関連イベント一覧
B. 主要リスク指標(KRI)
C. 情報セキュリティポリシーの見直し
D. 情報セキュリティ予算要求
正解: **B (**コメントを発表する**)**
Key risk indicators (KRIs) are the most useful to include in an information security status report for management because they measure and report the level of risk exposure or performance against predefined risk thresholds or targets, and alert management of any deviations or issues that may require attention or action. List of recent security events is not very useful to include in an information security status report for management because it does not provide any analysis or evaluation of the events or their impact on the organization's objectives or performance. Review of information security policies is not very useful to include in an information security status report for management because it does not reflect any progress or results of implementing or enforcing the policies. Information security budget requests are not very useful to include in an information security status report for management because they do not indicate any value or benefit of investing in information security initiatives or controls. References: https://www.isaca.org/resources/isaca- journal/issues/2016/volume-6/how-to-measure-the-effectiveness-of-information-security-using-iso-27004

質問: **524**
ある組織は、中核業務以外のすべてのIT機能を外部サービスプロバイダーにアウトソーシングしたいと考えています。望ましいセキュリティレベルを維持するために、調達プロセスに含めるべき最も重要な項目は次のうちどれですか？
A. 業界ベンチマークを実施し、ベンダーがビジネスに合致しているかどうかを判断する
B. 適切な対策を選択するためのリスク評価の実施
C. セキュリティ監査を実施し、改善すべきギャップを特定する
D. セキュリティへの影響を最小限に抑えるためのビジネス影響分析の実施
正解: **(**正解を表示します**)**
The correct answer is B because outsourcing IT functions introduces third-party risk, and the organization must perform a risk assessment during procurement to identify the

controls required to maintain the desired security level. A risk assessment helps determine data sensitivity, service criticality, regulatory requirements, access needs, vendor dependencies, contractual controls, monitoring requirements, and residual risk. Industry benchmarking may provide useful comparison, but it does not identify the organization's specific outsourcing risks. A security audit may be useful after vendor selection or as part of due diligence, but the first procurement need is to understand risk and define appropriate security requirements. A business impact analysis is valuable for continuity planning, but it is not the main activity for selecting security controls in outsourcing. CISM emphasizes that third-party arrangements should be governed through risk assessment, due diligence, contracts, monitoring, and control requirements. Therefore, risk assessment is the most important procurement activity.
Reference: CISM Information Risk Management; third-party risk management, outsourcing, procurement controls, due diligence, and vendor risk assessment principles.

質問: **525**
組織が、災害発生時にウォームサイトのサーバーバックアップが適切に維持され、使用可能であることを保証するための最善の方法は次のうちどれですか？
A. ウォームサイトのバックアップメディア保管設備を確認する
B. 温暖な地域に予備の機器を用意しておく
C. ウォームサイト施設の機器を使用してバックアップを読み取ります。
D. 施設を点検し、バックアップ機器の在庫を四半期ごとに確認する
正解: **(**正解を表示します**)**
The best way to ensure that backups at a warm site are properly maintained and usable during a disaster is to use the equipment at the warm site facility to read the backups. CISM emphasizes that backup and recovery capabilities must be tested, not merely documented or inspected. Reading the backups using warm-site equipment validates both the backup media and compatibility with the recovery environment. Reviewing storage facilities or inventorying backup media confirms that backups exist and are stored appropriately, but it does not prove they can be restored. Having duplicate equipment available is useful, but it does not confirm that the backup data is readable or usable. The core issue is recoverability, and the only reliable way to validate recoverability is through practical testing. In business continuity and disaster recovery management, testing verifies whether recovery procedures, media, systems, and personnel can achieve required recovery objectives. Therefore, using warm-site equipment to read the backups provides the strongest assurance that backups will be usable when needed.
References:
ISACA CISM Review Manual, Information Security Program Development and Management - backup testing and disaster recovery readiness ISACA CISM Exam Content Outline, Domain 3: Information Security Program Development and Management

