ISACA.CISM-JPN.v2026-03-02.q426

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：	426
バージョン：	v2026-03-02
ページの閲覧量：	107
問題集の閲覧量：	4583

https://www.jpnshiken.com/shiken/ISACA.CISM-JPN.v2026-03-02.q426.html

質問: **1**
ネットワーク スニッフィングは、次のような方法で実行され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. リモートで。
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: **2**
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のに最も効果的なのは次のどれですか。

A. リスク評価に基づく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立
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: **3**
組織の災害復旧計画 (DRP) を作成するときに、情報セキュリティ マネージャーが最初に行うべきことはどれですか。
A. ビジネス影響分析 (BIA) を実施する
B. 応答と回復を学習します。
C. コミュニケーション計画を確認します。
D. 対応および回復戦略を策定します。
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: **4**
IT 運用を海外でホストされる Infrastructure as a Service (IaaS) モデルに移行するときに最も重要な考慮事項は次のどれですか。
A. セキュリティ侵害が発生した場合、責任や罰則が発生する可能性があります。
B. データは不明な場所に保存され、簡単に取得できない可能性があります。
C. 原産国の法律や規制が適用されない場合があります。
D. データのラベル付けは、データが正しいクラウド タイプに割り当てられていることを保証するのに役立ちます。
正解: **(**正解を表示します**)**

質問: **5**
ある組織は最近の災害で収益の損失を経験しました。次のどれが組織の回復に最も適した準備でしょうか?
A. 災害復旧計画 (DRP)
B. ビジネス影響分析 (BIA)
C. 事業継続計画 (BCP)
D. インシデント対応計画
正解: **(**正解を表示します**)**

質問: **6**
サービス契約の次の要素のうち、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. 侵害の検出と通知
C. コンプライアンスステータスレポート
D. サービスプロバイダー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: **7**
情報セキュリティ マネージャーは、チケットが記録された後、セキュリティ インシデントがヘルプ デスクによって適切にエスカレーションされていないことに気づきました。この問題を解決するための最適な自動制御は次のどれですか。
A. ヘルプデスクワークフローに自動化された脆弱性スキャンを実装する
B. すべてのセキュリティインシデントのデフォルト設定を最高優先度に変更する
C. 自動化されたサービスレベルアグリーメント (SLA) レポートをヘルプデスクチケットシステムに統合する
D. インシデント対応ワークフローをヘルプデスクチケットシステムに統合する
正解: **(**正解を表示します**)**
The best automated control to resolve the issue of security incidents not being appropriately escalated by the help desk is to integrate incident response workflow into the help desk ticketing system. This will ensure that the help desk staff follow the predefined steps and procedures for handling and escalating security incidents, based on the severity, impact, and urgency of each incident. The incident response workflow will also provide clear guidance on who to notify, when to notify, and how to notify the relevant stakeholders and authorities.
This will improve the efficiency, effectiveness, and consistency of the incident response process.
References = CISM Review Manual, 16th Edition, page 2901; A Practical Approach to Incident Management Escalation2

質問: **8**
セキュリティ担当者の組織変更の際に情報セキュリティ管理を最も効果的にサポートするのはどれですか?
A. セキュリティ戦略とプログラムの正式化
B. スタッフ向け意識啓発プログラムの開発
C. セキュリティプロセスの最新の文書化の確保
D. セキュリティ運用チーム内でのプロセスの確立
正解: **C (**コメントを発表する**)**
Ensuring current documentation of security processes is the best way to support information security management in the event of organizational changes in security personnel. Documentation of security processes provides a clear and consistent reference for the roles, responsibilities, procedures, and standards of the information security program. It helps to maintain the continuity and effectiveness of the security operations, as well as the compliance with the security policies and regulations. Documentation of security processes also facilitates the knowledge transfer and training of new or existing security personnel, as well as the communication and collaboration with other

stakeholders. By ensuring current documentation of security processes, the information security manager can minimize the impact of organizational changes in security personnel, and ensure a smooth transition and alignment of the security program. References = CISM Review Manual 15th Edition, page 43, page 45.

質問**: 9**
金融会社の幹部は、最近サイバー攻撃が増加していることを懸念しており、リスクを軽減するための対策を講じる必要があります。組織は次のように対応するのが最善です。
A. インシデント対応チームの予算と人員レベルを増加します。
B. 侵入検知システム (IDS) を実装します。
C. リスクを再検証し、許容できるレベルまで軽減します。
D. 事業継続計画 (BCP) のテスト。
正解**: (**正解を表示します**)**
The best response for the organization to reduce risk from increasing cyberattacks is to revalidate and mitigate risks to an acceptable level. This means that the organization should review its current risk profile, identify any new or emerging threats, vulnerabilities, or impacts, and evaluate the effectiveness of its existing controls and countermeasures. Based on this analysis, the organization should implement appropriate risk treatment strategies, such as avoiding, transferring, accepting, or reducing the risks, to achieve its desired risk appetite and tolerance. The organization should also monitor and review the risk situation and the implemented controls on a regular basis, and update its risk management plan accordingly. This approach is consistent with the ISACA Risk IT Framework, which provides guidance on how to align IT risk management with business objectives and value12.
The other options are not the best responses because they are either too narrow or too reactive. Increasing budget and staffing levels for the incident response team may improve the organization's ability to respond to and recover from cyberattacks, but it does not address the root causes or the prevention of the attacks.
Implementing an intrusion detection system (IDS) may enhance the organization's detection and analysis capabilities, but it does not guarantee the protection or mitigation of the attacks. Testing the business continuity plan (BCP) may verify the organization's readiness and resilience to continue its critical operations in the event of a cyberattack, but it does not reduce the likelihood or the impact of the attack. References = Risk IT Framework 1 CISM Review Manual, 16th Edition | Print | English 2, Chapter 3: Information Risk Management, pages 97-
98, 103-104, 107-108, 111-112.

質問**: 10**
データ損失防止 (DLP) ツールが、送信中に個人を特定できる情報 (PII) にフラグを付けました。情報セキュリティ マネージャーが最初に行うべきことは何ですか。

A. DLP システム内のルールを確認して検証します。
B. ビジネス プロセス所有者とともに範囲と影響を検証します。
C. インシデント対応計画を開始します。
D. 問題を上級管理職にエスカレートします。
正解: **(**正解を表示します**)**

質問: **11**
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. 上級管理職
B. 情報セキュリティ管理者
C. システム所有者
D. コントロールの所有者
正解: **(**正解を表示します**)**

質問: **12**
クライアント情報を処理するアプリケーションへのアクセス レベルを決定する責任は、次のどれが負うべきでしょうか?
A. ビジネスクライアント
B. 情報セキュリティの破綻
C. アイデンティティおよびアクセス管理チーム
D. ビジネスユニット管理
正解: **(**正解を表示します**)**
The business client should be responsible for determining access levels to an application that processes client information, because the business client is the owner of the data and the primary stakeholder of the application. The business client has the best knowledge and understanding of the business requirements, objectives, and expectations of the application, and the sensitivity, value, and criticality of the data. The business client can also define the roles and responsibilities of the users and the access rights and privileges of the users based on the principle of least privilege and the principle of separation of duties. The business client can also monitor and review the access levels and the usage of the application, and ensure that the access levels are aligned with the organization's information security policies and standards.
The information security team, the identity and access management team, and the business unit management are all involved in the process of determining access levels to an application that processes client information, but they are not the primary responsible party. The information security team provides guidance, support, and oversight to the business client on the information security best practices, controls, and standards for the application, and ensures that the access levels are consistent with the organization's information security strategy and governance. The identity and access management team implements, maintains, and audits the access levels and the access control mechanisms

for the application, and ensures that the access levels are compliant with the organization's identity and access management policies and procedures. The business unit management approves, authorizes, and sponsors the access levels and the access requests for the application, and ensures that the access levels are aligned with the business unit's goals and strategies. References = ISACA, CISM Review Manual, 16th Edition, 2020, pages 125-126, 129-130, 133-134, 137-138.
ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1037.

質問: **13**
新しい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のレベルを決定する責任は誰が負うべきでしょうか?
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: **(**正解を表示します**)**
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: **14**
情報セキュリティ戦略委員会に報告するための指標を確立する際に最も重要な考慮事項は何ですか?
A. 指標を伝えるためのダッシュボードの開発
B. 指標のベースライン値について合意する
C. 業界標準に対する指標の期待値のベンチマーク
D. 指標を組織文化に合わせる
正解: **(**正解を表示します**)**
The most important consideration when establishing metrics for reporting to the information security strategy committee is D. Aligning the metrics with the organizational culture. This is because the metrics should reflect the values, beliefs, and behaviors of the organization and its stakeholders, and support the achievement of the strategic objectives and goals. The metrics should also be relevant, meaningful, and understandable for the intended audience, and provide clear and actionable information for decision making. The metrics should not be too technical, complex, or ambiguous, but rather focus on the key aspects of

information security performance, such as risk, compliance, maturity, value, and effectiveness.
References = CISM Review Manual 15th Edition, Chapter 1, Section 1.3.2, page 281; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 5, page 3

質問: **15**
効果的な情報セキュリティ メトリックの最も重要な特性は次のどれですか。
A. このメトリックは上級管理職に頻繁に報告されます。
B. このメトリックは、リスク許容度に対する残余リスクを表します。
C. このメトリックは、組織の固有のリスクとリスク許容度を比較します。
D. このメトリックは、業界のリスク管理フレームワークに直接マッピングされます。
正解: **(**正解を表示します**)**

質問: **16**
インシデント事後調査の結果、システムへのアクセスに既知の脆弱性が悪用されたことが判明しました。当該脆弱性は、問題となったシステムの修復作業の一環として修正されました。次に行うべき対応は、次のうちどれですか？
A. スキャンして、脆弱性が他のシステムに存在するかどうかを判断します。
B. 既存のすべてのシステムにパッチをインストールします。
C. 脆弱性管理プロセスを確認します。
D. 脆弱性の根本原因を上級管理職に報告します。
正解: **A (**コメントを発表する**)**

質問: **17**
情報セキュリティガバナンスフレームワークを確立する際に最初に行うべきことはどれですか?
A. 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します。
B. プログラムの独立したレビューを実施するために第三者と契約します。
C. ビジネスと文化の属性を理解します。
D. フレームワークの費用対効果分析を実施します。
正解: **(**正解を表示します**)**

質問: **18**
オンライン バンクは、進行中のネットワーク攻撃が成功していると判断しました。銀行はまず次のことを行う必要があります。
A. 影響を受けるネットワーク セグメントを分離します。
B. 根本原因を取締役会に報告します。
C. 個人を特定できる情報 (PII) が侵害されているかどうかを評価します。
D. ネットワーク全体をシャットダウンします。
正解: **(正解を表示します)**
The online bank should first isolate the affected network segment, as this is the most effective way to contain the attack and prevent it from spreading to other parts of the network or compromising more data or systems.
Isolating the affected network segment also helps to preserve the evidence and facilitate the investigation and recovery process. Reporting the root cause to the board of directors, assessing whether personally identifiable information (PII) is compromised, and shutting down the entire network are not the first actions that the online bank should take, as they may not be feasible or appropriate at the time of the attack, and may cause more disruption, confusion, or damage to the business operations and reputation. References = CISM Review Manual 2023, page 1641; CISM Review Questions, Answers & Explanations Manual 2023, page 362; ISACA CISM - iSecPrep, page 213

質問: **19**
経営陣は新しい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、2つの会社の統合中にアクセス権の競合により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。この懸念に最善に対処するには、情報セキュリティ マネージャーは次のことを行う必要があります。
A. 買収統合が発生したときにアクセス権を確認します。
B. アクセス権のリスク評価を実行します。
C. 競合するアクセス権に関する懸念を管理者にエスカレーションします。
D. 一貫したアクセス制御標準を実装します。
正解: **(正解を表示します)**
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: **20**
組織のシステムへの侵入が成功したことを示す最良の指標は次のどれですか?
A. 内部ネットワークトラフィックの減少
B. 不正申請の増加
C. 使用可能なストレージ容量の減少
D. ログイン失敗回数の増加
正解: **B (**コメントを発表する**)**

質問: **21**
解雇された従業員のシステムアクセスの削除を開始する際に最も重要な機能は次のどれですか?
A. 法的
B. 情報セキュリティ
C. ヘルプデスク
D. 人事 (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**: 22**
Software as a Service (SaaS) モデルを採用する場合、クライアント組織が単独で負う責任は次のどれですか?
A. ホストパッチ
B. 侵入テスト
C. インフラストラクチャの強化
D. データ分類
正解**: D (**コメントを発表する**)**
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: **23**
インシデント対応チームの有効性は、次の場合に最大限に発揮されます。
A. インシデント対応チームは定期的に会合を開き、ログ ファイルを確認します。
B. インシデントは、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特定されます。
C. インシデント対応チームのメンバーは、訓練を受けたセキュリティ担当者です。
D. 学んだ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。
正解: **(**正解を表示します**)**

質問: **24**
組織の品質プロセスは、次のもの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. セキュリティ構成コントロール。
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 システムのドキュメントのリポジトリ。
正解: **B (**コメントを発表する**)**
= 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: **25**
インシデント後レビューを実施する主な目的は次のとおりです。
A. インシデントの影響を再評価します。
B. 脆弱性を特定します。
C. 制御の改善を特定します。
D. 根本原因を特定します。
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 the incident to occur. Identifying the root cause helps to prevent or mitigate future incidents, as well as to improve the incident response process. Re-evaluating the impact of incidents, identifying vulnerabilities, and identifying control improvements are secondary objectives of a post-incident review, which are derived from the root cause analysis. References = CISM Review Manual, 16th Edition, page 3061; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1512 The primary objective of performing a post-incident review is to identify the root cause of the incident. After an incident has occurred, the post-incident review process involves gathering and analyzing evidence to determine the cause of the incident. This analysis will help to identify both the underlying vulnerability that allowed the incident to occur, as well as any control improvements that should be implemented to prevent similar incidents from occurring in the future. Additionally, the post-incident review process can also be used to re-evaluate the impact of the incident, as well as any potential implications for the organization.

質問: **26**
情報セキュリティ プログラムの主要業績評価指標 (KPI) を開発する際に最も重要な考慮事項は次のどれですか。
A. 財務報告との整合
B. ビジネスイニシアチブとの整合
C. 業界のフレームワークとの整合
D. リスク許容度との整合
正解: **(**正解を表示します**)**
Explore
The most important consideration when developing key performance indicators (KPIs) for the information security program is B. Alignment with business initiatives. This is because KPIs are measurable values that demonstrate how effectively the information security program is achieving its objectives and delivering value to the organization. KPIs should be aligned with the business initiatives, such as the strategic goals, the mission, the vision,

and the values of the organization, and support the achievement of the desired outcomes and benefits. KPIs should also reflect the needs, expectations, and challenges of the business stakeholders, and provide relevant, meaningful, and actionable information for decision making and improvement. KPIs should not be too technical, complex, or ambiguous, but rather focus on the key aspects of information security performance, such as risk, compliance, maturity, value, and effectiveness.
KPIs are measurable values that demonstrate how effectively the information security program is achieving its objectives and delivering value to the organization. KPIs should be aligned with the business initiatives, such as the strategic goals, the mission, the vision, and the values of the organization, and support the achievement of the desired outcomes and benefits. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 1, Section 1.3.2, page 281; CISM Domain - Information Security Program Development | Infosec2; KPIs in Information Security: The 10 Most Important Security Metrics3

質問**: 27**
セキュリティ情報およびイベント管理 (SIEM) システムをインストールすると、どのような種類の制御が実装されますか?
A. 予防的
B. 抑止力
C. 探偵
D. 修正
正解**: (**正解を表示します**)**
A security information and event management (SIEM) system is a type of detective control because it monitors and analyzes the security events or logs from different sources or systems, and detects any anomalies or incidents that may indicate a security breach or compromise. A preventive control is a type of control that prevents or blocks any unauthorized or malicious activity or access from occurring. A deterrent control is a type of control that discourages or warns any potential attackers or intruders from attempting any unauthorized or malicious activity or access. A corrective control is a type of control that restores or repairs any damage or disruption caused by an unauthorized or malicious activity or access. 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**: 28**
リソースが限られている組織で情報セキュリティ プログラムの資金を獲得するための最善の方法は次のどれですか。
A. 事業継続計画 (BCP) の有効性を実証します。

B. 主要業績評価指標 (KPI) の傾向を報告します。
C. プログラムがビジネス活動を可能にすることを実証します。
D. 同業組織におけるセキュリティ イベントの増加の証拠を提供します。
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: **29**
高価値資産を保護するため、または信頼性に懸念がある環境を処理するための最適な多層防御の実装は次のどれですか?
A. 区分化
B. 重複した冗長性
C. 継続的な監視
D. 多要素認証
正解: **A (**コメントを発表する**)**
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: **30**
ビジネス活動の残留リスクが許容可能なリスク レベルよりも低い場合、最善の行動方針は次のどれですか。
A. 制御の有効性を監視する
B. リスク評価フレームワークを更新する
C. 固有のリスクレベルを確認する
D. リスクの確率と影響を確認する
正解: **(正解を表示します)**
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: **31**
インシデント対応ポリシーには次の内容を含める必要があります。
A. テスト方法の説明。
B. 通知の要件。
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: **32**
継続計画にエンドユーザーを関与させることの主な利点は次のとおりです。
A. 特定のビジネスニーズをより深く理解します。
B. 情報セキュリティ管理よりも客観的です。
C. ビジネスへの全体的な影響を確認できます。
D. 技術的リスクとビジネス上のリスクのバランスをとることができます。
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: **33**
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: **34**
内部監査から、規制要件に準拠していない情報セキュリティ上の問題が多数報告されました。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. セキュリティ例外を作成します。
B. ギャップ分析を実行して、必要なリソースを決定します。
C. 脆弱性評価を実行します。
D. 業務運営に対するリスクを評価します。
正解: **D (**コメントを発表する**)**
The information security manager should first assess the risk to business operations that are caused by the information security issues reported by internal audit. This will help to prioritize the remediation actions and allocate the necessary resources. Creating a security exception, performing a gap analysis, or performing a vulnerability assessment are possible subsequent steps, but they are not the first action to take.
References = CISM Review Manual, 16th Edition, page 48

質問: **35**
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対する最適なアプローチは次のどれですか?
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ます。
B. インシデント対応の責任をクラウド プロバイダーに移譲します。
C. 既存のインシデント対応手順を引き続き使用します。
D. クラウド環境を網羅するようにインシデント対応手順を改訂します。
正解: **D (**コメントを発表する**)**
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**: 36**
管理を実装する際にリスク所有者からの意見を得る最も重要な理由はどれですか?
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. リスクを許容できるレベルに管理する
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**: 37**
頻繁に発生するインシデントをユーザーの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最善の方法は、次の内容を含めることです。
A. 退職面談の結果。
B. 以前のトレーニング セッション。

C. ヘルプデスクリクエストの例。
D. セキュリティアンケートへの回答。
正解**: (**正解を表示します**)**
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**: 38**
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**: B (**コメントを発表する**)**
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**: 39**
新しいアプリケーションが情報セキュリティ ポリシーに準拠していることを確認するための最良のアプローチは次のとおりです。
A. 実装前にアプリケーションのセキュリティを確認します。
B. 開発段階で機能を統合します。
C. 脆弱性分析を実行します。
D. アプリケーションのセキュリティを定期的に監査します。
正解**: B (**コメントを発表する**)**
Performing a vulnerability analysis is the best option to ensure that a new application complies with information security policy because it helps to identify and evaluate any

security flaws or weaknesses in the application that may expose it to potential threats or attacks, and provide recommendations or solutions to mitigate them. Reviewing the security of the application before implementation is not a good option because it may not detect or prevent all security issues that may arise after implementation or deployment. Integrating security functionality at the development stage is not a good option because it may not account for all security requirements or challenges of the application or its environment. Periodically auditing the security of the application is not a good option because it may not address any security issues that may occur between audits or after deployment. 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 /integrating-assurance-functions

質問: **40**
ランサムウェア攻撃が成功した場合の影響を軽減する最善の方法は何ですか?
A. 頻繁にバックアップを実行し、オフラインで保存します。
B. サイバー保険を購入または更新します。
C. 情報セキュリティ予算に身代金を支払うための規定を含めます。
D. ネットワークを監視し、侵入があった場合にアラートを発します。
正解: **(**正解を表示します**)**
Performing frequent backups and storing them offline is the best way to reduce the impact of a successful ransomware attack, as this allows the organization to restore its data and systems without paying the ransom or losing valuable information. Purchasing or renewing cyber insurance policies may help cover some of the costs and losses associated with a ransomware attack, but it does not prevent or mitigate the attack itself.
Including provisions to pay ransoms in the information security budget may encourage more attacks and does not guarantee the recovery of the data or the removal of the malware. Monitoring the network and providing alerts on intrusions may help detect and respond to a ransomware attack, but it does not reduce the impact of a successful attack that has already encrypted or exfiltrated the data. References = CISM Review Manual 2023, page 1661; CISM Review Questions, Answers & Explanations Manual 2023, page 312; CISM Exam Overview - Vinsys3

質問: **41**
情報セキュリティの観点から、技術関連品目の国境を越えた流通に関連する法的問題は、
A. ウェブサイトの取引と課税。
B. ソフトウェア パッチと企業データ。
C. 暗号化ツールと個人データ。
D. 競争と自由貿易の欠如。
正解: **(**正解を表示します**)**

Encryption tools and personal data are the most often associated with legal issues in the context of transborder flow of technology-related items because they involve the protection of privacy and security of individuals and organizations across different jurisdictions, and may be subject to different laws and regulations that govern their access, use, or transfer. Website transactions and taxation are not very often associated with legal issues in this context because they involve the exchange of goods and services and the collection of taxes across different jurisdictions, which may not be directly related to technology transfer or data flow. Software patches and corporate data are not very often associated with legal issues in this context because they involve the maintenance and improvement of software functionality and the management and sharing of business information, which may not be directly related to technology transfer or data flow. Lack of competition and free trade are not very often associated with legal issues in this context because they involve the market structure and trade policies of different jurisdictions, which may not be directly related to technology transfer or data flow. References: https://www.oecd-ilibrary.org/science-and-technology/oecd-declaration-on- transborder-data-flows_230240624407 https://legalinstruments.oecd.org/public/doc/108/108.en.pdf

質問: **42**
情報セキュリティ プログラムを開発する際に組織文化を考慮する最も重要な理由は次のうちどれですか?
A. 組織内の全員が情報セキュリティに責任を負います。
B. セキュリティ インシデントは組織全体に悪影響を及ぼします。
C. 組織がコンプライアンス要件を満たすのに役立ちます。
D. 情報セキュリティ予算の承認を迅速化します。
正解: **A** (コメントを発表する)

質問: **43**
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のに最も役立つのは次のうちどれですか?
A. 検出コントロール
B. 予防的管理
C. ディレクティブ制御
D. 是正制御
正解: **A** (コメントを発表する)

質問: **44**
オフプレミスのクラウド環境に保存されているデータへのアクセス制御を確認する際に、情報セキュリティ マネージャーが主に重点を置くべきは次のどれですか。
A. 組織構造の変更に応じてアクセス制御を見直し、更新する
B. 強力なパスワードポリシーを実装し、定期的なパスワード変更を強制する

C. 職務上必要な個人にのみアクセスを許可する
D. 機密データを保護するための強力な暗号化プロトコルの実装
正解: **(**正解を表示します**)**
The principle of least privilege-ensuring access is granted only to those whose job functions require it-is the primary control for securing data, especially in cloud environments.
"Access to information and systems should be based on the principles of least privilege and need to know, regardless of environment."
- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Access Control Management ISACA's CISM practice questions consistently highlight this principle as central to effective cloud security.

質問: **45**
ある小規模な組織が、多国籍クラウド コンピューティング ベンダーと契約を結んでいます。契約書に記載されていない場合、情報セキュリティ マネージャーにとって最も懸念されるのは次のうちどれでしょうか。
A. 加入者がベンダーの現地監査を実施する権利
B. コードリリースの条件付きソフトウェアコードのエスクロー
C. 加入者がデータへのアクセスを承認する権限
D. 同じ物理サーバー上で加入者のデータを混合する
正解: **(**正解を表示します**)**
The greatest concern to an information security manager if omitted from the contract with a multinational cloud computing vendor would be the authority of the subscriber to approve access to its data. This is because the subscriber's data may be subject to different legal and regulatory requirements in different jurisdictions, and the subscriber may lose control over who can access, process, or disclose its data. The subscriber should have the right to approve or deny access to its data by the vendor or any third parties, and to ensure that the vendor complies with the applicable data protection laws and standards. The authority of the subscriber to approve access to its data is also one of the key elements of the ISACA Cloud Computing Management Audit
/Assurance Program1.
References = CISM Review Manual, 16th Edition eBook2, Chapter 3: Information Security Program Development and Management, Section: Information Security Program Management, Subsection: Cloud Computing, Page 142.

質問: **46**
限定的なランサムウェア インシデントが発生した後に、運用を復旧できる最適な方法はどれですか?
A. 影響評価
B. 信頼性の高いイメージバックアップ

C. 根本原因分析
D. 文書化された根絶手順
正解: **B** (コメントを発表する)

質問: **47**
新たな高度な持続的脅威 (APT) 攻撃者から身を守るための最良の方法はどれですか?
A. インシデント対応チームへの継続的なトレーニングの提供
B. プロアクティブなシステム監視の実装
C. ハニーポット環境の実装
D. 情報セキュリティ啓発資料の更新
正解: (正解を表示します)
= Proactive systems monitoring is the best method to protect against emerging APT actors because it can help detect and respond to anomalous or malicious activities on the network, such as unauthorized access, data exfiltration, malware infection, or command and control communication. Proactive systems monitoring can also help identify the source, scope, and impact of an APT attack, as well as provide evidence for forensic analysis and remediation. Proactive systems monitoring can include tools such as intrusion detection and prevention systems (IDPS), security information and event management (SIEM) systems, network traffic analysis, endpoint detection and response (EDR), and threat intelligence feeds.
References = CISM Review Manual 15th Edition, page 201-2021; CISM Practice Quiz, question 922

質問: **48**
次の要因のうち、情報セキュリティ戦略の目標の実装を成功させる上で最も大きな影響を与えるのはどれですか?
A. 規制要件
B. コンプライアンス承認
C. 経営支援
D. 予算承認
正解: **C** (コメントを発表する)

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: **49**
情報セキュリティ プログラムの有効性にとって最も重要なのは次のどれですか?
A. セキュリティ メトリック
B. 組織文化
C. ITガバナンス
D. リスク管理
正解: **D** (コメントを発表する)
Risk management is the most important factor for the effectiveness of an information security program, as it provides a systematic and consistent approach to identify, assess, treat, and monitor the information security risks that could affect the organization's objectives. Risk management also helps to align the security program with the business strategy, prioritize the security initiatives and resources, and communicate the value of security to the stakeholders.
References = CISM Review Manual 2022, page 3071; CISM Exam Content Outline, Domain 4, Knowledge Statement 4.1

質問: **50**
侵入試行アラートを識別して相関させるために使用する最適なツールは次のどれですか?
A. 脅威分析ソフトウェア
B. ホスト侵入検知システム
C. SIEM
D. ネットワーク侵入検知システム
正解: **C** (コメントを発表する)

Comprehensive and Detailed Step-by-Step Explanation:
Security Information and Event Management (SIEM) systems are designed to collect, analyze, and correlate data from multiple sources, making them the BEST choice for identifying and correlating intrusion attempt alerts.
A). Threat analytics software: While this can provide insights, it is not specialized for real-time correlation and alerting across various platforms.
B). Host intrusion detection system (HIDS): HIDS monitors individual hosts and detects intrusions, but it does not correlate alerts from multiple sources.
C). SIEM: This is the BEST answer because SIEM integrates logs from diverse systems, applies correlation rules, and provides actionable insights into intrusion attempts.
D). Network intrusion detection system (NIDS): While NIDS detects network-level anomalies, it does not correlate alerts from other systems.
Reference: CISM Job Practice Area 3 (Information Security Program Development and Management) discusses tools and techniques for monitoring and detecting security events.

質問**: 51**
バランスト スコアカードは、情報セキュリティを最も効果的に実現します。
A. プロジェクト管理
B. ガバナンス。
C. パフォーマンス。
D. リスク管理。
正解**: (**正解を表示します**)**
A balanced scorecard most effectively enables information security govern-ance. Information security governance 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 managed effectively and efficiently1. A balanced scorecard is a tool for meas-uring and communicating the performance and progress of an organization toward its strategic goals. It typically includes four perspectives: financial, customer, internal pro-cess, and learning and growth2. A balanced scorecard can help information security managers to:
*Align information security objectives with business objectives and communicate them to senior management and other stakeholders
*Monitor and report on the effectiveness and efficiency of information security processes and controls
*Identify and prioritize improvement opportunities and corrective actions
*Demonstrate the value and benefits of information security investments
*Foster a culture of security awareness and continuous learning
Several sources have proposed models or frameworks for applying the balanced scorecard approach to information security governance34 . The other options are not the most effective applications of a balanced scorecard for information security. Pro-ject

management is the process of planning, executing, monitoring, and closing pro-jects to achieve specific objectives within constraints such as time, budget, scope, and quality.
A balanced scorecard can be used to measure the performance of individual projects or project portfolios, but it is not specific to information security projects. Per-formance is the degree to which an organization or a process achieves its objectives or meets its standards. A balanced scorecard can be used to measure the performance of information security processes or functions, but it is not limited to performance measurement.
Risk management is the process of identifying, analyzing, evaluating, treating, monitoring, and communicating risks that affect an organization's objec-tives. A balanced scorecard can be used to measure the risk exposure and risk appetite of an organization, but it is not a tool for risk assessment or treatment.
References: 1: Information Security Governance - ISACA 2: Balanced scorecard - Wikipedia 3: Key Per- formance Indicators for Security Governance Part 1 - ISACA 4: A Strategy Map for Se-curity Leaders:
Applying the Balanced Scorecard Framework to Information Security - Security Intelligence : How to Measure Security From a Governance Perspective - ISA-CA : Project management - Wikipedia : Performance measurement - Wikipedia : Risk management - Wikipedia

質問**: 52**
災害復旧計画 (DRP) を設計する際に、システムの復旧を優先するために、次のどれが必ず利用可能である必要がありますか?
A. ビジネス影響分析 (BIA) の結果
B. 主要業績評価指標 (KPI)
C. 回復手順
D. システムインベントリ
正解**: (**正解を表示します**)**
A business impact analysis (BIA) is a process that identifies and evaluates the potential effects of disruptions to critical business operations as a result of a disaster, accident, emergency, or threat. A BIA helps to determine the business continuity requirements and priorities for recovery of business functions and processes, including their dependencies on IT systems, applications, and data. A BIA also provides information on the financial and operational impacts of a disruption, the recovery time objectives (RTOs), the recovery point objectives (RPOs), and the minimum service levels for each business function and process. A BIA is an essential input for designing a disaster recovery plan (DRP), which is a documented and approved set of procedures and arrangements to enable an organization to respond to a disaster and resume its critical functions within a predetermined timeframe. A DRP must be based on the BIA results to ensure that the system restoration is prioritized according to the business needs and expectations. A DRP must also consider the availability and suitability of the recovery resources, such as backup systems, alternate sites, and personnel. A DRP should be tested and updated

regularly to ensure its effectiveness and alignment with the changing business environment and requirements. References = CISM Review Manual, 15th Edition, pages 175-1761; CISM Review Questions, Answers & Explanations Database, question ID 2182; Working Toward a Managed, Mature Business Continuity Plan - ISACA3; Part Two: Business Continuity and Disaster Recovery Plans - CISM Foundations: Module 4 Course4. A BIA is an important part of Disaster Recovery Planning (DRP). It helps identify the impact of a disruption on the organization, including the critical systems and processes that must be recovered in order to minimize that impact. The BIA results are used to prioritize system restoration and determine the resources needed to get the organization back into operation as quickly as possible.

質問: **53**
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ればよいでしょうか?
A. インシデントが確認されました。
B. インシデントは封じ込められました。
C. 潜在的なインシデントが記録されました。
D. インシデントは軽減されました。
正解: **A (**コメントを発表する**)**
= The information security manager should contact the information owner after the incident has been confirmed, as this is the first step of the incident response process. The information owner is the person who has the authority and responsibility for the information asset that is affected by the incident. The information owner needs to be informed of the incident as soon as possible, as they may have to make decisions or take actions regarding the protection, recovery, or restoration of the information asset. The information owner may also have to communicate with other stakeholders, such as the business units, customers, regulators, or media, depending on the nature and impact of the incident.
The other options are not the correct time to contact the information owner, as they occur later in the incident response process. Contacting the information owner after the incident has been contained, mitigated, or logged may delay the notification and escalation of the incident, as well as the involvement and collaboration of the information owner. Moreover, contacting the information owner after the incident has been contained or mitigated may imply that the incident response team has already taken actions that may affect the information asset without the consent or approval of the information owner. Contacting the information owner after a potential incident has been logged may cause unnecessary alarm or confusion, as the potential incident may not be a real or significant incident, or it may not affect the information owner's asset. References = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 219-220, 226-227.
CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1009.

質問: **54**
情報セキュリティマネージャーがクラウドサービスプロバイダーに関連するセキュリティリスクを評価しています。この評価を行う際に参照すべき最も適切な参考資料は次のうちどれですか？
A. 以前のプロバイダーのサービスレベル契約 (SLA)
B. セキュリティ管理フレームワーク
C. 脅威インテリジェンスレポート
D. プロバイダからの侵入テスト結果
正解: **B (**コメントを発表する**)**
Security control frameworks (e.g., ISO/IEC 27001, NIST SP 800-53, CSA Cloud Controls Matrix) provide a structured and standardized approach to assess the security posture of cloud providers. These frameworks ensure completeness and alignment with best practices.
"Standardized security frameworks enable consistent evaluation of third-party providers and alignment with industry-recognized security requirements."
- CISM Review Manual 15th Edition, Chapter 3: Third-Party Risk Management*
Penetration test results and SLAs are useful, but only frameworks provide comprehensive coverage.

