

# PrepPDF

## Pass Your Next Certification Exam Fast!

Everything you need to prepare, learn & pass your certification exam easily.

365 days free updates. First attempt guaranteed success.

| Choose the version that fits your needs   | PDF Version | Desktop Test Engine | Online Test Engine |
|---|-------------|---------------------|--------------------|
| Latest and Up-to-Date exam dumps with real exam questions answers.              | ✓           | ✓                   | ✓                  |
| Get 12-Months free updates without any extra charges.                           | ✓           | ✓                   | ✓                  |
| Experience same exam environment before appearing in the certification exam.    | ✗           | ✓                   | ✓                  |
| 100% exam passing guarantee in the first attempt.                               | ✓           | ✓                   | ✓                  |
| 20% discount on more than one license and 30% discount on 5+ license purchases. | ✗           | ✓                   | ✓                  |
| 100% secure purchase on SSL.  | ✓           | ✓                   | ✓                  |
| Completely private purchase without sharing your personal info with anyone.     | ✓           | ✓                   | ✓                  |

<http://www.preppdf.com>

Reasonable study tool and effective study materials - PrepPDF

**Exam** : **CISM-JPN**

**Title** : Certified Information  
Security Manager  
(CISM日本語版)

**Vendor** : ISACA

**Version** : DEMO

### QUESTION NO: 1

インシデント対応計画のエスカレーション手順を開発する際に確実に実行する必要がある最も重要なことはどれですか？

- A. 各プロセスには責任者が割り当てられます。
- B. 連絡先リストは定期的に更新されます。
- C. 最低限の規制要件が維持されます。
- D. 上級管理職の承認が文書化されています。

**Answer: B**

Explanation:

= The contact list is the most important element of the escalation procedures for an incident response plan, as it ensures that the appropriate stakeholders are notified and involved in the incident management process. A contact list should include the names, roles, responsibilities, phone numbers, email addresses, and backup contacts of the key personnel involved in the incident response, such as the incident response team, senior management, legal counsel, public relations, law enforcement, and external service providers. The contact list should be regularly updated and tested to ensure its accuracy and availability<sup>123</sup>. References =

1: Information Security Incident Response Escalation Guideline<sup>2</sup>, page 4

2: A Practical Approach to Incident Management Escalation<sup>1</sup>, section "Step 2: Log the escalation and record the related incident problems that occurred"

3: Computer Security Incident Handling Guide<sup>4</sup>, page 18

### QUESTION NO: 2

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. 上級管理職
- B. 情報所有者
- C. ビジネスマネージャー
- D. 情報セキュリティマネージャー

**Answer: A**

### QUESTION NO: 3

国境を越えて個人データを転送する必要がある場合、組織が最初に行うべきことは何ですか？

- A. データ処理のポリシーと標準を定義します。
- B. 適用可能なプライバシー原則を実装する
- C. 地方または地域の規制を評価する
- D. サイバー保険ポリシーの調査

**Answer: C**

Explanation:

Before transferring personal data across borders, an organization should first assess the local or regional regulations that apply to the data protection and privacy of the data subjects. This will help the organization to identify the legal requirements and risks involved in the data transfer, and to choose the appropriate tools and safeguards to ensure compliance and protection. For example, the organization may need to obtain consent from the data subjects,

use adequacy decisions, standard contractual clauses, or other mechanisms to ensure an adequate level of protection in the third country, or rely on specific derogations for certain situations. The other options are not the first steps to take, although they may be relevant at later stages of the data transfer process. References = Guide to the cross-border transfer of personal data in the GDPR New guidance issued by the EDPB on international transfers of personal data Requirements for transferring personal information across borders

**QUESTION NO: 4**

情報セキュリティ管理者がセキュリティ管理の実装に関して組織的なサポートを得るのに最も効果的なのは次のどれですか？

- A. 定期的な脆弱性評価の実施
- B. ビジネス影響分析 (BIA) の結果の伝達
- C. 効果的なステークホルダー関係の構築
- D. 組織のリスク管理フレームワークの定義