質問: **526**

組織のセキュリティ管理に関して最も懸念すべきは次のどれですか?
A. 一部のコントロールが許容範囲外で動作しています。
B. 主要管理指標 (KCI) が実装されていません。
C. コントロールの所有権は更新されていません。
D. 制御ギャップ分析は古くなっています。
正解: **B** (コメントを発表する)
Key Control Indicators (KCIs) are essential to measuring the effectiveness and performance of security controls. Without them:
The organization cannot assess if controls are working as intended
It's difficult to demonstrate due diligence
Risks may go unnoticed
While other answers point to operational concerns, the complete absence of KCIs presents a critical governance gap that compromises the organization's ability to monitor and manage control health.
"KCIs provide actionable metrics that support proactive control management and are fundamental to governance and assurance."
- CISM Review Manual 15th Edition, Chapter 1: Governance Metrics and Reporting*

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu 問**193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **527**
新しいセキュリティ イニシアチブの成功を促進するには何が最適でしょうか?
A. IT セキュリティ運営委員会を設立します。
B. 実装後のセキュリティ メトリックを監視します。
C. セキュリティポリシーを定期的に更新する
D. セキュリティに関する意思決定にビジネスを組み込む。
正解: **D** (コメントを発表する)

質問: **528**
高度な持続的脅威(APT)から企業を保護するために最も役立つのは、次のうちどれですか？
A. セキュリティポリシーを更新しました
B. セキュリティ基準の定義

C. 脅威インテリジェンス
D. 定期的なウイルス対策ソフトのアップデート
正解**: B (**コメントを発表する**)**
Threat intelligence is the most helpful method for protecting an enterprise from advanced persistent threats (APTs), as it provides relevant and actionable information about the sources, methods, and intentions of the adversaries who conduct APTs. Threat intelligence can help to identify and anticipate the APTs that target the enterprise, as well as to enhance the detection, prevention, and response capabilities of the information security program. Threat intelligence can also help to reduce the impact and duration of the APTs, as well as to improve the resilience and recovery of the enterprise. Threat intelligence can be obtained from various sources, such as internal data, external feeds, industry peers, government agencies, or security vendors.
The other options are not as helpful as threat intelligence, as they do not provide a specific and timely way to protect the enterprise from APTs. Updated security policies are important to establish the rules, roles, and responsibilities for information security within the enterprise, as well as to align the information security program with the business objectives, standards, and regulations. However, updated security policies alone are not enough to protect the enterprise from APTs, as they do not address the dynamic and sophisticated nature of the APTs, nor do they provide the technical or operational measures to counter the APTs. Defined security standards are important to specify the minimum requirements and best practices for information security within the enterprise, as well as to ensure the consistency, quality, and compliance of the information security program. However, defined security standards alone are not enough to protect the enterprise from APTs, as they do not account for the customized and targeted nature of the APTs, nor do they provide the situational or contextual awareness to deal with the APTs. Regular antivirus updates are important to keep the antivirus software up to date with the latest signatures and definitions of the known malware, viruses, and other malicious code. However, regular antivirus updates alone are not enough to protect the enterprise from APTs, as they do not detect or prevent the unknown or zero-day malware, viruses, or other malicious code that are often used by the APTs, nor do they provide the behavioral or heuristic analysis to identify the APTs. References = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 211-212, 215-216, 233-234, 237-238.
CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1021.
Advanced Persistent Threats and Nation-State Actors 1
Book Review: Advanced Persistent Threats 2
Advanced Persistent Threat (APT) Protection 3
Establishing Advanced Persistent Security to Combat Long-Term Threats 4 What is the difference between Anti - APT (Advanced Persistent Threat) and ATP (Advanced Threat Protection)5

質問**: 529**

マルチユーザー環境において、情報セキュリティ管理者が汎用管理者アカウントの使用を制限すべき主な理由は次のうちどれですか？
A. 不正なユーザーアクセスを防止するため
B. 説明責任の問題を防ぐため
C. システム監査証跡が迂回されないようにするため
D. 職務分担の維持を確実にするため
正解: **(**正解を表示します**)**

質問: **530**
情報セキュリティアーキテクチャを導入する最も適切な理由は次のうちどれですか？
A. 導入後の情報セキュリティロードマップとして機能する。
B. 情報セキュリティコンポーネントの導入を迅速化する。
C. セキュリティ要件の一貫した実装を促進する。
D. 統合の費用対効果を評価する。
正解: **(**正解を表示します**)**

