ISACA.CISM-JPN.v2026-09-24.q591

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：	591
バージョン：	v2026-09-24
ページの閲覧量：	128
問題集の閲覧量：	9885

https://www.jpnshiken.com/shiken/ISACA.CISM-JPN.v2026-09-24.q591.html

質問: **1**
重要なセキュリティパッチの適用を遅らせる最も適切な理由は次のうちどれですか？
A. 脆弱性管理の不足
B. 資源の制約
C. 技術の相互依存関係
D. ソフトウェア開発ライフサイクルとの矛盾
正解: **C (コメントを発表する)**
The best reason to delay a critical patch is technology interdependencies, where applying the patch could break compatibility or availability of interconnected systems; this risk must be evaluated and managed (e.g., testing, staged rollout, compensating controls) before deployment.

質問: **2**
ビジネスインパクト分析(BIA)を実施する最適な時期は次のとおりです。
A. 事業継続計画(BCP)をテストする場合。
B. 企業文化の変化について。
C. 経営方針の変更に伴い。
D. 災害復旧テストを実施する際。
正解: **(正解を表示します)**
A business impact analysis should be conducted when there are changes in management direction because strategic shifts can alter business priorities, critical processes, and risk tolerance. Since the BIA aligns recovery objectives with business priorities, it must reflect current organizational strategy and direction.

質問: **3**
セキュリティ手順を文書化しておくべき最も重要な理由は次のうちどれですか？
A. 政策要件の実施を指導する
B. 情報セキュリティ指標の報告プロセスを円滑化するため
C. 標準作業手順に関する規制要件を満たすため
D. ビジネスセキュリティ目標との整合性を示すため
正解: **(正解を表示します)**

Documented security procedures translate high-level policy requirements into specific, repeatable steps so controls are implemented consistently and correctly across the organization.

質問: **4**
次のうち、発生しつつある事態を示す最も適切な指標はどれですか？
A. 組織の情報システム内で発見された弱点
B. システムへのパッチ適用を試みた結果、エラーが発生した。
C. ウェブサイトが利用できないことに関する顧客からの苦情
D. 業界の競合他社で最近発生したセキュリティインシデント
正解: **C (**コメントを発表する**)**
https://www.techtarget.com/searchcio/definition/key-risk-indicator-KRI

質問: **5**
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業務データの一部を公開したことを確認しました。次に取るべき行動は次のうちどれですか？
A. クラウドプロバイダーのサービスレベル契約(SLA)を確認してください。
B. インシデント対応計画を発動する。
C. 組織のデータ損失防止(DLP)プロセスを開始します。
D. 漏洩したデータに関連するユーザーを特定します。
正解: **(**正解を表示します**)**
The next step should be to invoke the incident response plan. This ensures that a coordinated, structured approach is taken to contain the breach, assess its impact, and mitigate any further exposure of sensitive data. The plan will guide the organization through the process of managing the incident effectively.

質問: **6**
組織の戦略目標は、新たな国際市場への進出によって市場シェアを拡大することです。以下のうち、セキュリティ戦略がこの目標と整合していることを最もよく示しているのはどれですか？
A. セキュリティ意識向上プログラムは、新たな市場の言語に翻訳されました。
B. セキュリティプログラムには、新たな国際市場に特化したリスク評価が含まれています。
C. 組織は、国際事業における潜在的な損失をカバーするためにサイバー保険に加入しました。
D. セキュリティチームは、マーケティングアプリケーションへのアクセスに多要素認証(MFA)を導入しました。
正解: **B (**コメントを発表する**)**
Security strategy is aligned with business strategy when it supports the organization's specific objectives and risk environment. Expanding internationally introduces new regulatory, geopolitical, operational, privacy, and third-party risks, so market-specific risk assessments best show alignment.

質問: **7**
組織のネットワークへの不正なデバイスアクセスを防止するための最適な対策は、次のうちどれですか？
A. ステートフルインスペクションファイアウォールをインストールして、不正なネットワークトラフィックを防止します。

B. ネットワークレベルの認証とログインを実装して、デバイスのネットワークへのアクセスを制御します。
C. 自動資産インベントリ検出ツールからのログのレビュースケジュールを確立する。
D. ネットワークに接続されているすべてのシステムのネットワークアドレスとハードウェアアドレスのインベントリを保持します。
正解: **(**正解を表示します**)**
The best control for preventing unauthorized device access to an organization's network is to implement network-level authentication and login to regulate access of devices to the network.
This ensures that only authorized devices can access the network by verifying their credentials before allowing them to connect.