質問: **55**
情報セキュリティ マネージャーが完全機能継続性テストを実施する前に検証する必要がある最も重要な項目はどれですか。
A. 企業によるリスク受容が文書化されている
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ます
D. インシデント対応と復旧計画が簡単な言葉で文書化されている
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: **56**
セキュリティ プログラムを成功させるために最も重要な要件は次のどれですか?
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. 主要システムへの侵入テスト
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: **C** (コメントを発表する)
"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: **57**
情報セキュリティの主な目標は次のどれでしょうか?
A. 情報管理
B. データガバナンス
C. ビジネスの連携
D. 規制遵守
正解: **C** (コメントを発表する)

質問: **58**
サイバーセキュリティインシデント対応の有効性を促進する最も優れたものは次のうちどれですか?
A. セキュリティ情報およびイベント管理 (SIEM) ツールを利用します。
B. 業界をリードするネットワーク侵入テスト ツールを使用します。
C. すべてのインシデント対応関係者とのコミュニケーションを増やす。
D. マルウェア対策ソリューションのシグネチャを継続的に更新します。
正解: (正解を表示します)
Communication is a key factor for the effectiveness of cybersecurity incident response, as it ensures that all relevant parties are informed, coordinated, and aligned on the incident status, impact, actions, and responsibilities. Communication also helps to maintain trust, confidence, and transparency among the stakeholders, such as senior management, business units, customers, regulators, law enforcement, and media. References = CISM Review Manual, 16th Edition, Chapter 5, Section 5.4.2.11

質問: **59**
侵入テストは次のような場合に最も適しています:
A. 新しいシステムがまもなく稼働します。
B. 新しいシステムを設計中です。
C. セキュリティ ポリシーが開発中です。
D. セキュリティインシデントが発生しました。
正解: **A** (コメントを発表する)
= Penetration testing is most appropriate when a new system is about to go live, because it is a method of evaluating the security of a system by simulating an attack from a malicious

source. Penetration testing can help to identify and exploit vulnerabilities, assess the impact and risk of a breach, and provide recommendations for remediation and improvement. Penetration testing can also help to validate the effectiveness of the security controls and policies implemented for the new system, and ensure compliance with relevant standards and regulations. Penetration testing is usually performed after the system has undergone other types of testing, such as functional, performance, and usability testing, and before the system is deployed to the production environment. Penetration testing is not as appropriate when a new system is being designed, because the system is still in the early stages of development and may not have all the features and functionalities implemented. Penetration testing at this stage may not provide a realistic or comprehensive assessment of the system's security, and may cause delays or disruptions in the development process. Penetration testing is also not as appropriate when a security policy is being developed, because the policy is a high-level document that defines the goals, objectives, and principles of information security for the organization. Penetration testing is a technical and operational activity that tests the implementation and enforcement of the policy, not the policy itself. Penetration testing is also not as appropriate when a security incident has occurred, because the incident may have already compromised the system and caused damage or loss. Penetration testing at this stage may not be able to prevent or mitigate the incident, and may interfere with the incident response and recovery efforts. Penetration testing after an incident may be useful for forensic analysis and lessons learned, but it is not the primary or immediate response to an incident. References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 229-230, 233-234.

質問**: 60**
情報セキュリティガバナンスフレームワークの承認の責任者は誰ですか?
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**: (**正解を表示します**)**
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**: 61**

ある組織がバックアップ機能を新しいクラウドベースのソリューションに更新しました。この変更が意図したとおりに機能していることを最も効果的に検証できるテストは次のうちどれですか？
A. シミュレーションテスト
B. ブラックボックステスト
C. 並列テスト
D. テーブルトップテスト
正解: **C** (コメントを発表する)

質問: **62**
決済カードのデータ セキュリティ標準の導入によって得られる最大のメリットは次のどれですか?
A. 業界における情報資産の総合的な保護を実現します。
B. ハッカーによるカード決済に関連した犯罪を抑止します。
C. 各組織におけるサイバーセキュリティへの予算配分を最適化します。
D. より幅広い、より洗練された支払い方法が可能になります。
正解: **A** (コメントを発表する)
The greatest benefit of payment card data security standards is that they drive consistent, industry-wide protection of information assets (A). CISM governance emphasizes that standards such as those for payment cards establish minimum baselines that improve security maturity across the entire ecosystem. They do not eliminate attacks (B), optimize budgets (C), or directly enable new payment methods (D). Instead, they raise the overall level of protection, reduce systemic risk, and support trust in payment systems by ensuring consistent application of fundamental security controls.
References: ISACA CISM Review Manual (Governance-industry standards, baseline security); CISM Exam Content Outline (Domain 2).

質問: **63**
組織が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を統合していることを示す最良の指標は次のどれですか?
A. セキュリティ パフォーマンス メトリックは、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、影響はビジネス損失に応じて測定されます。
C. ビジネス目標が変更されるたびに、セキュリティ ポリシーがレビューされます。
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: **A (**コメントを発表する**)**
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: **64**
IT サービス プロバイダーによる組織の情報セキュリティ要件への準拠を確実にするために、最も役立つのは次のどれですか。
A. ITサービスプロバイダーの外部セキュリティ監査の要求
B. ITサービスプロバイダーからの定期的な報告の要求
C. 社内IT部門との情報セキュリティ要件の定義
D. ITサービスプロバイダーとのビジネス復旧計画の定義
正解: **(**正解を表示します**)**
Requiring regular reporting from the IT service provider is the best way to ensure compliance with the organization's information security requirements, as it allows the organization to monitor the performance, security incidents, service levels, and compliance status of the IT service provider. Reporting also helps to identify any gaps or issues that need to be addressed or resolved. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 184, section 4.3.3.2.

質問: **65**
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: **(**正解を表示します**)**

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: **66**
情報セキュリティ ポリシーの開発に最も影響を与えるのは次のどれでしょうか。
A. ビジネス戦略
B. 過去と現在の脅威
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: **67**
インシデント後レビューを実施する主な目的は次のとおりです。
A. インシデントの影響を再評価します。
B. 脆弱性を特定します。
C. 制御の改善を特定します。
D. 根本原因を特定します。
正解: **D (**コメントを発表する**)**
= 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**: 68**
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 リスク評価を分析します。
B. セキュリティ異常を分析します。
C. 侵入テストの結果を分析します。
D. 脆弱性評価を分析します。
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**: 69**

マルウェアに関連するインシデント発生後のサードパーティによるフォレンジック調査に備えるために、インシデント対応チームは次のことを行う必要があります。
A. 感染したシステムを隔離します。
B. 証拠を保存します。
C. 感染したシステムのイメージを作成します。
D. マルウェアをクリーンアップします。
正解: **B** (コメントを発表する)
According to the CISM Review Manual, the incident response team should preserve the evidence as the first step to prepare for a third-party forensics investigation, as it helps to maintain the integrity and admissibility of the evidence in a court of law. Preserving the evidence may include isolating and imaging the infected systems, but these are not the only actions required. Cleaning the malware may destroy or alter the evidence and should be avoided until the investigation is completed.
References = CISM Review Manual, 27th Edition, Chapter 3, Section 3.6.2, page 165

質問: **70**
Web アプリケーションにログインした後、さまざまなアプリケーション ポイントで追加の認証がチェックされます。このようなアプローチをとる主な理由は次のどれですか。
A. アクセス権が分類要件を満たしていることを確認する
B. Webアプリケーションの可用性を確保する
C. 強力な2要素認証プロトコルをサポートする
D. アプリケーションログの分析を容易にするため
正解: **A** (コメントを発表する)

質問: **71**
次のどれがビジネス影響分析 (BIA) の主な目的ですか?
A. セキュリティの役割と責任を定義する
B. 投資収益率 (ROI) を決定する
C. インシデントの重大度レベルを確立する
D. 情報資産の重要性を判断する
正解: **D** (コメントを発表する)
A business impact analysis (BIA) is a process that identifies and evaluates the potential effects of disruptions to critical business operations as a result of a disaster, accident or emergency. The primary purpose of a BIA is to determine the criticality of information assets and the impact of their unavailability on the organization's mission, objectives and reputation. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 178, section 4.3.2.1.

質問: **72**
標準的なセキュリティ構成を実装する主な目的は何ですか?

A. サポートされていない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します。
B. サポートされていないシステムの管理と監視の運用上の負担を最小限に抑えます。
C. 脆弱性を制御し、構成の変更による脅威を軽減します。
D. サポートされているシステムとサポートされていない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**: 73**
クラウドベースのモデルへの移行を決定する際に、最初に考慮すべき点は次のとおりです。
A. 共有環境でのストレージ。

B. データの可用性。
C. データ分類。
D. データの物理的な場所。
正解: **(**正解を表示します**)**
The first consideration when deciding to move to a cloud-based model should be data classification, because it helps the organization to identify the sensitivity, value, and criticality of the data that will be stored, processed, or transmitted in the cloud. Data classification can help the organization to determine the appropriate level of protection, encryption, and access control for the data, and to comply with the relevant legal, regulatory, and contractual requirements. Data classification can also help the organization to evaluate the suitability, compatibility, and trustworthiness of the cloud service provider and the cloud service model, and to negotiate the terms and conditions of the cloud service contract.
Storage in a shared environment, availability of the data, and physical location of the data are all important considerations when deciding to move to a cloud-based model, but they are not the first consideration. Storage in a shared environment can affect the security, privacy, and integrity of the data, as the data may be co- located with other customers' data, and may be subject to unauthorized access, modification, or deletion.
Availability of the data can affect the reliability, performance, and continuity of the data, as the data may be inaccessible, corrupted, or lost due to network failures, service outages, or disasters. Physical location of the data can affect the compliance, sovereignty, and jurisdiction of the data, as the data may be stored or transferred across different countries or regions, and may be subject to different laws, regulations, or policies.
However, these considerations depend on the data classification, as different types of data may have different levels of risk, impact, and expectation in the cloud environment.
References = ISACA, CISM Review Manual, 16th Edition, 2020, pages 95-96, 99-100, 103-104, 107-108.
ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1031.

質問: **74**
新しく導入されたセキュリティ意識向上プログラムが効果的であったことを示す最良の証拠は次のどれですか?
A. 各部門の従業員は必要な研修を完了しました。
B. トレーニング開始以来、フィッシング攻撃が成功したという報告はありません。
C. 上級管理職は、継続的な意識啓発トレーニングへの資金提供をサポートしています。
D. フィッシング攻撃の報告件数が増加しています。
正解: **(**正解を表示します**)**

質問: **75**

情報セキュリティ マネージャーは、エンドポイント デバイスの侵害について通知を受けました。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 デバイスをワイプしてリセットします。
B. エンドポイントデバイスを分離します。
C. エンドポイントデバイスの電源をオフにします。
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: **76**
ある部門から、セキュリティ対策がもはや効果的ではないとの報告がありました。情報セキュリティ管理者にとって最善の対応策は次のどれですか？
A. 制御状態を評価します。
B. コントロールを置き換えます。
C. 管理者に障害を報告します。

D. 多層防御をチェックします。
正解: **A** (コメントを発表する)
Upon learning a control is ineffective, the first action should be to assess the state of the control to verify the issue, determine its root cause, and assess the risk exposure. The CISM Review Manual emphasizes that assessment comes before taking further steps like replacement or escalation, as it informs appropriate, risk- based action.
Reference:ISACA CISM Review Manual, 16th Edition, Page 131-132, "Control Assessment and Continuous Improvement".

質問: **77**
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情報を本社に報告し、広範囲に分散した事象に対して統一された対応を行えるようにしたいと考えています。これらの目的を最もよく達成できるのは、次のうちどれでしょうか。
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. アウトソーシングされたインシデント対応チーム
D. 集中型インシデント対応チーム
正解: (正解を表示します)
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: **78**
組織の情報セキュリティ戦略を策定する際に、どこに重点を置くべきかを理解するのに最も役立つのは次のどれですか。
A. ギャップ分析
B. プロジェクト計画

C. 脆弱性評価
D. ビジネス影響分析 (BIA)
正解**: (**正解を表示します**)**
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**: 79**
組織の情報セキュリティ プログラムの有効性を最もよく理解できる結果は次のうちどれですか。
A. セキュリティスポットチェック
B. 内部監査
C. エンタープライズリスク評価
D. 統制自己評価(CSA)
正解**: (**正解を表示します**)**
Control self-assessments (CSAs) (D) best provide an understanding of the effectiveness of an organization's information security program because they focus specifically on whether security controls are operating as intended on an ongoing basis. In CISM, program effectiveness is measured not only by design adequacy, but by consistent execution and performance of controls across the organization.
CSAs enable control owners and business stakeholders to evaluate control implementation, identify weaknesses, and report effectiveness in a structured and repeatable manner. This provides management with broad, timely, and actionable insight into how well the security program is functioning day to day. Internal audits (B) offer independent assurance but are typically periodic and retrospective. Enterprise risk assessments (C) focus on identifying and prioritizing risks, not on validating control performance. Security spot checks (A) are limited in scope and do not provide a comprehensive program view.

CISM emphasizes that effective security programs rely on continuous monitoring and self-assessment mechanisms to demonstrate control effectiveness, support improvement, and inform governance reporting.
References:
ISACA CISM Review Manual, Information Security Program Development and Management - monitoring, measurement, and control effectiveness ISACA CISM Exam Content Outline, Domain 3: Information Security Program Development and Management

質問: **80**
情報セキュリティ マネージャーが上級管理職に対して情報セキュリティとリスク プログラムの有効性を証明するために最も効果的な方法は次のとおりです。
A. 監査レポート
B. リスク評価を更新しました
C. 情報セキュリティインシデントの発生件数
D. 月次メトリクス
正解: **(**正解を表示します**)**

質問: **81**
外部セキュリティ監査で、コントロールの不遵守が複数報告されました。情報セキュリティ マネージャーが上級管理職に伝える上で最も重要なのは次のうちどれですか。
A. 根本原因分析に基づく所有者の対応を管理する
B. コンプライアンス違反が組織のリスクプロファイルに与える影響
C. 是正活動を開始するための非コンプライアンスレポート
D. リスク移転のビジネスケース
正解: **(**正解を表示します**)**
The impact of noncompliance on the organization's risk profile is the MOST important information for the information security manager to communicate to senior management, because it helps them understand the potential consequences of not adhering to the established controls and the need for corrective actions.
Noncompliance may expose the organization to increased threats, vulnerabilities, and losses, as well as legal, regulatory, and contractual liabilities.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 84: "The information security manager should report on information security risk, including noncompliance and changes in information risk, to key stakeholders to facilitate the risk management decision-making process." CISM Review Manual, 16th Edition, ISACA, 2020, p. 85: "Noncompliance with information security policies, standards, and procedures may result in increased threats, vulnerabilities, and losses, as well as legal, regulatory, and contractual liabilities for the enterprise."

質問: **82**

サイバーセキュリティ インシデント発生時に適切な関係者が意思決定を行うために重要なのは次のどれですか。
A. ステークホルダー計画
B. エスカレーション計画
C. 最新のリスク登録簿
D. 資産分類
正解: **(**正解を表示します**)**
Comprehensive and Detailed Step-by-Step Explanation:
During a cybersecurity incident, it is vital to ensure that the right people are involved and that decision- making occurs promptly.
* A. Stakeholder plan: While identifying stakeholders is important, it does not outline decision-making during an incident.
* B. Escalation plan: This is the BEST answer because it specifies how incidents are escalated to the appropriate level of authority, ensuring timely and effective decisions.
* C. Up-to-date risk register: Although useful for understanding risks, it does not facilitate decision- making in real-time incidents.
* D. Asset classification: This helps identify critical assets but does not address decision-making protocols during an incident.
Reference: CISM Job Practice Area 4 (Information Security Incident Management) highlights the importance of escalation procedures to manage incidents efficiently.

質問: **83**
組織の情報セキュリティのビジョンと戦略をサポートするのに最適な情報源は次のどれですか?
A. 能力成熟度モデル
B. メトリクスダッシュボード
C. エンタープライズ情報セキュリティアーキテクチャ
D. ガバナンスポリシー
正解: **(**正解を表示します**)**

質問: **84**
組織の情報セキュリティ ポリシーを確立する際に、最も重要な考慮事項は次のどれですか。
A. 職務記述書には、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. 上級管理職がポリシーを支持します。
D. 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**: 85**
情報セキュリティ文化が成功していることを示す最良の指標は次のどれですか?
A. 侵入テストは定期的に実行され、発見された問題は修正されます。
B. エンドユーザーはインシデントを識別して報告する方法を知っています。
C. 個人には職務に基づいて役割が与えられます。
D. 情報セキュリティに割り当てられた予算は十分です。
正解**: (**正解を表示します**)**
The best indication of a successful information security culture is that end users know how to identify and report incidents. This shows that the end users are aware of the information security policies, procedures, and practices of the organization, and that they understand their roles and responsibilities in protecting the information assets and resources. It also shows that the end users are engaged and committed to the information security goals and objectives of the organization, and that they are willing to cooperate and collaborate with the information security team and other stakeholders in preventing, detecting, and responding to information security incidents. A successful information security culture is

one that fosters a positive attitude and behavior toward information security among all members of the organization, and that aligns the information security strategy with the business strategy and the organizational culture1.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:
Information Security Culture, page 281.

質問: **86**
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援を得る
C. 主要リスク指標 (KRI) の特定をサポートする
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: **87**
情報セキュリティ アーキテクチャを実装する最も適切な理由は次のうちどれですか?
A. 情報セキュリティ コンポーネントの展開を迅速化します。
B. 展開後の情報セキュリティ ロードマップとして機能します。
C. セキュリティ要件の一貫した実装を容易にします。
D. 統合の費用対効果を評価します。
正解: **(**正解を表示します**)**

質問: **88**
重大な情報セキュリティインシデントの発生後、情報セキュリティ管理者が是正措置を決定するのに最も役立つのは次のどれですか?
A. インシデントのコストを計算する
B. 事後評価の実施
C. 影響分析の実行
D. 証拠の保存
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**: 89**
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の主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が優先されます
B. 情報セキュリティガイドラインは企業全体に伝達されている_
C. 組織は規制要件に準拠し続けます。
D. ビジネスリスクは許容できるレベルに管理されています。
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: **90**
次のイベントのうち、組織が情報セキュリティ フレームワークを再検討する必要が生じる可能性が最も高いのはどれですか。
A. ITが提供する新しいサービス
B. リスク環境の変化
C. 最近のサイバーセキュリティ攻撃
D. 実装された新しい技術
正解: **(正解を表示します)**
Changes to the risk landscape are the most likely events to require an organization to revisit its information security framework, because they may affect the organization's risk appetite, risk tolerance, risk profile, and risk treatment strategies. The information security framework should be aligned with the organization's business objectives and risk management approach, and should be reviewed and updated regularly to reflect the changing internal and external environment.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 35: "The information security framework should be reviewed and updated regularly to ensure that it remains aligned with the enterprise's business objectives and risk management approach and reflects the changing internal and external environment." CISM Review Manual, 16th Edition, ISACA, 2020, p. 36: "Changes in the risk landscape may require the enterprise to revisit its risk appetite, risk tolerance, risk profile, and risk treatment strategies."

質問: **91**
新しいソフトウェア アプリケーションの開発効率を向上させるには、セキュリティ要件を定義する必要があります。
A. コードレビューに基づく。
B. 利用可能なセキュリティ評価ツールに基づきます。
C. 機能要件を満たした後。
D. 他の要件と同時に。
正解: **(正解を表示します)**
Security requirements should be defined concurrently with other requirements to ensure that security is built into the software development process from the beginning and not added as an afterthought. This will also improve the efficiency of the development process by reducing the need for rework and testing. Security requirements should be based on the business objectives, risk assessment, and security policies of the organization, not on code review, security assessment tools, or functional requirements. References = CISM Review Manual 15th Edition, page 1241; CISM Item Development Guide, page 62

質問: **92**
組織のシステムへのサイバー攻撃を可能にするバックドアが確認されました。ソフトウェア開発ライフサイクルに以下のどれを統合すれば、組織は将来同様の攻撃を最も効果的に軽減できるでしょうか？
A. 強化されたユーザー受け入れテスト (UAT)
B. 職務の分離
C. カスタマイズされた開発者トレーニング
D. 脆弱性テスト
正解: **(**正解を表示します**)**
Integrating vulnerability testing (D) into the SDLC is the most effective way to identify backdoors and security weaknesses before deployment. CISM emphasizes secure development practices, including testing and validation, as essential controls. UAT (A) focuses on functionality, separation of duties (B) addresses governance, and training (C) is supportive but insufficient on its own. Vulnerability testing provides direct detection of exploitable flaws.
References: ISACA CISM Review Manual (Program management-secure SDLC practices); CISM Exam Content Outline (Domain 3).

質問: **93**
複数の店舗を持つ小売業者に新しく任命された情報セキュリティ マネージャーは、HVAC (暖房、換気、空調) ベンダーが店舗にリモート アクセスしてリアルタイムの監視と機器診断を行えることを発見しました。情報セキュリティ マネージャーが最初に取るべき行動は次のどれですか。
A. ベンダーの侵入テストを実施します。
B. ベンダーの技術的セキュリティ管理を確認する
C. ベンダー契約を確認する
D. リアルタイムアクセスを切断する
正解: **(**正解を表示します**)**
Reviewing the vendor contract should be the information security manager's first course of action when discovering an HVAC vendor has remote access to the stores to enable real-time monitoring and equipment diagnostics. The vendor contract should specify the terms and conditions of the vendor's access to the retailer' s network, such as the scope,

purpose, duration, frequency, and method of access. The vendor contract should also define the roles and responsibilities of both parties regarding security, privacy, compliance, liability, and incident response. Reviewing the vendor contract will help the information security manager to understand the contractual obligations and expectations of both parties, and to identify any gaps or issues that need to be addressed or resolved1. The other options are not the first course of action for the information security manager when discovering an HVAC vendor has remote access to the stores. Conducting a penetration test of the vendor may be a useful way to assess the vendor's security posture and potential vulnerabilities, but it should be done with the vendor's consent and cooperation, and after reviewing the vendor contract2.
Reviewing the vendor's technical security controls may be a necessary step to verify the vendor's compliance with security standards and best practices, but it should be done after reviewing the vendor contract and in accordance with the agreed-upon audit procedures3. Disconnecting the real-time access may be a drastic measure that could disrupt the vendor's service delivery and violate the vendor contract, unless there is a clear and imminent threat or breach that warrants such action. References: 1: Vendor Access: Addressing the Security Challenge with Urgency - BeyondTrust 2: Penetration Testing - NIST 3: Reduce Risk from Third Party Access | BeyondTrust : Third-Party Vendor Security Risk Management & Prevention

質問**: 94**
ビジネスでは、アプリケーションのレガシー バージョンを運用する必要がありますが、アプリケーションにパッチを適用できません。ビジネスへのリスクの露出を制限するために、レガシー アプリケーションの前面にファイアウォールが実装されています。どのリスク処理オプションが適用されていますか?
A. 軽減
B. 受け入れる
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: **95**
ある組織が、パブリック クラウド サービス プロバイダーとインシデント対応能力を調整しています。情報セキュリティ マネージャーの最初の行動方針は何でしょうか?
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します。
B. プロバイダーの監査ログと監視制御を評価します。
C. プロバイダーのインシデント定義と通知基準を確認します。
D. インシデントのエスカレーション プロセスを更新します。
正解: **(**正解を表示します**)**
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: **96**
ある組織が新興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考慮すべき最も重要な項目は次のうちどれですか？
A. 技術の脆弱性
B. 安全な構成
C. システムの互換性
D. 技術に関する業界レビュー
正解: **(**正解を表示します**)**

質問: **97**
重大な影響を及ぼす新しい規制が間もなく施行されると知らされた場合、グローバル情報セキュリティ マネージャーはまず何をすべきでしょうか?
A. ギャップ分析を実行します。
B. ビジネス影響分析 (BIA) を実行します。
C. 脆弱性評価を実行します。
D. プライバシー影響評価 (PIA) を実行します。
正解: **(**正解を表示します**)**

質問: **98**
情報セキュリティ プログラムの有効性について取締役会に報告する最良の方法は、次の事項を提示することです。
A. 同業他社の業界ベンチマーク。
B. 主要なパフォーマンス メトリックを示すダッシュボード。
C. プロセス改善によるコスト削減のレポート。
D. 最新の監査結果の要約。
正解: **B (**コメントを発表する**)**

質問: **99**
組織がセキュリティ インシデントが発生したことを影響を受ける関係者に通知する最も重要な理由はどれですか。
A. 情報セキュリティ意識の向上
B. 事件の根本原因を明らかにする
C. 組織に対する好意を高める
D. 通知に関する規制を遵守するため
正解: **(**正解を表示します**)**
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: **100**
新しいシステムの実装中に、中断、不正な変更、エラーの可能性を積極的に最小限に抑えるプロセスは次のどれですか。
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**: C (**コメントを発表する**)**
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**: 101**
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 マネージャーが次に行うべきことは何ですか?
A. 経営委員会から戦略に関する合意を得る。
B. ビジネス目標との整合性を確認します。
C. 組織のリスク許容度を定義します。
D. 戦略を実行するためのプロジェクト計画を策定します。
正解**: D (**コメントを発表する**)**
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**: 102**
セキュリティ基準への非準拠が特定された場合、情報セキュリティ管理者が最初に行うべきことは何ですか?

A. 非準拠を検証します。
B. 上級管理職に違反を報告します。
C. 非コンプライアンスをリスク レジスタに含めます。
D. 非準拠を軽減するための補償制御を実装します。
正解: **A** (コメントを発表する)

質問: **103**
許容可能なリスク レベルを決定する際に、次のうち最も重要な考慮事項はどれですか。
A. 脅威プロファイル
B. システムの重要度
C. 脆弱性スコア
D. リスクマトリックス
正解: **C** (コメントを発表する)
The effectiveness of an incident response team will be greatest when the incident response process is updated based on lessons learned. This ensures that the team can continuously improve its performance and capabilities, and address any gaps or weaknesses identified during previous incidents. Updating the incident response process based on lessons learned also helps to align the process with the changing business and security environment, and to incorporate best practices and standards. Meeting on a regular basis to review log files, having trained security personnel as team members, and using a security information and event monitoring (SIEM) system are all important factors for an incident response team, but they are not sufficient to ensure the effectiveness of the team. Reviewing log files may help to detect and analyze incidents, but it does not guarantee that the team can respond appropriately and efficiently. Having trained security personnel may enhance the skills and knowledge of the team, but it does not ensure that the team can work collaboratively and communicate effectively. Using a SIEM system may facilitate the identification and prioritization of incidents, but it does not ensure that the team can follow the established procedures and protocols. References = CISM Review Manual, 16th Edition, page 1361; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1492

質問: **104**
組織がインシデント対応チームが適切に準備されていることを確認するための最良の方法はどれですか?
A. サードパーティのフォレンジック会社によるトレーニングの提供
B. 対応チームの業界認定の取得
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: (正解を表示します)

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**: 105**
情報セキュリティ プログラムの成功にとって最も重要な要素は次のどれですか?
A. 情報セキュリティのための包括的なリスク評価プログラム
B. 情報セキュリティ管理者のビジネスに関する知識
C. 適切な訓練を受け、十分なリソースを備えたセキュリティスタッフ
D. 継続的な監査と未解決の項目への対処
正解**: B (**コメントを発表する**)**
The explanation given in the manual is:
The information security manager's knowledge of the business is the most critical factor for information security program success because it enables him or her to align security objectives with business goals and communicate effectively with senior management and other stakeholders. The other choices are important elements of an information security program but not as critical as the information security manager's knowledge of the business.
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.
An information security manager is a professional who oversees and coordinates the implementation and maintenance of an information security program. An information security manager should have a good understanding of the business environment, culture,

strategy, processes, and needs of an organization to ensure that security supports its objectives.

質問: **106**
組織全体で報告される情報セキュリティ インシデントを文書化する最も重要な理由はどれですか?
A. 軽減されていないリスクを特定します。
B. セキュリティに対するビジネス投資をサポートします。
C. インシデントの再発を防ぐ。
D. 組織のセキュリティ体制を評価します。
正解: **(**正解を表示します**)**

質問: **107**
回復時間目標 (RTO) は、次の要素によって最もよく決定されます。
A. ビジネスマネージャー
B. 事業継続責任者
C. 経営管理
D. データベース管理者 (DBA)。
正解: **(**正解を表示します**)**
Business managers are best suited to determine the recovery time objectives (RTOs) for their business processes and functions, as they have the knowledge and authority to assess the impact of downtime and the acceptable level of service continuity. RTOs are the maximum acceptable time that a business process or function can be disrupted before it causes significant harm to the organization's objectives, reputation, or compliance. References = CISM Review Manual, 16th Edition, Chapter 5, Section 5.2.1.11

質問: **108**
組織は情報セキュリティ ガバナンス フレームワークを実装しています。プログラムの有効性を関係者に伝えるには、次の事項を確立することが最も重要です。
A. 制御自己評価 (CSA) プロセス。
B. 利害関係者への自動レポート。

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メトリック。
正解: **(**正解を表示します**)**
= 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: **109**
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に、情報セキュリティ マネージャーが取る最も重要な行動はどれですか。
A. エスカレーション プロセスに従います。
B. 侵害の兆候を特定します。
C. 法執行機関に通報します。
D. 法医学調査員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: **110**
効果的な情報セキュリティ プログラムを確立するための最初のステップは次のどれですか?
A. コンプライアンスレビューを実施します。
B. 説明責任を割り当てます。
C. ビジネス影響分析 (BIA) を実行します。
D. ビジネスケースを作成します。
正解: **(正解を表示します)**
According to the CISM Review Manual, the first step to establishing an effective information security program is to create a business case that aligns the program objectives with the organization's goals and strategies. A business case provides the rationale and justification for the information security program and helps to secure the necessary resources and support from senior management and other stakeholders. A business case should include the following elements:

The scope and objectives of the information security program
The current state of information security in the organization and the gap analysis The benefits and value proposition of the information security program The risks and challenges of the information security program The estimated costs and resources of the information security program The expected outcomes and performance indicators of the information security program The implementation plan and timeline of the information security program References = CISM Review Manual, 16th Edition, Chapter 3, Section 2, pages 97-99.

質問: **111**
インシデントを認識できるようにサービスデスクスタッフをトレーニングすることの主な利点は次のどれですか?
A. インシデント対応計画をタイムリーに実行できます。
B. インシデントメトリックを伝達できます。
C. リスク対応オプションを迅速に特定できます。
D. インシデント分類時間を改善できます。
正解: **(**正解を表示します**)**
The service desk is often the first point of contact for users. If trained properly, they can quickly recognize signs of an incident and escalate it, triggering the incident response process promptly.
This early detection and escalation are essential for minimizing damage and response time.
"Training frontline support staff ensures timely detection and escalation of incidents, which is critical for effective containment."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Roles and Responsibilities*

質問: **112**
セキュリティ重視の文化を構築する際に最も重要な考慮事項は次のどれですか?
A. 同業他社と比較した現在のセキュリティ戦略ベンチマーク
B. 情報セキュリティに関する地域の規則と法律
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、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).

質問: **113**
インシデント対応の有効性の評価を最もよくサポートするプロセスは次のどれですか?
A. 根本原因分析
B. インシデント後のレビュー
C. 保管の連鎖
D. インシデントログ
正解: **(**正解を表示します**)**
A post-incident review (PIR) is the process of evaluating the effectiveness of the incident response after the incident has been resolved. A PIR aims to identify the strengths and weaknesses of the response process, the root causes and impacts of the incident, the lessons learned and best practices, and the recommendations and action plans for improvement1. A PIR can help an organization enhance its incident response capabilities, reduce the likelihood and severity of future incidents, and increase its resilience and maturity2.
A PIR is the best process to support the evaluation of incident response effectiveness, because it provides a systematic and comprehensive way to assess the performance and outcomes of the response process, and to identify and implement the necessary changes and improvements. A PIR involves collecting and analyzing relevant data and feedback from various sources, such as incident logs, reports, evidence, metrics, surveys, interviews, and observations. A PIR also involves comparing the actual response with the expected or planned response, and measuring the achievement of the response objectives and the satisfaction of the stakeholders3.
A PIR also involves documenting and communicating the findings, conclusions, and recommendations of the evaluation, and ensuring that they are followed up and implemented.
The other options are not as good as a PIR in supporting the evaluation of incident response effectiveness, because they are either more specific, limited, or dependent on a PIR. A root cause analysis (RCA) is a technique to identify the underlying factors or reasons that caused the incident, and to prevent or mitigate their recurrence. An RCA can help an organization understand the nature and origin of the incident, and to address the problem at its source, rather than its symptoms. However, an RCA is not sufficient to evaluate the effectiveness of the response process, because it does not cover other aspects, such as the response performance, outcomes, impacts, lessons, and best practices. An RCA is usually a part of a PIR, rather than a separate process. A chain of custody (CoC) is a process of maintaining and documenting the integrity and security of the evidence collected during the incident response. A CoC can help an organization ensure that the evidence is reliable, authentic, and admissible in legal or regulatory proceedings. However, a CoC is not a process to evaluate the effectiveness of the

response process, but rather a requirement or a standard to follow during the response process. A CoC does not provide any feedback or analysis on the response performance, outcomes, impacts, lessons, or best practices. An incident logging is a process of recording and tracking the details and activities of the incident response. An incident logging can help an organization monitor and manage the response process, and to provide an audit trail and a source of information for the evaluation.
However, an incident logging is not a process to evaluate the effectiveness of the response process, but rather an input or a tool for the evaluation. An incident logging does not provide any assessment or measurement on the response performance, outcomes, impacts, lessons, or best practices. References = 1: CISM Review Manual 15th Edition, Chapter 5, Section 5.5 2: Post-Incident Review: A Guide to Effective Incident Response 3: Post-Incident Review: A Guide to Effective Incident Response : CISM Review Manual 15th Edition, Chapter 5, Section 5.5 : CISM Review Manual 15th Edition, Chapter 5, Section 5.5 : CISM Review Manual 15th Edition, Chapter 5, Section 5.4 : CISM Review Manual 15th Edition, Chapter 5, Section 5.3

質問**: 114**
インシデント対応計画をタイムリーに実行するのに最も効果的なのは次のどれですか?
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**: (**正解を表示します**)**
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**: 115**
コンピューティング設備の共有代替場所を選択する際に考慮すべき最も重要なのは次のどれですか?