質問: **531**
ある組織は情報セキュリティインシデントに適切に対応しました。しかし、情報セキュリティマネージャーは、インシデント管理手順に規定されている手順の一部が対応チームによって実行されていなかったことを知りました。情報セキュリティマネージャーが最初にとるべき手順は何でしょうか？
A. インシデント対応チームに追加のトレーニングを実施する。
B. インシデント管理手順から該当の手順を削除します。
C. インシデント対応チームにインタビューを行う。
D. インシデント管理手順を確認する。
正解: **(**正解を表示します**)**

質問: **532**
組織が業務において自社所有のモバイルデバイスの使用を導入する場合、情報セキュリティマネージャーの主な責任は次のうちどれですか？
A. デバイスにリモートワイプ機能が必要です。
B. セキュリティ意識向上トレーニングを実施する。
C. 既存のセキュリティポリシーを見直し、更新する。
D. デバイス上でパスワードとデータ暗号化を強制する。
正解: **C (**コメントを発表する**)**
The primary responsibility of an information security manager in an organization that is implementing the use of company-owned mobile devices in its operations is to review and update existing security policies. Security policies are the foundation of an organi-zation's security program, as they define the goals, objectives, principles, roles, respon-sibilities, and requirements for protecting information and systems. Security policies should be

reviewed and updated regularly to reflect changes in the organization's envi-ronment, needs, risks, and technologies1. Implementing the use of company-owned mobile devices in its operations is a significant change that may introduce new threats and vulnerabilities, as well as new opportunities and benefits, for the organiza-tion. Therefore, the information security manager should review and update existing security policies to address the following aspects2:
*The scope, purpose, and ownership of company-owned mobile devices
*The acceptable and unacceptable use of company-owned mobile devices
*The security standards and best practices for company-owned mobile devices
*The roles and responsibilities of users, managers, IT staff, and vendors regarding compa-ny-owned mobile devices
*The procedures for provisioning, managing, monitoring, and decommissioning company-owned mobile devices
*The incident response and reporting process for company-owned mobile devices By reviewing and updating existing security policies, the information security manager can ensure that the organization's security program is aligned with its business objec-tives and risk appetite, as well as compliant with applicable laws and regulations. The other options are not the primary responsibility of an information security manager in an organization that is implementing the use of company-owned mobile devices in its operations. They are possible actions or controls that may be derived from or support-ed by the updated security policies. Requiring remote wipe capabilities for devices is a technical control that can help prevent data loss or theft in case of device loss or com-promise3. Conducting security awareness training is an administrative control that can help educate users about the security risks and responsibilities associated with using company-owned mobile devices. Enforcing passwords and data encryption on the de-vices is a technical control that can help protect data confidentiality and integrity on company-owned mobile devices.
References:
1: Information Security Policy - NIST 2: Mobile Device Security Policy - SANS 3: Remote Wipe: What It Is
& How It Works - Lifewire : Security Awareness Training - NIST : Mobile Device Encryption - NIST

質問**: 533**
新たなサイバーセキュリティの脅威に関する情報を受け取った後、情報セキュリティ管理者が取るべき最も重要な行動は次のうちどれですか？
A. ログ監視の相関ルールを更新して、潜在的な新たな脅威を検出します。
B. 新たな脅威が現実化した場合に、組織に及ぼす影響を評価する。
C. 情報に基づいた意思決定を可能にするため、脅威を直ちに上級管理職に報告してください。

D. 脅威によって悪用された脆弱性について、エンタープライズアーキテクチャ(EA)をレビューします。
正解: **B** (コメントを発表する)

質問: **534**
セキュリティ機器の管理手順を更新する際に、最も重要な考慮事項は次のうちどれですか？
A. 組織のセキュリティフレームワークに基づいたアップデート
B. 手続き変更に関する経営陣への通知
C. リスク技術とプロセスの変更に基づくアップデート
D. 経営陣による手続きの審査と承認
正解: (正解を表示します)
According to the CISM Manual, updating procedures for managing security devices should be based on changes in risk technology and process, not on the organization's security framework, notification to management of the procedural changes, or review and approval of procedures by management1. These are not the most important considerations when updating procedures for managing security devices, as they do not reflect the actual impact of the changes on the security posture of the organization.
The CISM Manual states that "procedures for managing security devices should be updated whenever there are significant changes in the risk technology or process that affect the security devices" (IR 8287A)1. For example, if a new security device is introduced or an existing one is replaced, its procedures should be updated accordingly. Similarly, if a new risk technology or process is implemented that affects how security devices are configured, monitored, or maintained, its procedures should be updated as well1.
The CISM Manual also provides guidance on how to update procedures for managing security devices in a systematic and consistent manner. It recommends using a change management process that involves identifying, analyzing, approving, implementing, and evaluating changes to security device procedures1. It also suggests using a change control board (CCB) that consists of representatives from different stakeholders who review and approve changes to security device procedures before they are implemented1.
References: 1: IR 8287A - Managing Security Devices | CSRC NIST