**Answer: A**

Explanation:

The best way to obtain organizational support for the implementation of security controls is to establish effective stakeholder relationships. Stakeholders are the individuals or groups that have an interest or influence in the organization's information security objectives, activities, and outcomes. They may include senior management, business owners, users, customers, regulators, auditors, vendors, and others. By establishing effective stakeholder relationships, the information security manager can communicate the value and benefits of security controls to the organization's performance, reputation, and competitiveness. The information security manager can also solicit feedback and input from stakeholders to ensure that the security controls are aligned with the organization's needs and expectations. The information security manager can also foster collaboration and cooperation among stakeholders to facilitate the implementation and operation of security controls. The other options are not the best way to obtain organizational support for the implementation of security controls, although they may be some steps or outcomes of the process. Conducting periodic vulnerability assessments is a technical activity that can help identify and prioritize the security weaknesses and gaps in the organization's information assets and systems. However, it does not necessarily obtain organizational support for the implementation of security controls unless the results are communicated and justified to the stakeholders. Communicating business impact analysis (BIA) results is a reporting activity that can help demonstrate the potential consequences of disruptions or incidents on the organization's critical business processes and functions. However, it does not necessarily obtain organizational support for the implementation of security controls unless the results are linked to the organization's risk appetite and tolerance. Defining the organization's risk management framework is a strategic activity that can help establish the policies, procedures, roles, and responsibilities for managing information security risks in a consistent and effective manner. However, it does not necessarily obtain organizational support for the implementation of security controls unless the framework is endorsed and enforced by the stakeholders

**QUESTION NO: 5**

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. 関連する事業主に管理権限を引き渡します。
- 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. 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。
- 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。

**Answer:** B

#### QUESTION NO: 6

機密情報が誤って組織外に漏洩した場合の最善の対応策は次のどれですか？

- A. コンプライアンス要件を確認します。
- B. 露出について伝えます。
- C. インシデントを宣言します。
- D. 暗号化キーを変更します。

**Answer:** C

Explanation:

Declaring an incident is the best course of action when confidential information is inadvertently disseminated outside the organization, as it triggers the incident response process, which aims to contain, analyze, eradicate, recover, and learn from the incident. Declaring an incident also helps to communicate the exposure to the relevant stakeholders, such as senior management, legal authorities, customers, or regulators, and to comply with the applicable laws and regulations regarding notification and disclosure. Changing the encryption keys, reviewing compliance requirements, or communicating the exposure are possible steps within the incident response process, but they are not the first course of action.

References = CISM Review Manual 2022, page 3121; CISM Exam Content Outline, Domain 4, Task

4.12; CISM 2020: Incident Management; How to Respond to a Data Breach

#### QUESTION NO: 7

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

**Answer:** D

Explanation:

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>

#### QUESTION NO: 8

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. 情報セキュリティ予算の承認を迅速化します。
- 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. 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。

**Answer: A**

#### QUESTION NO: 9

組織のネットワーク内のモノのインターネット (IoT)

デバイスがハッキングされたことが確認された場合、最初に取り組むべきステップは何でしょうか？

- A. ネットワークを監視します。
- B. フォレンジック分析を実行します。
- C. デバイスをネットワークから切断します。
- D. インシデント対応チームにエスカレーションする

**Answer: C**

Explanation:

= Disconnecting the device from the network is the first step when an IoT device in an organization's network is confirmed to have been hacked, as it prevents the attacker from further compromising the device or using it as a pivot point to attack other devices or systems on the network. Disconnecting the device also helps preserve the evidence of the attack for later forensic analysis and remediation. Disconnecting the device should be done in accordance with the incident response plan and the escalation procedures<sup>123</sup>. References =  
1: CISM Review Manual 15th Edition, page 2004  
2: CISM Practice Quiz, question 1072  
3: IoT Security: Incident Response, Forensics, and Investigations, section "IoT Incident Response"