A. 組織のリスク許容度
B. 組織の使命
C. リソースの可用性
D. インシデント対応チームのトレーニング
正解: **(**正解を表示します**)**
The organization's risk tolerance is the most important factor to consider when choosing a shared alternate location for computing facilities, as it determines the acceptable level of risk exposure and the required recovery time objective (RTO) for the organization. A shared alternate location is a facility that is used by multiple organizations for disaster recovery purposes, and it may have limited resources, availability, and security. Therefore, the organization must assess its risk tolerance and ensure that the shared alternate location can meet its recovery requirements and protect its information assets.
References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.3.2, page 2291; CISM Online Review Course, Module 4, Lesson 3, Topic 22; BCMpedia, Alternate Site3

質問: **116**
事業継続計画 (BCP) を策定する際に最初に行うべきことはどれですか?
A. 組織戦略を定義します。
B. 現在の回復ポリシーを確認します。
C. 重要なプロセスに優先順位を付けます。
D. 既存のサイバー保険の補償範囲を確認します。
正解: **(**正解を表示します**)**

質問: **117**
情報セキュリティガバナンスフレームワークを実装する際に最初に確立する必要があるの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: **A (**コメントを発表する**)**
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: **118**
重要なビジネス アプリケーションの可用性を妨げる可能性のある脆弱性の導入を防ぐのに最も効果的なのは次のうちどれですか。
A. パッチ管理プロセス
B. バージョン管理
C. 変更管理コントロール
D. 論理アクセス制御
正解: **(**正解を表示します**)**
= Change management controls are the most effective in preventing the introduction of vulnerabilities that may disrupt the availability of a critical business application. Change management controls are the policies, procedures, and practices that govern the initiation, approval, implementation, testing, and documentation of changes to the information systems and infrastructure. Change management controls help to ensure that changes are authorized, planned, controlled, and monitored, and that they do not introduce any unintended or adverse effects on the security, functionality, performance, or reliability of the system or application. Change management controls also help to identify and mitigate any potential risks or issues that may arise from the changes, and to ensure that the changes are aligned with the business objectives and requirements. By implementing change management controls, the organization can prevent the introduction of vulnerabilities that may disrupt the availability of a critical business application, as well as enhance the quality and efficiency of the change process. References = CISM Review Manual 15th Edition, page 105, page 106.

質問: **119**
組織の情報資産を一貫して保護するために必要なのは次のうちどれですか?
A. 分類モデル
B. 制御評価
C. データの所有権
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**: 120**
取締役会への月次情報セキュリティレポートに含めることが最も重要なのは次のどれですか?
A. セキュリティ指標の傾向分析
B. リスク評価結果
C. セキュリティインシデントの根本原因分析
D. 脅威情報
正解**: (**正解を表示します**)**
The most important information to include in monthly information security reports to the board is the trend analysis of security metrics. Security metrics are quantitative and qualitative measures that indicate the performance and effectiveness of the information security program and the alignment with the business objectives. Trend analysis is the process of comparing and evaluating the changes and patterns of security metrics over time. Trend analysis can help to identify the strengths and weaknesses of the information security program, the progress and achievements of the security goals and initiatives, the gaps and opportunities for improvement, and the impact and value of the information security investments. Trend analysis can also help to communicate the current and future security risks and challenges, and the recommended actions and strategies to address them. Trend analysis can provide the board with a clear and concise overview of the information security status and direction, and enable informed and timely decision making. References =
* CISM Review Manual 15th Edition, page 1631
* The CISO's Guide to Reporting Cybersecurity to the Board2
* CISM 2020: Information Security Metrics and Reporting, video 13

質問: **121**
組織は、第三者が重要な機能を別の外部プロバイダーにアウトソーシングしていることを知りました。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次のどれですか。
A. サードパーティの外部プロバイダーの独立した監査を実施します。
B. 第三者との契約を解除することをお勧めします。
C. サードパーティと外部プロバイダーとの契約を評価します。
D. 契約した第三者の外部監査を実施します。
正解: **(**正解を表示します**)**
According to the CISM Review Manual, the information security manager should evaluate the third party's agreements with its external provider to ensure that the security requirements and controls are adequate and consistent with the organization's expectations. Engaging or conducting an audit may be a subsequent step, but not the most important one. Recommending canceling the contract may be premature and impractical. References = CISM Review Manual, 27th Edition, Chapter 3, Section 3.4.2, page 1431.

質問: **122**
組織の環境の変化により、セキュリティ制御が適切でなくなる可能性があります。情報セキュリティ マネージャーの最善の行動方針は何でしょうか?
A. これまでのリスク評価と対策を確認します。
B. 新たなリスク評価を実施し、
C. 新たなリスクを軽減するための対策を評価します。
D. 新たなリスクを第三者に移転します。
正解: **(**正解を表示します**)**
According to the CISM Review Manual, the information security manager's best course of action when security controls may no longer be adequate due to changes in the organization's environment is to perform a new risk assessment. A risk assessment is a process of identifying, analyzing, and evaluating the risks that affect the organization's information assets and business processes. A risk assessment should be performed periodically or whenever there are significant changes in the organization's environment, such as new threats, vulnerabilities, technologies, regulations, or business objectives. A

risk assessment helps to determine the current level of risk exposure and the adequacy of existing security controls. A risk assessment also provides the basis for developing or updating the risk treatment plan, which defines the appropriate risk responses, such as implementing new or enhanced security controls, transferring the risk to a third party, accepting the risk, or avoiding the risk.
The other options are not the best course of action in this scenario. Reviewing the previous risk assessment and countermeasures may not reflect the current state of the organization's environment and may not identify new or emerging risks. Evaluating countermeasures to mitigate new risks may be premature without performing a new risk assessment to identify and prioritize the risks. Transferring the new risk to a third party may not be feasible or cost-effective without performing a new risk assessment to evaluate the risk level and the available risk transfer options.
References = CISM Review Manual, 16th Edition, Chapter 2, Section 1, pages 43-45.

質問**: 123**
財務部門のディレクターが組織の予算アプリケーションをアウトソーシングすることを決定し、潜在的なプロバイダーを特定しました。IN 情報セキュリティ マネージャーが最初に開始する必要があるアクションは次のうちどれですか。
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取得する
D. 組織とサービス プロバイダーの統計の役割を一致させます。
正解**: A (**コメントを発表する**)**
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**: 124**
Software as a Service (SaaS) ベンダーの使用に関連するリスクを評価するための最良の方法はどれですか?
A. 情報セキュリティ要件が契約に含まれていることを確認します。
B. ベンダーに顧客参照を要求します。
C. ベンダーに情報セキュリティアンケートの回答を義務付けます。
D. ベンダーの独立管理レポートの結果を確認します。
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: **125**
IT システムに必要な保護レベルを決定するための最適な入力は次のどれですか?
A. 脆弱性評価
B. 脅威分析
C. 内部監査の調査結果
D. 資産分類
正解: **(**正解を表示します**)**

質問: **126**
ランサムウェア攻撃後に組織がデータを回復するのに最適なバックアップの種類はどれですか?
A. オンラインバックアップ
B. 増分バックアップ
C. 差分バックアップ
D. オフラインバックアップ
正解: **(**正解を表示します**)**

Comprehensive and Detailed Step-by-Step Explanation:
Recovering from ransomware requires backups that are unaffected by the ransomware attack. Here's why offline backups are most effective:
A). Online backup: These are connected to the network and may also be compromised during an attack.
B). Incremental backup: While efficient, incremental backups rely on previous backups and are typically stored online, making them vulnerable to ransomware.
C). Differential backup: Similar to incremental backups, these are not immune if stored online or on compromised systems.
D). Offline backup: This is the BEST choice as offline backups are stored in a location that is not connected to the network, preventing ransomware from encrypting them.
Reference: CISM Job Practice Area 4 (Information Security Incident Management) includes guidance on establishing robust backup strategies for recovery.

質問**: 127**
インシデントのエスカレーション プロセスを開発する場合、最も良いアプローチは、次の基準に基づいてインシデントを分類することです。
A. 回復にかかる推定時間。
B. 影響を受ける情報資産。
C. 復旧ポイント目標 (RPO)。
D. 根本的な原因。
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**: 128**
インシデント対応チームの主な機能はどれですか?
A. ビジネス影響分析 (BIA) を提供する
B. 効果的なインシデント軽減策を提供する
C. 重大なインシデントに対する単一の連絡先を提供する
D. ゼロデイ脆弱性のリスク評価を提供する
正解**: (**正解を表示します**)**

質問: **129**
情報セキュリティ戦略の策定において、最も重要なのは誰の意見ですか?
A. プロセスオーナー
B. エンドユーザー
C. セキュリティ アーキテクト。
D. 監査役
正解: **A (**コメントを発表する**)**
Process owners are the people who are responsible for the design, execution, and improvement of the business processes that support the organization's objectives and operations. Process owners have the greatest importance in the development of an information security strategy, as they provide the input and feedback on the business requirements, expectations, and priorities that the information security strategy should address and support. Process owners also help to identify and assess the risks and impacts that the business processes face, and to define and implement the security controls and measures that can mitigate or reduce them.
Process owners also facilitate the alignment and integration of the information security strategy with the business strategy, as well as the communication and collaboration among the various stakeholders and functions involved in the information security program. End users, security architects, and corporate auditors are all important stakeholders in the information security program, but they do not have the greatest importance in the development of an information security strategy. End users are the people who use the information systems and services that the information security program protects and enables. End users provide the input and feedback on the usability, functionality, and performance of the information systems and services, as well as the security awareness and behavior that they exhibit. Security architects are the people who design and implement the security architecture that supports the information security strategy. Security architects provide the input and feedback on the technical requirements, capabilities, and solutions that the information security strategy should leverage and optimize. Corporate auditors are the people who evaluate and verify the compliance and effectiveness of the information security program. Corporate auditors provide the input and feedback on the standards, regulations, and best practices that the information security strategy should follow and adhere to. Therefore, process owners have the greatest importance in the development of an information security strategy, as they provide the input and feedback on the business requirements, expectations, and priorities that the information security strategy should address and support. References = CISM Review Manual 2023, page 31 1; CISM Practice Quiz 2

質問: **130**

情報セキュリティ マネージャーは、ユーザー ワークステーションに必要な最小限のセキュリティ制御の詳細を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どれでしょうか。
A. ガイドライン
B. ポリシー
C. 手順
D. 標準
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: **131**
セキュリティ インシデントの分類方法を開発する場合、カテゴリは次の条件を満たす必要があります。
A. 業界標準に準拠します。
B. インシデント ハンドラーによって作成されます。
C. 合意された定義を持つ。
D. レポート要件に準拠します。
正解: (正解を表示します)
When developing a categorization method for security incidents, the categories must have agreed-upon definitions. This means that the categories should be clear, consistent, and understandable for all the parties involved in the incident response process, such as the incident handlers, the stakeholders, the management, and the external authorities. Having agreed-upon definitions for the categories can help to ensure that the incidents are classified and reported accurately, that the appropriate actions and resources are allocated, and that the communication and coordination are effective. Aligning with industry standards, creating by the incident handler, and aligning with reporting requirements are not mandatory for developing a categorization method for security incidents, although they may be desirable or beneficial depending on the context and objectives of the organization. Aligning with industry standards can help to adopt best practices and benchmarks for incident response, but it may not be feasible or suitable for all types of incidents or organizations. Creating by the incident handler can allow for flexibility and customization of the categories, but it may also introduce inconsistency and ambiguity if the definitions are not shared or agreed upon by others. Aligning with reporting requirements can help to comply with legal or contractual obligations, but it may not cover all the aspects or dimensions of the incidents that need to be categorized. References = CISM Review Manual, 16th Edition, pages 200-2011; CISM Review Questions, Answers & Explanations Manual,
10th Edition, page 822

When developing a categorization method for security incidents, the categories MUST have agreed-upon definitions. This is because having clear and consistent definitions for each category of incidents will help to ensure a common understanding and communication among the incident response team and other stakeholders. It will also facilitate the accurate and timely identification, classification, reporting and analysis of incidents. Having agreed-upon definitions will also help to avoid confusion, ambiguity and inconsistency in the incident management process

質問: **132**
バッファオーバーフローを最もよく表すのは次のどれですか?
A. 関数が処理できる以上のデータで関数が実行される
B. プログラムには、セキュリティ上のリスクをもたらす隠された意図しない機能が含まれています。
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. データをキャプチャする秘密チャネルの一種
正解: **A (**コメントを発表する**)**
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: **133**
組織の侵入検知システム (IDS) のパフォーマンスを確認する際に、最も懸念される傾向は次のどれでしょうか。
A. 誤検出の減少
B. 誤検出の増加
C. 偽陰性の増加
D. 偽陰性の減少
正解: **(**正解を表示します**)**
An increase in false negatives would be of greatest concern when reviewing the performance of an organization's IDSs, because it means that the IDSs are failing to detect and alert on actual attacks that are occurring on the network. False negatives can lead to serious security breaches, data loss, reputational damage, and legal liabilities for the

organization. False positives, on the other hand, are alerts that are triggered by benign or normal activities that are mistaken for attacks. False positives can cause annoyance, inefficiency, and desensitization, but they do not pose a direct threat to the security of the network. Therefore, a decrease in false positives would be desirable, and an increase in false positives would be less concerning than an increase in false negatives.
References = CISM Review Manual, 16th Edition, page 2231; Intrusion Detection Systems | NIST

質問**: 134**
情報セキュリティ戦略を提示する際に上級管理職の支持を得るために最も重要なのは次のどれですか?
A. 戦略は経営陣が許容できるリスクレベルと一致しています。
B. この戦略は、効果のない情報セキュリティ制御に対処します。
C. 戦略は業界のベンチマークと標準に準拠しています。
D. 戦略は、組織の成熟度と脅威の環境に対処します。
正解**: (**正解を表示します**)**
The most important factor to obtain senior leadership support when presenting an information security strategy is that the strategy aligns with management's acceptable level of risk because it ensures that the strategy is consistent and compatible with the organization's risk appetite and thresholds, and reflects management's expectations and priorities for security risk management. The strategy addresses ineffective information security controls is not a very important factor because it does not indicate how the strategy will improve or enhance the security controls or performance. The strategy aligns with industry benchmarks and standards is not a very important factor because it does not indicate how the strategy will differentiate or innovate the organization's security capabilities or practices. The strategy addresses organizational maturity and the threat environment is not a very important factor because it does not indicate how the strategy will advance or adapt the organization's security posture or resilience. 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**: 135**
複数年計画を策定する際に、情報セキュリティ マネージャーが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を確実に実施する
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を拡張できるようにする

D. 毎年の予算増加の予測を示す

正解: **(**正解を表示します**)**

= 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**: 136**
分散型サービス拒否 (DDoS) 攻撃に対する実行可能な封じ込め戦略は次のどれですか?
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. 攻撃者が悪用するファイアウォール 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オフにする
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: **137**
インシデント対応計画を策定する際に、主に考慮すべき事項は次のどれですか?
A. インシデントの定義
B. 規制の遵守
C. 管理サポート
D. 以前に報告されたインシデント
正解: **(**正解を表示します**)**
Management support is the primary consideration when developing an incident response plan, as it is essential for obtaining the necessary resources, authority, and commitment for the plan. Management support also helps to ensure that the plan is aligned with the organization's business objectives, risk appetite, and security strategy, and that it is communicated and enforced across the organization. Management support also facilitates the coordination and collaboration among different stakeholders, such as business units, IT functions, legal, public relations, and external parties, during an incident response.
The definition of an incident (A) is an important component of the incident response plan, as it provides the criteria and thresholds for identifying, classifying, and reporting security incidents. However, the definition of an incident is not the primary consideration, as it is derived from the organization's security policies, standards, and procedures, and may vary depending on the context and impact of the incident.
Compliance with regulations (B) is also an important factor for the incident response plan, as it helps to ensure that the organization meets its legal and contractual obligations, such as notifying the authorities, customers, or partners of a security breach, preserving the evidence, and reporting the incident outcomes.
However, compliance with regulations is not the primary consideration, as it is influenced by the nature and scope of the incident, and the applicable laws and regulations in different jurisdictions.
Previously reported incidents (D) are a valuable source of information and lessons learned for the incident response plan, as they help to identify the common types, causes, and impacts of security incidents, as well as the strengths and weaknesses of the current incident response processes and capabilities. However, previously reported incidents are not the primary consideration, as they are not predictive or comprehensive of the future incidents, and may not reflect the changing threat landscape and business environment.

References = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Plan, page 181-1821 Learn more:

質問: **138**
組織の情報セキュリティの姿勢を最も包括的に理解できるのは次のどれですか?
A. セキュリティ成熟度評価結果
B. 組織環境の脅威分析
C. 脆弱性評価の結果
D. 外部侵入テストの結果
正解: **(正解を表示します)**
A security maturity assessment evaluates not only current vulnerabilities but also governance structures, risk management practices, incident response, and ongoing improvement processes. It provides a holistic and strategic view of the security posture. "Maturity assessments provide a comprehensive evaluation of an organization's security controls and their alignment with business objectives."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Maturity Models* Other methods like penetration tests or vulnerability assessments offer snapshots of technical weaknesses, but they lack strategic depth.

質問: **139**
競合他社がランサムウェア攻撃を受けたことを知った場合、情報セキュリティ管理者が最初に行うべきことは何ですか?
A. 全スタッフを対象にランサムウェア認識トレーニングを実施します。
B. セキュリティ システムの侵害の兆候を更新します。
C. 完全なデータバックアップを実行します。
D. 現在のリスク評価を確認します。
正解: **(正解を表示します)**

質問: **140**
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ために最も役立つの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の証明書
C. 侵入テストレポート
D. 第三者監査レポート
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**: 141**
組織がセキュリティ インシデントを特定して封じ込めるのに最も効果的なのは次のどれですか。
A. リスク評価
B. 脅威モデリング
C. 継続的な監視
D. テーブルトップ演習
正解**: (**正解を表示します**)**
= Continuous monitoring is the process of collecting, analyzing, and reporting on the security status of an organization's information systems and networks. Continuous monitoring enables an organization to identify and contain security incidents by providing timely and accurate information on the security events, alerts, incidents, and threats that may affect the organization. Continuous monitoring also helps to measure the effectiveness and compliance of the security controls, policies, and procedures that are implemented to protect the organization's information assets. Continuous monitoring can be performed using various tools and methods, such as security information and event management (SIEM) tools, intrusion detection and prevention systems (IDS/IPS), vulnerability scanners, log analyzers, and audit trails.
References = CISM Manual1, Chapter 6: Incident Response Planning (IRP), Section 6.2: Continuous Monitoring2
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles 2: 3

質問**: 142**
組織の内部ネットワークの定期的な脆弱性スキャンにより、多くのユーザー ワークステーションにパッチが適用されていないバージョンのソフトウェアがインストールされていることが判明しました。情報セキュリティ マネージャーが上級管理職に関連リスクを理解させる最善の方法は何でしょうか。
A. リスクの影響を通常のメトリックの一部として含めます。
B. セキュリティ運営委員会にレビューを実施することを推奨します。
C. リスク評価を定期的に更新する
D. 上級管理者に定期的な通知を直接送信する
正解**: (**正解を表示します**)**
Including the impact of the risk as part of regular metrics is the best way for the information security manager to help senior management understand the related risk of having many user workstations with unpatched versions of software because it quantifies and

communicates the potential consequences and likelihood of such a risk in terms of business objectives and performance indicators. Recommending the security steering committee conduct a review is not a good way because it does not provide any specific information or analysis about the risk or its impact. Updating the risk assessment at regular intervals is not a good way because it does not ensure that senior management is aware or informed about the risk or its impact. Sending regular notifications directly to senior managers is not a good way because it may be perceived as intrusive or annoying, and may not convey the severity or urgency of the risk or its impact. References: https://www.isaca.
org/resources/isaca-journal/issues/2015/volume-6/measuring-the-value-of-information-security-investments
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/how-to-measure-the-effectiveness-of- your-information-security-management-system

質問**: 143**
AI 開発の要件収集フェーズで医療機関が対処する必要がある最も重要なの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. 計算リソースが不十分
D. データラベル付けの非効率性
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

質問: **144**
ネットワーク インフラストラクチャへのセキュリティ投資について上級管理職の承認を得るのに最も効果的なのは次のうちどれですか。
A. ビジネスの脆弱性を実証するためにネットワークに対する侵入テストを実行する
B. ネットワークのセキュリティのベストプラクティスに関する競合他社のパフォーマンスを強調する
C. 対象を絞ったセキュリティ制御がビジネス目標に結びついていることを実証する
D. 複数のベンダーから比較可能なセキュリティ実装の見積もりを提示する
正解: **(**正解を表示します**)**
The most effective way to gain senior management approval of security investments in network infrastructure is by demonstrating that targeted security controls tie to business objectives.
Security investments should be tied to business objectives and should support the overall goals of the organization. By demonstrating that the security controls will directly support the organization's business objectives, senior management will be more likely to approve the investment.
According to the Certified Information Security Manager (CISM) Study Manual, "To gain senior management's approval for investments in security, it is essential to show how the security controls tie to business objectives and are in support of the overall goals of the organization." While performing penetration tests against the network, highlighting competitor performance, and presenting comparable security implementation estimates from vendors are all useful in presenting the value of security investments, they are not as effective as demonstrating how the security controls will support the organization's business objectives.
Reference:
Certified Information Security Manager (CISM) Study Manual, 15th Edition, Page 305.

質問: **145**
インシデントトリアージの主な目的は次のどれですか?
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: **C (**コメントを発表する**)**
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**: 146**
別の国のクラウド サービス プロバイダーを使用する計画を立てる際に、セキュリティに関して最も重要な考慮事項は次のどれですか。
A. クライアントデータを論理的に分離する機能
B. サービスレベル契約 (SLA) を満たす能力
C. ビジネスの回復力要件を満たす能力
D. 契約上の義務を履行する能力
正解**: (**正解を表示します**)**
When dealing with a provider in another country, the most important consideration is the ability to enforce contractual obligations (D). CISM highlights jurisdictional risk, including differences in laws, regulations, and legal enforcement mechanisms. Logical separation (A), SLAs (B), and resiliency (C) are important but depend on enforceable contracts to be meaningful. Without enforceability, the organization may lack effective recourse in the event of security failures or breaches.
References: ISACA CISM Review Manual (Governance-legal, regulatory, and third-party risk); CISM Exam Content Outline (Domain 2).

質問**: 147**
ビジネス影響分析 (BIA) BEST により、組織は次のことを確立できます。
A. 総所有コスト (TCO)。
B. 復元の優先順位。
C. 年間損失予想値 (ALE)。

D. 回復方法。
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: **148**
次のうち、リスク選好度に基づいてリスク受け入れの決定に責任を負う立場に最も適しているのは誰でしょうか?
A. 情報セキュリティ管理者
B. 最高リスク管理責任者 (CRO)
C. 情報セキュリティ運営委員会
D. リスクオーナー
正解: **D (**コメントを発表する**)**
The risk owner is the best positioned to be accountable for risk acceptance decisions based on risk appetite, because the risk owner is the person or entity with the accountability and authority to manage a risk1. The risk owner is responsible for evaluating the risk level, comparing it with the risk appetite, and deciding whether to accept, avoid, transfer, or mitigate the risk2. The risk owner is also accountable for monitoring and reporting on the risk status and outcomes3. The information security manager, the chief risk officer (CRO), and the information security steering committee may have some roles and responsibilities in the risk management process, but they are not the primary accountable parties for risk acceptance decisions.
References = CISM Review Manual, 16th Edition, page 754; Risk Acceptance

質問: **149**

適切に実装された安全な伝送プロトコルは、トランザクションを保護します。
A. 盗聴から。
B. サービス拒否 (DoS) 攻撃から保護します。
C. クライアントのデスクトップ上。
D. サーバーのデータベース内。
正解: **A (**コメントを発表する**)**
Secure transmission protocols are network protocols that ensure the integrity and security of data transmitted across network connections. The specific network security protocol used depends on the type of protected data and network connection. Each protocol defines the techniques and procedures required to protect the network data from unauthorized or malicious attempts to read or exfiltrate information1. One of the most common threats to network data is eavesdropping, which is the interception and analysis of network traffic by an unauthorized third party. Eavesdropping can compromise the confidentiality, integrity, and availability of network data, and can lead to data breaches, identity theft, fraud, espionage, and sabotage2. Therefore, secure transmission protocols protect transactions from eavesdropping by using encryption, authentication, and integrity mechanisms to prevent unauthorized access and modification of network data. Encryption is the process of transforming data into an unreadable format using a secret key, so that only authorized parties can decrypt and access the data. Authentication is the process of verifying the identity and legitimacy of the parties involved in a network communication, using methods such as passwords, certificates, tokens, or biometrics. Integrity is the process of ensuring that the data has not been altered or corrupted during transmission, using methods such as checksums, hashes, or digital signatures3. Some examples of secure transmission protocols are:
* Secure Sockets Layer (SSL) and Transport Layer Security (TLS), which are widely used protocols for securing web, email, and other application layer communications over the Internet. SSL and TLS use symmetric encryption, asymmetric encryption, and digital certificates to establish secure sessions between clients and servers, and to encrypt and authenticate the data exchanged.
* Internet Protocol Security (IPsec), which is a protocol and algorithm suite that secures data transferred over public networks like the Internet. IPsec operates at the network layer and provides end-to-end security for IP packets. IPsec uses two main protocols: Authentication Header (AH), which provides data integrity and authentication, and Encapsulating Security Payload (ESP), which provides data confidentiality, integrity, and authentication. IPsec also uses two modes: transport mode, which protects the payload of IP packets, and tunnel mode, which protects the entire IP packet.
* Secure Shell (SSH), which is a protocol that allows secure remote login and command execution over insecure networks. SSH uses encryption, authentication, and integrity to protect the data transmitted between a client and a server. SSH also supports port

forwarding, which allows secure tunneling of other network services through SSH connections.
References = 1: 6 Network Security Protocols You Should Know | Cato Networks 2: Eavesdropping Attacks - an overview | ScienceDirect Topics 3: Network Security Protocols - an overview | ScienceDirect Topics : SSL /TLS (Secure Sockets Layer/Transport Layer Security) - Definition : IPsec - Wikipedia : Secure Shell - Wikipedia

質問: **150**
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最も重要な行動はどれですか?
A. 新しい脅威が現実化した場合に組織に与える影響を評価します。
B. 情報に基づいた意思決定ができるよう、直ちに上級管理職に脅威を報告します。
C. 脅威によって悪用される脆弱性についてエンタープライズ アーキテクチャ (EA) を確認します。
D. ログ監視の相関ルールを更新して、発生する可能性のある脅威を検出します。
正解: **(**正解を表示します**)**

質問: **151**
組織内で堅牢な情報セキュリティ文化を構築するために最も重要なのは次のどれですか?
A. 組織全体で成熟した情報セキュリティ意識向上トレーニングを実施
B. 従業員による組織のセキュリティポリシーの遵守の厳格な実施
C. IT環境の開発と運用に組み込まれたセキュリティ管理
D. 情報セキュリティポリシーの上級管理職による承認
正解: **D (**コメントを発表する**)**
= Mature information security awareness training across the organization is the most important factor for building a robust information security culture, because it helps to educate and motivate the employees to understand and adopt the security policies, procedures, and best practices that are aligned with the organizational goals and values. Information security awareness training should be tailored to the specific roles, responsibilities, and needs of the employees, and should cover the relevant topics, such as:
The importance and value of information assets and the potential risks and threats to them The legal, regulatory, and contractual obligations and compliance requirements related to information security The organizational security policies, standards, and guidelines that define the expected and acceptable behaviors and actions regarding information security The security controls and tools that are implemented to protect the information assets and how to use them effectively and efficiently The security incidents and breaches that may occur and how to prevent, detect, report, and respond to them The security best practices and tips that can help to enhance the security posture and culture of the organization

Information security awareness training should be delivered through various methods and channels, such as:
Online courses, webinars, videos, podcasts, and quizzes that are accessible and interactive Classroom sessions, workshops, seminars, and simulations that are engaging and practical Posters, flyers, newsletters, emails, and social media that are informative and catchy Games, competitions, rewards, and recognition that are fun and incentivizing
Information security awareness training should be conducted regularly and updated frequently, to ensure that the employees are aware of the latest security trends, challenges, and solutions, and that they can demonstrate their knowledge and skills in a consistent and effective manner.
Mature information security awareness training can help to create a positive and proactive security culture that fosters trust, collaboration, and innovation among the employees and the organization, and that supports the achievement of the strategic objectives and the mission and vision of the organization.
References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 144-146, 149-150.

質問: **152**
組織の事業部門にセキュリティ制御スイートが正常に実装されたら、情報セキュリティ マネージャーにとって次のことが最も重要になります。
A. 制御パフォーマンスを業界レベルと比較するテストを実行します。
B. コントロールが継続的に有効であるかどうかを定期的にテストします。
C. 関連する事業主に管理権限を引き渡します。
D. 将来のシステム アップグレードに備えてコントロールを適応させる準備をします。
正解: **(**正解を表示します**)**

質問: **153**
組織が新興技術を採用する場合、情報セキュリティ機能の主な責任は次のどれですか?
A. 新しいテクノロジーのためのセキュリティトレーニングの開発
B. 新しいセキュリティ制御の設計
C. 技術の利用規定の作成
D. 潜在的なセキュリティリスクの評価

正解: **D** (コメントを発表する)
The primary responsibility of the information security function when an organization adopts emerging technologies is to assess the potential security risk, which means identifying and evaluating the threats, vulnerabilities, and impacts that the new technologies may pose to the organization's data, systems, and objectives. Assessing the potential security risk helps the information security function to determine the appropriate security requirements, controls, and measures to mitigate the risk and ensure the safe and secure adoption of the emerging technologies.
References = Performing Risk Assessments of Emerging Technologies, CISM Review Manual 15th Edition Learn more:
1. isaca.org2. isaca.org3. niccs.cisa.gov4. venturebeat.com
10of30
An organization is planning to outsource network management to a service provider. Including which of the following in the contract would be the MOST effective way to mitigate information security risk? A.
Requirement for regular information security awareness B. Right-to-audit clause C. Service level agreement (SLA) D. Requirement to comply with corporate security policy answer: (Refer to the Information Security Manager (CISM) documents and learning resources by ISACA available at https://store.isaca.org/s/store#
/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles to verify the answer of the following questions very carefully.) Use the following format please: **Verified Answer** = (From CISM Manual or related resources) **Very Short Explanation** = (From CISM Manual or related resources) **References** = (From CISM Manual or related resources)
==========

質問: **154**
情報セキュリティ投資の資金を獲得するためにビジネス ケースを使用する場合、ビジネス ケースが次の条件を満たすときに最も効果的です。
A. 経営陣の意図と情報セキュリティの指示を明確な言葉で表現します。
B. 情報セキュリティの目標を組織の戦略に合わせて再調整します。
C. 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します。
D. 投資を組織の戦略計画に関連付けます。
正解: (正解を表示します)

質問: **155**
情報セキュリティ マネージャーは、プロセスの非効率性が生じるため、IT 担当者が情報セキュリティ ポリシーを遵守していないことを知りました。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. IT 部門内でユーザー意識向上トレーニングを実施します。
B. IT 部門が情報セキュリティのポリシーと手順を更新することを提案します。

C. ポリシー違反に関連するリスクを判断します。
D. 内部監査にポリシー策定プロセスのレビューを実施するよう依頼する。
正解**: (**正解を表示します**)**
The information security manager should first determine the risk related to noncompliance with the policy, as this will help to understand the impact and likelihood of the policy violation and the potential consequences for the organization. The information security manager can then use the risk assessment results to communicate the importance of the policy to the IT personnel, propose any necessary changes to the policy or the processes, or request an audit of the policy development process, depending on the situation. Conducting user awareness training, updating policies and procedures, or requesting an audit are possible actions that the information security manager can take after determining the risk, but they are not the first step. References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Assessment, page 86; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 59, page 60.

質問**: 156**
潜在的なシステムの脆弱性に対処するための技術的ソリューションのビジネスケースに最も適した入力は次のどれですか?
A. リスク評価
B. ビジネス影響分析 (BIA)
C. 侵入テストの結果
D. 脆弱性スキャン結果
正解**: (**正解を表示します**)**
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**: 157**
大規模なセキュリティ侵害に対応する際に、証拠収集に外部のフォレンジック専門家を関与させる最も重要な理由は次のうちどれですか?
A. 対応チームに証拠取り扱いに関する専門的な訓練を提供する

B. 証拠が社内スタッフに開示されるのを防ぐため
C. 証拠が資格のあるリソースによって処理されるようにするため
D. インシデント対応プロセスを検証する
正解: **C** (コメントを発表する)

質問: **158**
新しい情報セキュリティ マネージャーが組織内の情報セキュリティ ガバナンスの現状を評価するために最も役立つのは次のうちどれですか。
A. ビジネスの優先順位を理解するためにビジネス影響分析(BIA)を実施する
B. ビジネスプロセスにおける情報セキュリティポリシーと実践の統合を分析する
C. 定量的および定性的なリスク分析を実行する
D. ガバナンスフレームワーク内で特定された主要人物へのインタビュー
正解: (正解を表示します)
Analyzing how security policies and practices are integrated into business processes (B) provides the clearest view of governance effectiveness. CISM defines governance as the alignment of security with business objectives, supported by defined roles, accountability, and decision-making structures. BIAs (A) and risk analyses (C) provide valuable inputs but do not directly assess governance maturity. Interviews (D) can supplement understanding but are subjective without observing real integration. By evaluating whether security is embedded in procurement, development, operations, and decision workflows, a new security manager can determine whether governance is formalized, consistently applied, and supported by management.
References: ISACA CISM Review Manual (Governance-structure, integration, and effectiveness); CISM Exam Content Outline (Domain 2).