質問: **535**
重要なアプリケーション向けの監視システムの開発に関するビジネスケースを経営陣が支持する最も適切な理由は、次のうちどれですか？
A. 業界の同業者が最近、同様のアプリケーションで情報漏洩の被害に遭いました。
B. このシステムは、他のユースケースにも複製可能です。
C. システム導入コストは、ダウンタイムによる影響よりも小さい。
D. 解決策は組織のリスク許容範囲内です。

正解: (正解を表示します)
A monitoring system for a critical application can help detect and prevent incidents that could affect the availability, integrity, and confidentiality of the application and its data. The impact of downtime could include loss of revenue, reputation, customer satisfaction, and regulatory compliance. Therefore, the cost of implementing the system should be justified by the potential savings from avoiding or minimizing these impacts.
References = CISM Review Manual, 15th Edition, page 173; An Introduction to Metrics, Monitoring, and Alerting; Business-critical applications: What are they and how do you protect them from cyberattack?

質問: **536**
マルウェア感染が確認された直後に必ず発生しなければならない事象は次のうちどれですか？
A. 準備
B. 回復
C. 封じ込め
D. 根絶
正解: (正解を表示します)
Containment is the action that MUST happen immediately following the identification of a malware incident because it aims to isolate the affected systems or networks from the rest of the environment and prevent the spread or escalation of the malware. Containment can involve disconnecting the systems or networks from the internet, blocking or filtering certain ports or protocols, or creating separate VLANs or subnets for the isolated systems or networks. Containment is part of the incident response process and should be performed as soon as possible after detecting a malware incident12. Preparation (A) is the phase that happens before the identification of a malware incident, where the organization establishes the incident response plan, team, roles, resources, and tools. Preparation is essential for ensuring the readiness and capability of the organization to respond to malware incidents effectively and efficiently12. Recovery (B) is the phase that happens after the containment and eradication of a malware incident, where the organization restores the normal operations of the systems or networks, verifies the functionality and security of the systems or networks, and implements the preventive and corrective measures to avoid or mitigate future malware incidents. Recovery is the final phase of the incident response process and should be performed after ensuring that the malware incident is fully resolved and the systems or networks are clean and secure12. Eradication (D) is the phase that happens after the containment of a malware incident, where the organization removes the malware and its traces from the systems or networks, identifies the root cause and impact of the malware incident, and collects and preserves the evidence for analysis and investigation. Eradication is an important phase of the incident response process, but it does not happen immediately after the identification of a malware

incident12. References = 1: CISM Review Manual 15th Edition, page 308-3091; 2: Cybersecurity Incident Response Exercise Guidance - ISACA2

質問: **537**
復旧時間目標(RTO)は、次のうちどれから得られる出力ですか？
A. 事業継続計画(BCP)
B. 災害復旧計画(DRP)
C. サービスレベル契約(SLA)
D. 事業影響分析(BIA)
正解: **D (コメントを発表する)**
Business impact analysis (BIA) is the process that provides the output of recovery time objectives (RTOs), which are the maximum acceptable time frames for restoring business functions or processes after a disruption. Business continuity plan (BCP) is the document that describes the strategies and procedures for ensuring the continuity of critical business functions or processes in the event of a disruption. Disaster recovery plan (DRP) is the document that describes the technical steps and resources for restoring IT systems and data in the event of a disruption. Service level agreement (SLA) is the document that defines the expectations and obligations between a service provider and a service consumer, such as availability, performance, and security. References: https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1 /business-impact-analysis-bia-and-disaster-recovery-planning-drp https://www.isaca.org/resources/isaca- journal/issues/2017/volume-6/service-level-agreements-in-the-cloud

質問: **538**
インシデント対応計画を企業戦略に合わせる際に、最初に更新すべき項目は次のうちどれですか？
A. 災害復旧計画(DRP)
B. インシデント通知計画
C. リスク対応シナリオ
D. セキュリティ手順
正解: **(正解を表示します)**
The answer to the question is C. Risk response scenarios. This is because risk response scenarios are the predefined plans and actions that the organization will take to respond to specific types of incidents, such as cyberattacks, natural disasters, or data breaches. Risk response scenarios should be aligned with the corporate strategy, which defines the vision, mission, goals, and objectives of the organization, and guides the decision- making and resource allocation processes. By aligning the risk response scenarios with the corporate strategy, the organization can ensure that the incident response plan supports the achievement of the desired outcomes and benefits, and minimizes the impact and disruption to the business operations and performance.