#### QUESTION NO: 10

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。**

**Answer: B**

Explanation:

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

**QUESTION NO: 11**

情報資産の保護レベルを決定する際に、最も参考になるのは次のうちどれですか？

- A. 情報セキュリティプログラムへの影響
- B. コントロールのコスト
- C. 事業機能への影響
- D. 交換費用

**Answer: C**

Explanation:

The level of protection for an information asset should be based on the impact to the business function that depends on the asset. The impact to the business function reflects the value and criticality of the information asset to the organization, and the potential consequences of its loss, compromise, or unavailability. The impact to the business function can be measured in terms of financial, operational, reputational, legal, or strategic effects. The higher the impact, the higher the level of protection required.

Impact on information security program, cost of controls, and cost to replace are not the best factors to provide guidance when deciding the level of protection for an information asset.

Impact on information security program is a secondary effect that depends on the impact to the business function. Cost of controls and cost to replace are important considerations for implementing and maintaining the protection, but they do not determine the level of protection needed. Cost of controls and cost to replace should be balanced with the impact to the business function and the risk appetite of the organization. References = CISM Certified Information Security Manager Study Guide, Chapter 2: Information Risk Management, page 671; CISM Foundations: Module 2 Course, Part One: Information Risk Management2; CISM Review Manual 15th Edition, Chapter 2: Information Risk Management, page 693 When deciding the level of protection for an information asset, the most important factor to consider is the impact to the business function. The value of the asset should be evaluated in terms of its importance to the organization's operations and how its security posture affects the organization's overall security posture.

Additionally, the cost of implementing controls, the potential impact on the information security program, and the cost to replace the asset should be taken into account when

determining the appropriate level of protection for the asset.

**QUESTION NO: 12**

組織のセキュリティ要件を満たさない新しいサードパーティのクラウドアプリケーションに関連するリスクに対処するために、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. 契約にセキュリティ要件を含めます。
- B. リスクレジスタを更新します。
- C. 事業主に相談してください。
- D. アプリケーションのネットワーク アクセスを一時的に制限します。

**Answer: C**

Explanation:

Consulting with the business owner is the FIRST course of action that the information security manager should take to address the risk associated with a new third-party cloud application that will not meet organizational security requirements, because it helps to understand the business needs and expectations for using the application, and to communicate the security risks and implications. The information security manager and the business owner should work together to evaluate the trade-offs between the benefits and the risks of the application, and to determine the best course of action, such as modifying the requirements, finding an alternative solution, or accepting the risk.

References =

CISM Review Manual, 16th Edition, ISACA, 2020, p. 41: "The information security manager should consult with the business owners to understand their needs and expectations for using third-party services, and to communicate the security risks and implications." CISM Review Manual, 16th Edition, ISACA, 2020, p. 42: "The information security manager and the business owners should collaborate to evaluate the trade-offs between the benefits and the risks of using third-party services, and to determine the best course of action, such as modifying the requirements, finding an alternative solution, or accepting the risk." Best Practices to Manage Risks in the Cloud - ISACA: "The information security manager should work with the business owner to define the security requirements for the cloud service, such as data protection, access control, incident response, and compliance."

**QUESTION NO: 13**

ある組織がネットワーク管理をサービスプロバイダーにアウトソーシングすることを計画しています。情報セキュリティリスクを軽減するには、次のどれを契約に含めるのが最も効果的でしょうか。

- A. 定期的な情報セキュリティ意識の要件
- B. 監査権条項
- C. サービスレベル契約 (SLA)
- D. 企業のセキュリティポリシーに準拠する要件

**Answer: D**

Explanation:

The most effective way to mitigate information security risk when outsourcing network management to a service provider is to include a requirement for the service provider to comply with the corporate security policy in the contract. This requirement ensures that the

service provider follows the same security standards, procedures, and controls as the organization, and protects the confidentiality, integrity, and availability of the organization's data and systems. The requirement also defines the roles and responsibilities, the reporting and escalation mechanisms, and the penalties for non-compliance.