質問: **159**
上級管理職は、組織の侵入防止システム (IPS) が業務運営を繰り返し妨害する可能性があるという懸念を表明しています。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示すベストな例は次のどれですか。
A. 偽陰性の増加
B. 偽陰性の減少
C. 誤検出を減らす
D. 誤検出の増加
正解: (正解を表示します)
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: **160**
新しい規制枠組みがビジネス システムに与える影響を確実に評価する責任を負う役割は次のどれですか。
A. 上級管理職
B. 法定代理人
C. 情報セキュリティ管理者
D. アプリケーション所有者
正解: **A** (コメントを発表する)

質問: **161**
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 メトリック ダッシュボード。
D. 主要リスク指標 (KRI)。
正解: **C** (コメントを発表する)
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: **162**

情報セキュリティをサポートするために組織の文化を変革するのに最も効果的なのは次のどれですか?
A. 定期的なコンプライアンス監査
B. 強力な経営サポート
C. 堅牢な技術的セキュリティ管理
D. セキュリティインシデント報告に対するインセンティブ
正解: **(**正解を表示します**)**
According to the CISM Review Manual (Digital Version), page 5, information security culture is the set of values, attitudes, and behaviors that shape how an organization and its employees view and practice information security. Transforming the information security culture requires a change management process that involves the following steps: creating a sense of urgency, forming a powerful coalition, developing a vision and strategy, communicating the vision, empowering broad-based action, generating short-term wins, consolidating gains and producing more change, and anchoring new approaches in the culture1. Among the four options, strong management support is the best enabler for transforming the information security culture, as it can provide the necessary leadership, resources, sponsorship, and alignment for the change management process. Periodic compliance audits, robust technical security controls, and incentives for security incident reporting are important elements of information security, but they are not sufficient to change the culture without strong management support. References = 1: CISM Review Manual (Digital Version), page 5

質問: **163**
災害復旧プログラムの管理を支援するために Disaster Recovery as a Service (DRaaS) を使用している組織の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た柔軟な導入オプションを組織に提供します。
B. これにより、組織は中核業務を優先することができます。
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. 低コストで専門の対応チームを利用できるようになります。
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**: 164**
データベース内の情報をどのように分類するかを決定するのに最適な人は誰でしょうか?
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**: 165**
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. ステークホルダーコミュニケーション計画
B. 保管手順
C. 復旧時間目標 RTO）

D. 平均応答時間（MTTR）
正解: **(**正解を表示します**)**

質問: **166**
生産システムのセキュリティ メカニズムが制御目標を満たしているかどうかを確認するのに最適な時期はいつですか?
A. 品質および受入チェック中
B. 監視活動と自動化ツールを通じて継続的に
C. 侵入テストで推奨された修復が完了した後
D. 年次内部監査およびコンプライアンス監査中
正解: **(**正解を表示します**)**
While audits and assessments provide periodic insights, the best time to verify that security mechanisms meet control objectives is continuously-through monitoring and automation. Continuous monitoring allows the organization to detect misconfigurations, anomalies, or control failures in real-time, significantly improving response capabilities. Modern environments, especially in production systems, require real-time feedback loops to maintain compliance and effectiveness due to rapidly evolving threats and configuration changes.
"Continuous monitoring provides assurance that controls are operating effectively in real time, enabling timely corrective actions."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Control Monitoring*

質問: **167**
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、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。
B. 計画は脅威と脆弱性のレビューに基づいています。
C. 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。
D. 計画では実装に関する IT コストがまとめられています。

正解: **B** (コメントを発表する)

質問: **168**
環境が急速に変化する組織では、経営管理は情報セキュリティリスクを受け入れています。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、次の点を確認することです。
A. 変更アクティビティが文書化されます。
B. 承認の根拠は定期的に見直されます。
C. 受け入れはビジネス戦略と一致しています。
D. リスク受容フレームワークへの準拠。
正解: **B** (コメントを発表する)
= In an organization with a rapidly changing environment, the information security risk landscape may also change frequently due to new threats, vulnerabilities, impacts, or controls. Therefore, the information security manager should ensure that the risk acceptance decisions made by the business management are periodically reviewed to verify that they are still valid and aligned with the current risk appetite and tolerance of the organization. The rationale for acceptance should be documented and updated as necessary to reflect the changes in the risk environment and the business objectives. The information security manager should also monitor the accepted risks and report any deviations or issues to the business management and the senior management.
References =
CISM Review Manual 15th Edition, page 1131
CISM Review Questions, Answers & Explanations Manual 9th Edition, page 482 CISM Domain 2: Information Risk Management (IRM) [2022 update]3

質問: **169**
情報セキュリティガバナンスフレームワークを確立する際に、情報セキュリティマネージャーが理解することが最も重要です。
A. 情報セキュリティのベストプラクティス。
B. 企業文化。
C. 脅威環境。
D. リスク管理手法。
正解: (正解を表示します)

質問: **170**
ある事業部門は最近、組織の新しい強力なパスワード ポリシーをビジネス 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。ヘルプ デスクには現在、パスワード リセット 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どれですか。

A. エンドユーザートレーニングを提供します。
B. 上級管理職にエスカレーションします。
C. ポリシーの適用を継続します。
D. ビジネス影響分析 (BIA) を実施します。
正解: **A** (コメントを発表する)

質問: **171**
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次のとおりです。
A. リスク評価を実行する
B. ギャップ分析を実行する
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状態を確認する
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: **172**
ビジネスに合わせた情報セキュリティ プログラムを計画する際に最も役立つ情報源は次のどれですか?
A. セキュリティリスクレジスタ
B. 情報セキュリティポリシー
C. ビジネス影響分析 (BIA)
D. エンタープライズ アーキテクチャ (EA)
正解: **C** (コメントを発表する)
A business-aligned information security program is one that supports the organization's business objectives and aligns the information security strategy with the business functions. A business impact analysis (BIA) is a process that identifies the critical business processes, assets, and functions of an organization, and assesses their potential impact in the event of a disruption or loss. A BIA helps to prioritize the information security requirements and controls that are needed to protect the organization's critical assets and functions from various threats and risks. Therefore, a BIA is one of the most useful sources when planning a business-aligned information security program. References = CISM

Review Manual 15th Edition, page 254; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 229.
The most useful source when planning a business-aligned information security program is a Business Impact Analysis (BIA). A BIA is a process of identifying and evaluating the potential effects of disruptions to an organization's operations, and helps to identify the security controls and measures that should be implemented to reduce the impact of those disruptions. The BIA should include an assessment of the organization's information security posture, including its security policies, risk register, and enterprise architecture. With this information, organizations can develop an information security program that is aligned to the organization's business objectives.

質問: **173**
インシデントへの対応を優先するには、次のうちどれを最初に行う必要がありますか?
A. 分析
B. 封じ込め
C. エスカレーション
D. トリアージ
正解: **B** (コメントを発表する)

質問: **174**
次のどれが、新たなインシデントの発生を最もよく示す指標でしょうか?
A. システムのパッチ適用を試みましたが、エラーが発生しました
B. 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
C. 業界の競合他社における最近のセキュリティインシデント
D. 組織の情報システム内で特定された弱点
正解: (正解を表示します)

質問: **175**
パスワード標準への準拠を確保するための最良の方法はどれですか?
A. パスワード同期ソフトウェアの実装
B. パスワードクラッキングソフトウェアの使用
C. パスワード構文ルールの自動適用
D. ユーザー意識向上プログラム
正解: (正解を表示します)
Automated enforcement of password syntax rules is the best method to ensure compliance with password standards. Password syntax rules define the minimum and maximum length, character types, and construction of passwords. By enforcing these rules automatically, the system can prevent users from creating or using weak or insecure passwords that do not meet the standards. According to NIST, password syntax rules should allow at least 8 characters and up to 64 characters, accept all printable ASCII

characters and Unicode characters, and encourage the use of long passphrases1. The other options are not methods to ensure compliance with password standards, but rather methods to verify or improve password security.
Implementing password-synchronization software can help users manage multiple passwords across different systems, but it does not ensure that the passwords comply with the standards2. Using password-cracking software can help test the strength of passwords and identify weak or compromised ones, but it does not ensure that users follow the standards3. A user-awareness program can help educate users about the importance of password security and the best practices for creating and using passwords, but it does not ensure that users comply with the standards. References: 1: NIST Password Guidelines and Best Practices for
2020 - Auth0 2: Password synchronization - Wikipedia 3:

質問**: 176**
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回復したという通知を送信します。次に行うべきことはどれですか?
A. 上級管理職向けのエグゼクティブサマリーを作成する
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. 学んだ教訓を記録するために会議を開催します。
D. 分析のためにデジタル証拠を保護し、保存します。
正解**: (**正解を表示します**)**
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**: 177**

情報セキュリティインシデント対応プロセスの主な目的はどれですか?
A. インシデントのトリアージの実施
B. 社内外の関係者とのコミュニケーション
C. 重要な業務への悪影響を最小限に抑える
D. インシデントの分類
正解: **(正解を表示します)**
The primary objective of the information security incident response process is to minimize the negative impact to critical operations. An information security incident is an event that threatens or compromises the confidentiality, integrity, or availability of the organization's information assets or processes. The information security incident response process is a process that defines the roles, responsibilities, procedures, and tools for detecting, analyzing, containing, eradicating, recovering, and learning from information security incidents.
The main goal of the information security incident response process is to restore the normal operations as quickly and effectively as possible, and to prevent or reduce the harm or loss caused by the incident to the organization, its stakeholders, or its environment.
Conducting incident triage (A) is an important activity of the information security incident response process, but not the primary objective. Incident triage is the process of prioritizing and assigning the incidents based on their severity, urgency, and impact. Incident triage helps to allocate the appropriate resources, personnel, and time to handle the incidents, and to escalate the incidents to the relevant authorities or parties if needed.
However, incident triage is not the ultimate goal of the information security incident response process, but a means to achieve it.
Communicating with internal and external parties (B) is also an important activity of the information security incident response process, but not the primary objective.
Communicating with internal and external parties is the process of informing and updating the stakeholders, such as management, employees, customers, partners, regulators, or media, about the incident status, actions, and outcomes. Communicating with internal and external parties helps to maintain the trust, confidence, and reputation of the organization, and to comply with the legal and contractual obligations, such as notification or reporting requirements. However, communicating with internal and external parties is not the ultimate goal of the information security incident response process, but a means to achieve it.
Classifying incidents (D) is also an important activity of the information security incident response process, but not the primary objective. Classifying incidents is the process of categorizing and labeling the incidents based on their type, source, cause, or impact. Classifying incidents helps to identify and understand the nature and scope of the incidents, and to apply the appropriate response procedures and controls. However, classifying incidents is not the ultimate goal of the information security incident response process, but a means to achieve it.

References = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Plan, page 1811

質問: **178**
ビジネス影響分析 (BIA) の設計フェーズで最も重要な考慮事項は次のどれですか?
A. ビジネスパフォーマンスを監視するための品質指標の選択
B. エンドツーエンドのプロセスが中断される可能性を推定する
C. 事業の失敗に備えた予備資金の確保
D. ビジネス運営に重要な機能を特定する
正解: **(正解を表示します)**
The design phase of a BIA must begin with identifying critical business functions, since they determine:
Which systems/processes need protection
Recovery priorities
Acceptable downtime (RTO/MTD)
Without clearly defining what's critical, the BIA cannot guide resource allocation or continuity strategies effectively.
"A successful BIA must begin with identifying which business functions are critical to achieving organizational objectives."
- CISM Review Manual 15th Edition, Chapter 3: Business Continuity and Disaster Recovery, Section: BIA Methodology*

質問: **179**
災害復旧テストを実施する最も適切なタイミングは、次のとおりです。
A. 主要なビジネス プロセスが再設計されました。
B. 事業継続計画 (BCP) が更新されました。
C. セキュリティリスクプロファイルがレビューされました
D. 非準拠インシデントが報告されました。
正解: **(正解を表示します)**
The most appropriate time to conduct a disaster recovery test would be after the business continuity plan (BCP) has been updated, as it ensures that the disaster recovery plan (DRP) is aligned with the current business requirements, objectives, and priorities. The BCP should be updated regularly to reflect any changes in the business environment, such as new threats, risks, processes, technologies, or regulations. The disaster recovery test should validate the effectiveness and efficiency of the DRP, as well as identify any gaps, issues, or improvement opportunities123. References =
* 1: CISM Review Manual 15th Edition, page 2114
* 2: CISM Practice Quiz, question 1042
* 3: Business Continuity Planning and Disaster Recovery Testing, section "Testing the Plan"

質問: **180**
ある組織は、人気のソーシャル ネットワーク プラットフォームを活用して自社の製品やサービスを宣伝することを計画しています。情報セキュリティ マネージャーがこの取り組みをサポートするために取るべき最善の行動は次のどれですか。
A. ソーシャル ネットワークにコンテンツを公開するためのプロセスを確立します。
B. ソーシャル ネットワークの使用に関連するセキュリティ リスクを評価します。
C. ソーシャル ネットワーク プラットフォームの脆弱性評価を実施します。
D. ソーシャル ネットワークの使用に関するセキュリティ制御を開発します。
正解: **(**正解を表示します**)**
The best course of action for the information security manager to support the initiative of leveraging popular social network platforms to promote the organization's products and services is to assess the security risk associated with the use of social networks. Security 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 security risk assessment, the information security manager can provide valuable input to the decision-making process regarding the benefits and costs of using social networks, as well as the appropriate security controls and mitigation strategies to reduce the risk to an acceptable level. The other options are not the best course of action, although they may be part of the security risk management process. Establishing processes to publish content on social networks is an operational task that should be performed after assessing the security risk and implementing the necessary controls. Conducting vulnerability assessments on social network platforms is a technical activity that may not be feasible or effective, as the organization does not have control over the platforms' infrastructure and configuration. Developing security controls for the use of social networks is a preventive measure that should be based on the results of the security risk assessment and aligned with the organization's risk appetite and tolerance

質問: **181**
情報セキュリティイニシアチブの投資収益率 (ROI) を計算するのが難しい場合、ビジネスケースに含めるのに最も適しているのはどれですか?
A. 成熟度の予測増加
B. リスクの推定削減
C. 時間の経過に伴う予測コスト
D. 効率性の向上の推定
正解: **(**正解を表示します**)**
The best thing to include in a business case when the return on investment (ROI) for an information security initiative is difficult to calculate is an estimated reduction in risk. Risk reduction is the expected benefit of implementing an information security initiative, as it reduces the likelihood and impact of threats and vulnerabilities that may affect the

organization's information assets and systems. By estimating the reduction in risk, the information security manager can demonstrate the value and benefits of the information security initiative to the organization's performance, reputation, and competitiveness. The information security manager can also compare the estimated reduction in risk with the estimated cost of the information security initiative to determine its cost-effectiveness and feasibility. The other options are not the best thing to include in a business case, although they may be some inputs or outputs of the risk assessment process. A projected increase in maturity level is a potential outcome of implementing an information security initiative, as it improves the organization's capabilities and processes for managing information security risks. However, it does not necessarily reflect the actual reduction in risk or the ROI of the information security initiative. A projected cost over time is a component of calculating the ROI of an information security initiative, as it reflects the total cost of ownership and maintenance of the initiative. However, it does not indicate the expected benefit or value of the initiative. An estimated increase in efficiency is a possible benefit of implementing an information security initiative, as it may enhance the organization's productivity and performance. However, it may not be directly related to the reduction in risk or the ROI of the information security initiative.

質問: **182**
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: **(**正解を表示します**)**
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: **183**
リモートユーザーである従業員が、仮想プライベートネットワーク（VPN）接続を使用して、社内サーバーからラップトップに財務データをコピーしました。これをデータ漏洩インシデントとして分類するかどうかを判断する上で最も重要な要素はどれですか？
A. 監査ログの確認
B. 従業員の職務
C. データの所有権
D. 有効な使用例
正解: **(**正解を表示します**)**

質問: **184**
電子メールのデジタル署名は次のようになります。
A. 電子メール メッセージの機密性を保護します。
B. 受信者に対して電子メール メッセージの整合性を確認します。
C. 電子メール メッセージの不正な変更を自動的に修正します。
D. 電子メール メッセージの不正な変更を防止します。
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: **185**

情報セキュリティマネージャーは、組織のクラウドプロバイダーが意図せず組織のビジネスデータの一部を公開したことを確認しました。次に行うべき対応は次のうちどれですか？
A. インシデント対応計画を呼び出します。
B. 公開されたデータに関連付けられているユーザーを識別します。
C. クラウド プロバイダーのサービス レベル アグリーメント (SLA) を確認します。
D. 組織のデータ損失防止 (DLP) プロセスを開始します。
正解: **(**正解を表示します**)**

質問: **186**
事業継続計画 (BCP) の成功にとって最も重要なプロセスは次のどれですか?
A. 計画の見直しに取締役会と上級管理職を参加させる
B. プライマリサイトとリカバリサイトで計画のコピーを維持する
C. テストとトレーニングにすべての関係者を参加させる
D. 定期的な内部監査と外部監査のスケジュール設定
正解: **(**正解を表示します**)**

質問: **187**
リスク評価の一環として、セキュリティ管理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、考慮すべき最も重要な属性は次のうちどれですか？
A. リスク所有者は、修復後にリスクを再評価できます。
B. リスク所有者は、リスクに対してアクションを実行する権限を持ちます。
C. リスク所有者は、リスク レジスタをタイムリーに更新できます。
D. リスク所有者は、失敗した関連コントロールも所有します。
正解: **B (**コメントを発表する**)**
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: **188**
ビジネス目標に影響を及ぼす可能性のある新たな脅威や新たなリスクに関する最も有用な情報を情報セキュリティ管理者に提供するものは次のどれですか?
A. 外部監査報告書
B. 内部脅威分析レポート
C. 業界脅威インテリジェンスレポート
D. 内部脆弱性評価レポート
正解: **(正解を表示します)**
An industry threat intelligence report (C) provides the most useful insight into new and emerging threats because it aggregates intelligence across organizations, sectors, and geographies. CISM emphasizes the importance of understanding the external threat landscape to anticipate risks that may not yet be visible internally. Audit reports (A) and vulnerability assessments (D) are retrospective and organization-specific.
Internal threat analysis (B) focuses on known issues rather than emerging trends. Threat intelligence supports proactive risk identification and helps align security strategy with evolving business risks.
References: ISACA CISM Review Manual (Risk management-threat intelligence, emerging risk identification); CISM Exam Content Outline (Domain 1).

質問: **189**
情報セキュリティ メトリックを導入する主な目的は次のとおりです。
A. プログラムの有効性をベンチマークと比較します。
B. 技術的な操作が仕様を満たしていることを確認します。
C. 意思決定に必要な情報を提供します。
D. 継続的なセキュリティ予算要件をサポートします。
正解: **(正解を表示します)**

質問: **190**
次のどれがビジネス継続性管理において最も重要な考慮事項でしょうか?
A. 人間の安全の確保
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の確保
D. 重要な情報資産の保護
正解: **A (コメントを発表する)**

= 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**: 191**
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**: 192**
ある組織が災害復旧活動の実行をアウトソーシングすることを計画しています。アウトソーシング契約に含めるべき最も重要な項目は次のどれですか。
A. 災害宣言の対象となる場合の定義
B. 定期的にバックアップを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**: 193**
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**: 194**
情報セキュリティ管理者が、セキュリティ ポリシーに繰り返し従っていない部門を特定した場合、次に取るべき行動は何でしょうか。
A. 部門ユーザーにセキュリティ意識向上トレーニングを繰り返し実施するよう要求します。
B. ポリシーへの準拠を強制するための追加の制御を導入します。
C. 部門内のシステムの脆弱性評価を実行します。
D. ポリシー違反を上級管理職に報告します。
正解**: (**正解を表示します**)**

質問: **195**
経験豊富なメンバーのグループからインシデント対応チームが編成されました。最初の訓練でチームにとって最も有益なのはどのタイプの演習でしょうか?
A. レッドチーム演習
B. ブラックボックス侵入テスト
C. 災害復旧訓練
D. テーブルトップ演習
正解: **D** (コメントを発表する)
= A tabletop exercise is the best type of exercise for an incident response team at the first drill, as it is a low- cost, low-risk, and high-value method to test and evaluate the incident response plan, procedures, roles, and capabilities. A tabletop exercise is a simulation of a realistic scenario that involves a security incident, and requires the participation and discussion of the incident response team members and other relevant stakeholders. The tabletop exercise allows the incident response team to identify and address the gaps, issues, or challenges in the incident response process, and to improve the communication, coordination, and collaboration among the team members and other parties. The tabletop exercise also helps to enhance the knowledge, skills, and confidence of the incident response team members, and to prepare them for more complex or advanced exercises or real incidents.
A red team exercise (A) is a type of exercise that involves a group of ethical hackers or security experts who act as adversaries and attempt to compromise the organization's security defenses, systems, or processes. A red team exercise is a high-cost, high-risk, and high-value method to test and evaluate the security posture and resilience of the organization, and to identify and exploit the security weaknesses or vulnerabilities. However, a red team exercise is not the best type of exercise for an incident response team at the first drill, as it is more suitable for a mature and experienced team that has already tested and validated the incident response plan, procedures, roles, and capabilities.
A black box penetration test (B) is a type of security testing that simulates a malicious attack on the organization's systems or processes, without any prior knowledge or information about them. A black box penetration test is a high-cost, high-risk, and high-value method to test and evaluate the security posture and resilience of the organization, and to identify and exploit the security weaknesses or vulnerabilities. However, a black box penetration test is not the best type of exercise for an incident response team at the first drill, as it is more suitable for a mature and experienced team that has already tested and validated the incident response plan, procedures, roles, and capabilities.
A disaster recovery exercise is a type of exercise that simulates a catastrophic event that disrupts or destroys the organization's critical systems or processes, and requires the activation and execution of the disaster recovery plan, procedures, roles, and capabilities. A disaster recovery exercise is a high-cost, high- risk, and high-value method to test and evaluate the disaster recovery posture and resilience of the organization, and to identify

and address the recovery issues or challenges. However, a disaster recovery exercise is not the best type of exercise for an incident response team at the first drill, as it is more suitable for a mature and experienced team that has already tested and validated the incident response plan, procedures, roles, and capabilities.
References = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Plan, Subsection: Testing and Maintenance, page 184-1851

質問**: 196**
ファイアウォールが包括的な境界防御を提供するように構成されているかどうかを判断するための最良の方法はどれですか？
A. 現在のファイアウォールルールセットの検証
B. 内部ソースからのファイアウォールのポートスキャン
C. 外部ソースからのpingテスト
D. ファイアウォールに対する模擬サービス拒否 (DoS) 攻撃
正解**: (**正解を表示します**)**
A validation of the current firewall rule set is the best method for determining whether a firewall has been configured to provide a comprehensive perimeter defense because it verifies that the firewall rules are consistent, accurate, and effective in allowing or blocking traffic according to the security policies and standards of the organization. A port scan of the firewall from an internal source is not a good method because it does not test the firewall's behavior from an external perspective, which is more relevant for perimeter defense. A ping test from an external source is not a good method because it only tests the firewall's availability and responsiveness, not its security or functionality. A simulated denial of service (DoS) attack against the firewall is not a good method because it only tests the firewall's resilience and performance under high traffic load, not its security or functionality. 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/the-value-of-penetration-testing https://www.isaca.org/resources/isaca- journal/issues/2016/volume-5/security-scanning-versus-penetration-testing

質問: **197**
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次のとおりです。
A. リスク評価を実行します。
B. セキュリティ認識の状態を確認します。
C. 情報セキュリティポリシーを確認します。
D. ギャップ分析を実行します。
正解: **(**正解を表示します**)**
According to the CISM Review Manual, performing a risk assessment is the most important course of action for an information security manager during the due diligence phase of an acquisition, as it helps to identify and evaluate the potential threats, vulnerabilities and impacts that may affect the information assets of the target organization. A risk assessment also provides the basis for performing a gap analysis, reviewing the information security policies and awareness, and developing a remediation plan. References = CISM Review Manual, 27th Edition, Chapter 3, Section 3.4.1, page 1411.

質問: **198**
インシデント対応プロセスにおける根絶フェーズの主な目標は次のとおりです。
A. 厳格な保管チェーンを維持します。
B. インシデントの効果的なトリアージと封じ込めを提供します。
C. 脅威を除去し、影響を受けたシステムを復元する
D. 影響を受けたシステムから法医学的証拠を取得します。
正解: **(**正解を表示します**)**
The primary goal of the eradication phase in an incident response process is to remove the threat and restore affected systems because it eliminates any traces or remnants of malicious activity or compromise from the systems or network, and returns them to their normal or secure state. Maintaining a strict chain of custody is not a goal of the eradication phase, but rather a requirement for preserving and documenting digital evidence throughout the incident response process. Providing effective triage and containment of the incident is not a goal of the eradication phase, but rather a goal of the containment phase, which isolates and stops the spread of malicious activity or compromise. Obtaining forensic evidence from the affected system is not a goal of the eradication phase, but rather a goal of the identification phase, which collects and analyzes data or artifacts related to malicious activity or compromise. 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: **199**
ある組織は最近、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がありましたが、一部の従業員はコミュニケーション計画に完全に従わなかったようです。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指示を強化する
B. 適切な従業員による卓上テストを実施する
C. 従業員が計画に従うようインセンティブを与える
D. ビジネス影響分析 (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: **200**
情報セキュリティ チームは、顧客向けサイトの認証要件を強化することを計画していますが、ユーザー エクスペリエンスに悪影響を与えるのではないかと懸念されています。情報セキュリティ マネージャーにとって最善の対応策は次のどれですか。
A. 顧客にセキュリティ意識向上トレーニングを提供します。
B. セキュリティ リスクに対するビジネスへの影響を評価します。
C. ビジネスに対するセキュリティ リスクを定量化します。
D. 業界のベストプラクティスを参照してください。
正解: **(**正解を表示します**)**

質問: **201**
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、アプリケーションが収容されています。
組織の物理アクセス制御ポリシーを開発するための最良のアプローチは何ですか?
A. 顧客のセキュリティ ポリシーを確認します。
B. リスク評価を実施して、セキュリティ リスクと軽減制御を決定します。
C. 各システムおよびアプリケーションのアクセス制御要件を開発します。
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: **(**正解を表示します**)**

= 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**: 202**
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 マネージャー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. 災害復旧手順を文書化する
C. リスク評価を実施する
D. ビジネス影響分析 (BIA) を実行する

正解: **(**正解を表示します**)**
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: **203**
組織が直面している継続的な脅威について、最も包括的な洞察を提供するのは次のどれですか?
A. ビジネス影響分析 (BIA)
B. リスクレジスター
C. 侵入テスト
D. 脆弱性評価
正解: **(**正解を表示します**)**
A risk register is a document that records and tracks the information security risks facing an organization, such as their sources, impacts, likelihoods, responses, and statuses. A risk register provides the most comprehensive insight into ongoing threats facing an organization, as it covers both internal and external threats, as well as their current and potential effects on the organization's assets, processes, and objectives. A risk register also helps to prioritize and monitor the risk mitigation actions and controls, and to communicate the risk information to relevant stakeholders. Therefore, option B is the most appropriate answer.
Option A is not the best answer because a business impact analysis (BIA) is a process that identifies and evaluates the critical business functions, assets, and dependencies of an organization, and assesses their potential impact in the event of a disruption or loss. A BIA does not provide a comprehensive insight into ongoing threats facing an organization, as it focuses more on the consequences of the threats, rather than their sources, likelihoods, or responses. A BIA is mainly used to support the business continuity and disaster recovery planning, rather than the information security risk management.
Option C is not the best answer because penetration testing is a method of simulating a malicious attack on an organization's IT systems or networks, to evaluate their security posture and identify any vulnerabilities or weaknesses that could be exploited by real attackers. Penetration testing does not provide a comprehensive insight into ongoing threats facing an organization, as it only covers a specific scope, target, and scenario, rather than the whole range of threats, sources, and impacts. Penetration testing is mainly used to validate and improve the technical security controls, rather than the information security risk management.

Option D is not the best answer because vulnerability assessment is a process of scanning and analyzing an organization's IT systems or networks, to detect and report any flaws or gaps that could pose a security risk.
Vulnerability assessment does not provide a comprehensive insight into ongoing threats facing an organization, as it only covers the technical aspects of the threats, rather than their business, legal, or regulatory implications. Vulnerability assessment is mainly used to identify and remediate the security weaknesses, rather than the information security risk management. References = CISM Review Manual 15th Edition1, pages 258-259; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 306.
A risk register provides the MOST comprehensive insight into ongoing threats facing an organization. This is because a risk register is a document that records and tracks the identified risks, their likelihood, impact, mitigation strategies, and status. A risk register helps an organization to monitor and manage the threats that could affect its objectives, assets, and operations. A risk register also helps an organization to prioritize its response efforts and allocate its resources accordingly.

質問**: 204**
機密性、整合性、可用性 (CIA) の 3 つの要素のうち、機密性の概念を最もよくサポートするのは次のアクティビティのどれですか。
A. 管理者資格情報のハッシュ化の保証
B. サービスレベル契約 (SLA) の適用
C. 転送中のデータの暗号化の確保
D. 正式な変更管理プロセスの活用
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**: 205**
インシデント対応計画を作成する際に、セキュリティ インシデントを明確に定義することの主な利点は、次の点です。
A. 利害関係者へのインシデント対応プロセス
B. インシデント対応チームに適切な人員を配置し、トレーニングを行います。
C. 効果的なエスカレーションおよび対応手順を開発します。

D. テーブルトップテストをより効率的にします。
正解: **(**正解を表示します**)**
The primary benefit of establishing a clear definition of a security incident is that it helps to develop effective escalation and response procedures. A security incident is an event or an attempt that disrupts or threatens the normal operations, security, or privacy of an organization's information or systems1. A clear definition of a security in-cident helps to:
*Distinguish between normal and abnormal events, and between security-relevant and non-security-relevant events
*Determine the severity and impact of an incident, and the appropriate level of response
*Assign roles and responsibilities for incident detection, reporting, analysis, containment, eradication, recovery, and post-incident activities
*Establish criteria and thresholds for escalating incidents to higher authorities or external parties
*Define the communication channels and protocols for incident notification and coordina-tion
*Document the incident response process and procedures in a formal plan According to NIST, a clear definition of a security incident is one of the key compo-nents of an effective incident response capability2. The other options are not the prima-ry benefits of establishing a clear definition of a security incident. Communicating the incident response process to stakeholders is important, but it is not the main purpose of defining a security incident. Adequately staffing and training incident response teams is essential, but it depends on other factors besides defining a security inci-dent. Making tabletop testing more effective is a possible outcome, but not a direct benefit of defining a security incident.
References: 2: NIST SP
800-61 Rev. 2 Computer Security Incident Handling Guide 1: NIST Glossary - Security Incident : What is a securi-ty incident? - TechTarget : 10 types of security incidents and how to handle them - TechTarget : 45 CFR 164.304 - Definitions - Electronic Code of Federal Regulations

質問: **206**
法医学的分析中に特定のファイルのデータ復旧を試みる場合の最大の課題は次の場合です。
A. ディスク上のパーティション テーブルが削除されました。
B. タイルが上書きされました。
C. ディレクトリ内のすべてのファイルが削除されました。
D. 高レベルのディスクフォーマットが実行されました。
正解: **(**正解を表示します**)**
Data recovery is the process of restoring data that has been lost, corrupted, or deleted. When a file is deleted, it is usually not physically erased from the disk, but only marked as free space by the operating system.

Therefore, it may be possible to recover the file by using specialized tools that scan the disk for the file's data.
However, if the file has been overwritten by another file or data, then the original file's data is lost and cannot be recovered. The other options are not as challenging as overwriting, because they only affect the logical structure of the disk, not the physical data. For example, the partition table, the directory, and the formatting information can be reconstructed or bypassed by using forensic tools. References = CISM Review Manual, 16th Edition, Chapter 5, Section 5.4.1.2

質問**: 207**
組織の新たな情報セキュリティ戦略をサポートするため、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ステップは次のうちどれですか？
A. セキュリティ トレーニング プログラムを更新します。
B. 標準と手順を更新します。
C. ビジネス戦略との整合性を評価します。
D. 技術的な管理を確認します。
正解**: (**正解を表示します**)**

質問**: 208**
ビジネスアプリケーションに深刻な脆弱性が検出されました。この脆弱性は外部の攻撃者によって悪用され、システムに侵入される可能性があります。情報セキュリティ管理者にとって最善の対応策は何でしょうか？
A. ビジネスアプリケーションの所有者に修正をすぐに適用するよう依頼する
B. 一時的な修復を実施する
C. アプリケーションを直ちにシャットダウンします
D. ビジネスアプリケーションの所有者にリスクを報告する
正解**: (**正解を表示します**)**
The best course of action is to implement temporary remediation (B) to reduce exposure while a permanent fix is planned and approved. CISM emphasizes balancing risk reduction with business continuity. Immediate shutdown (C) or unilateral action (A) may disrupt business operations without proper authorization. Reporting the risk (D) is necessary but insufficient on its own. Temporary controls, such as access restrictions or additional monitoring, reduce risk while enabling informed decision-making by the business owner. References: ISACA CISM Review Manual (Program management-risk response and operational controls); CISM Exam Content Outline (Domain 3).