Risk response scenarios are the predefined plans and actions that the organization will take to respond to specific types of incidents. Risk response scenarios should be aligned with the corporate strategy, which defines the vision, mission, goals, and objectives of the organization. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 4, Section 4.2.2, page 2111; CISM domain 4: Information security incident management [2022 update] | Infosec2; A Guide to Effective Incident Management Communications3

質問: **539**
効果的な情報セキュリティプログラムを示す最良の指標は、次のうちどれですか？
A. リスクは許容できるレベルに抑えられています。
B. 職員から報告されたセキュリティインシデントの件数が増加しました。
C. 主要リスク指標(KRI)が設定される。
D. 方針は上級管理職によって審査および承認されます。
正解: **(**正解を表示します**)**
Comprehensive and Detailed Step-by-Step Explanation:
An effective information security program aims to manage risks to acceptable levels while supporting business objectives.
A). Risk is treated to an acceptable level: This is the BEST answer as it directly reflects the program's success in mitigating risks within the organization's tolerance levels.
B). The number of security incidents reported by staff has increased: An increase in reported incidents might indicate improved awareness but does not necessarily reflect overall effectiveness.
C). Key risk indicators (KRIs) are established: KRIs are important for monitoring risks but do not indicate whether risks are being effectively managed.
D). Policies are reviewed and approved by senior management: While essential, this action alone does not demonstrate the program ' s effectiveness.
Reference: CISM Job Practice Area 2 (Risk Management) highlights the importance of risk treatment and its alignment with organizational risk tolerance.

質問: **540**
標的型メール攻撃によるセキュリティインシデントの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. データ損失防止(DLP)システムを導入する
B. 受信クラウドメールサービスをすべて無効にする
C. 組織全体で意識向上トレーニングを実施する
D. 利用規約への同意を求める
正解: **C (**コメントを発表する**)**
Conducting awareness training across the organization is the best way to reduce the risk of security incidents from targeted email attacks because it helps to educate and empower

the employees to recognize and avoid falling for such attacks. Targeted email attacks, such as phishing, spear phishing, or business email compromise, rely on social engineering techniques to deceive and manipulate the recipients into clicking on malicious links, opening malicious attachments, or disclosing sensitive information. Awareness training can help to raise the level of security culture and behavior among the employees, as well as to provide them with practical tips and best practices to protect themselves and the organization from targeted email attacks.
Therefore, conducting awareness training across the organization is the correct answer.
References:
https://almanac.upenn.edu/articles/one-step-ahead-dont-get-caught-by-targeted-email-attacks
https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec
https://www.csoonline.com/article/3334617/what-is-spear-phishing-examples-tactics-and-techniques.html

質問**: 541**
国内企業の経営陣が、事業を複数の海外拠点に拡大する計画を発表しました。この計画を知った情報セキュリティマネージャーが最初にとるべき行動は次のうちどれでしょうか？
A. 国際情報セキュリティ基準とのギャップ分析を実施する
B. セキュリティトレーニングおよび意識向上に関する資料を適宜更新する。
C. 新しい拠点に影響を与える法的および規制上の要件を調査する
D. 各新規拠点ごとに、地域に合わせた情報セキュリティポリシーを作成する。
正解**: (**正解を表示します**)**
The first step is to research legal and regulatory requirements for the new locations. Different countries have varying security and privacy laws, and understanding these is critical before adapting policies or procedures.
"Security requirements will vary depending on local legal and regulatory obligations, which must be understood as part of international expansion."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Compliance Requirements The ISACA CISM practice database also highlights this step as the initial and critical move in international expansions.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu ｷ193問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **542**
組織全体で実施された最近の情報セキュリティ意識向上キャンペーンの効果を最もよく示しているのは、次のうちどれですか？
A. セキュリティインシデント件数の減少
B. 報告されたセキュリティインシデント数の増加
C. セキュリティインシデントの影響の軽減
D. セキュリティインシデントのエスカレーション頻度の増加
正解: **C** (コメントを発表する)