References = A Risk-Based Management Approach to Third-Party Data Security, Risk and Compliance, CISM Domain 2: Information Risk Management (IRM) [2022 update]

**QUESTION NO: 14**

組織のマーケティング部門は、情報セキュリティポリシーに準拠していないオンラインコラボレーション

サービスを使用したいと考えています。リスク評価が実行され、リスクの受け入れが進められています。リスクの受け入れの承認は、次の者によって提供される必要があります。

- A. 最高リスク管理責任者 (CRO)。
- B. ビジネス上級管理職。
- C. 情報セキュリティマネージャー。
- D. コンプライアンス担当者。

**Answer: B**

Explanation:

Risk acceptance is the decision to accept the level of residual risk after applying security controls, and to tolerate the potential impact and consequences of a security incident.

Approval of risk acceptance should be provided by business senior management, as they are the owners and accountable parties of the business processes, activities, and assets that are exposed to the risk. Business senior management should also have the authority and responsibility to allocate the resources, personnel, and budget to implement and monitor the risk acceptance decision, and to report and escalate the risk acceptance status to the board of directors or the executive management.

The chief risk officer (CRO) (A) is a senior executive who oversees the organization's risk management function, and provides guidance, direction, and support for the identification, assessment, treatment, and monitoring of risks across the organization. The CRO may be involved in the risk acceptance process, such as by reviewing, endorsing, or advising the risk acceptance decision, but the CRO is not the ultimate approver of risk acceptance, as the CRO is not the owner or accountable party of the business processes, activities, and assets that are exposed to the risk.

The information security manager is the manager who leads and coordinates the information security function, and provides guidance, direction, and support for the development, implementation, and maintenance of the information security program and activities. The information security manager may be involved in the risk acceptance process, such as by conducting the risk assessment, recommending the risk treatment options, or documenting the risk acceptance decision, but the information security manager is not the ultimate approver of risk acceptance, as the information security manager is not the owner or accountable party of the business processes, activities, and assets that are exposed to the risk.

The compliance officer (D) is the officer who oversees the organization's compliance function, and provides guidance, direction, and support for the identification, assessment, implementation, and monitoring of the compliance requirements and obligations across the

organization. The compliance officer may be involved in the risk acceptance process, such as by verifying, validating, or advising the risk acceptance decision, but the compliance officer is not the ultimate approver of risk acceptance, as the compliance officer is not the owner or accountable party of the business processes, activities, and assets that are exposed to the risk.

References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Treatment, Subsection: Risk Acceptance, page 95-961

#### QUESTION NO: 15

リスクを適切に軽減するための予防管理が実行できない場合、情報セキュリティ管理者にとって最も重要なアクションは次のどれですか？

- A. 影響の管理
- B. 許容できないリスクレベルの特定
- C. 脆弱性の評価
- D. 潜在的な脅威の評価

**Answer: A**

Explanation:

When preventive controls to appropriately mitigate risk are not feasible, the most important action for the information security manager is to manage the impact, which means taking measures to reduce the likelihood or severity of the consequences of the risk. Managing the impact can involve using alternative controls, such as engineering, administrative, or personal protective controls, that can lower the exposure or harm to the organization. The other options, such as identifying unacceptable risk levels, assessing vulnerabilities, or evaluating potential threats, are part of the risk assessment process, but they are not actions to mitigate risk when preventive controls are not feasible. References:

<https://bcmmetrics.com/risk-mitigation-evaluating-your-controls/>

<https://www.osha.gov/safety-management/hazard-prevention>

<https://www.cdc.gov/niosh/topics/hierarchy/default.html>

#### QUESTION NO: 16

情報セキュリティ戦略の策定と実施を任された新しく採用された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しょうか。