質問**: 209**
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: **210**
次のどれが主にビジネス影響分析 (BIA) の影響を受けますか?
A. セキュリティ戦略
B. IT戦略
C. リスク軽減戦略
D. 回復戦略
正解: **(**正解を表示します**)**

質問: **211**
コールセンターでソーシャル エンジニアリングを実施する最も良い理由は次のとおりです。
A. 追加のセキュリティ トレーニングの対象となる候補者を特定します。
B. 攻撃が成功する可能性を最小限に抑えます。
C. 情報セキュリティイニシアチブのための資金を獲得する。
D. パスワードポリシーを改善します。
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: **212**
次のどれが組織の情報セキュリティ戦略に最も大きな影響を与えますか?
A. 組織のリスク許容度
B. 組織構造
C. 業界のセキュリティ標準
D. 情報セキュリティ意識
正解: **(**正解を表示します**)**
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: **213**

ある組織は、クラウドベースのアプリケーションの実装を間もなく開始しようとしています。独立した侵入テストの結果を受け、高い評価の脆弱性があることがわかりました。次に挙げる方法のうち、最も適切なものはどれでしょうか。
A. アプリケーションを実装し、クラウド サービス プロバイダーに脆弱性の修正を依頼します。
B. 脆弱性が組織のリスク許容レベル内であるかどうかを評価します。
C. 初期テストの結果を検証するために、さらに侵入テストを実施します。
D. 脆弱性が修正されるまで実装を延期します。
正解: **(**正解を表示します**)**
The best way to proceed when an independent penetration test results show a high-rated vulnerability in a cloud-based application that is close to going live is to assess whether the vulnerability is within the organization's risk tolerance levels. This is because the organization should not implement the application without understanding the potential impact and likelihood of the vulnerability being exploited, and the cost and benefit of fixing or mitigating the vulnerability. The organization should also consider the contractual and legal obligations, service level agreements, and performance expectations of the cloud service provider and the application users. By assessing the risk tolerance levels, the organization can make an informed and rational decision on whether to accept, transfer, avoid, or reduce the risk, and how to allocate the resources and responsibilities for managing the risk.
Implementing the application and requesting the cloud service provider to fix the vulnerability is not the best way to proceed, because it exposes the organization to unnecessary and unacceptable risk, and it may violate the terms and conditions of the cloud service contract. The organization should not rely on the cloud service provider to fix the vulnerability, as the provider may not have the same level of urgency, accountability, or capability as the organization. The organization should also not assume that the vulnerability will not be exploited, as cyberattackers may target the cloud-based application due to its high visibility, accessibility, and value.
Commissioning further penetration tests to validate initial test results is not the best way to proceed, because it may delay the implementation of the application, and it may not provide any additional or useful information.
The organization should trust the results of the independent penetration test, as it is conducted by a qualified and objective third party. The organization should also not waste time and resources on conducting redundant or unnecessary tests, as it may affect the budget, schedule, and quality of the project.
Postponing the implementation until the vulnerability has been fixed is not the best way to proceed, because it may not be feasible or desirable for the organization. The organization should consider the business impact and opportunity cost of postponing the implementation, as it may affect the organization's reputation, revenue, and customer satisfaction. The organization should also consider the technical feasibility and complexity

of fixing the vulnerability, as it may require significant changes or modifications to the application or the cloud environment. The organization should not adopt a zero-risk or risk-averse approach, as it may hinder the organization's innovation and competitiveness. References = ISACA, CISM Review Manual, 16th Edition, 2020, pages 97-98, 101-102, 105-106, 109-110.
ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1025.

質問: **214**
新たなリスクと脅威の状況を分析する場合、情報セキュリティ管理者はまず次のことを行う必要があります。
A. ビジネス資産への脅威をマッピングします。
B. 新たな脅威の発生源を特定します。
C. 脅威が現実化した場合の影響を判断します。
D. 業界内の過去の脅威を確認します。
正解: **B** (コメントを発表する)

質問: **215**
データ損失防止 (DLP) ソリューションを実装する主な利点は次のとおりです。
A. 組織のウイルス対策制御を強化します。
B. データ損失のリスクを排除します。
C. 組織の検出制御を補完します。
D. セキュリティ意識向上プログラムの必要性を軽減します。
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: **216**

分散型サービス拒否 (DDoS) 攻撃の影響を軽減するのに最も効果的なのは次のどれでしょうか?
A. サーバーに状態制限を課します。
B. サイトを複数の ISP に分散します。
C. 攻撃をソースでブロックします。
D. ネットワークセキュリティを強化します。
正解: **(**正解を表示します**)**
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: **217**
情報セキュリティへの投資収益率を最もよく示すのは次のどれですか?
A. 年間損失予想値 ALE)の増加
B. 報告されたインシデント数の増加
C. 年間損失予想値の減少 ALE)
D. 報告されたインシデント数の減少
正解: **C (**コメントを発表する**)**
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: **218**
攻撃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どれですか。
A. 組織に対する攻撃のコスト

B. 攻撃者の所在地
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: **(**正解を表示します**)**
= 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?

質問: **219**
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、次の事項を確実に含める必要があります。
A. 重要なデータのインベントリ。
B. エスカレーションの基準。
C. ビジネス影響分析 (BIA)。
D. 重要なインフラストラクチャ図。
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: **220**
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. フォレンジック分析を実施します。
C. 関係する関係者に通知します。
D. 学んだ教訓を実行します。
正解: **(正解を表示します)**

質問: **221**
情報セキュリティ トレーニング プログラムが最も効果的であることを保証するには、その内容が次のようになっている必要があります。
A. 最近の事件に基づく。
B. 従業員の役割に基づきます。
C. ビジネス プロセスに合わせて調整されます。
D. 情報セキュリティポリシーに重点を置いています。
正解: **(正解を表示します)**
To help ensure that an information security training program is MOST effective, its contents should be based on employees' roles, as different roles have different information security responsibilities, needs, and risks. A role-based training program can tailor the content and delivery methods to suit the specific learning objectives and outcomes for each role, and enhance the relevance and retention of the information security knowledge and skills. Based on recent incidents is not the best answer, as it may not cover all the information security topics that are important for the organization, and may not address the root causes or preventive measures of the incidents. Based on employees' roles is more comprehensive and proactive than based on recent incidents.
Aligned to business processes is not the best answer, as it may not reflect the individual roles and responsibilities of the employees, and may not cover all the information security aspects that are relevant for the organization. Based on employees' roles is more specific and personalized than aligned to business processes. Focused on information security policy is not the best answer, as it may not provide sufficient details or examples to help the employees understand and apply the information security policy in their daily work. Based on employees' roles is more practical and engaging than focused on information security policy. References = CISM Review Manual, 16th Edition, page 2241; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1002 To help ensure that an information security training program is MOST effective, its contents should be based on employees' roles. This is because different roles have different responsibilities and access levels to information and systems, and therefore face different types of threats and risks. By tailoring the training content to the specific needs and

expectations of each role, the training program can increase the relevance and retention of the information security knowledge and skills for the employees. Role-based training can also help employees understand their accountability and obligations for protecting information assets in their daily tasks

質問: **222**
情報セキュリティ予算の配分方法を定義する際に最も重要なのは次のどれですか?
A. 規制コンプライアンス基準
B. 情報セキュリティ戦略
C. 情報セキュリティポリシー
D. ビジネス影響評価
正解: **(**正解を表示します**)**
Information security strategy is the most important factor when defining how an information security budget should be allocated because it helps to align the security objectives and initiatives with the business goals and priorities. An information security strategy is a high-level plan that defines the vision, mission, scope, and direction of the security program, as well as the roles and responsibilities, governance structures, policies and standards, risk management approaches, and performance measurement methods. An information security strategy helps to identify and prioritize the security needs and requirements of the organization, as well as to allocate the resources and funding accordingly. An information security strategy also helps to communicate the value and benefits of security to the stakeholders and justify the security investments. Therefore, information security strategy is the correct answer.
References:
https://www.techtarget.com/searchsecurity/tip/Cybersecurity-budget-breakdown-and-best-practices
https://www.csoonline.com/article/3671108/how-2023-cybersecurity-budget-allocations-are-shaping-up.html
https://www.statista.com/statistics/1319677/companies-it-budget-allocated-to-security-worldwide/

質問: **223**
あるスタートアップ企業は、セキュリティレビューを実施していなかったため、脆弱性のある複数の新規アプリケーションを本番環境に導入しました。今後、効果的なアプリケーションリスク管理を実現するために、BESTはどのように役立つでしょうか？
A. 展開前にアプリケーションの自動スキャンを実行します。
B. 既存の開発チームにセキュリティ エンジニアを追加します。
C. 既存の変更管理に情報セキュリティを統合する
D. アプリケーション セキュリティのための新しいガバナンス カウンシルを作成します。
正解: **(**正解を表示します**)**

Integrating information security into existing change management processes ensures that security considerations are included in all application changes and deployments. This addresses the root cause of bypassed security reviews and provides a consistent, repeatable process to manage risk going forward.
"Integrating security into change management ensures that changes to systems and applications undergo appropriate security review and testing prior to implementation, thereby addressing vulnerabilities proactively."
- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Change Management*

質問: **224**
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、次の者にあります。
A. 内部監査マネージャー。
B. 情報セキュリティ担当者。
C. 運営委員会。
D. 取締役会。
正解: **D (**コメントを発表する**)**
The board of directors is the ultimate authority and accountability for ensuring the objectives of an information security framework are being met, as they are responsible for setting the strategic direction, approving the policies, overseeing the performance, and ensuring the compliance of the organization. The board of directors also delegates the authority and resources to the information security officer, the steering committee, and the internal audit manager, who are involved in the design, implementation, monitoring, and improvement of the information security framework.
References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.1.1, page 2131; CISM Online Review Course, Module 4, Lesson 1, Topic 12; CISM domain 1: Information security governance Updated 2022

質問: **225**
メッセージのネイティブ暗号化を提供する電子メール ソフトウェア パッケージの一般的な欠点は、暗号化が次の点であることです。
A. 添付ファイルを暗号化できません
B. 製品ドメイン間で相互運用できません。
C. キーの長さが不十分です。
D. キー回復メカニズムがありません。
正解: **(**正解を表示します**)**
Email software packages that provide native encryption of messages use proprietary algorithms and formats that are not compatible with other email software packages. This means that the encryption cannot interoperate across product domains, and the recipients

of encrypted messages must use the same email software package as the sender to decrypt and read the messages. This limits the usability and scalability of native encryption, and may also pose security risks if the encryption algorithms or formats are not well-tested or widely accepted. A common drawback of email software packages that provide native encryption of messages is that the encryption cannot interoperate across product domains1234. References = CISM Review Manual 15th Edition, page 206. The Top 10 Email Encryption Solutions In 2023 - Expert Insights2, The Best Email Encryption Services for 2023 | PCMag3, The Top 12 Email Encryption Services for 2023 - Right Inbox4.
A common drawback of email software packages that provide native encryption of messages is that the encryption cannot interoperate across product domains. This means that emails sent from one product cannot be read by another product, as the encryption keys used are not compatible. This can be a problem when sending emails to people who use different software packages, as the encrypted emails cannot be read.

質問**: 226**
サイバーセキュリティの脅威状況を定期的にレビューする主な理由はどれですか?
A. 新たな傾向と既存の組織のセキュリティ体制を比較する
B. 最悪のシナリオを上級管理職に伝える
C. 新たな脅威を軽減するための情報セキュリティ専門家のトレーニング
D. 組織の情報セキュリティを拡大する機会を特定する
正解**: (**正解を表示します**)**
The primary reason to perform regular reviews of the cybersecurity threat landscape is to compare emerging trends with the existing organizational security posture, as this helps the information security manager to identify and prioritize the gaps and risks that need to be addressed. The cybersecurity threat landscape is dynamic and constantly evolving, and the organization's security posture may not be adequate or aligned with the current and future threats. By reviewing the threat landscape regularly, the information security manager can assess the effectiveness and maturity of the security program, and recommend appropriate actions and controls to improve the security posture and reduce the likelihood and impact of cyberattacks. References = CISM Review Manual 2023, page 831; CISM Review Questions, Answers & Explanations Manual 2023, page 322; ISACA CISM - iSecPrep, page 173

質問: **227**
上級管理職に情報セキュリティ戦略計画をレビューして承認してもらう主な理由は、次の点を確実にするためです。
A. 組織には計画を実行するために必要な資金があります。
B. 法律および規制の要件への準拠。
C. 情報セキュリティへの取り組みへのスタッフの参加。
D. 計画はコーポレートガバナンスと一致しています。
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: **228**
制御目標を定義する際に考慮すべき最も重要なのは次のどれですか?
A. 業界のベストプラクティス
B. 情報セキュリティフレームワーク
C. 最近の監査からのコントロール推奨事項
D. 組織のリスク許容度

正解: **(**正解を表示します**)**
The organization's risk appetite is the most important factor to consider when defining control objectives, because it reflects the amount and type of risk that the organization is willing to accept or avoid in pursuit of its goals. Control objectives should align with the risk appetite and support the achievement of the organization's objectives. Industry best practices, an information security framework, and control recommendations from a recent audit are also useful sources of guidance, but they are not as critical as the risk appetite. References = CISM Review Manual, 16th Edition, page 75

質問: **229**
次のどれが事業継続計画 (BCP) 内のトリガーを定義しますか?
A. 組織のニーズ
B. 災害復旧計画 (DRP)
C. 情報セキュリティポリシー
D. ギャップ分析
正解: **(**正解を表示します**)**
The needs of the organization define the triggers within a business continuity plan (BCP). Triggers are the events or conditions that initiate the activation of the BCP. The triggers should be based on the organization's business objectives, risk appetite, recovery time objectives, and recovery point objectives. The triggers should also be aligned with the organization's information security policy, disaster recovery plan, and gap analysis. However, these are not the primary factors that define the triggers, but rather the supporting elements that help implement the BCP. The needs of the organization are the main drivers for determining the triggers, as they reflect the organization's priorities, expectations, and requirements for business continuity. References = CISM Review Manual (Digital Version) 1, Chapter 4: Information Security Incident Management, pages 191-
192, 195-196, 199-200.
Business Continuity Management Guideline 2, page 5, Section 4.2.1: Triggers Business Continuity Plan - Open Risk Manual 3, page 1, Section 1: Introduction

質問: **230**
情報セキュリティ運営委員会の最も重要な機能はどれですか?
A. 組織資産へのデータ分類の割り当て
B. 組織のリスク評価プロセスの開発
C. ビジネスから多様な視点を得る
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: **231**
情報セキュリティ管理者がマルチユーザー環境での汎用管理者アカウントの使用を制限する必要がある主な理由はどれですか?
A. 職務の分離が維持されるようにする
B. 不正なユーザーアクセスを防ぐため
C. システム監査証跡がバイパスされないようにするため
D. 説明責任の問題を防ぐため
正解: **D (**コメントを発表する**)**

質問: **232**
経験豊富な情報セキュリティ マネージャーが新しい組織に加わり、すべての主要な IT プロセスの監査を開始します。脆弱性管理プログラムに関する次の調査結果のうち、最も懸念すべきものはどれですか。
A. 特定された脆弱性の数は業界のベンチマークを超えています。
B. 特定された脆弱性は公開されておらず、認識プログラムで伝達されていません。
C. 脆弱性は外部コンサルタントではなく社内スタッフによって特定されます。
D. 特定された脆弱性は記録されず、タイムリーに解決されません。
正解: **(**正解を表示します**)**

質問: **233**
組織が Disaster Recovery as a Service (DRaaS) を使用する最も適切な理由はどれですか?
A. ビジネス部門がテストを実行する必要がなくなります。
B. 企業の年間コストを削減します。
C. オフサイト施設を維持する必要がなくなります。
D. 回復に伴うリスクを第三者に移転します。
正解: **(**正解を表示します**)**

質問: **234**
情報セキュリティガバナンスの有効性を監視するための最適なツールは次のどれですか?
A. 主要業績評価指標 (KPI)
B. バランストスコアカード
C. ビジネス影響分析 (BIA)
D. リスクプロファイル

正解: **(**正解を表示します**)**
Key performance indicators (KPIs) are the best tool to monitor the effectiveness of information security governance because they are quantifiable and measurable metrics that reflect the achievement of the information security objectives and the alignment of the information security strategy with the business goals.
KPIs can help to evaluate the performance, efficiency, quality, and value of the information security processes and activities, and to identify the areas of improvement or adjustment.
KPIs can also provide feedback to the management and the stakeholders on the status and progress of the information security governance. Some examples of KPIs for information security governance are: percentage of compliance with security policies and standards, number and severity of security incidents, return on security investment, and maturity level of information security capabilities12.
A balanced scorecard is a strategic management tool that translates the vision and mission of the organization into four perspectives: financial, customer, internal process, and learning and growth. A balanced scorecard can help to align the information security strategy with the business strategy, but it is not a tool to monitor the effectiveness of information security governance. A balanced scorecard can include KPIs as part of its measurement system, but it is not a substitute for KPIs13.
A business impact analysis (BIA) is a process of assessing the potential consequences of a disruption to the organization's critical business functions or processes. A BIA can help to identify the critical assets, dependencies, recovery priorities, and recovery objectives for the information security program, but it is not a tool to monitor the effectiveness of information security governance. A BIA is a one-time or periodic activity, not a continuous monitoring process14.
A risk profile is a representation of the organization's exposure to various types of risks, such as operational, financial, strategic, or reputational. A risk profile can help to identify the sources, likelihood, and impact of potential threats to the organization's assets and objectives, and to determine the risk appetite and tolerance for the information security program, but it is not a tool to monitor the effectiveness of information security governance. A risk profile is a snapshot of the organization's risk posture at a given point in time, not a dynamic monitoring tool15. References = CISM Review Manual, 16th Edition, pages 23-241; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.122; CISM Review Questions, Answers & Explanations Database, Question ID 10093; CISM Review Questions, Answers & Explanations Database, Question ID 10104; CISM Review Questions, Answers & Explanations Database, Question ID 10115

質問: **235**
情報セキュリティ プログラムに対する管理サポートを維持するための最も有用な手法は次のとおりです。
A. 業務運営のセキュリティについて経営陣に通知します。
B. 包括的なセキュリティ意識向上およびトレーニング プログラムを実装します。

C. 標準に準拠しなかった場合のリスクと結果を特定します。
D. 同等の組織のセキュリティ プログラムをベンチマークします。
正解: **(**正解を表示します**)**
= According to the CISM Review Manual, one of the key success factors for an information security program is to maintain management support and commitment. This can be achieved by providing regular reports to management on the security status of the organization, the effectiveness of the security controls, and the alignment of the security program with the business objectives and strategy. By informing management about the security of business operations, the information security manager can demonstrate the value and benefits of the security program, and ensure that management is aware of the security risks and issues that need to be addressed. This technique can also help to build trust and confidence between the information security manager and the senior management, and foster a culture of security within the organization1 The other options are not as effective as informing management about the security of business operations. Implementing a comprehensive security awareness and training program is important, but it is mainly targeted at the end users and staff, not the senior management. Identifying the risks and consequences of failure to comply with standards can help to justify the need for security controls, but it can also create a negative impression of the security program as being too restrictive or punitive. Benchmarking the security programs of comparable organizations can provide some insights and best practices, but it may not reflect the specific needs and context of the organization, and it may not be relevant or applicable to the management's expectations and priorities1 References = 1: CISM Review Manual, 16th Edition, ISACA, 2020, pp. 28-29...

質問: **236**
ある組織は、販売部門を拡張するためにインターネット販売会社を買収しました。情報セキュリティ管理者がセキュリティ ポリシーのフレームワークに新しいビジネス モデルを確実に組み込むための最初のステップは、次のとおりです。
A. ギャップ分析を実行します。
B. 両社のポリシーを別々に実装する
C. 両社のポリシーを統合します。
D. 脆弱性評価を実行します。
正解: **(**正解を表示します**)**
Performing a gap analysis is the first step to ensure the security policy framework encompasses the new business model because it is a process of comparing the current state of security policies and controls with the desired or required state. A gap analysis helps to identify the strengths and weaknesses of the existing security policy framework, as well as the opportunities and threats posed by the new business model. A gap analysis also helps to prioritize the actions and resources needed to close the gaps and align the

security policy framework with the new business objectives and requirements. Therefore, performing a gap analysis is the correct answer.
References:
* https://secureframe.com/blog/security-frameworks
* https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the- right-one

質問: **237**
リスクの影響が重要でないと判断され、その可能性も非常に低い場合の最も適切なリスク対応は次のどれですか?
A. 軽減
B. 受け入れる
C. 避ける
D. 転送
正解: **(**正解を表示します**)**

質問: **238**
新しいサーバーが適切に保護されていることを最も効果的に保証できるのは次のどれですか?
A. 安全なコードレビューの実行
B. 技術的なセキュリティ基準の施行
C. 侵入テストの実施
D. セキュリティスキャンを開始しています
正解: **B (**コメントを発表する**)**
Enforcing technical security standards is the most effective way to ensure that a new server is appropriately secured because it ensures that the server complies with the organization's security policies and best practices, such as encryption, authentication, patching, and hardening. Performing secure code reviews is not relevant for securing a new server, unless it is running custom applications that need to be verified for security flaws.
Conducting penetration testing is not sufficient for securing a new server, because it only identifies vulnerabilities that can be exploited by attackers, but does not fix them. Initiating security scanning is not sufficient for securing a new server, because it only detects known vulnerabilities or misconfigurations, but does not enforce security standards or remediate issues. 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-3/secure-code-review https://www.isaca.org/resources/isaca- journal/issues/2017/volume-2/the-value-of-penetration-testing https://www.isaca.org/resources/isaca-journal /issues/2016/volume-5/security-scanning-versus-penetration-testing

質問: **239**
最悪の混乱シナリオを特定するのに最も役立つのは次のどれでしょうか?
A. ビジネス影響分析 (BIA)
B. ビジネスプロセス分析
C. SWOT分析
D. キャストメリット分析
正解: **A (**コメントを発表する**)**
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.

質問: **240**
リスクと管理の所有権の割り当てを可能にする最適な方法はどれですか?
A. 業界で認められた制御フレームワークに準拠
B. リスク管理フレームワークの導入
C. 上級管理職の賛同を得る
D. 情報セキュリティ戦略の策定
正解: **(**正解を表示します**)**
Obtaining senior management buy-in is the best way to enable the assignment of risk and control ownership because it helps to establish the authority and accountability of the risk and control owners, as well as to provide them with the necessary resources and support to perform their roles. Risk and control ownership refers to the assignment of specific responsibilities and accountabilities for managing risks and controls to individuals or groups within the organization. Obtaining senior management buy-in helps to ensure that risk and control ownership is aligned with the organizational objectives, structure, and culture, as well as to communicate the expectations and benefits of risk and control ownership to all stakeholders. Therefore, obtaining senior management buy-in is the correct answer.
References:
https://www.protechtgroup.com/en-au/blog/risk-control-management
https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/risk/working%20papers
/23_getting_risk_ownership_right.ashx
https://www.linkedin.com/pulse/risk-controls-who-owns-them-david-tattam

質問: **241**
新しい情報セキュリティ プログラムを確立する際の主な目的は次のどれですか?
A. セキュリティ戦略の実行
B. 組織リスクの最小化
C. リソースの最適化
D. 運用セキュリティの促進
正解: **A (**コメントを発表する**)**
According to the CISM Review Manual, the primary objective when establishing a new information security program is to execute the security strategy that has been defined and approved by the senior management. The security strategy provides the direction, scope, and goals for the information security program, and aligns with the business objectives and requirements. Minimizing organizational risk, optimizing resources, and facilitating operational security are possible outcomes or benefits of the information security program, but they are not the primary objective.
References = CISM Review Manual, 27th Edition, Chapter 3, Section 3.1.1, page 1151.

質問: **242**
潜在的なセキュリティ侵害に対するセキュリティ オペレーション センターの対応において、最も大きな課題となるのは次のどれですか。
A. IT システム クロックが集中ログ サーバーと同期されていません。
B. オペレーティング システムはベンダーによってサポートされなくなりました。
C. パッチ管理システムは、パッチをタイムリーに展開しません。
D. 組織にはクラウド サービスを使用する分散型データ センターがあります。
正解: **(**正解を表示します**)**
A security operations center (SOC) relies on the centralized logging server to collect, store, analyze and correlate security events from various sources such as firewalls, intrusion detection systems, antivirus software, etc. The centralized logging server uses the timestamps of the events to perform the analysis and correlation. If the IT system clocks are not synchronized with the centralized logging server, the SOC will face difficulties in identifying the sequence and causality of the events, which will affect its ability to detect

and respond to potential security breaches. Therefore, this presents the greatest challenge to the SOC's awareness of potential security breaches.
Operating systems that are no longer supported by the vendor may pose a security risk, but they can be mitigated by applying compensating controls such as isolation, segmentation, monitoring, etc. The patch management system that does not deploy patches in a timely manner may also increase the vulnerability exposure, but it can be remediated by prioritizing and applying the critical patches as soon as possible. An organization that has a decentralized data center that uses cloud services may face some challenges in ensuring the security and compliance of the cloud environment, but it can leverage the cloud service provider' s security capabilities and tools to enhance the SOC's visibility and control. Therefore, these options are not the greatest challenges to the SOC's awareness of potential security breaches. 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; RSI Security, Common Challenges of SOC Teams3; Infosec Matter, Security Operations Center: Challenges of SOC Teams4

質問: **243**
金融機関の経営陣は、運用上のリスクを受け入れ、その結果、重要な監視プロセスを一時的に停止することになりました。この状況で情報セキュリティ管理者が最も懸念すべきことは、次のうちどれですか?
A. コンプライアンス リスクへの影響。
B. 短期的な影響を判断できない。
C. リスク文化への影響。
D. リスク管理のベストプラクティスからの逸脱
正解: **C (**コメントを発表する**)**
Comprehensive and Detailed Explanation = The impact on the risk culture is the greatest concern for the information security manager, because it reflects the attitude and behavior of the organization towards risk management. If management accepts an operational risk that compromises a critical monitoring process, it may indicate a lack of awareness, commitment, or accountability for risk management. This may erode the trust and confidence of the stakeholders, regulators, and customers, and expose the organization to further risks. The impact on compliance risk, the inability to determine short-term impact, and the deviation from risk management best practices are also important, but they are secondary to the impact on the risk culture.
References = CISM Review Manual 15th Edition, page 48. CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, question ID 421.

質問: **244**

ある組織は、アプリケーションの脆弱性に起因す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ていることを確認するための最良の方法は、次のうちどれですか？
A. 内部監査を実施します。
B. 侵入テストを実施します。
C. 脆弱性評価を実行します。
D. 補正コントロールを準備します。
正解: **(**正解を表示します**)**
After implementing controls, performing a vulnerability assessment is the best way to verify that all previously identified weaknesses have been addressed. The CISM Review Manual specifies that vulnerability assessments systematically scan for known vulnerabilities and confirm remediation effectiveness. Penetration testing is valuable but is typically used to exploit vulnerabilities, not comprehensively verify their remediation as efficiently as vulnerability assessments.
Reference:ISACA CISM Review Manual, 16th Edition, Page 164-165, "Vulnerability Management and Assessment".

質問: **245**
情報セキュリティ リソースの要件を特定する際に、情報セキュリティ マネージャーが考慮すべき最も重要なのは次のどれですか。
A. 潜在的なリソースの可用性
B. 情報セキュリティインシデント
C. 情報セキュリティ戦略
D. 現在のリソースレベル
正解: **(**正解を表示します**)**

質問: **246**
従業員のセキュリティ意識向上トレーニング プログラムを実施した後、どのような結果が期待されるでしょうか?
A. 受信メール内で検出されたウイルスの数の減少
B. 報告されたソーシャルエンジニアリング攻撃の減少
C. 報告されたソーシャルエンジニアリングの試みの増加
D. ユーザーから報告された誤検知件数の増加
正解: **(**正解を表示します**)**
This outcome indicates that the employees are more aware of the signs and techniques of social engineering and are able to report them to the appropriate authorities. This also helps to prevent successful attacks and reduce the impact of potential breaches.
References: The CISM Review Manual 2023 states that "security awareness training should include information on how to identify and report social engineering attempts" and that "the effectiveness of security awareness training can be measured by the number and

quality of reported incidents" (p. 121). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "An increase in reported social engineering attempts is the best indicator that the security awareness training program has been effective, as it shows that the employees are more vigilant and proactive in detecting and reporting such attempts" (p. 45).

質問: **247**
侵入検知システム (IDS) によって外部ネットワークベースの攻撃が報告されたときにファイアウォール ログを確認する主な理由はどれですか。
A. ペイロード署名を検証する
B. ネットワーク構成を確認する
C. インシデント対応戦略を策定する
D. インシデントを検証する
正解: **(**正解を表示します**)**

質問: **248**
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次のことを行う必要があります。
A. 主要リスク指標 (KRI) を確認する
B. ギャップ分析を実行する
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: **B (**コメントを発表する**)**
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: **249**
セキュリティ インシデントを効果的に封じ込めるアプローチを開発する際に、最も重要な考慮事項は次のどれですか。
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分離する
B. ビジネスに影響を及ぼす可能性のある評判の損失を軽減する
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: **(**正解を表示します**)**

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: **250**
情報セキュリティ投資に関する経営上の意思決定は、以下の点に基づいて行われる場合に最も効果的です。
A. 脅威と脆弱性を識別および分析するプロセス。
B. セキュリティイベントの履歴から決定された年間損失予想値 ALE)、
C. 一貫性のある定期的なリスク評価の報告。
D. 経営陣によるリスク分析の正式な承認、
正解: **(**正解を表示します**)**
Management decisions concerning information security investments will be most effective when they are based on the reporting of consistent and periodic assessments of risks. This will help management to understand the current and emerging threats, vulnerabilities, and impacts that affect the organization's information assets and business processes. It will also help management to prioritize the allocation of resources and funding for the most critical and cost-effective security controls and solutions. The reporting of consistent and periodic assessments of risks will also enable management to monitor the performance and effectiveness of the information security program, and to adjust the security strategy and objectives as needed. References = CISM Review Manual 15th Edition, page 28.

質問: **251**
新しい情報セキュリティ マネージャーが規制対象外の組織の情報セキュリティ戦略を策定する際に、次のどれを確認するのが最も役立ちますか?
A. 経営陣のビジネス目標と目的
B. その他の非規制企業の戦略
C. リスク評価結果
D. 業界のベストプラクティスと管理の推奨事項
正解: **(**正解を表示します**)**
When a new information security manager is developing an information security strategy for a non-regulated organization, reviewing the management's business goals and objectives would be the most helpful. This is because the information security strategy should be aligned with and support the organization's vision, mission, values, and strategic

direction. The information security strategy should also enable the organization to achieve its desired outcomes, such as increasing revenue, reducing costs, enhancing customer satisfaction, or improving operational efficiency. By reviewing the management's business goals and objectives, the information security manager can understand the business context, needs, and expectations of the organization, and design the information security strategy accordingly. The information security manager can also communicate the value proposition and benefits of the information security strategy to the management and other stakeholders, and gain their support and commitment.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:
Information Security Strategy, page 211; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 48, page 452.

質問: **252**
サイバーセキュリティ侵害の最も一般的な原因は次のどれですか?
A. 適切なパスワードローテーションの欠如
B. 人為的ミス
C. 特権アカウントの不正使用
D. 制御ベースラインの欠如
正解: **(正解を表示します)**
Human error remains the leading cause of cybersecurity breaches, including mishandling data, misconfigurations, and falling for phishing attacks.
"Human error continues to be one of the most common causes of data breaches and security incidents."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Root Cause Analysis*

質問: **253**
セキュリティ標準への非準拠に対処するための最適なアプローチは次のどれですか?
A. 新しいセキュリティ標準を開発します。
B. セキュリティ例外プロセスを維持します。
C. セキュリティ要件が満たされるまで、影響を受けるアクティビティを中止します。
D. 影響を受ける資産に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: **254**
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.

質問: **255**
インシデント対応計画にインシデント分類基準を含めることの最大の利点は次のどれですか?
A. インシデント管理コストを監視および制御する機能
B. 混乱の影響をより明確に把握
C. 情報資産の効果的な保護
D. 回復リソースの割り当ての最適化
正解: **D (**コメントを発表する**)**
The explanation given in the manual is:
Incident classification criteria enable an organization to prioritize incidents based on their impact and urgency. This allows for an optimized allocation of recovery resources to minimize business disruption and ensure timely restoration of normal operations. The other choices are benefits of incident management but not directly related to incident classification criteria.

質問: **256**
情報セキュリティ意識向上トレーニング プログラムの主な利点は次のどれですか?
A. 人間の行動に影響を与える
B. 組織のセキュリティ文化の評価
C. リスクの説明責任の定義
D. セキュリティポリシーの適用
正解: **(**正解を表示します**)**
Influencing human behavior is the primary benefit of an information security awareness training program because it helps to reduce the human errors and vulnerabilities that can compromise the security of data and systems. An information security awareness training program is a process or a program that informs and empowers users to protect data and computing assets from security risks and cyberattacks. It includes educational offerings that cover regulatory requirements, compliance policies, and safe computing practices. An information security awareness training program helps to influence human behavior by raising awareness of the security threats and challenges, enhancing knowledge and skills of the security best practices and controls, and fostering a positive security culture and attitude among the users. By influencing human behavior, an information security awareness training program can improve the security posture and performance of the organization, as well as prevent or mitigate the impact of security incidents. Therefore, influencing human behavior is the correct answer.
References:
https://www.isms.online/iso-27002/control-6-3-information-security-awareness-education-and-training/
https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/the-benefits-of-information-security-and- privacy-awareness-training-programs
https://threatcop.com/blog/benefits-and-purpose-of-security-awareness-training/.