質問: **543**
包括的な情報セキュリティ管理システムを導入する最も適切な理由は次のうちどれですか？
A. 組織戦略との継続的な整合性を確保するため
B. 情報セキュリティプログラムに対する上級管理職の支持を得るため
C. 主要リスク指標(KRI)の特定を支援する
D. 外部規制要件への準拠を容易にするため
正解: **A** (コメントを発表する)
According to the CISM Review Manual, 15th Edition, the primary objective of an information security management system (ISMS) is to align the information security strategy with the business strategy and ensure that information security objectives are consistent with the business objectives1. This helps the organization to achieve its goals and protect its information assets from threats and risks.
References = 1: CISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, page 11.

質問: **544**
インシデント対応チームは、インシデントの原因となった脅威を取り除くために必要な措置を、以下のどの段階で文書化すべきでしょうか？
A. 事後検証
B. 根絶
C. 封じ込め
D. 識別
正解: (正解を表示します)
The eradication phase of incident response is the stage where the incident response team documents and performs the actions required to remove the threat that caused the incident1. This phase involves identifying and eliminating the root cause of the incident, such as malware, compromised accounts, unauthorized access, or misconfigured

systems2. The eradication phase also involves restoring the affected systems to a secure state, deleting any malicious files or artifacts, and verifying that the threat has been completely removed2. The eradication phase is the first step in returning a compromised environment to its proper state2.
The other phases of incident response are:
Preparation: The phase where the incident response team prepares for potential incidents by defining roles, responsibilities, procedures, tools, and resources1.
Detection and analysis: The phase where the incident response team identifies and prioritizes the incidents based on their severity, impact, and urgency1.
Containment: The phase where the incident response team isolates the affected systems or networks to prevent the spread of the incident and minimize the damage1.
Recovery: The phase where the incident response team restores the normal operations of the systems or networks, and implements any necessary changes or improvements to prevent recurrence1.
Post-incident review: The phase where the incident response team evaluates the effectiveness of the incident response process, identifies the lessons learned, and provides recommendations for improvement1. References = 3: Critical Incident Stress Management: CISM Implementation Guidelines 2:
What is the Eradication Phase of Incident Response? - RSI Security 1: Incident Response Models - ISACA

質問: **545**
新任の情報セキュリティマネージャーは、組織が問題解決に短期的な解決策を用いる傾向があることに気づきました。リソースの配分と支出は効果的に追跡されておらず、コンプライアンス要件が満たされているという保証もありません。このようなボトムアップ型のセキュリティアプローチを是正するために、まず最初に何をすべきでしょうか？
A. 監査委員会を設置する。
B. 情報セキュリティ運営委員会を設置する。
C. 脅威分析を実施する。
D. 情報セキュリティ意識向上トレーニングプログラムを実施する。
正解: **(**正解を表示します**)**

質問: **546**
経営幹部が企業のセキュリティ管理フレームワークの構築に関与する主な理由は次のうちどれですか？
A. 監査人の企業セキュリティに関する勧告を満たすため
B. 必要な最低限の管理レベルを確立する
C. 企業セキュリティの望ましい状態を決定する
D. 企業セキュリティに関する業界のベストプラクティスを確実に遵守するため
正解: **(**正解を表示します**)**

質問: **547**
AIセキュリティ意識向上プログラムを開発する際に、以下のうち最も重要なものはどれですか？
A. インタラクティブなトレーニング環境の構築
B. ユーザーの役割に合わせたトレーニングの実施
C. AIとのユーザーインタラクションのレベルを定義する
D. 組織の成熟度を評価する
正解: **(**正解を表示します**)**
The correct answer is B because awareness training is most effective when it is aligned with user roles, responsibilities, and exposure to risk. An AI security awareness program should address how different users interact with AI tools, what data they may enter, what decisions they may make, and what risks apply to their specific functions. For example, developers, executives, analysts, HR staff, legal teams, and general users may face different AI-related risks. Interactive training can improve engagement, but it is not more important than relevance to the user's role. Defining the level of interaction with AI is useful input for tailoring the program, but the broader objective is role-based training. Assessing organizational maturity may help planning, but it does not ensure users receive relevant guidance. CISM program management emphasizes awareness and training appropriate to roles and responsibilities. Therefore, aligning training to user roles is the most important consideration.
Reference: CISM Information Security Program Development and Management; security awareness, role- based training, AI risk awareness, and user responsibility principles.