- A. 情報セキュリティチームの能力と専門知識
- B. 組織のミッションステートメントとロードマップ
- C. これまでの成功した情報セキュリティ戦略
- D. 組織の情報技術 (IT) 戦略

**Answer: B**

Explanation:

= The most useful source of information for a newly hired information security manager who has been tasked with developing and implementing an information security strategy is the organization's mission statement and roadmap. The mission statement defines the organization's purpose, vision, values, and goals, and the roadmap outlines the organization's strategic direction, priorities, and initiatives. By reviewing the mission statement and roadmap, the information security manager can understand the organization's business objectives, risk appetite, and security needs, and align the information security

strategy with them. The information security strategy should support and enable the organization's mission and roadmap, and provide the security governance, policies, standards, and controls to protect the organization's information assets and processes. The capabilities and expertise of the information security team (A) are important factors for the information security manager to consider, but they are not the most useful source of information for developing and implementing an information security strategy. The information security team is responsible for executing and maintaining the information security program and activities, such as risk management, security awareness, incident response, and compliance. The information security manager should assess the capabilities and expertise of the information security team to identify the strengths, weaknesses, opportunities, and threats, and to plan the resource allocation, training, and development of the team. However, the capabilities and expertise of the information security team do not directly inform the information security strategy, which should be driven by the organization's business objectives, risk appetite, and security needs.

A prior successful information security strategy is a possible source of information for the information security manager to refer to, but it is not the most useful one. A prior successful information security strategy is a strategy that has been implemented and evaluated by another organization or a previous information security manager, and has achieved the desired security outcomes and benefits. The information security manager can learn from the best practices, lessons learned, and challenges of a prior successful information security strategy, and apply them to the current organization or situation. However, a prior successful information security strategy may not be relevant, applicable, or suitable for the organization, as it may not reflect the current or future business objectives, risk appetite, and security needs of the organization, or the changing threat landscape and business environment. The organization's information technology (IT) strategy (D) is also a possible source of information for the information security manager to consult, but it is not the most useful one. The IT strategy is a strategy that defines the IT vision, goals, and initiatives of the organization, and how IT supports and enables the business processes and activities. The information security manager should review the IT strategy to understand the IT infrastructure, systems, and services of the organization, and how they relate to the information security program and activities. However, the IT strategy is not the primary driver of the information security strategy, which should be aligned with the organization's business objectives, risk appetite, and security needs, and not only with the IT objectives, capabilities, and requirements.

References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Information Security Strategy Development, page 23-241

**QUESTION NO: 17**

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。

**Answer: C**

**Explanation:**

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.

**QUESTION NO: 18**

セキュリティレビューの結果、ファイルサーバー上の機密情報が組織内の権限のないユーザーによってアクセスされたことが判明しました。情報セキュリティマネージャーが最初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す
- B. ロールベースのアクセス制御 (RBAC) を実装する
- C. 情報へのアクセスを削除する
- D. ファイルサーバーから情報を削除します

**Answer: A**

**Explanation:**

The first step is to invoke the incident response plan to ensure a systematic, controlled, and compliant response to the security incident.

"The incident response plan should be activated immediately to investigate, contain, and resolve incidents of unauthorized access."

- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Incident Response Plan Execution\* ISACA practice questions also reinforce that invoking the incident response plan is the essential first response to contain the breach.

**QUESTION NO: 19**

インシデント対応チームのトレーニングを強化するための最良の方法はどれですか？

- A. インシデント後のレビューを実行します。
- B. インシデントの主要業績評価指標 (KPI) を確立します。
- C. 組織単位へのインタビューを実施します。
- D. 緊急対応活動に参加する。

**Answer: A**

Explanation:

Performing post-incident reviews is the best way to enhance training for incident response teams because it allows them to identify the strengths and weaknesses of their response, learn from the lessons and best practices, and implement corrective actions and improvement plans for future incidents. Post-incident reviews also help to evaluate the effectiveness and efficiency of the incident response process and procedures, and to update them as needed.