質問: **257**
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) に準拠していないことに気付きました。次のうち、最善の対応策はどれですか。
A. 問題を上級管理職に通知します。

B. 問題を法務担当者に報告します。
C. 契約の再交渉を開始します。
D. 問題の範囲を評価します。
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: **258**
上級管理職への情報セキュリティ状況レポートに含めるべき最も重要な項目は次のどれですか?
A. 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のリスト
正解: **A (**コメントを発表する**)**
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: **259**
セキュリティ例外を許可する主な理由はどれですか?
A. リスクはビジネスにかかるコストによって正当化されます。
B. リスクはセキュリティ上の利点によって正当化されます。
C. リスクはセキュリティにかかるコストによって正当化されます。
D. リスクはビジネスへの利益によって正当化されます。
正解: **(**正解を表示します**)**
= A security exception is a formal authorization to deviate from a security policy, standard, or control, due to a valid business reason or requirement. The primary reason for granting a security exception is that the risk associated with the deviation is justified by the benefit

to the business, such as increased efficiency, productivity, customer satisfaction, or competitive advantage. The security exception should be approved by the appropriate authority, such as the senior management or the risk committee, based on a risk assessment and a cost-benefit analysis. The security exception should also be documented, communicated, monitored, and reviewed periodically123. References =
* 1: CISM Review Manual 15th Edition, page 364
* 2: CISM Practice Quiz, question 1132
* 3: Security Policy Exception Management, section "Security Policy Exception Management Process"

質問: **260**
災害をタイムリーに宣言する主な目的は次のとおりです。
A. 回復プロセスに経営幹部が関与することを確実にします。
B. 災害復旧プロセスの欠陥を評価し、修正します。
C. 重要な物理資産をさらなる損失から保護します。
D. 組織の重要なサービスの継続性を確保します。
正解: **(**正解を表示します**)**
The primary objective of timely declaration of a disaster is to ensure the continuity of the organization's essential services, which are the services that are critical for the survival and operation of the organization, and that cannot be interrupted or delayed without causing severe consequences. By declaring a disaster, the organization can activate its disaster recovery plan (DRP), which is a set of documented procedures and resources to recover the essential services in the event of a disaster. The DRP should include the roles and responsibilities, the communication channels, the recovery strategies, the backup and restoration procedures, and the testing and maintenance activities for the disaster recovery process1.
References = CISM Review Manual, 16th Edition eBook2, Chapter 9: Business Continuity and Disaster Recovery, Section: Disaster Recovery Planning, Subsection: Disaster Declaration, Page 372.

質問: **261**
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. モバイル デバイス管理 (MDM) ソリューションを実装します。
B. 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。
C. 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。
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: **C (**コメントを発表する**)**

質問: **262**

サービス拒否 (DoS) 攻撃が失敗した後、特定される弱点は次のようなものになります。
A. コストに関係なく、迅速に解決および排除されます。
B. 最終的に解決されるまで追跡され、報告されます。
C. セキュリティ認識プログラムに記載されています。
D. 同様の弱点が見つかった場合は記録され、後で再検査されます。
正解: **(**正解を表示します**)**

質問: **263**
組織の重要なサードパーティプロバイダーの 1 つでデータ侵害が発生した場合、情報セキュリティマネージャーが最初に取るべき行動は次のどれですか?
A. 広報担当者に知らせてください。
B. 第三者の応答を監視します。
C. インシデント対応計画を呼び出します。
D. 侵害について顧客に通知します。
正解: **C (**コメントを発表する**)**
The first course of action when one of the organization's critical third-party providers experiences a data breach is to invoke the incident response plan, which means activating the incident response team and following the predefined procedures and protocols to respond to the breach. Invoking the incident response plan helps to coordinate the communication and collaboration with the third-party provider, assess the scope and impact of the breach, contain and eradicate the threat, recover the affected systems and data, and report and disclose the incident to the relevant stakeholders and authorities.
References = Cybersecurity Incident Response Exercise Guidance - ISACA, Plan for third-party cybersecurity incident management

質問: **264**
情報セキュリティ マネージャーは、組織内の主要なデータ処理システムに影響を与える新しい脆弱性について通知を受けました。次のうち、最初に実行する必要があるのはどれですか。
A. 上級管理職に通知する
B. リスクを再評価する
C. 補償制御を実装する
D. 事業主に新しい改善計画を依頼する
正解: **B (**コメントを発表する**)**
The first step when a new vulnerability is identified is to re-evaluate the risk associated with the vulnerability.
This may require an update to the risk assessment and the implementation of additional controls. Informing senior management of the vulnerability is important, but should not be the first step. Implementing compensating controls may also be necessary, but again,

should not be the first step. Asking the business owner for a remediation plan may be useful, but only after the risk has been re-evaluated.
The information security manager should first re-evaluate the risk posed by the new vulnerability to determine its impact and likelihood. Based on this assessment, appropriate actions can be taken such as informing senior management, implementing compensating controls, or requesting a remediation plan from the business owner.
The other choices are possible actions but not necessarily the first one.
A vulnerability is a weakness that can be exploited by an attacker to compromise a system or network2. A vulnerability can affect key data processing systems within an organization if it exposes sensitive information, disrupts business operations, or damages assets2. A vulnerability assessment is a process of identifying and evaluating vulnerabilities and their potential consequences2

質問**: 265**
ある組織では、フィッシング メッセージに関連するインシデントが急増しています。根本的な原因は、ベンダーによるサポートが終了した古い電子メール フィルタリング システムです。情報セキュリティ マネージャーが最初に取るべき行動は次のうちどれですか。
A. エンドユーザーのセキュリティ意識向上の実践を強化します。
B. 電子メール システムを一時的にクラウド プロバイダーにアウトソーシングします。
C. システムを置き換えるためのビジネスケースを作成します。
D. ファイアウォール上の送信トラフィックを監視します。
正解**: C (**コメントを発表する**)**
Developing a business case to replace the system is the FIRST course of action that the information security manager should take, because it helps to justify the need for a new and effective email filtering system that can prevent or reduce phishing incidents. A business case should include the problem statement, the proposed solution, the costs and benefits, the risks and assumptions, and the expected outcomes and metrics.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 42: "A business case is a document that provides the rationale and justification for an information security investment. It should include the problem statement, the proposed solution, the costs and benefits, the risks and assumptions, and the expected outcomes and metrics." Email Filtering Explained: What Is It and How Does It Work: "Email filtering is a process used to sort emails and identify unwanted messages such as spam, malware, and phishing attempts. The goal is to ensure that they don't reach the recipient's primary inbox. It is an essential security measure that helps protect users from unwanted or malicious messages." Cloud-based email phishing attack using machine and deep learning ...: "This attack is used to attack your email account and hack sensitive data easily."

質問**: 266**

情報セキュリティ運営委員会の設立によって組織は主にどのようなメリットを得られるのでしょうか?
A. 情報セキュリティリスク意識の向上
B. 情報セキュリティとビジネスとの連携強化
C. 情報セキュリティリソース管理への重点化
D. ビジネスに影響を与える業界のセキュリティトレンドとの整合性の向上
正解: **(**正解を表示します**)**

質問: **267**
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確立するための主な基準は次のどれですか。
A. 残留リスク
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

質問: **268**
セキュリティギャップを解決するためのアウトソーシングの承認を得るために最初に行うべきステップは次のどれですか?
A. 追加のメトリックを収集します。
B. 費用対効果分析を実行します。
C. 上級管理職に資金援助の要請を提出します。
D. アウトソーシング会社のデューデリジェンスを開始します。
正解: **(**正解を表示します**)**
The first step to gain approval for outsourcing to address a security gap is to perform a cost-benefit analysis, because it helps to evaluate the feasibility and viability of the outsourcing option and compare it with other alternatives. A cost-benefit analysis is a method of estimating and comparing the costs and benefits of a project or a decision, in terms of financial, operational, and strategic aspects. A cost-benefit analysis can help to:

Identify and quantify the expected costs and benefits of outsourcing, such as the initial and ongoing expenses, the potential savings and revenues, the quality and efficiency of the service, the risks and opportunities, and the alignment with the business objectives and requirements Assess and prioritize the criticality and urgency of the security gap, and the impact and likelihood of the related threats and vulnerabilities Determine the optimal level and scope of outsourcing, such as the type, duration, and frequency of the service, the roles and responsibilities of the parties involved, and the performance and security standards and metrics Justify and communicate the rationale and value proposition of outsourcing, and provide evidence and support for the decision making process Establish and document the criteria and process for selecting and evaluating the outsourcing provider, and the contractual and legal terms and conditions A cost-benefit analysis should be performed before submitting a funding request to senior management, because it can help to demonstrate the need and the return on investment of the outsourcing project, and to secure the budget and the resources. A cost-benefit analysis should also be performed before beginning due diligence on the outsourcing company, because it can help to narrow down the list of potential candidates and to focus on the most relevant and suitable ones. Collecting additional metrics may be a part of the cost-benefit analysis, but it is not the first step, because it requires a clear definition and understanding of the objectives and scope of the outsourcing project.
References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 173-174, 177-178.

質問**: 269**
情報セキュリティ管理者は、事業部門のリーダーが顧客にリーチするためにソーシャル メディア プラットフォームの使用を増やすことを奨励していることを知りました。従業員がソーシャルメディア上で機密情報を公開するリスクを軽減するには、次のうちどれを最初に行うべきですか?
A. 組織全体のソーシャル メディア ポリシーを確立します。
B. ソーシャル メディア サイトの悪用に対する制裁を策定します。
C. 従業員がアクセスするソーシャル メディア サイトを監視します。
D. 企業デバイスでのソーシャル メディア アクセスを制限します。
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: **270**
次のうち、情報セキュリティ プログラムに対する上級管理職のコミットメントを得るための情報セキュリティ管理者の取り組みを促進するのに最も適しているのはどれですか?
A. 固有のリスクの証拠を提示する
B. セキュリティ成熟度レベルの報告
C. コンプライアンス要件の提示
D. 残存リスクの伝達
正解: **(正解を表示します)**
Communicating the residual risk is the best way to facilitate an information security manager's efforts to obtain senior management commitment for an information security program. The residual risk is the level of risk that remains after applying the security controls and mitigation measures. The residual risk reflects the effectiveness and efficiency of the information security program, as well as the potential impact and exposure of the organization. The information security manager should communicate the residual risk to the senior management in a clear, concise, and relevant manner, using quantitative or qualitative methods, such as risk matrices, heat maps, dashboards, or reports. The communication of the residual risk should also include the comparison with the inherent risk, which is the level of risk before applying any security controls, and the risk appetite, which is the level of risk that the organization is willing to accept. The communication of the residual risk should help the senior management to understand the value and performance of the information security program, as well as the need and justification for further investment or improvement. Presenting evidence of inherent risk, reporting the security maturity level, and presenting compliance requirements are all important aspects of the information security program, but they are not the best ways to obtain senior management commitment. These aspects may not directly demonstrate the benefits or outcomes of the information security program, or they may not align with the business objectives or priorities of the organization. For example, presenting evidence of inherent risk may show the potential threats and vulnerabilities that the organization faces, but it may not indicate how the information security program addresses or reduces them. Reporting the security maturity level may show the progress and status of the information security program, but it may not relate to the risk level or the business impact. Presenting compliance requirements may show the legal or regulatory obligations that the organization must fulfill, but it may not reflect the actual security needs or goals of the organization. Therefore, communicating the residual risk is the best way to obtain senior management commitment for an information security program, as it shows the results and value of the information security program for the organization. References = CISM Review Manual 2023, page 41 1; CISM Practice Quiz 2

質問: **271**
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: **272**
情報セキュリティ プログラムの要件が雇用および人員配置プロセスと一致している場合、組織にとっての主なメリットは何ですか?
A. セキュリティインシデントの報告手順に従います。
B. セキュリティスタッフ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ます。
D. アクセスはタスク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**: 273**
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. メトリクスレポート
B. 侵入防止
C. ファイアウォールの調整
D. 事件調査
正解**: B (**コメントを発表する**)**

質問: **274**
組織のセキュリティ体制を理解するために、組織の上級管理職が次のことを行うことが最も重要です。
A. 最新のインシデント対応テストの結果を評価します。
B. 報告されたセキュリティ インシデントの数を確認します。
C. 確立されたセキュリティ メトリックが報告されていることを確認します。
D. リスク軽減の取り組みの進捗状況を評価します。
正解: **D** (コメントを発表する)
According to the CISM Review Manual, an organization's security posture is the overall condition of its information security, which is determined by the effectiveness of its security program and the alignment of its security objectives with its business goals. To understand the security posture, the senior leadership needs to have a holistic view of the security risks and the actions taken to address them. Therefore, assessing the progress of risk mitigation efforts is the most important activity for the senior leadership, as it provides them with the information on how well the security program is performing and whether it is meeting the expected outcomes. Evaluating the results of the most recent incident response test, reviewing the number of reported security incidents, and ensuring established security metrics are reported are all useful activities for the senior leadership, but they are not sufficient to understand the security posture. They only provide partial or isolated information on the security performance, which may not reflect the overall security condition or the alignment with the business objectives. References = CISM Review Manual, 16th Edition, Chapter 1, Information Security Governance, pages 28-29.

質問: **275**
情報セキュリティ マネージャーが組織の情報セキュリティ プログラムの有効性を向上させるための最良の方法はどれでしょうか?
A. セキュリティとパフォーマンスの競合の解決に重点を置きます。
B. コントロールを決定する際にビジネス部門と IT 部門が協力します。
C. 変更管理プロセスに情報セキュリティ要件を含めます。
D. 自動化されたセキュリティ チャネルを実装するには、IT 部門から支援を受けます。
正解: (正解を表示します)
The best way for an information security manager to improve the effectiveness of an organization's information security program is to collaborate with business and IT functions in determining controls.
Collaboration is a key factor for ensuring that the information security program is aligned with the organization's business objectives, risk appetite, and security strategy, and that it supports the business processes and activities. Collaboration also helps to gain the buy-in, involvement, and ownership of the business and IT functions, who are the primary stakeholders and users of the information security program.

Collaboration also facilitates the communication, coordination, and integration of the information security program across the organization, and enables the information security manager to understand the needs, expectations, and challenges of the business and IT functions, and to propose the most appropriate and effective security controls and solutions.

Focusing on addressing conflicts between security and performance (A) is a possible way to improve the effectiveness of an information security program, but not the best one. Security and performance are often competing or conflicting goals, as security controls may introduce overhead, complexity, or delays that affect the efficiency, usability, or availability of the systems or processes. Addressing these conflicts may help to optimize the balance and trade-off between security and performance, and to enhance the user satisfaction and acceptance of the security controls. However, focusing on addressing conflicts between security and performance does not necessarily improve the alignment, integration, or communication of the information security program with the business and IT functions, nor does it ensure the involvement or ownership of the stakeholders.

Including information security requirements in the change control process is also a possible way to improve the effectiveness of an information security program, but not the best one. The change control process is a process that manages the initiation, approval, implementation, and review of changes to the systems or processes, such as enhancements, updates, or fixes. Including information security requirements in the change control process may help to ensure that the changes do not introduce new or increased security risks or impacts, and that they comply with the security policies, standards, and procedures. However, including information security requirements in the change control process does not necessarily improve the collaboration, communication, or coordination of the information security program with the business and IT functions, nor does it ensure the buy-in or involvement of the stakeholders.

Obtaining assistance from IT to implement automated security controls (D) is also a possible way to improve the effectiveness of an information security program, but not the best one. Automated security controls are security controls that are implemented by using software, hardware, or other technologies, such as encryption, firewalls, or antivirus, to perform security functions or tasks without human intervention. Obtaining assistance from IT to implement automated security controls may help to improve the efficiency, consistency, or reliability of the security controls, and to reduce the human errors, negligence, or malicious actions. However, obtaining assistance from IT to implement automated security controls does not necessarily improve the collaboration, communication, or integration of the information security program with the business and IT functions, nor does it ensure the ownership or involvement of the stakeholders.

References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:

Information Security Strategy Development, Subsection: Collaboration, page 24-251

質問: **276**
セキュリティ情報およびイベント管理 (SIEM) システムによって提供される最大の価値は次のどれですか?
A. セキュリティポリシーのリポジトリベースの維持
B. ビジネスプロセスに対するエクスプロイトの影響の測定
C. リスク発生の監視を容易にする
D. ビジネス継続計画のためにイベントログを別の場所にリダイレクトする
正解: **(正解を表示します)**
A security information and event management (SIEM) system is a tool that collects, analyzes, and correlates security events from various sources, such as firewalls, intrusion detection systems, antivirus software, and other devices. A SIEM system can provide real-time alerts, dashboards, reports, and forensic analysis of security incidents. The greatest value of a SIEM system is that it can facilitate the monitoring of risk occurrences by identifying anomalies, trends, patterns, and indicators of compromise that may otherwise go unnoticed. A SIEM system can also help with incident response, compliance, and audit activities by providing evidence and documentation of security events.
References =
* ISACA, CISM Review Manual, 16th Edition, 2020, page 2291
* ISACA, CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, 2020, question ID 2082 The greatest value provided by a Security Information and Event Management (SIEM) system is facilitating the monitoring of risk occurrences. SIEM systems collect, analyze and alert on security-related data from various sources such as firewall logs, intrusion detection/prevention systems, and system logs. This allows organizations to identify security threats in real-time and respond quickly, helping to mitigate potential harm to their systems and data.

質問: **277**
次のうち、情報セキュリティ プログラムの付加価値を最もよく示しているのはどれですか?
A. セキュリティ ベースライン
B. ギャップ分析
C. SWOT分析
D. バランス スコアカード
正解: **(正解を表示します)**
A balanced scorecard is a tool that can be used to demonstrate the added value of an information security program by measuring and reporting on key performance indicators (KPIs) and key risk indicators (KRIs) aligned with strategic objectives. Security baselines, a gap analysis and a SWOT analysis are all useful for assessing and improving security posture, but they do not necessarily show how security contributes to business value.

質問: **278**

情報資産を分類しているときに、情報セキュリティ マネージャーは、いくつかの運用データベースに所有者が割り当てられていないことに気付きました。この状況に対処する最善の方法は何でしょうか。
A. データベース管理者 (DBA) に責任を割り当てます。
B. データベースに機密コンテンツが含まれていないか確認します。
C. 上級管理職向けにデータベースのレポートを作成します。
D. これらのデータベースに最高の分類レベルを割り当てます。
正解: **(**正解を表示します**)**
Information asset classification is the process of identifying, labeling, and categorizing information assets based on their value, sensitivity, and criticality to the organization. Information asset classification helps to establish appropriate security controls, policies, and procedures for protecting the information assets from unauthorized access, use, disclosure, modification, or destruction. One of the key elements of information asset classification is assigning owners to each information asset. Owners are responsible for managing the information asset throughout its lifecycle, including defining its security requirements, implementing security controls, monitoring its usage and performance, reporting any incidents or breaches, and ensuring compliance with legal and regulatory obligations. Therefore, assigning responsibility to the database administrator (DBA) is the best way to address the situation where several production databases do not have owners assigned to them. References = CISM Review Manual 15th Edition1, page 256; Information Asset and Security Classification Procedure2.

質問: **279**
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. リスク評価。
B. 戦略。
C. 標準。
D. 主要業績評価指標 (KPI)。
正解: **(**正解を表示します**)**

質問: **280**
次のどれがリスク所有者の責任ですか?
A. 管理責任者とのリスク対応計画活動の実施
B. 制御の有効性の評価
C. リスク対応計画の承認
D. リスク軽減策の選択の承認
正解: **(**正解を表示します**)**
A risk owner is a person or entity that is responsible for ensuring that risk is managed effectively. One of the primary responsibilities of a risk owner is to implement controls that will help mitigate or manage the risk.

While risk assessments, determining the organization's risk appetite, and monitoring control effectiveness are all important aspects of managing risk, it is the responsibility of the risk owner to take the necessary actions to manage the risk.

質問**: 281**
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. セキュリティギャップ分析を実行します。
B. ビジネス影響分析 (BIA) を実施します。
C. 定期的な意識啓発トレーニングを実施します。
D. ネットワーク侵入テストを実行します。
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**: 282**
データ所有者がユーザーのアクセス権限を定義する際に使用する最適なアプローチは次のどれですか?
A. ユーザーロールに基づいてアクセス権限を定義します。
B. ベンダーが推奨するユーザー アカウント設定を採用します。
C. ユーザーのアクセス権限のリスク評価を実行します。
D. ID およびアクセス管理 (IDM) ツールを実装します。

正解: **(**正解を表示します**)**
This approach is the best because it ensures that users have the minimum level of access required to perform their job functions, which reduces the risk of unauthorized access or misuse of data. User roles are defined based on the business needs and responsibilities of the users, and they can be easily managed and audited.
References: The CISM Review Manual 2023 states that "the data owner is responsible for defining the access privileges for each user role" and that "the data owner should ensure that the principle of least privilege is applied to all users" (p. 82). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Defining access privileges based on user roles is the best approach because it allows the data owner to assign the minimum level of access required for each role and to review and update the roles periodically" (p. 23).

質問: **283**
情報セキュリティ プログラムの主な成果は次のどれでしょうか?
A. 戦略的連携
B. リスクの排除
C. コスト削減
D. 脅威の軽減
正解: **A (**コメントを発表する**)**
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: **284**
情報セキュリティ プログラムの有効性に関して主要な利害関係者へのレポートに含めることが最も重要なのは次のどれですか。
A. セキュリティ メトリック
B. セキュリティベースライン
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の露出
正解: **A (**コメントを発表する**)**
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: **285**
ある組織は、その環境内で外部からのブルート フォース攻撃の脅威が増加していることを確認しました。組織の重要なシステムに対するこのリスクを軽減する最も効果的な方法は、次のうちどれですか。
A. 多要素認証を実装します。
B. ログの監視と分析の頻度を増やします。
C. セキュリティ情報およびイベント管理システム (SIEM) を実装する。
D. 侵入検知システム (IDS) の感度を高めます。
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**: 286**
情報セキュリティ ガバナンス フレームワークの有効性は、次の場合に最も高まります。
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. 経営陣によって法令遵守の文化が推進されています。
C. リスク管理は運用および戦略活動に組み込まれています。
D. IS監査人はガバナンス活動を評価する権限を持つ
正解**: B (**コメントを発表する**)**
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: **287**
情報セキュリティ ガバナンス メトリックを実装する主な目的は次のとおりです。
A. ベストプラクティスとの整合性を測定します。
B. セキュリティを望ましい状態に導きます。
C. 制御操作を改良します。
D. 運用およびプログラムの指標を評価します。
正解: **(**正解を表示します**)**

質問: **288**
次の役割のうち、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: **(**正解を表示します**)**
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: **289**
情報セキュリティに関連する主要リスク指標 (KRI) を監視する主な理由はどれですか?
A. 許容できないリスクを警告する
B. 残存リスクを特定する

C. リスク許容度を再評価する
D. 制御パフォーマンスのベンチマーク
正解**: (**正解を表示します**)**
Key risk indicators (KRIs) are metrics that measure the level of risk exposure and the likelihood of occurrence of potential adverse events that can affect the organization's objectives and performance. KRIs are used to monitor changes in the risk environment and to provide early warning signals for potential issues that may require management attention or intervention. KRIs are also used to communicate the risk status and trends to the relevant stakeholders and to support risk-based decision making12.
The primary reason to monitor KRIs related to information security is to alert on unacceptable risk.
Unacceptable risk is the level of risk that exceeds the organization's risk appetite, tolerance, or threshold, and that poses a significant threat to the organization's assets, operations, reputation, or compliance. Unacceptable risk can result from internal or external factors, such as cyberattacks, data breaches, system failures, human errors, fraud, natural disasters, or regulatory changes. Unacceptable risk can have severe consequences for the organization, such as financial losses, legal liabilities, operational disruptions, customer dissatisfaction, or reputational damage12.
By monitoring KRIs related to information security, the organization can identify and assess the sources, causes, and impacts of unacceptable risk, and take timely and appropriate actions to mitigate, transfer, avoid, or accept the risk. Monitoring KRIs can also help the organization to evaluate the effectiveness and efficiency of the existing information security controls, policies, and procedures, and to identify and implement any necessary improvements or enhancements. Monitoring KRIs can also help the organization to align its information security strategy and objectives with its business strategy and objectives, and to ensure compliance with the relevant laws, regulations, standards, and best practices12.
While monitoring KRIs related to information security can also serve other purposes, such as identifying residual risk, reassessing risk appetite, or benchmarking control performance, these are not the primary reason for monitoring KRIs. Residual risk is the level of risk that remains after applying the risk treatment options, and it should be within the organization's risk appetite, tolerance, or threshold. Reassessing risk appetite is the process of reviewing and adjusting the amount and type of risk that the organization is willing to take in pursuit of its objectives, and it should be done periodically or when there are significant changes in the internal or external environment. Benchmarking control performance is the process of comparing the organization's information security controls with those of other organizations or industry standards, and it should be done to identify and adopt the best practices or to demonstrate compliance12. References = Integrating KRIs and KPIs for Effective Technology Risk Management, The Power of KRIs in Enterprise Risk Management (ERM) - Metricstream, What Is a Key Risk Indicator? With

Characteristics and Tips, KRI Framework for Operational Risk Management | Workiva, Key risk indicator - Wikipedia

質問: **290**
組織は、第三者を選択する際にデューデリジェンスを実施しています。このプロセス中に情報が不正に共有されるリスクを軽減するために最も役立つのは次のうちどれですか。
A. 安全な通信チャネルの使用
B. 相互秘密保持契約（NDA）の締結
C. サードパーティのプライバシーポリシーの要求
D. 業界の参照の取得
正解: **(正解を表示します)**
The best option to reduce the risk of unauthorized sharing of information during the due diligence process is B: Establishing mutual non-disclosure agreements (NDAs). This is because NDAs are legal contracts that bind the parties to keep confidential any information that is exchanged or disclosed during the due diligence process. NDAs can help to protect the sensitive data, intellectual property, trade secrets, or business strategies of both the organization and the third party from being leaked, stolen, or misused by unauthorized parties.
NDAs can also specify the terms and conditions for the use, storage, and disposal of the information, as well as the consequences for breaching the agreement.
References = CISM Review Manual 15th Edition, Chapter 3, Section 3.2.1, page 1341; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 70, page 18

質問: **291**
ある組織は、規制当局の監視下にある金融アプリケーションの監視とサポートをサードパーティベンダーに委託しています。以下のコントロールのうち、組織のリスクを最も効果的に管理できるのはどれですか？
A. ベンダー契約に不遵守に対する罰則条項を含める
B. システムとデータ間の職務分離の実装
C. ベンダーの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. 主要リスク指標（KRI）の監視
正解: **(正解を表示します)**

質問: **292**
上級管理職から情報セキュリティ戦略への支持を得るのに最も効果的なのは次のうちどれですか?
A. ビジネス影響分析 (BIA) の結果
B. 競合他社における重大な違反
C. サードパーティのセキュリティ監査結果

D. 費用便益分析結果
正解: **(**正解を表示します**)**
Senior management engagement is most effectively achieved when information security risks are clearly connected to real, tangible business consequences. A major breach at a competitor (B) provides a credible, industry-relevant example that demonstrates potential financial, operational, reputational, and regulatory impacts in a way executives readily understand. While BIA results (A), audit findings (C), and cost-benefit analyses (D) are important inputs, they are often abstract or internally focused. CISM guidance emphasizes that executive support is strongest when security messaging is business-driven, externally validated, and tied to strategic risk awareness. A peer breach highlights that the threat is realistic, imminent, and applicable to the organization's context, which increases urgency and executive buy-in for the security strategy.
References: ISACA CISM Review Manual (Governance-executive communication, stakeholder engagement); CISM Exam Content Outline (Domain 2).

質問: **293**
コンプライアンス活動の不必要な重複を減らすための最適なアプローチは次のどれですか?
A. 管理手順の文書化
B. コンプライアンス要件の標準化
C. コントロールの自動化
D. 保証活動の統合
正解: **(**正解を表示します**)**
= Standardization of compliance requirements is the best approach to reduce unnecessary duplication of compliance activities, as it allows for a common understanding of the objectives and expectations of various stakeholders, such as regulators, auditors, customers, and business partners. Standardization also facilitates the alignment of compliance activities with the organization's risk appetite and tolerance, and enables the identification and elimination of redundant or conflicting controls. References = CISM Review Manual, 27th Edition, page 721; CISM Review Questions, Answers & Explanations Database, 12th Edition, question 952 Learn more:

質問: **294**
災害復旧計画 (DRP) テストを実行する際に最も大きな固有のリスクは次のどれですか?
A. 結果と教訓の文書化が不十分
B. 影響を受けるユーザーへのコミュニケーション不足
C. 運用環境の混乱
D. 部門間の連携不足
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**: 295**
さまざまな情報セキュリティのシナリオに備えてコンピュータ インシデント対応チームを準備するのに最も適しているのは次のうちどれですか。
A. 侵入テスト
B. 法医学認定
C. 災害復旧訓練
D. 卓上演習
正解**: (**正解を表示します**)**

質問**: 296**
業務において会社所有のモバイル デバイスの使用を導入している組織の情報セキュリティ マネージャーの主な責任は次のどれですか。
A. デバイスのリモートワイプ機能を要求します。
B. セキュリティ意識向上トレーニングを実施します。
C. 既存のセキュリティ ポリシーを確認して更新します。
D. デバイス上でパスワードとデータの暗号化を強制します。
正解**: (**正解を表示します**)**
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**: 297**
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、最も重要なデューデリジェンス活動は次のどれですか。
A. サービス プロバイダーのセキュリティ認識のレベルを評価します。
B. サービス プロバイダーの最近の独立監査レポートを確認します。
C. サービスプロバイダーに情報セキュリティポリシーの遵守を要求します。
D. 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します。
正解**: (**正解を表示します**)**

質問**: 298**

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どれですか?
A. 新たなセキュリティ技術
B. リスクプロファイルの変更
C. 定義されたリスク許容度
D. 脆弱性スキャンの進行状況
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: **299**
情報セキュリティ戦略を策定する上で、最初に行うべきステップは次のどれですか?
A. 情報セキュリティリスクの許容レベルを決定する
B. セキュリティのベースラインとコントロールを特定するためのロードマップを作成する
C. 現在の状態に基づいてギャップ分析を実行する
D. 情報セキュリティを推進する主要な関係者を特定する
正解: **(**正解を表示します**)**
The first step in developing an information security strategy is to identify key stakeholders who can provide support, guidance and resources for information security initiatives. These stakeholders may include senior management, business unit leaders, legal counsel, audit and compliance officers and other relevant parties. By engaging these stakeholders early on, an information security manager can ensure that the strategy aligns with business objectives and expectations, as well as gain buy-in and commitment from them.
Determining acceptable levels of risk, creating a roadmap and performing a gap analysis are all important steps in developing an information security strategy, but they should follow after identifying key stakeholders.

質問: **300**
ビジネス影響分析 (BIA) は、主に次の目的で定期的に実行する必要があります。
A. 環境の変化に対する脆弱性を検証します。
B. 資産の重要性を分析します。
C. 規制への準拠を確認します。

D. コントロールの有効性を検証します。
正解: **(**正解を表示します**)**
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: **301**
サイバーセキュリティ インシデント対応で使用される事前に決定された封じ込め方法は、主に次の点に基づく必要があります。
A. 影響を受けるユーザーの数。
B. インシデント ハンドラーの機能。
C. 確認されたインシデントの種類。
D. 予測されるインシデントの継続時間。
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: **302**
復旧時間目標 (RTO) は次のどれの出力ですか?
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. ビジネス影響分析 (BIA)
正解: **(正解を表示します)**
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: **303**
サードパーティのホスティングプロバイダーが可用性要件を満たすことができることを最も保証するものは次のどれですか?
A. 監査権条項
B. 第三者のインシデント対応計画
C. サービスレベル契約（SLA）
D. 第三者の事業継続計画（BCP）
正解: **C (コメントを発表する)**
A Service Level Agreement (SLA) is the contractual document that specifies and guarantees the availability levels the third-party hosting provider must meet. It provides the clearest and most enforceable commitment to availability.
"SLAs establish measurable commitments that can be monitored and enforced, providing a high level of assurance that service availability will meet business requirements."
- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Outsourcing and Third-Party Management*
ISACA's practice questions highlight SLAs as the most direct and reliable assurance for third-party service availability.

質問: **304**
ある組織の人事部門では、政府の規制に従うために、退職後 3 日以内にすべての企業 IT システムから従業員のアカウント権限を削除することを義務付けています。ただし、システムごとにユーザー ディレクトリが異なり、権限を削除するのに現在最大 4 週間かかります。次のうち、規制への準拠を最も効果的に実現できるのはどれですか。
A. 多要素認証 (MFA) システム
B. アイデンティティ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: **B (**コメントを発表する**)**
= 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: **305**
事業継続計画 (BCP) の改善にとって最も重要なのは次のどれですか?
A. 学んだ教訓を取り入れる
B. マネジメントレビューの実施
C. IT レジリエンス ソリューションの実装

D. 重要なビジネスプロセスの文書化
正解: **(**正解を表示します**)**

質問: **306**
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。これらの変更を義務付けるポリシーが作成され、ビジネスマネージャーによって承認されました。情報セキュリティマネージャーが最初に取るべき行動は次のどれですか？
A. 情報セキュリティ啓発資料に要件を含める
B. ポリシーコンプライアンス評価を実行する
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: **307**
情報セキュリティ ガバナンス フレームワークを実装することによる主な利点は次のどれですか?
A. このフレームワークは、ビジネス目標に対するリスクの影響に対する管理責任を定義します。
B. フレームワークは、リスクとコントロールのバランスを取りながらビジネス目標を達成するための方向性を示します。
C. このフレームワークは、テクノロジーを安全に使用して収益を最大化するためのロードマップを提供します。
D. フレームワークは、ビジネス目標と戦略の妥当性を確認できます。
正解: **(**正解を表示します**)**
An information security governance framework is a set of principles, policies, standards, and processes that guide the development, implementation, and management of an effective information security program that supports the organization's objectives and strategy. The framework provides direction to meet business goals while balancing risks and controls, as it helps to align the information security activities with the business needs,

priorities, and risk appetite, and to ensure that the security resources and investments are optimized and justified.
References = CISM Review Manual 2022, page 321; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.22; CISM domain 1: Information security governance Updated 2022

質問: **308**
クラウド サービス プロバイダーである A 社は、自社のクラウド サービスに B 社のテクノロジーを組み込むことで新たな利益を得るため、B 社を買収する手続きを進めています。会社 A の情報セキュリティ マネージャーが主に重点を置くべきは次のどれですか。
A. B社の組織構造
B. A社のセキュリティポリシーに準拠するためのコスト
C. A社のセキュリティアーキテクチャ
D. B社のセキュリティポリシー
正解: **D (**コメントを発表する**)**
According to the CISM Review Manual, the security architecture of an organization defines the security principles, standards, guidelines and procedures that support the information security strategy and align with the business objectives. When acquiring another company, the information security manager of the acquiring company should focus on ensuring that the security architecture of the acquired company is compatible with its own, or that any gaps or conflicts are identified and resolved.
References = CISM Review Manual, 27th Edition, Chapter 2, Section 2.1.2, page 751.