質問: **548**
ある組織が、インシデント対応機能をパブリッククラウドサービスプロバイダーと連携させようとしています。情報セキュリティマネージャーが最初にとるべき行動は何でしょうか？
A. プロバイダーのインシデント対応チームのスキルセットを特定する。
B. プロバイダーの監査ログ記録と監視管理を評価する。
C. プロバイダーのインシデント定義と通知基準を確認する。
D. インシデントエスカレーションプロセスを更新する。
正解: **C (**コメントを発表する**)**
When an organization is aligning its incident response capability with a public cloud service provider, the information security manager's first course of action should be to review the provider's incident definitions and notification criteria. This is because the provider's incident definitions and notification criteria may differ from the organization's own, and may affect the scope, severity, and urgency of the incidents that need to be reported and handled. By reviewing the provider's incident definitions and notification criteria, the information security manager can ensure that there is a common understanding and

agreement on what constitutes an incident, how it is classified, and when and how it is communicated. This will help to avoid confusion, delays, or conflicts in the incident response process, and to establish clear roles and responsibilities between the organization and the provider. References = CISM Review Manual, 16th Edition, page 1021 Reviewing the provider's incident definitions and notification criteria is the FIRST course of action when aligning the organization's incident response capability with a public cloud service provider. This is because the organization needs to understand how the provider defines and classifies incidents, what their roles and responsibilities are, and how they will communicate with the organization in case of an incident. This will help the organization align its own incident response processes and expectations with the provider's and ensure a coordinated and effective response.

質問: **549**
組織全体に情報セキュリティの責任を伝える最も効果的な方法は、次のうちどれですか？
A. セキュリティ意識向上プログラムの実施
B. 職務記述書に情報セキュリティに関する責任を明記する
C. スキルマトリックスの作成
D. セキュリティポリシーにおける情報セキュリティ責任の定義
正解: **B (**コメントを発表する**)**
Documenting information security responsibilities within job descriptions is the most effective way to convey information security responsibilities across an organization because it clearly defines the roles, expectations, and accountabilities of each employee regarding information security. It also helps to align the information security objectives with the business goals and performance indicators, and to ensure compliance with the security policies and standards.
References = CISM Review Manual 15th Edition, What is CISM? - Digital Guardian

質問: **550**
アプリケーション内で特定された重大なITセキュリティリスクの責任を負わせるのに最も適した人物は誰でしょうか？
A. 最高情報責任者(CIO)
B. 最高情報セキュリティ責任者(CISO)
C. ビジネスアプリケーションの所有者
D. リードアプリケーション開発者
正解: **(**正解を表示します**)**
The business application owner (C) is best positioned to own application-related security risks because they are accountable for the business outcomes, value, and operational impact of the application. CISM consistently assigns risk ownership to business roles, not technical implementers. The CISO (B) advises on security posture, the CIO (A) oversees IT strategy, and developers (D) implement controls-but none are accountable for accepting

or prioritizing business risk. Assigning ownership to the application owner ensures that risk decisions reflect business priorities and align with risk appetite.
References: ISACA CISM Review Manual (Governance-risk ownership and accountability); CISM Exam Content Outline (Domain 2).

質問: **551**
情報セキュリティフレームワークを採用する主な利点は、以下の点です。
A. 信頼できる新興脅威情報。
B. セキュリティおよび脆弱性報告ガイドライン。
C. 一般的な利用可能性指標。
D. 標準化されたセキュリティ管理。
正解: **(**正解を表示します**)**
A standardized security control is a set of rules, guidelines, or best practices that are designed to protect the confidentiality, integrity, and availability of information assets and systems. An information security framework is a collection of standardized security controls that are aligned with the organization's objectives, strategy, and risk appetite. Adopting an information security framework provides a primary benefit of ensuring consistency, efficiency, and effectiveness in the implementation and management of information security across the organization.
References = CISM Review Manual 2022, page 321; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.22; What is an Information Security Framework?; Information Security Frameworks: What Are They and Why Do You Need One?