References: The CISM Review Manual 2023 states that "post-incident reviews are an essential part of the incident response process" and that "they provide an opportunity to assess the performance of the incident response team, identify areas for improvement, and document lessons learned and best practices" (p. 191).

The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Performing post-incident reviews is the best way to enhance training for incident response teams, as it enables them to learn from their experience and improve their skills and knowledge" (p. 97).

#### QUESTION NO: 20

情報セキュリティガバナンスの有効性を判断するために組織が実施する必要がある最も重要なのは次のうちどれですか？

- A. プログラムメトリクス
- B. 主要リスク指標 ( KRI )
- C. リスクレジスタ
- D. セキュリティ戦略

**Answer: A**

Explanation:

Program metrics measure the effectiveness of governance processes and provide a basis for continuous improvement and informed decision-making.

"Metrics are essential for evaluating governance performance, demonstrating effectiveness, and identifying areas for improvement."

- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Monitoring and Metrics\* ISACA's practice questions confirm that program metrics are key to evaluating governance effectiveness.

#### QUESTION NO: 21

ある組織が新しい会社を買収する過程にあります。統合前に新しく買収したデータ資産を保護する方法を決定するための最適なアプローチは次のうちどれでしょうか。

- A. 契約にセキュリティ要件を含める
- B. セキュリティ制御を評価します。

- C. リスク評価を実行する
- D. データアーキテクチャを確認します。

**Answer: C**

Explanation:

Performing a risk assessment is the best approach to determine how to protect newly acquired data assets prior to integration, as it will help to identify the threats, vulnerabilities, impacts, and likelihoods of the data assets, and to prioritize the appropriate risk treatment options. Including security requirements in the contract is a good practice, but it may not be sufficient to address the specific risks of the data assets. Assessing security controls and reviewing data architecture are also important steps, but they should be done after performing a risk assessment, as they will depend on the risk level and the risk app The best approach to determine how to protect newly acquired data assets prior to integration is to perform a risk assessment. A risk assessment will identify the various threats and vulnerabilities associated with the data assets and help the organization develop an appropriate security strategy. This risk assessment should include an assessment of the security controls in place to protect the data, a review of the data architecture, and a review of any contractual requirements related to security.

#### QUESTION NO: 22

クラウドストレージ

ソリューションを評価する際、最初に考慮すべき点は次のとおりです。

- A. 暗号化キーのサービスレベル契約 (SLA)
- B. 組織のデータ分類ポリシーとの整合性
- C. 組織の機密データがどのように転送されるか
- D. クラウドに保存されるデータの量

**Answer: B**

Explanation:

The first consideration when evaluating cloud storage solutions is alignment with the organization's data classification policy (B). CISM emphasizes that security requirements must be driven by data sensitivity and business value. Before assessing encryption methods, SLAs, or data transfer mechanisms, the organization must determine what type of data will be stored and what protection level is required. Data classification informs confidentiality, integrity, availability, privacy, and regulatory requirements. Evaluating SLAs (A) or transfer methods (C) without understanding data sensitivity risks misalignment with governance and compliance obligations. Data volume (D) is an operational consideration, not a security driver.

References: ISACA CISM Review Manual (Risk management-data classification, cloud risk evaluation); CISM Exam Content Outline (Domain 1).

#### QUESTION NO: 23

サードパーティのバックアップ

サイトが組織の情報セキュリティ基準を継続的に満たしていることを保証するために最も役立つのは次のどれですか。

- A. サービスレベル契約 (SLA)
- B. 覚書 ( MoU )

- C. 事業継続計画 ( BCP )
- D. 災害復旧計画 ( DRP )

**Answer: A**

Explanation:

A Service Level Agreement (SLA) is a legally binding document that defines the performance and compliance expectations for third-party services, including information security requirements. It is the best mechanism to ensure that the third-party backup site meets ongoing security standards.