質問: **309**
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: **310**
情報セキュリティマネージャーは、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。このアップグレードについて上級管理職の支持を得るために、最も役立つのは次のうちどれですか？
A. リスクに基づいた現在のオペレーティングシステムの評価
B. 新しいオペレーティングシステムにおけるパフォーマンスの改善の概要
C. 現在のオペレーティングシステムの問題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のセキュリティ機能のリスト
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: **311**
経営陣の情報セキュリティサポートに影響を与える最も重要な情報は次のとおりです。
A. ビジネス戦略との整合性の証明。
B. 全体的な脅威の状況の特定。
C. 競合他社への攻撃が成功したという報告。
D. 組織のリスクの特定。
正解: **(**正解を表示します**)**
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: **312**
新しい情報セキュリティ マネージャーは、組織が問題に対処するために短期的な解決策を使用する傾向があることに気付きました。リソースの割り当て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はありません。セキュリティに対するこのボトムアップ アプローチを逆転させるには、まず何をすべきでしょうか。
A. 情報セキュリティ運営委員会を設置します。
B. 監査委員会を設置する。
C. 情報セキュリティ意識向上トレーニング プログラムを実施します。
D. 脅威分析を実施します。
正解: **(**正解を表示します**)**

質問: **313**
情報セキュリティ プログラムのサポートを構築する場合、次の要素のうちどれが最も重要ですか?
A. 脅威分析
B. ビジネス影響分析 (BIA)
C. 情報リスク評価
D. 既存の脆弱性の特定
正解: **(**正解を表示します**)**

質問: **314**
次のうち、サードパーティプロバイダーで情報セキュリティインシデントが発生した場合のデータ損失について責任を負うのは誰ですか?
A. 情報セキュリティ管理者
B. データをホストするサービスプロバイダー
C. インシデント対応チーム
D. ビジネスデータの所有者
正解: **(**正解を表示します**)**
The business data owner is accountable for data loss in the event of an information security incident at a third- party provider because they are ultimately responsible for the protection and use of their data, regardless of where it is stored or processed. The information security manager is not accountable for data loss at a third- party provider, but rather responsible for implementing and enforcing the security policies and standards that govern the relationship with the provider. The service provider that hosts the data is not accountable for data loss at their site, but rather liable for any breach of contract or service level agreement that may result from such an incident. The incident response team is not

accountable for data loss at a third-party provider, but rather responsible for responding to and managing the incident according to the incident response plan.
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/2018/volume-3/incident- response-lessons-learned

質問: **315**
情報セキュリティ プログラムへの投資を最もよくサポートするのは次のうちどれですか?
A. ビジネス影響分析 (BIA)
B. リスク評価結果
C. ビジネスケース
D. ギャップ分析結果
正解: **(正解を表示します)**

質問: **316**
情報セキュリティ プログラムとビジネス戦略の整合性を判断する最も効果的な方法はどれですか?
A. ビジネス継続性テストの結果を評価します。
B. 主要業績評価指標 (KPI) を確認します。
C. インシデントのビジネスへの影響を評価します。
D. ビジネス プロセス所有者を関与させます。
正解: **(正解を表示します)**
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: **317**
情報セキュリティ管理者が取締役会に伝える上で最も関連性が高いのは次のどれですか。
A. 露出レベル
B. 脆弱性評価
C. 固有のリスクのレベル
D. 脅威評価
正解: **(**正解を表示します**)**

質問: **318**
次の指標のうち、情報セキュリティ プログラムのパフォーマンスを正確に測定できるものはどれですか?
A. 意思決定を可能にする定性的傾向と定量的傾向の組み合わせ
B. セキュリティ例外を正確に測定する定性的な指標の集合
C. 業界のベンチマークと比較される定量的指標の集合
D. セキュリティ プログラムに割り当てられたさまざまな基準から導き出された単一の数値スコア
正解: **B (**コメントを発表する**)**

質問: **319**
組織の Software as a Service (SaaS) ベンダーで侵害が発生した後、情報セキュリティ マネージャーが上級管理職に対して推奨する最良の方法は次のうちどれですか。
A. 法律顧問に相談してください。
B. ベンダーとの関係を終了します。
C. ベンダー契約を再交渉します。
D. ベンダーのリスク評価を更新します。
正解: **(**正解を表示します**)**

質問: **320**
完全な再構築が必要な侵害されたシステムを回復する場合、最初に考慮すべき事項は次のうちどれですか?

A. パッチ管理ファイル
B. ネットワークシステムログ
C. 構成管理ファイル
D. 侵入検知システム (IDS) ログ
正解: **(正解を表示します)**
Patch management files are the files that contain the patches or updates for the software applications and systems that are installed on the compromised system. Patch management files are essential to recover a compromised system that needs a complete rebuild, as they can help to restore the functionality, security, and performance of the system. Without patch management files, the system may not be able to run properly or securely, and may expose the organization to further risks or vulnerabilities. Network system logs, configuration management files, and intrusion detection system (IDS) logs are also important for recovering a compromised system, but they should be considered after patch management files. Network system logs can help to identify the source and scope of the attack, configuration management files can help to restore the original settings and policies of the system, and IDS logs can help to detect any malicious activities or anomalies on the system. References = CISM Review Manual, 16th Edition, pages 193-1941; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 672

質問: **321**
ソーシャル エンジニアリングによる企業ネットワークへの不正アクセスに対する最善の技術的防御は次のどれですか。
A. チャレンジ/レスポンス情報の要求
B. 多要素認証の要求
C. 頻繁なパスワード変更の強制
D. 複雑なパスワード形式の強制
正解: **(正解を表示します)**
Social engineering is a technique used by attackers to manipulate individuals into divulging sensitive information or performing actions that can compromise the security of an organization. Multi-factor authentication (MFA) is a security mechanism that requires users to provide at least two forms of authentication to verify their identity. By requiring MFA, even if an attacker successfully obtains a user's credentials through social engineering, they will not be able to access the network without the additional form of authentication.

質問: **322**
情報セキュリティ管理者が組織の情報セキュリティ戦略の包括性を判断するために最も効果的なのは次のどれですか?
A. 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. ビジネス影響分析 (BIA)
正解: **(**正解を表示します**)**
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: **323**
中断中に、許容できる時間枠内で、事前に定義された容量で製品とサービスの提供を組織が維持できるようにする最適な方法は、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. ビジネス影響分析 (BIA)
正解: **B (**コメントを発表する**)**
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: **324**
ランサムウェア攻撃からの回復のためのインシデント対応計画をテストする場合、検証することが最も重要なのは次のどれですか?
A. デジタル通貨はすぐに利用可能になります。
B. ネットワーク アクセスには 2 要素認証が必要です。
C. データのバックアップはオフサイトの場所から回復可能です。
D. 代替ネットワーク リンクがすぐに利用可能になります。

正解: **(**正解を表示します**)**
Data backups are recoverable from an offsite location is the most important thing to verify when testing an incident response plan for recovery from a ransomware attack, as it ensures that the organization can restore its data and resume its operations without paying the ransom or losing critical information. Data backups should be performed regularly, stored securely, and tested for integrity and availability. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 191, section 4.3.4.1.

質問: **325**
情報セキュリティ戦略と組織の目標との整合性を判断する最も正確な方法は、次のうちどれを測定しますか?
A. ブロックされた侵入試行の数
B. 上級管理職がレビューしたビジネスケースの数
C. ビジネスに対する脅威の特定数の傾向
D. ビジネス プロセスに統合されたコントロールの割合
正解: **(**正解を表示します**)**
Measuring the percentage of controls integrated into business processes is the most accurate way to determine the alignment of an information security strategy with organizational goals, as this reflects the extent to which the information security program supports and enables the business objectives and activities, and reduces the friction and resistance from the business stakeholders. The percentage of controls integrated into business processes also indicates the maturity and effectiveness of the information security program, and the level of awareness and acceptance of the information security policies and standards among the business users. Number of blocked intrusion attempts, number of business cases reviewed by senior management, and trends in the number of identified threats to the business are not the most accurate ways to determine the alignment of an information security strategy with organizational goals, as they do not measure the impact and value of the information security program on the business performance and outcomes, and may not reflect the business priorities and expectations. References = CISM Review Manual 2023, page 291; CISM Review Questions, Answers & Explanations Manual 2023, page 372; ISACA CISM - iSecPrep, page 223; CISM Exam Overview - Vinsys4

質問: **326**
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. 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。
B. 保険を購入することでリスクを移転します。
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: **327**
セキュリティ リスク管理を組織に統合する場合、次の点を確認することが最も重要です。
A. ビジネス ユニットがリスク管理方法を承認します。
B. リスク処理プロセスが定義されます。
C. 情報セキュリティポリシーが文書化され、理解されています。
D. リスク管理方法論は確立されたフレームワークに従います。
正解: **(**正解を表示します**)**
When integrating security risk management into an organization, it is most important to ensure that the risk management methodology follows an established framework, such as ISO 31000, NIST SP 800-30, or COBIT. This is because a framework provides a consistent and structured approach to identify, assess, treat, and monitor risks, and to align the risk management process with the organization's objectives, culture, and governance. A framework also helps to ensure compliance with relevant standards and regulations, and to facilitate communication and reporting of risks to stakeholders. References: The CISM Review Manual 2023 states that "the risk management methodology should follow an established framework that provides a consistent and structured approach to risk management" and that "the framework should be aligned with the enterprise's objectives, culture, and governance, and should comply with applicable standards and regulations" (p. 94). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "The risk management methodology follows an established framework is the correct answer because it is the most important factor to ensure the successful integration of security risk management into an organization, as it provides a common language and process for managing risks across the organization" (p. 29). Additionally, the article Integrating Risk Management into Business Processes from the ISACA Journal 2018 states that "a risk management framework provides a systematic and comprehensive approach to risk management that covers the entire risk management cycle, from risk identification to risk monitoring and reporting" and that "a risk management framework should be aligned with the organization's strategy, culture, and governance, and should follow recognized standards and best practices, such as ISO 31000, NIST SP 800-30, or COBIT" (p. 1)

質問: **328**
システム管理者が読み取り専用アクセスに制限されることが最も重要であるのは次のどれですか?
A. ユーザーアクセスログファイル
B. 管理者ユーザープロファイル
C. 管理者ログファイル

D. システムログオプション
正解: **(**正解を表示します**)**
User access log files contain records of user activities and actions on the system, which can be used for auditing, monitoring, and investigating purposes. System administrators should not be able to modify or delete these files to ensure their integrity and availability.
References = CISM Review Manual, 16th Edition, Chapter 3, Section 3.3.2.11

質問: **329**
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: **(**正解を表示します**)**
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: **330**
組織が重要なビジネス 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 サービスを使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. ホストするデータを識別します。
B. ビジネス要件を分析します。
C. リスク評価を実行します。
D. ギャップ分析を実行します。
正解: **(**正解を表示します**)**

質問: **331**

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: **332**
ある組織は、コールセンターアプリケーションにIT障害があることを確認しました。このリスクを負うべき者は、次のうち誰ですか？
A. コールセンター長
B. 最高経営責任者（CEO）
C. IT部門の責任者
D. 情報セキュリティ管理者
正解: **(**正解を表示します**)**

質問: **333**
情報セキュリティ マネージャーにとって、組織のさまざまな保証機能を統合することは、主に次のことを可能にするために重要です。
A. 一貫したセキュリティ。

B. 包括的な監査
C. セキュリティを意識した文化
D. ポリシーの遵守
正解: **A** (コメントを発表する)
Consistent security is the primary reason for integrating the various assurance functions of an organization for the information security manager because it ensures that the security policies and standards are applied uniformly and effectively across different domains, processes, and systems of the organization.
Comprehensive audits are not the primary reason for integrating the various assurance functions, but rather a possible outcome or benefit of doing so. A security-aware culture is not the primary reason for integrating the various assurance functions, but rather a desirable state or goal of the organization. Compliance with policy is not the primary reason for integrating the various assurance functions, but rather a basic requirement or expectation of the organization. References: https://www.isaca.org/resources/isaca-journal/issues/2016
/volume-4/integrating-assurance-functions https://www.isaca.org/resources/isaca-journal/issues/2017/volume-
3/how-to-measure-the-effectiveness-of-your-information-security-management-system

質問: **334**
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どれですか?
A. インシデント指標は業界ベンチマークと頻繁に比較されます
B. 新入社員はセキュリティトレーニングの受講が義務付けられています
C. セキュリティは組織文化に組み込まれている
D. 上級管理職がセキュリティ対策を承認し、支持している
正解: (正解を表示します)
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: **335**
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に含めることが最も重要なのは次のどれですか。
A. 脆弱性スキャン結果
B. 競合他社のベンチマーク分析
C. 以前のセキュリティ予算

D. ビジネス要件
正解: **D (**コメントを発表する**)**
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: **336**
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 マネージャーが最初に行うべきことは次のうちどれですか。
A. リスク評価を実施します。
B. 災害復旧手順を文書化します。
C. ビジネス要件を特定します。
D. ビジネス影響分析 (BIA) を実行します。
正解: **D (**コメントを発表する**)**
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: **337**
年次監査で組織の事業継続計画 (BCP) が 1 年以上見直されていない、または更新されていないことが判明した場合、情報セキュリティ管理者にとって最も懸念すべき事項は次のどれですか。
A. 実際のインシデントが発生した場合、BCP が古くなると、復旧の効率が低下する可能性があります。
B. 業界のベストプラクティスに従わないと、組織の評判が損なわれる可能性があります。
C. 監査の結果は、組織の全体的なリスク評価に影響を及ぼす可能性があります。

D. BCP が更新されないと、社内ポリシーに準拠しなくなる可能性があります。
正解: **(**正解を表示します**)**
A BCP is a document that outlines the processes and procedures to maintain or resume critical business functions and minimize the impact of a disruption on the organization's objectives, customers, and stakeholders. A BCP should be reviewed and updated regularly to reflect the changes in the organization's environment, risks, resources, and requirements. An outdated BCP may result in less efficient recovery if an actual incident occurs, as it may not account for the current situation, dependencies, priorities, or recovery strategies. This may lead to increased downtime, losses, or damages for the organization. References = CISM Review Manual 2022, page 3101; CISM Exam Content Outline, Domain 4, Knowledge Statement 4.82; CISM 2020: Business Continuity3; Part Two: Business Continuity and Disaster Recovery Plans

質問: **338**
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が完了した時点でマルウェアが引き続き拡散していると確信する必要がありますか?
A. 封じ込め
B. 回復
C. 根絶
D. 識別
正解: **A (**コメントを発表する**)**
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 that 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: **339**
ソーシャル エンジニアリング攻撃に関連するリスクを識別する最良の方法は次のとおりです。
A. 侵入検知システム (IDS) を監視する
B. シングル サインオン (SSO) 認証の遅延を確認します。

C. 情報セキュリティの実践に関するユーザーの知識をテストします。
D. 電子メール フィルタリング システムのビジネス リスク評価を実行します。
正解: **C (**コメントを発表する**)**
The best way to identify the risk associated with a social engineering attack is to test user knowledge of information security practices. Social engineering is a type of attack that exploits human psychology and behavior to manipulate, deceive, or influence users into divulging sensitive information, granting unauthorized access, or performing malicious actions. Therefore, user knowledge of information security practices is a key factor that affects the likelihood and impact of a social engineering attack. By testing user knowledge of information security practices, such as through quizzes, surveys, or simulated attacks, the information security manager can measure the level of awareness, understanding, and compliance of the users, and identify the gaps, weaknesses, or vulnerabilities that need to be addressed.
Monitoring the intrusion detection system (IDS) (A) is a possible way to detect a social engineering attack, but not to identify the risk associated with it. An IDS is a system that monitors network or system activities and alerts or responds to any suspicious or malicious events. However, an IDS may not be able to prevent or recognize all types of social engineering attacks, especially those that rely on human interaction, such as phishing, vishing, or baiting. Moreover, monitoring the IDS is a reactive rather than proactive approach, as it only reveals the occurrence or consequences of a social engineering attack, not the potential or likelihood of it.
Reviewing single sign-on (SSO) authentication lags (B) is not a relevant way to identify the risk associated with a social engineering attack. SSO is a method of authentication that allows users to access multiple applications or systems with one set of credentials. Authentication lags are delays or failures in the authentication process that may affect the user experience or performance. However, authentication lags are not directly related to social engineering attacks, as they do not indicate the user's knowledge of information security practices, nor the attacker's attempts or success in compromising the user's credentials or access.
Performing a business risk assessment of the email filtering system (D) is also not a relevant way to identify the risk associated with a social engineering attack. An email filtering system is a system that scans, filters, and blocks incoming or outgoing emails based on predefined rules or criteria, such as spam, viruses, or phishing. A business risk assessment is a process that evaluates the potential threats, vulnerabilities, and impacts to the organization's business objectives, processes, and assets. However, performing a business risk assessment of the email filtering system does not address the risk associated with a social engineering attack, as it only focuses on the technical aspects and performance of the system, not the human factors and behavior of the users.
References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Identification, Subsection: Threat Identification, page 87-881

質問: **340**
情報セキュリティ マネージャーがアウトソーシング先の第三者との契約期間中に定期的に実行する必要がある最も重要なアクティビティは次のどれですか。
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. 財務調整レビュー
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: **341**
インシデントの分類は、次の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. 必要なリソースの割り当て
C. リスクの重大度とインシデントの優先度
D. 対応と封じ込めの要件
正解: **C (**コメントを発表する**)**
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: **342**

情報セキュリティ管理者が既存の制御を定期的に見直す主な理由は次のうちどれですか?
A. セキュリティ対策の優先順位付け
B. 冗長な制御を避けるため
C. エンドユーザーの制御に関する苦情に対処するため
D. 新たなリスクに対応するため
正解: **D** (コメントを発表する)

質問: **343**
ユーザーが、企業の機密データを保存している個人用モバイル デバイスが盗まれたと報告しました。次のどれが、データ漏洩のリスクを最も最小限に抑えるでしょうか。
A. ユーザーが個人のモバイル デバイスを使用できないようにします。
B. 事件を警察に通報してください。
C. デバイスをリモートでワイプします。
D. ユーザーの企業データへのアクセスを削除します。
正解: (正解を表示します)
Wiping the device remotely is the best option to minimize the risk of data exposure from a stolen personal mobile device. This action will erase all the data stored on the device, including the sensitive corporate data, and prevent unauthorized access or misuse. Wiping the device remotely can be done using enterprise mobility management (EMM) or mobile device management (MDM) tools that allow administrators to remotely manage and secure mobile devices. Alternatively, some mobile devices have built-in features that allow users to wipe their own devices remotely using another device or a web portal.
Preventing the user from using personal mobile devices is not a feasible option, as it may affect the user's productivity and convenience. Moreover, this option does not address the immediate risk of data exposure from the stolen device.
Reporting the incident to the police is a good practice, but it does not guarantee that the device will be recovered or that the data will be protected. The police may not have the resources or the authority to track down the device or access it.
Removing the user's access to corporate data is a preventive measure that can limit the damage caused by a stolen device, but it does not eliminate the risk of data exposure from the data already stored on the device.
The user may have cached or downloaded data that can still be accessed by an attacker even if the user's access is revoked. References = Guidelines for Managing the Security of Mobile Devices in the Enterprise NIST Special Publication, Section
3.1.11, page 3-8
CISM Review Manual, Chapter 3, page 121
Mobile device security - CISM Certification Domain 2: Information Risk Management Video Boot Camp
2019, Section 3.3, 00:03:10

質問: **344**
次のうち、サイバー攻撃に対応する組織の能力を最も正確に示すものを情報セキュリティ管理者に提供するのはどれですか?
A. インシデント対応計画のウォークスルー
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. 赤チーム演習
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: **345**
インシデント対応計画の策定のためにセキュリティ インシデントの分類を確立する場合、次のうち最も価値のある情報を提供するものはどれですか。
A. 事業継続計画 (BCP)
B. 上級管理職からの推奨事項
C. ビジネス影響分析 (BIA) の結果
D. 脆弱性評価結果
正解: **(**正解を表示します**)**

質問: **346**
詳細な事業継続計画 (BCP) は主に次の点に基づく必要があります。
A. 利用可能なローカルベンダーの機能。
B. 上級管理職によって検証された戦略。
C. すべてのアプリケーションをカバーする戦略。
D. 実行に必要なコストとリソース。
正解: **(**正解を表示します**)**

質問: **347**
次のリスクのうち、リスク移転の例となるものはどれですか?

A. サードパーティ製アプリケーションの活用
B. リスクの所有権を別の部門に移す
C. オフサイトバックアップの実施
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**)**
Purchasing cybersecurity insurance is a textbook example of risk transfer - transferring financial risk to a third party (the insurer).
"Risk transfer shifts the impact of a risk to another party, such as through insurance or outsourcing."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Treatment*

質問: **348**
組織は、定められた期限までに現地の規制要件を遵守しない場合、厳しい罰金や罰則に直面することになります。上級管理職は、情報セキュリティマネージャーに対し、コンプライアンス達成のための行動計画を策定するよう指示しました。
計画目的に最も役立つ情報を提供するのは次のどれでしょうか?
A. ビジネス影響分析 (BIA) の結果
B. 違反した場合の期限と罰則
C. ギャップ分析の結果
D. 現在実施されているセキュリティ管理の一覧
正解: **(**正解を表示します**)**
Results from a gap analysis would provide the most useful information for planning purposes when preparing an action plan to achieve compliance with local regulatory requirements by an established deadline. A gap analysis is an assessment of the difference between an organization's current state of compliance and its desired level or standard. It is a process used to identify potential areas for improvement by comparing actual performance with expected performance. A gap analysis can help to prioritize the actions needed to close the gaps and comply with the regulatory requirements, as well as to estimate the resources and time required for each action1. The other options are not as useful as results from a gap analysis for planning purposes when preparing an action plan to achieve compliance with local regulatory requirements by an established deadline. Deadlines and penalties for noncompliance are important factors to consider, but they do not provide information on how to achieve compliance or what actions are needed2. Results from a business impact analysis (BIA) are useful for identifying the critical processes and assets that need to be protected, but they do not provide information on how to comply with the regulatory requirements or what actions are needed3. An inventory of security controls currently in place is useful for assessing the current state of compliance, but it does not provide information on how to comply with the regulatory requirements or what actions are needed4.

References: 3: Business impact analysis (BIA) - Wikipedia 2: Compliance Gap Analysis & Effectiveness Evaluation | SMS 1: What is Gap Analysis in Compliance | Scytale 4: Gap Analysis & Risk Assessment - Riddle Compliance

質問: **349**
効果的な情報セキュリティガバナンスの最もよい指標は次のどれですか?
A. 情報セキュリティは、情報セキュリティ チーム全体の責任とみなされます。
B. 情報セキュリティ制御はリスク所有者に割り当てられます。
C. 情報セキュリティは企業統治に統合されています。
D. 情報セキュリティガバナンスは、外部のセキュリティフレームワークに基づいています。
正解: **(**正解を表示します**)**
Information security governance (ISG) 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 through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk1. Effective ISG ensures that information security is integrated into corporate governance and is considered an essential component of enterprise governance2. Information security is not just the responsibility of the information security team, but of all stakeholders in the organization3. Information security controls are not assigned to risk owners, but to control owners who are accountable for implementing and maintaining the controls4. Information security governance is not based on an external security framework, but on the organization's own objectives, risk appetite, and compliance requirements. References = 1: CISM Review Manual (Digital Version), page 3 2: CISM Review Manual (Digital Version), page 4 3: CISM Review Manual (Digital Version), page 5 4: CISM Review Manual (Digital Version), page 14 : CISM Review Manual (Digital Version), page 16

質問: **350**
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: **351**
ある組織は、取締役会がセキュリティ侵害の可能性について懸念を表明したことを受け、最近サイバーセキュリティ保険に加入しました。この認識されたリスクへの対応として、組織は以下のことを行いました。
A. セキュリティ侵害に関連するリスクを回避しました
B. 内部セキュリティ支出を安全に削減できる
C. 違反の影響に対して最終的な責任を負う
D. 侵害に対する冗長な制御を実施している
正解: **C (**コメントを発表する**)**
Even with cybersecurity insurance, the organization remains ultimately accountable for the impact of a breach (C). Insurance represents risk transfer, not risk elimination or avoidance. CISM clearly states that accountability for risk cannot be transferred; only financial impact may be partially offset. Insurance does not justify reducing security controls (B) and does not constitute redundant controls (D). Avoidance (A) would require eliminating the risky activity entirely. Management must continue to manage, monitor, and mitigate risk in line with appetite, regardless of insurance coverage.
References: ISACA CISM Review Manual (Risk management-risk response strategies, risk transfer); CISM Exam Content Outline (Domain 1).

質問: **352**
セキュリティ イニシアチブの効果的な戦略的整合を促進するために最適なものはどれですか。
A. ビジネス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. 定期的なセキュリティ監査が第三者によって実施されます。
D. 組織単位が優先事項に貢献し、合意する
正解: **D (**コメントを発表する**)**
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: **353**
次の活動のうち、違反につながる制御の失敗に対処するために設計されているものはどれですか?
A. リスク評価
B. インシデント管理
C. 根本原因分析
D. 脆弱性管理
正解: **(**正解を表示します**)**
Incident management is the activity designed to handle a control failure that leads to a breach. Incident management is the process of identifying, analyzing, responding to, and learning from security incidents that may compromise the confidentiality, integrity, or availability of information assets. Incident management aims to minimize the impact of a breach, restore normal operations as quickly as possible, and prevent or reduce the likelihood of recurrence. Incident management involves several steps, such as: Establishing an incident response team with clear roles and responsibilities Developing and maintaining an incident response plan that defines the procedures, tools, and resources for handling incidents Implementing detection and reporting mechanisms to identify and communicate incidents Performing triage and analysis to assess the scope, severity, and root cause of incidents Containing and eradicating the threat and preserving evidence for investigation and legal purposes Recovering and restoring the affected systems and data to a secure state Evaluating and improving the incident response process and controls based on lessons learned and best practices References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 223-232.

質問: **354**
ハードディスクからフォレンジック データを取得する際にディスク ハッシュ値を作成して外部に保存する主な理由は次のとおりです。
A. 分析中に機密性を検証します。
B. 誤って変更された場合に元のデータを復元します。
C. 分析中に整合性を検証します。

D. メディア障害が発生した場合に備えてバックアップを提供します。
正解: **C (**コメントを発表する**)**
The disk hash value is a unique identifier that is calculated from the binary data of the disk. It is used to verify that the disk image is an exact copy of the original disk and that no changes have occurred during the acquisition or analysis process. The disk hash value is stored externally, such as on a CD-ROM or a USB drive, to prevent tampering or corruption. The disk hash value can also be used as evidence in court to prove the authenticity and reliability of the digital evidence123 References = 1: CISM Review Manual 15th Edition, ISACA, 2017, page 2532: Guide to Computer Forensics and Investigations Fourth Edition, page 4-103:
Forensic disk acquisition over the network, Andrea Fortuna, 2018.
The main purpose of creating and storing an external disk hash value when performing forensic data acquisition from a hard disk is to validate the integrity of the data during the analysis. This is done by comparing the original hash value of the disk to the hash value created during the acquisition process, which can be used to ensure that the data has not been tampered with or corrupted in any way. Additionally, by creating a hash value of the disk, it can be used to quickly verify the integrity of any data that is accessed from the disk in the future.

質問: **355**
脆弱性管理にリスクベースのアプローチを採用する場合、脆弱性を優先順位付けする際に考慮すべき最も重要なのは次のどれですか。
A. 脆弱性に関する入手可能な情報
B. 資産とそれに含まれるデータの機密性
C. ITリソースの可用性と制約
D. パッチが開発されテストされているかどうか
正解: **(**正解を表示します**)**
Comprehensive and Detailed Step-by-Step Explanation:
Risk-based vulnerability management prioritizes vulnerabilities based on the potential impact on critical assets.
* A. The information available about the vulnerability: While important for assessing risk, it does not directly determine the priority.
* B. The sensitivity of the asset and the data it contains: This is the BEST answer because prioritizing vulnerabilities based on the criticality of the affected assets ensures that high-impact threats are addressed first.
* C. IT resource availability and constraints: These are logistical considerations but should not outweigh risk impact.
* D. Whether patches have been developed and tested: Patches are important for remediation but do not determine prioritization.
Reference: CISM Job Practice Area 2 (Risk Management) emphasizes considering asset criticality when prioritizing vulnerabilities.