質問: **552**
ある組織が、厳格な保守手順とスケジュールが定められた新しいシステムを導入しました。この情報はどこに文書化すべきでしょうか？
A. 規格
B. ポリシー
C. ガイドライン
D. 手順
正解: **(**正解を表示します**)**
Procedures are the detailed steps or instructions for performing specific tasks or activities. They are usually aligned with standards, policies and guidelines, but they are more specific and prescriptive. System maintenance instructions and schedules are examples of procedures that should be documented and followed to ensure the proper functioning and security of the system.
References: The CISM Review Manual 2023 defines procedures as "the lowest level in the hierarchy of documentation. They are detailed steps that a user must follow to accomplish an activity" (p. 80). The CISM Item Development Guide also provides the following

explanation for this answer: "Procedures are the correct answer because they provide the specific steps to be followed to maintain the system" (p. 11).

質問: **553**
侵入テストにおいて、最も重要な問題は次のうちどれですか？
A. 独立したグループにテストを実施させる
B. 監査からの許可取得
C. 内部情報に頼らずにテストを実施する
D. 明確な目標と成功 -失敗の基準を持つこと
正解: **(正解を表示します)**
The most important issue in a penetration test is having a defined goal as well as success and failure criteria.
A penetration test is a simulated cyber attack against a computer system or an application to check for exploitable vulnerabilities. The goal of a penetration test is to identify and evaluate the security risks and weaknesses of the target system or application, and to provide recommendations for improvement. The success and failure criteria of a penetration test are the metrics and indicators that measure the effectiveness and efficiency of the test, and the extent to which the test achieves its goal. By having a defined goal as well as success and failure criteria, the penetration tester can plan and execute the test in a systematic and structured manner, and can communicate and report the results and findings in a clear and concise way. The other options are not the most important issue in a penetration test, although they may be some factors or considerations that affect the test. Having an independent group perform the test is a desirable practice, as it can provide an unbiased and objective assessment of the target system or application. However, it is not essential, as long as the penetration tester follows ethical hacking principles and standards. Obtaining permission from audit is a mandatory requirement, as it ensures that the penetration test is authorized and compliant with the organization's policies and regulations. However, it is not an issue, as it is a prerequisite for conducting the test. Performing the test without the benefit of any insider knowledge is an optional approach, as it simulates a real-world attack by an external hacker who does not have access to the internal design or configuration of the target system or application. However, it is not always feasible or effective, as some vulnerabilities may be hidden or inaccessible from an outsider's perspective.

質問: **554**
新しいシステムの導入時に、混乱、不正な変更、およびエラーの可能性を事前に最小限に抑えるプロセスは次のうちどれですか？
A. 構成管理
B. パスワード管理
C. 変更管理

D. バージョン管理
正解: **(**正解を表示します**)**
Change management is the process of planning, implementing, and monitoring changes to information systems in a controlled and coordinated manner. Change management proactively minimizes the likelihood of disruption, unauthorized alterations, and errors by ensuring that changes are aligned with the organization's objectives, policies, and procedures. Change management also involves identifying and mitigating the risks associated with changes, as well as communicating and documenting the changes to all relevant stakeholders12.
References = 1: CISM Review Manual (Digital Version), page 271 2: CISM Review Manual (Print Version), page 271

質問: **555**
攻撃後の事後レビューを実施する際に、情報セキュリティマネージャーにとって最も役立つのは次のうちどれですか？
A. 組織にとっての攻撃のコスト
B. 攻撃者の位置
C. 攻撃者が使用した操作方法
D. 侵入検知システム(IDS)ログの詳細
正解: **C (**コメントを発表する**)**
= The method of operation used by the attacker is the most useful information for an information security manager when conducting a post-incident review of an attack. This information can help identify the root cause of the incident, the vulnerabilities exploited, the impact and severity of the attack, and the effectiveness of the existing security controls. The method of operation can also provide insights into the attacker's motives, skills, and resources, which can help improve the organization's threat intelligence and risk assessment. The cost of the attack to the organization, the location of the attacker, and the details from IDS logs are all relevant information for a post-incident review, but they are not as useful as the method of operation for improving the incident handling process and preventing future attacks. References = CISM Review Manual 2022, page 316; CISM Item Development Guide 2022, page 9; ISACA CISM: PRIMARY goal of a post-incident review should be to?

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-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/CISM-JPN-mondaishu　**1193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」