"SLAs should include security, availability, and performance expectations to align third-party services with organizational policies."

- CISM Review Manual 15th Edition, Chapter 3: Program Development, Section: Third-Party Relationships\*

#### QUESTION NO: 24

情報セキュリティプログラムを成功裏に実装するために最も重要なのは次のどれですか？

- A. プログラムに適切なセキュリティリソースが割り当てられています。
- B. 主要業績評価指標 (KPI) が定義されます。
- C. バランススコアカードは運営委員会によって承認されます。
- D. プログラムは、グローバルなセキュリティ標準を使用して開発されています。

**Answer: A**

Explanation:

The successful implementation of an information security program depends largely on the availability and allocation of adequate security resources, such as budget, staff, technology, and training. Without sufficient resources, the program may not be able to achieve its objectives, comply with the security strategy, or address the security risks. Key performance indicators (KPIs), a balanced scorecard, and global security standards are also important elements of an information security program, but they are not as critical as the resource allocation.

References = CISM Review Manual, 16th Edition, page 69

#### QUESTION NO: 25

セキュリティ制御を設計する際に最も重要なことは次のとおりです。

- A. リスクベースのアプローチを適用する
- B. 機密データに技術的制御を適用する
- C. ビジネス影響分析(BIA)の結果を考慮する
- D. 予防管理に重点を置く

**Answer: A**

Explanation:

A risk-based approach (A) is fundamental to control design in CISM. Controls must be proportionate to risk, aligned with business objectives, and consistent with risk appetite. Focusing solely on technical controls (B), BIA results (C), or preventive controls (D) limits effectiveness. A risk-based approach ensures balanced use of preventive, detective, and corrective controls.

References: ISACA CISM Review Manual (Risk management-control selection); CISM Exam

Content Outline (Domain 1).

**QUESTION NO: 26**

どのタイプのフェイルオーバー

サイトを採用するかを決定する際に最も重要な考慮事項は次のどれですか。

- A. 相互合意
- B. 災害復旧テスト結果
- C. 復旧時間目標 (RTO)
- D. データ保持要件

**Answer: C**

Explanation:

The most important consideration when determining which type of failover site to employ is the recovery time objectives (RTOs). A failover site is a backup site that can be used to restore the functionality and operations of an organization's primary site in the event of a disaster or disruption. There are different types of failover sites, such as hot sites, warm sites, and cold sites, that vary in terms of availability, cost, and complexity. A recovery time objective (RTO) is a metric that defines the maximum acceptable amount of time that an organization can tolerate to restore a system or an application after a disaster or disruption. By determining the RTOs for each system or application, the organization can choose the most suitable type of failover site that can meet its recovery needs and expectations. For example, if the RTO for a critical system is very low, the organization may opt for a hot site that can provide immediate failover and minimal downtime. However, if the RTO for a non-critical system is high, the organization may choose a cold site that requires manual setup and activation, but has lower cost and maintenance. The other options are not the most important consideration when determining which type of failover site to employ, although they may be some factors or constraints that affect the decision. Reciprocal agreements are arrangements between two or more organizations that agree to provide backup facilities or resources to each other in case of a disaster or disruption. Reciprocal agreements can help reduce the cost and complexity of setting up and maintaining a failover site, but they may not guarantee the availability or compatibility of the backup facilities or resources.

Disaster recovery test results are outcomes of testing and validating the functionality and performance of a failover site. Disaster recovery test results can help evaluate and improve the effectiveness and efficiency of a failover site, but they do not determine which type of failover site to employ. Data retention requirements are policies and regulations that define how long and in what format an organization must store its data. Data retention requirements can affect the design and configuration of a failover site, but they do not dictate which type of failover site to employ

**QUESTION NO: 27**

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****Answer:** D

Explanation:

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).