質問: **356**
情報セキュリティガバナンス プログラムを効果的に実装するために最も重要なのは次のどれですか?
A. 従業員はカスタマイズされた情報セキュリティトレーニングを受ける
B. プログラム予算は上級管理職によって承認され、監視されます
C. プログラムの目標は組織に伝達され、理解されます。
D. 情報セキュリティの役割と責任が文書化されています。
正解: **C** (コメントを発表する)
The program goals are communicated and understood by the organization is the most important factor for the effective implementation of an information security governance program because it ensures that the program is aligned with the business objectives and supported by the stakeholders. Employees receive customized information security training is not the most important factor, but rather a means to achieve the program goals and raise awareness among the staff. The program budget is approved and monitored by senior management is not the most important factor, but rather a resource to enable the program activities and measure its performance. Information security roles and responsibilities are documented is not the most important factor, but rather a way to define and assign the program tasks and accountabilities. References: https://www.isaca.org/resources/isaca-journal/issues/2015/volume-1/how-to-measure-the-effectiveness-of-information-security- governance https://www.isaca.org/resources/isaca-journal/issues/2016/volume-2/how-to-align-security- initiatives-with-business-goals-and-objectives

質問: **357**
オンライン取引会社が、ネットワーク攻撃がファイアウォールを突破したことを発見しました。情報セキュリティ マネージャーの最初の対応は何でしょうか?
A. ビジネスへの影響を評価します。
B. 緩和制御を実装します。
C. ファイアウォールのログを調べて攻撃者を特定します。
D. 規制当局にインシデントを通知します。
正解: (正解を表示します)

質問: **358**
情報セキュリティ活動を変更管理プロセスに統合することの主な利点は次のとおりです。
A. 変更に必要なコントロールが含まれていることを確認します。
B. ビジネス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します。
C. 共謀やコンプライアンスの脅威からビジネスを保護します。
D. 組織を不正な変更から保護します。
正解: **A** (コメントを発表する)

質問: **359**
インシデント対応チームが初期調査中に適切なアクションを決定するために最も効果的なのは次のどれですか?
A. チームの技術的能力
B. 過去の事件の履歴データ
C. 影響を受ける部門からのフィードバック
D. インシデントトリアージの手順
正解: **D (**コメントを発表する**)**

質問: **360**
インシデント対応者の有効性を高めるために最も重要なのは次のどれですか?
A. 経営陣とのコミュニケーション
B. スタッフとIT部門の統合
C. 応答シナリオのテスト
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: **361**
成熟した情報セキュリティ プログラムを示す最良の指標は次のどれですか?
A. セキュリティインシデントは適切に管理されています。
B. セキュリティ支出は予算を下回っています。
C. セキュリティ リソースが最適化されます。
D. セキュリティ監査の結果が削減されます。
正解: **(**正解を表示します**)**
A mature information security program is one that is aligned with the business strategy, objectives, and culture, and that delivers value to the organization by effectively managing the information security risks and enhancing the security posture. Optimizing the security resources means that the program uses the available human, financial, and technical resources in the most efficient and effective way, and that it continuously monitors and improves the performance and maturity of the security processes and controls.
References = CISM Review Manual 2022, page 331; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.22; What is a Mature Information Security Program?; How to Measure the Maturity of Your Cybersecurity Program

質問: **362**
ある組織では、シフト勤務のスタッフが共有するデスクトップ コンピュータの代わりにタブレットを活用しています。これらのタブレットには重要なビジネス データが含まれており、盗難のリスクが本質的に高まっています。このリスクを軽減するのに最も役立つのは次のどれでしょうか。
A. モバイルデバイス管理 (MDM) を展開する
B. リモートワイプ機能を実装します。
C. 許容される使用ポリシーを作成します。

D. モバイルデバイスのリスク評価を実施する
正解: **(**正解を表示します**)**
A key risk indicator (KRI) is a metric that provides an early warning of potential exposure to a risk. A KRI should be relevant, measurable, timely, and actionable. The most important factor in an organization's selection of a KRI is the criticality of information, which means that the KRI should reflect the value and sensitivity of the information assets that are exposed to the risk. For example, a KRI for data breach risk could be the number of unauthorized access attempts to a database that contains confidential customer data. The criticality of information helps to prioritize the risks and focus on the most significant ones.
References:
https://www.isaca.org/credentialing/cism https://www.wiley.com/en-us /CISM+Certified+Information+Security+Manager+Study+Guide-p-9781119801948

質問: **363**
ビジネス影響分析 (BIA) BEST により、組織は次のことを確立できます。
A. 総所有コスト (TCO)。
B. 復元の優先順位。
C. 年間損失予想値 (ALE)。
D. 回復方法。
正解: **(**正解を表示します**)**

質問: **364**
効果的な情報セキュリティ戦略を開発するための最も重要な入力は次のどれですか?
A. ビジネスプロセスと要件
B. リスクとビジネスへの影響の評価
C. セキュリティの現状と望ましい状態
D. 明確に定義された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: **365**
組織が使用するクラウド アプリケーションに重大な脆弱性があることが判明しました。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ます。
B. ファイアウォール内のアプリケーションへの接続を一時停止します
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ます。
D. 組織のインシデント対応プロセスを開始します。
正解: **D (**コメントを発表する**)**

= 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: **366**
内乱が始まったばかりの国に子会社があることを知った場合、組織が最初に行うべきことは何ですか?
A. リスク プロファイルの変化を評価します。
B. インシデント対応計画を呼び出します。
C. 災害復旧計画 (DRP) をアクティブ化します。
D. セキュリティ意識向上トレーニングを実施します。
正解: **(**正解を表示します**)**

質問: **367**
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. 主要リスク指標 (KRI) のしきい値設定
B. 定期的なセキュリティ意識向上プログラムの実施
C. セキュリティイベントログ記録の定期的な分析
D. ネットワークアクティビティのリアルタイム監視

正解: **(**正解を表示します**)**

質問: **368**
ホワイト ボックス コントロール テストではなくブラック ボックス コントロール テストを実行する主な利点は次のとおりです。
A. 潜在的な本番環境の問題が少なくなります。
B. IT スタッフの準備が少なくて済みます。
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します。
正解: **(**正解を表示します**)**
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: **369**
個人情報の保護に関する新しい世界的規制に準拠するための最善の方法は次のどれですか?
A. リスク処理計画を実行します。
B. ベンダーとの契約および作業範囲記述書 (SOW) を確認します。
C. データの地域化制御を実装します。
D. コントロールの現在の状態と目的の状態を決定します。
正解: **(**正解を表示します**)**
The best way to achieve compliance with new global regulations related to the protection of personal information is to determine the current and desired state of controls, as this helps the information security manager to identify the gaps and requirements for

compliance, and to prioritize and implement the necessary actions and measures to meet the regulatory standards. The current state of controls refers to the existing level of protection and compliance of the personal information, while the desired state of controls refers to the target level of protection and compliance that is required by the new regulations. By comparing the current and desired state of controls, the information security manager can assess the maturity and effectiveness of the information security program, and plan and execute a risk treatment plan to address the risks and issues related to the protection of personal information. Executing a risk treatment plan, reviewing contracts and statements of work (SOWs) with vendors, and implementing data regionalization controls are also important, but not as important as determining the current and desired state of controls, as they are dependent on the outcome of the gap analysis and the risk assessment, and may not be sufficient or appropriate to achieve compliance with the new regulations. References = CISM Review Manual 2023, page 491; CISM Review Questions, Answers & Explanations Manual 2023, page 352; ISACA CISM - iSecPrep, page 203

質問**: 370**
インシデント対応チームは、次のどのフェーズで、インシデントの原因となった脅威を除去するために必要なアクションを文書化する必要がありますか?
A. インシデント後のレビュー
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**: 371**
リスクを許容レベルまで軽減するための最適な制御を選択する場合、情報セキュリティ マネージャーの決定は主に次の要素に基づいて行う必要があります。
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**: D (**コメントを発表する**)**
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**: 372**
情報セキュリティ マネージャーは、情報が不適切に分類されている = 侵害のリスクがあると考えています。情報セキュリティ マネージャーの最善のアクションは次のどれですか。
A. 問題を内部監査に報告して推奨事項を確認してください。
B. データを再分類し、ビジネス リスクに合わせてセキュリティ レベルを上げます。
C. 関連するシステム所有者にデータを再分類するように指示します。
D. リスク評価を完了し、その結果をデータ所有者に伝えます。
正解**: D (**コメントを発表する**)**
= 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: **373**
情報セキュリティポリシーは、主に以下の事項との整合性を反映する必要があります。
A. 業界のベストプラクティス。
B. データセキュリティ標準。
C. 情報セキュリティフレームワーク。
D. 上級管理職の意図。
正解: **D** (コメントを発表する)

質問: **374**
グローバルにビジネスを展開している組織が、給与情報の処理にサードパーティのサービス プロバイダーを利用することを計画しています。次の問題のうち、組織にとって最大のリスクとなるものはどれですか。
A. 第三者には、レビューに利用できる独立したコントロール評価がありません。
B. 第三者は、データが生成される地域の現地規制への準拠の証拠を提示していません。
C. 第三者との契約には、違反があった場合の賠償に関する免責条項が含まれていません。
D. サードパーティのサービス レベル契約 (SLA) には稼働時間の保証は含まれていません。
正解: (正解を表示します)
The third party's lack of compliance with local regulations poses the greatest risk to the organization, as it may expose the organization to legal, regulatory, or reputational

consequences, such as fines, sanctions, lawsuits, or loss of customer trust. Payroll information is considered sensitive personal data that may be subject to different privacy and security laws depending on the jurisdiction where it is generated, processed, or stored. Therefore, the organization should ensure that the third party adheres to the applicable regulations and standards, and obtains the necessary certifications or attestations to demonstrate compliance.
References = CISM Review Manual 2022, page 361; CISM Exam Content Outline, Domain 1, Task
1.22; Ensuring Vendor Compliance and Third-Party Risk Mitigation; How to Manage Access Risk Regarding Third-Party Service Providers

質問: **375**
災害復旧計画 (DRP) を正常に実行する能力に最も大きな影響を与えるのは次のどれですか。
A. 計画の机上演習の実施
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: **(**正解を表示します**)**
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: **376**
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に、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次の点です。
A. プログラムの戦略的目標を考慮します。
B. 組織のビジネス戦略を考慮します。
C. 業界ベンチマークを活用します。
D. プログラムのリスクと補償制御を特定します。
正解: **(**正解を表示します**)**

質問: **377**
大規模な多国籍企業の情報セキュリティ マネージャー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、最も懸念すべきことは何でしょうか。
A. ベンダーのサービス 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: **C** (コメントを発表する)
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: **378**
新しく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すべてのセキュリティ関連のポリシーと手順を更新するように求められています。次に何をすべきでしょうか?
A. ベストビジネスプラクティスに従って更新します。

B. 現在の IT 環境のリスク評価を実行します。
C. 現在のビジネスの方向性を理解します。
D. 現在のセキュリティ ポリシーをインベントリして確認します。
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: **379**
情報セキュリティ マネージャーがセキュリティとビジネス目標を一致させるための最善の行動方針は次のどれですか。
A. ビジネス影響分析 (BIA) の実施
B. ビジネス戦略の見直し
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: **D (**コメントを発表する**)**
= 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: **380**
どの時点でリスクの所有権を割り当てる必要がありますか?
A. リスク対応計画が実行されるとき
B. 資産の所有権が割り当てられている場合
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: **(**正解を表示します**)**

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**: 381**
災害復旧に対する復旧ポイント目標 (RPO) の貢献は次のとおりです。
A. 停止期間を最小限に抑えます。
B. 単一障害点を排除します。
C. バックアップ戦略を定義する
D. 平均故障間隔 (MTBF) を短縮します。
正解**: (**正解を表示します**)**
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**: 382**
組織のビジネス機能の重要性を判断するのに最も役立つのは次のどれですか?
A. 災害復旧計画 (DRP)
B. ビジネス影響分析 (BIA)
C. 事業継続計画 (BCP)
D. セキュリティ評価レポート (SAR)

正解: **B** (コメントを発表する)
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: **383**
次のどれが、ポリシーに沿って組織に最低限の情報セキュリティ要件を伝えるのに最適でしょうか?
A. 標準
B. 手順
C. 規制
D. ベースライン
正解: (正解を表示します)
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: **384**

資産価値を決定するための主な基準となるのは次のどれですか?
A. 資産の交換にかかる費用
B. 資産が利用できない場合のビジネスコスト
C. 資産の原価から減価償却費を差し引いた金額
D. 総所有コスト (TCO)
正解: **B (**コメントを発表する**)**
The primary basis for determining the value of assets should be the business cost when assets are not available. This is because the value of assets is not only determined by their acquisition or replacement cost, but also by their contribution to the organization's business objectives and processes. The business cost when assets are not available reflects the potential impact of losing or compromising the assets on the organization's operations, performance, reputation, and compliance. The business cost when assets are not available can be estimated by conducting a business impact analysis (BIA), which identifies the criticality, dependencies, and recovery requirements of the assets. By using the business cost when assets are not available as the primary basis for determining the value of assets, the organization can prioritize the protection and management of the assets according to their importance and risk level. References = CISM Review Manual 15th Edition, page 64, page 65.

質問: **385**
セキュリティ管理の実装の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考慮すべき事項は次のどれですか?
A. 業界ベンチマークとの整合
B. ビジネス影響分析 (BIA) の結果
C. 事件による評判低下の可能性
D. セキュリティ予算の可用性
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: **386**
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: **(正解を表示します)**
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*

質問: **387**
情報セキュリティ チームは、脅威アクターがアプリケーション内で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。最初に実行する必要があるのは次のうちどれですか。
A. 追加のアプリケーション コントロールをインストールします。
B. 上級管理職に通知します。
C. インシデント対応計画を呼び出します。
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: **388**
情報セキュリティ管理者は、情報資産管理プログラムを確認する際に、まず何を確認すべきでしょうか?
A. システム所有者が特定されました。
B. 主要なアプリケーションが保護されました。
C. 情報資産は機密扱いになっています。

D. 情報資産がインベントリ化されました。
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: **389**
組織の情報セキュリティ プログラムに影響を及ぼす新しい規制要件が発表されました。情報セキュリティ マネージャーが最初に取るべき行動は次のうちどれですか。
A. ギャップ分析を実行します。
B. ベンチマークを実施します。
C. 法務部門に通知します。
D. ビジネスへの混乱を判断します。
正解: **C (**コメントを発表する**)**
= A new regulatory requirement affecting an organization's information security program is released. The information security manager's first course of action should be to notify the legal department, as they are responsible for ensuring compliance with the relevant laws and regulations. The legal department can advise the information security manager on how to interpret and implement the new requirement, as well as what are the potential implications and risks for the organization12.
References = 1: CISM Review Manual (Digital Version), page 271 2: CISM Review Manual (Print Version), page 271 Learn more:
1. isaca.org2. csoonline.com

質問: **390**
事業継続計画 (BCP) で復旧戦略を定義する際に最も重要な考慮事項は次のうちどれですか?
A. 法的および規制上の要件
B. 災害の可能性
C. サービス中断に対する組織の許容度
D. バックアップ サイトの地理的な場所
正解: **(**正解を表示します**)**
= The organizational tolerance to service interruption is the most important consideration when defining a recovery strategy in a business continuity plan (BCP), as it reflects the degree of risk that the organization is willing to accept in the event of a disaster. The organizational tolerance to service interruption determines the acceptable level of downtime, data loss, or disruption that the organization can tolerate, and thus guides the

selection of recovery objectives, strategies, and resources. Legal and regulatory requirements are external factors that influence the recovery strategy, but are not the primary consideration. Likelihood of a disaster is a factor that affects the recovery strategy, but is not the most important one. Geographical location of the backup site is a factor that affects the recovery strategy, but is not as critical as organizational tolerance to service interruption. References = CISM Review Manual, 16th Edition, page 1731; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 792 Learn more:
1. isaca.org2. amazon.com3. gov.uk

質問**: 391**
注目度の高いセキュリティ インシデントに対応しているときに、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欠陥があることに気づきました。計画を更新する最適な時期はいつでしょうか。
A. 事件に対応している間
B. 卓上演習中
C. インシデント後のレビュー中
D. リスク再評価後
正解**: (**正解を表示します**)**
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: **392**
情報システムの機密性と可用性を確保するために適切な管理が確実に実施されるようにする責任は誰にありますか?
A. ビジネスマネージャー
B. 情報所有者
C. 上級管理職
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: **393**
クラウド サービス プロバイダーを使用する際に、データが混在したり公開されたりしないようにするための最善の方法は次のどれですか。
A. 独立した監査レポートを取得します。
B. プロバイダーに厳格なデータ分類手順に従うことを要求します。
C. 契約書にセキュリティ違反に対する高額な罰金を盛り込みます。
D. プロバイダーの情報セキュリティ ポリシーを確認します。
正解: **(**正解を表示します**)**
Requiring the provider to follow stringent data classification procedures is the BEST way to ensure data is not co-mingled or exposed when using a cloud service provider, because it helps to define the sensitivity and confidentiality levels of the data and the corresponding security controls and access policies that should be applied. Data classification procedures can help to prevent unauthorized access, disclosure, modification, or deletion of the data, as well as to segregate the data from other customers' data.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 72: "Data classification is the process of assigning a level of sensitivity to data that reflects its importance and the impact of its disclosure, alteration, or destruction." CISM Review Manual, 16th Edition, ISACA, 2020, p. 73: "Data classification should be based on the business requirements for confidentiality, integrity, and availability of the data, and should consider the legal, regulatory, and contractual obligations of the enterprise." Best Practices to Manage Risks in the Cloud - ISACA: "Commingling of data: A big concern many enterprises have with public cloud services is the commingling of data with that of the cloud provider's other customers. One of your first questions should be: "How do you ensure that my data is not commingled with others?" How does the cloud provider ensure that only your team has access to your data?"

質問: **394**

組織のデータ保持戦略とそれに続くポリシーを決定する最も効果的なものは次のうちどれですか?
A. サプライヤーの要件
B. ビジネス要件
C. ビジネス影響分析（BIA）
D. リスク選好度
正解: **(**正解を表示します**)**

質問: **395**
情報セキュリティガバナンスの望ましい成果は次のどれですか?
A. 侵入テスト
B. リスク管理の改善
C. ビジネスの俊敏性
D. 成熟モデル
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: **396**
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すか?
A. ヘルプデスクに通話ログを確認するようにトレーニングします。
B. ヘルプデスクにインシデント後のレビューへの参加を要求します。
C. ヘルプデスクにセキュリティインシデントの基準を提供します。
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ます。
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: **397**
多国籍企業の情報セキュリティ管理者は、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。次のうち、最も懸念されるのはどれですか?
A. さまざまな脅威環境
B. 異なるレポートライン
C. 矛盾する法的要件
D. 労働文化の違い
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

質問: **398**
インシデント対応チームはどのようなタイプの制御ですか?
A. 予防的
B. 修正
C. 探偵
D. ディレクティブ
正解: **B (**コメントを発表する**)**

質問: **399**

インシデント対応チームは最近、未知の種類のサイバーイベントに遭遇しました。チームは問題を解決できましたが、特定にかなりの時間を要しました。今後、同様のインシデントをより迅速に特定できるようにするには、どのような方法が最も効果的でしょうか？
A. チームのパフォーマンス指標を確立する
B. インシデント後のレビューを実行する
C. SIEMソリューションを実装する
D. 脅威分析を実行する
正解: **(**正解を表示します**)**
Performing a post-incident review (also known as a lessons-learned session) is the best way to ensure similar incidents are identified and addressed more efficiently in the future. This review helps in understanding what went wrong, what went right, and how processes can be improved. The knowledge gained from the review can be incorporated into incident response plans and training.
"Post-incident reviews help determine root causes, assess the effectiveness of the response, and identify opportunities for improvement."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Post-incident Analysis Additionally, the ISACA CISM Practice Question Database emphasizes that post-incident reviews are essential for improving future response times and understanding patterns of threats.

質問: **400**
情報セキュリティが組織の戦略と一致していることを確認する最も重要な理由はどれですか?
A. 組織のリスク許容度を特定する
B. セキュリティプロセスを改善する
C. セキュリティの役割と責任を一致させる
D. セキュリティリスク管理を最適化する
正解: **(**正解を表示します**)**
= The most important reason to ensure information security is aligned with the organization's strategy is to optimize security risk management. Information security is not an isolated function, but rather an integral part of the organization's overall objectives, processes, and governance. By aligning information security with the organization's strategy, the information security manager can ensure that security risks are identified, assessed, treated, and monitored in a consistent, effective, and efficient manner1. Alignment also enables the information security manager to communicate the value and benefits of information security to senior management and other stakeholders, and to justify the allocation of resources and investments for security initiatives2. Alignment also helps to establish clear roles and responsibilities for information security across the organization, and to foster a culture of security awareness and accountability3. Therefore, alignment is essential for optimizing security risk management, which is the process of balancing the protection of information assets with the business objectives and risk

appetite of the organization4. References = 1: CISM Exam Content Outline | CISM Certification | ISACA 2: CISM_Review_Manual Pages 1-30 - Flip PDF Download | FlipHTML5 3: CISM 2020: Information Security & Business Process Alignment 4: CISM Review Manual 15th Edition, Chapter 2, Section 2.1

質問: **401**
技術的なセキュリティ管理が不十分なまま、新しいアプリケーションが本番環境に導入されました。根本原因として最も可能性が高いのは次のどれですか?
A. 不十分なインシデント対応管理
B. 法的審査の欠如
C. 変更管理が不十分
D. 品質管理の欠如
正解: **(**正解を表示します**)**
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

質問: **402**
IT プロジェクトは、制作後にセキュリティ制御が多すぎるために予算を超過しました。プロジェクトに適切な制御が適用されるようにするために、次のどれが最も役立ちますか?
A. プロジェクト管理の各段階に情報セキュリティを組み込む
B. プロジェクトのビジネスケース分析中に責任を特定する
C. データ分類フレームワークを作成し、関係者に提供する
D. 関係者に最低限の情報セキュリティ要件を提供する
正解: **(**正解を表示します**)**
The best way to ensure that relevant controls are applied to a project is to involve information security at each stage of project management. This will help to identify and address the security risks and requirements of the project from the beginning, and to integrate security controls into the project design, development, testing, and implementation. This will also help to avoid adding unnecessary or ineffective controls post-production, which can increase the project cost and complexity, and reduce the project performance and quality. By involving information security at each stage of project management, the information security manager can ensure that the project delivers the expected security value and aligns with the organization's security strategy and objectives.
References = CISM Review Manual 15th Edition, page 41.

質問: **403**

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と整合させる際に考慮すべき最も重要なことはどれですか?
A. 規制と基準
B. 人々と文化
C. 経営陣と取締役会の指示
D. プロセスとテクノロジー
正解: **(**正解を表示します**)**
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**: 404**
情報セキュリティ マネージャーがサードパーティのフォレンジック プロバイダーを選択する際に確認する必要がある最も重要な項目は次のどれですか。
A. 監査権条項の存在
B. プロバイダーのビジネス継続性テストの結果
C. プロバイダーの技術的能力
D. プロバイダーのインシデント対応計画の存在
正解**: C (**コメントを発表する**)**
The technical capabilities of the provider are the MOST important thing for an information security manager to verify when selecting a third-party forensics provider because they determine the quality, reliability, and validity of the forensic services and results that the provider can deliver. The technical capabilities of the provider include the skills, experience, and qualifications of the forensic staff, the methods, tools, and standards that the forensic staff use, and the facilities, equipment, and resources that the forensic staff have. The information security manager should verify that the technical capabilities of the provider match the forensic needs and expectations of the organization, such as the type,

scope, and complexity of the forensic investigation, the legal and regulatory requirements, and the time and cost constraints12. The existence of a right-to-audit clause (A) is an important thing for an information security manager to verify when selecting a third-party forensics provider, but it is not the MOST important thing. A right-to-audit clause is a contractual provision that grants the organization the right to audit or review the performance, compliance, and security of the provider. A right-to-audit clause can help to ensure the accountability, transparency, and quality of the provider, as well as to identify and resolve any issues or disputes that may arise during or after the forensic service. However, a right-to-audit clause does not guarantee that the provider has the technical capabilities to conduct the forensic service effectively and efficiently12. The results of the provider's business continuity tests (B) are an important thing for an information security manager to verify when selecting a third-party forensics provider, but they are not the MOST important thing. The results of the provider's business continuity tests can indicate the ability and readiness of the provider to continue or resume the forensic service in the event of a disruption, disaster, or emergency. The results of the provider's business continuity tests can help to assess the availability, resilience, and recovery of the provider, as well as to mitigate the risks of losing or compromising the forensic evidence or data. However, the results of the provider's business continuity tests do not ensure that the provider has the technical capabilities to perform the forensic service accurately and professionally12. The existence of the provider's incident response plan (D) is an important thing for an information security manager to verify when selecting a third-party forensics provider, but it is not the MOST important thing. The existence of the provider's incident response plan can demonstrate the preparedness and capability of the provider to detect, report, and respond to any security incidents that may affect the forensic service or the organization. The existence of the provider's incident response plan can help to protect the confidentiality, integrity, and availability of the forensic evidence or data, as well as to comply with the legal and contractual obligations. However, the existence of the provider's incident response plan does not confirm that the provider has the technical capabilities to execute the forensic service competently and ethically12. References = 1: CISM Review Manual 15th Edition, page 310-3111; 2: A Risk-Based Management Approach to Third-Party Data Security, Risk and Compliance - ISACA2

質問**: 405**

オフィスでのカメラの使用を禁止するポリシーに違反して、従業員にはウェブカメラが有効なスマートフォンとタブレット コンピューターが配布されました。情報セキュリティ マネージャーが最初に取るべき行動は次のうちどれですか。

A. ポリシーを修正します。

B. 根本原因分析を実行します。

C. リスク評価を実施し、

D. 許容される使用ポリシーを伝えます。

正解: (正解を表示します)
= The information security manager's first course of action in this situation should be to conduct a risk assessment, which is a process of identifying, analyzing, and evaluating the information security risks that arise from the violation of the policy prohibiting the use of cameras at the office. The risk assessment can help to determine the likelihood and impact of the unauthorized or inappropriate use of the cameras on the smartphones and tablet computers, such as capturing, transmitting, or disclosing sensitive or confidential information, compromising the privacy or security of the employees, customers, or partners, or violating the legal or regulatory requirements. The risk assessment can also help to identify and prioritize the appropriate risk treatment options, such as implementing technical, administrative, or physical controls to disable, restrict, or monitor the camera usage, enforcing the policy compliance and awareness, or revising the policy to reflect the current business needs and environment. The 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 policy and the risk management process.
Revising the policy, performing a root cause analysis, and communicating the acceptable use policy are all possible courses of action that the information security manager can take after conducting the risk assessment, but they are not the first ones. Revising the policy is a process of updating and modifying the policy to align with the business objectives and strategy, to address the changes and challenges in the business and threat environment, and to incorporate the feedback and suggestions from the risk assessment and the stakeholders.
Performing a root cause analysis is a process of investigating and identifying the underlying causes and factors that led to the violation of the policy, such as the lack of awareness, training, or enforcement, the inconsistency or ambiguity of the policy, or the conflict or gap between the policy and the business requirements or expectations.
Communicating the acceptable use policy is a process of informing and educating the employees and the other users of the smartphones and tablet computers about the purpose, scope, and content of the policy, the roles and responsibilities of the users, the benefits and consequences of complying or violating the policy, and the methods and channels of reporting or resolving any policy issues or incidents. References = CISM Review Manual 15th Edition, pages 51-531; CISM Practice Quiz, question 1482

質問: **406**
自国で電子商取引活動を行っている組織が、厳格なセキュリティ法が施行されている別の国に新しいオフィスを開設しました。このシナリオでは、全体的なセキュリティ戦略は次の基準に基づいて策定する必要があります。
A. 最も厳しい要件。
B. セキュリティ組織の構造。

C. 国際セキュリティ標準。
D. リスク評価結果。
正解: **(**正解を表示します**)**

質問: **407**
インシデント管理計画が効果的に実行されるようにするために最も重要なのは次のどれですか?
A. 経営陣の支援と承認が得られました。
B. インシデント対応成熟度評価が実施されました。
C. 評判の良いマネージド セキュリティ サービス プロバイダーを採用しました。
D. インシデント対応チームは適切なトレーニングを受けています。
正解: **(**正解を表示します**)**

質問: **408**
フォレンジック検査を実施する前に、情報セキュリティ管理者は次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. 新しいメディアに元のデータのイメージを作成します。
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再配置します。
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: **409**
ある組織の情報セキュリティ チームは、最近の情報セキュリティ運営委員会の会議でリスク レジスタを発表しました。委員会にとって最も懸念すべきことは次のうちどれですか?
A. 一部のリスクについては所有者が特定されませんでした。
B. ビジネス アプリケーションのリスクが最も多かった。
C. リスク軽減行動計画にはスケジュールがありませんでした。
D. リスク軽減行動計画のマイルストーンが遅れた。
正解: **(**正解を表示します**)**
The most concerning issue for the information security steering committee should be that no owners were identified for some risks in the risk register. This means that there is no clear accountability and responsibility for managing and mitigating those risks, and that the risks may not be properly addressed or monitored. The risk owners are the persons who have the authority and ability to implement the risk treatment options and to accept the residual risk. The risk owners should be identified and assigned for each risk in the risk register, and they should report the status and progress of the risk management activities to the information security steering committee.
References = CISM Review Manual, 16th Edition eBook1, Chapter 2: Information Risk Management, Section: Risk Management, Subsection: Risk Register, Page 104.

質問: **410**
特定されたリスクを軽減するために追加のリスク対策が必要かどうかを決定する主な権限を持つのは誰ですか?
A. 情報セキュリティ管理者
B. ITリスクマネージャー
C. 内部監査員
D. リスクオーナー
正解: **D (**コメントを発表する**)**
The risk owner is the person who has the authority and accountability to make decisions about the risk, including whether to accept, avoid, transfer, or mitigate it. The risk owner is

also responsible for implementing and monitoring the risk treatment plan and reporting on the risk status. The risk owner is usually the business process owner or the information owner of the asset affected by the risk. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 64, section 2.2.1.2.

質問: **411**
セキュリティ インシデントのエスカレーション手順に含めることが最も重要なのは次のどれですか?
A. セキュリティ プログラムの主な目的
B. 回復手順
C. 通知基準
D. 封じ込め手順
正解: **(正解を表示します)**
The most important thing to include in security incident escalation procedures is notification criteria. This is because notification criteria define who needs to be informed of an incident, when, and how, depending on the severity, impact, and nature of the incident. Notification criteria help to ensure that the appropriate stakeholders are aware of the incident and can take the necessary actions to respond, mitigate, and recover from it. Notification criteria also help to comply with legal and regulatory requirements for reporting incidents to external parties, such as customers, authorities, or media.
Notification criteria define who needs to be informed of an incident, when, and how, depending on the severity, impact, and nature of the incident. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 4, Section 4.2.2, page 2121; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 1, page 1

質問: **412**
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すのは次のどれですか?
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イニシアチブに対して費用対効果分析が行われます。
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**: 413**
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**: 414**
インシデント管理チームは、セキュリティ イベントの疑いがあると警告されます。セキュリティ マネージャーにとって、疑わしいイベントをセキュリティ インシデントとして分類する前に、次のことが最も重要です。
A. インシデントのフォレンジック分析を実施します。
B. インシデント対応計画に従う
C. ビジネス プロセスの所有者に通知します。

D. 事業継続計画 (BCP) に従います。
正解: **(**正解を表示します**)**
Before classifying the suspected event as a security incident, it is most important for the security manager to follow the incident response plan, which is a predefined set of procedures and guidelines that outline the roles, responsibilities, and actions of the incident management team and the organization in the event of a security event or incident. Following the incident response plan can help to ensure a consistent, coordinated, and effective response to the suspected event, as well as to minimize the impact and damage to the business processes, functions, and assets. Following the incident response plan can also help to determine the nature, scope, and severity of the suspected event, and to decide whether it meets the criteria and threshold for being classified as a security incident that requires further escalation, investigation, and resolution. Following the incident response plan can also help to document and report the incident details, activities, and outcomes, and to provide feedback and recommendations for improvement and optimization of the incident response process and plan.
Conducting an incident forensic analysis, notifying the business process owner, and following the business continuity plan (BCP) are all important steps in the incident response process, but they are not the most important ones before classifying the suspected event as a security incident. Conducting an incident forensic analysis is a technical and detailed process that involves collecting, preserving, analyzing, and presenting evidence related to the incident, and it is usually performed after the incident has been classified, contained, and eradicated. Notifying the business process owner is a communication and notification process that involves informing the relevant stakeholders of the incident status, impact, and actions, and it is usually performed after the incident has been classified and assessed. Following the business continuity plan (BCP) is a recovery and restoration process that involves resuming and restoring the normal business operations and functions after the incident has been resolved and lessons learned have been identified and implemented. References = CISM Review Manual 15th Edition, pages 237-2411; CISM Practice Quiz, question 1422

質問: **415**
機密性の高いデータを保存する重要なシステムの開発中に、情報セキュリティ マネージャーが主に重点を置くべきものは何ですか?
A. 検出された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. 規制要件への準拠
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**: 416**
情報資産の分類を決定する最も適切な方法はどれですか?
A. 市場における情報資産の価値
B. ビジネスプロセスにとっての重要性
C. データ所有者からのリスク評価
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**: 417**
災害復旧計画 (DRP) を実行する能力に最も大きなプラスの影響を与えるのは次のどれですか?
A. 計画をオフサイトの場所に保管する
B. 計画をすべての関係者に伝える
C. 定期的に計画を更新する
D. 計画のウォークスルーを実施する
正解**: (**正解を表示します**)**
A walk-through of the disaster recovery plan (DRP) is a method of testing the plan by simulating a disaster scenario and having the participants review their roles and responsibilities, as well as the procedures and resources required to execute the plan. A

walk-through has the greatest positive impact on the ability to execute the DRP, as it helps to identify and resolve any gaps, errors, or inconsistencies in the plan, as well as to enhance the awareness and readiness of the stakeholders involved in the recovery process. References = CISM Review Manual, 16th Edition, Chapter 5, Section 5.3.2.21

質問: **418**
情報セキュリティ プログラムは、以下の点と密接に連携している場合に成功に最も適しています。
A. 情報セキュリティのベスト プラクティス。
B. 業界の枠組みとして認識されています。
C. 情報セキュリティポリシー。
D. 情報セキュリティ戦略。
正解: **(正解を表示します)**
An information security program is best positioned for success when it is closely aligned with the information security strategy, which defines the organization's vision, mission, goals, objectives, and risk appetite for information security. The information security strategy provides the direction and guidance for developing and implementing the information security program, ensuring that it supports the organization's business processes and objectives. The information security strategy also helps to establish the scope, boundaries, roles, responsibilities, and resources for the information security program.
References = CISM Manual, Chapter 3: Information Security Program Development (ISPD), Section 3.1:
Information Security Strategy1
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles

質問: **419**
情報資産のビジネス価値は、次の要素から生まれます。
A. 脅威プロファイル。
B. その重要性。
C. リスク評価。
D. その交換コスト。
正解: **(正解を表示します)**
The business value of an information asset is derived from its criticality, which is the degree of importance or dependency of the asset to the organization's objectives, operations, and stakeholders. The criticality of an information asset can be determined by assessing its impact on the confidentiality, integrity, and availability (CIA) of the information, as well as its sensitivity, classification, and regulatory requirements. The higher the criticality of an information asset, the higher its business value, and the more resources and controls are needed to protect it.

References = CISM Review Manual 2022, page 371; CISM Exam Content Outline, Domain 1, Task 1.32; IT Asset Valuation, Risk Assessment and Control Implementation Model1; Managing Data as an Asset3

質問: **420**
脆弱性スキャナーが不完全な結果を返す理由として最も可能性が高いのは次のどれですか?
A. ホスト名が完全に列挙されていません。
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. 認証されていない脆弱性スキャンが実行されています。
D. ゼロデイ脆弱性シグネチャが取り込まれていません。
正解: **(**正解を表示します**)**

質問: **421**
新しいセキュリティ ソリューションの実装を承認する前に、上級管理職はビジネス ケースを要求します。投資の正当性を最もよく裏付けるのは次のどれですか。
A. ソリューションはビジネス戦略に貢献します。
B. このソリューションにより、ビジネス リスク許容レベルが向上します。
C. ソリューションによりビジネスの回復力が向上します。
D. このソリューションは、規制違反のコストを削減します。
正解: **A (**コメントを発表する**)**
The best way to support the justification for investment in a new security solution is to show how the solution contributes to the business strategy of the organization. The business strategy defines the vision, mission, goals, and objectives of the organization, and the security solution should align with and support them. The security solution should also demonstrate how it adds value to the organization, such as by enabling new business opportunities, enhancing customer satisfaction, or increasing competitive advantage. The business case should include the expected benefits, costs, risks, and alternatives of the security solution, and provide a clear rationale for choosing the preferred option1.
References = CISM Review Manual, 16th Edition eBook2, Chapter 1: Information Security Governance, Section: Information Security Strategy, Subsection: Business Case Development, Page 33.

質問: **422**
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. オリジナルと画像のデジタル ハッシュを実行します。
D. 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。
正解: **(**正解を表示します**)**

質問: **423**
情報セキュリティ戦略を見直す際に、最も重要な考慮事項は次のどれですか?
A. 最近のセキュリティインシデント
B. 新規事業への取り組み
C. 業界のセキュリティ標準
D. 内部監査の調査結果
正解: **(**正解を表示します**)**
New business initiatives are the most important consideration, as security must align with business changes to effectively protect assets and support growth.
"The security strategy must be aligned with new business initiatives to ensure it continues to protect critical assets and support enterprise goals."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Business Alignment* ISACA practice questions stress that aligning with new business initiatives ensures relevance and effectiveness.

質問: **424**
組織内でセキュリティ文化を構築するための主な目的は次のどれですか?
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優先する
C. リスクを許容レベルまで低減する
D. 上級管理職に管理の有効性を示す
正解: **C (**コメントを発表する**)**
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: **425**
次の要素のうち、組織の情報セキュリティ ガバナンス モード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: **426**
組織内で望ましい情報セキュリティ文化を実現するのに最も役立つのは次のどれですか?
A. 情報セキュリティ意識向上トレーニングとキャンペーン
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の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

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 **1041**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」