**QUESTION NO: 28**

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。

**Answer:** D

Explanation:

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

**QUESTION NO: 29**

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。

**Answer: B**

Explanation:

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.

**QUESTION NO: 30**

従業員の意図しない行動により、重大なデータ損失インシデントが発生しました。情報セキュリティ

マネージャーが組織内での再発を防止するための最善の方法は次のうちどれですか。

- A. 補正制御を実装します。
- B. 将来のインスタンスへの影響を伝えます。
- C. データ損失防止 (DLP) ソリューションを強化します。
- D. セキュリティ意識向上トレーニング プログラムを改善します。

**Answer: D**

**QUESTION NO: 31**

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。

**Answer: A**

Explanation:

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

#### **QUESTION NO: 32**

情報資産分類の主な目的は次のどれですか？

- A. 脆弱性の軽減
- B. コンプライアンス管理
- C. リスク管理
- D. 脅威の最小化

**Answer: C**

Explanation:

The primary objective of information asset classification is C. Risk management. This is because information asset classification is a process of assigning labels or categories to information assets based on their value, sensitivity, and criticality to the organization.

Information asset classification helps the organization to identify, assess, and treat the risks associated with the information assets, and to apply the appropriate level of protection and controls to them. Information asset classification also helps the organization to comply with the legal, regulatory, and contractual obligations regarding the information assets, and to optimize the use of resources and costs for information security.

Information asset classification is a process of assigning labels or categories to information assets based on their value, sensitivity, and criticality to the organization. Information asset classification helps the organization to identify, assess, and treat the risks associated with the information assets, and to apply the appropriate level of protection and controls to them.

(From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 2, Section 2.2.1, page 751; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 7, page 3; Certified Information Security Manager Exam Prep Guide - Packt Subscription2

#### **QUESTION NO: 33**

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。

**Answer: C**

Explanation:

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

#### QUESTION NO: 34

効果的な災害復旧計画プロセスを示す最良の指標は次のどれですか？

- A. 宣言された災害にはホットサイトが必要です。
- B. 災害復旧プロセス全体を通じて保管チェーンが維持されます。
- C. 各イベントの後に事後レビューが行われます。
- D. 復旧時間目標 (RTO) は復旧ポイント目標 (RPO) よりも短くなります。

**Answer: C**

#### QUESTION NO: 35

組織の情報セキュリティ

プログラムを効果的にするために、導入することが最も重要なのは次のうちどれですか。

- A. 文書化された情報セキュリティプロセス
- B. 包括的なIT戦略
- C. 上級管理職のサポート
- D. 定義され割り当てられた予算

**Answer: C**

Explanation:

Senior management support is the most important factor to have in place for an organization's information security program to be effective because it helps to establish the vision, direction, and goals of the program, as well as to allocate the necessary resources and authority to implement and maintain it. Senior management support also helps to foster a security culture within the organization, where security is seen as a shared responsibility and a business enabler. Senior management support also helps to ensure compliance with internal and external security policies and standards, as well as to communicate the value and impact of security to stakeholders. Therefore, senior management support is the correct answer.

References:

<https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance->

indicators-for-security- governance-part-1

[https://www.ffiec.gov/press/PDF/FFIEC\\_IT\\_Handbook\\_Information\\_Security\\_Booklet.pdf](https://www.ffiec.gov/press/PDF/FFIEC_IT_Handbook_Information_Security_Booklet.pdf)

[https://www.cdse.edu/Portals/124/Documents/student-guides/IF011-guide.pdf?](https://www.cdse.edu/Portals/124/Documents/student-guides/IF011-guide.pdf?ver=UA7IDZRN_y066rLB8oAW_w%3d%3d)

[ver=UA7IDZRN\\_y066rLB8oAW\\_w%3d%3d](https://www.cdse.edu/Portals/124/Documents/student-guides/IF011-guide.pdf?ver=UA7IDZRN_y066rLB8oAW_w%3d%3d)