質問: **8**
インシデント対応計画を策定する際、組織内でよく発生するインシデントが適切に処理されることを確実にするための最も効果的な方法は次のうちどれですか？
A. インシデント対応計画をリスクフレームワークに整合させる
B. インシデント対応リーダーの指名
C. 意識向上トレーニングの実施
D. 対応シナリオのリハーサル
正解: **(**正解を表示します**)**
Rehearsing response scenarios ensures the incident response team is prepared to handle incidents specific to the organization effectively by practicing roles, validating procedures, and identifying gaps in the plan.

質問: **9**
組織のインシデント対応能力を評価する上で、最も費用対効果の高い方法は次のうちどれですか？
A. 侵入テスト
B. テーブルトップエクササイズ
C. 第三者評価
D. 上級管理職面接
正解: **(**正解を表示します**)**
The most cost-effective method for assessing an organization's incident response capabilities is a tabletop exercise. Tabletop exercises simulate a security incident in a controlled, discussion- based environment, allowing the incident response team to review and practice their procedures without the need for full-scale simulations or external assessments.

質問: **10**
インシデント発生後のレビューにおいて、インシデント対応チームの改善点を特定するための最適なデータソースは次のうちどれでしょうか？
A. 事件発生時に作成された文書
B. 関係するシステムからのログ
C. 対応チームメンバーへのインタビュー
D. イベントの総合タイムライン

正解: (正解を表示します)
During a post-incident review, the best data source for identifying improvements to the incident team response would be interviews with response team members. These interviews can provide insights into the team's experiences, challenges faced during the incident, and suggestions for process improvements from those directly involved in the response.
While documents created during the incident, logs from systems involved, and a consolidated event timeline are all valuable sources of information, interviews can capture qualitative feedback and detailed perspectives that are essential for improving the incident response process.

質問: **11**
侵入テストの主な目的は以下のとおりです。
A. 監査基準を遵守する。
B. ネットワーク容量を決定する。
C. ファイアウォールの設定を検証します。
D. ある時点での脆弱性を特定する。
正解: (正解を表示します)
The primary purpose of a penetration test is to identify exploitable vulnerabilities in systems, applications, or networks at a specific point in time. It simulates real-world attack techniques to determine whether weaknesses exist and can be successfully exploited, providing a snapshot of the organization's security posture.

質問: **12**
インシデント後の検証により、主要な関係者がセキュリティ侵害発生後にアプリケーションを停止すべきかどうかを決定するのに、許容範囲を超える時間を要していたことが明らかになりました。この問題を解決するために、経営陣が取るべき最善の行動は次のうちどれでしょうか？
A. 封じ込め手順を確立する。
B. エスカレーション手順を確認する。
C. インシデント対応分類を更新します。
D. 頻繁なインシデント対応訓練を義務付ける。
正解: (正解を表示します)
The best course of action is to review and improve the escalation procedures. This will ensure that there is a clear, predefined process for quickly escalating incidents to the appropriate stakeholders, enabling faster decision-making during critical situations like a security breach.
Proper escalation procedures ensure that the right individuals are notified and involved at the right time, improving the organization's ability to respond promptly to security incidents. While containment procedures, updated classifications, and training are important, the primary issue in this case is the delay in decision-making, which can be best addressed by reviewing escalation procedures.

質問: **13**
ランサムウェア攻撃を発見した場合、最初に行うべきことは次のうちどれですか？
A. 不変バックアップを使用する

B. システムに対してヒューリスティックスキャンを実行する
C. 送信元トラフィックをブロックする
D. 影響を受けたシステムを隔離します。
正解: **(**正解を表示します**)**
The first priority in a ransomware attack is containment. Isolating the affected system helps stop encryption from spreading to shared drives, other endpoints, and critical systems.

質問: **14**
組織がセキュリティインシデントを適切にエスカレーションするために、以下のうちどれが重要ですか？
A. 事業継続計画および復旧計画
B. セキュリティインシデントログ履歴
C. 災害復旧宣言手続き
D. インシデントの分類およびカテゴリ分けプロセス
正解: **D (**コメントを発表する**)**
Proper incident classification and categorization are critical for ensuring that security incidents are escalated appropriately based on their severity and impact. A well-defined classification framework helps determine response priorities, escalation paths, and necessary actions. While business continuity plans, incident logs, and disaster recovery procedures are important, they do not directly drive the escalation process as effectively as classification and categorization.

質問: **15**
インシデントの深刻度を判断する上で最も重要な情報は、組織の以下の情報から得られます。
A. 事業継続方針
B. コンプライアンス要件。
C. リスク評価結果。
D. リスク許容度。
正解: **C (**コメントを発表する**)**
The most important input for determining the severity of an incident is the organization's risk evaluation results. These results assess the potential impact of the incident on business operations, assets, and data, helping to prioritize the incident and guide the response accordingly.

質問: **16**
情報セキュリティマネージャーが経営陣から戦略的な支援を得るために、最も役立つのは次のうちどれでしょうか？
A. 情報セキュリティ成熟度モデル
B. 組織内におけるセキュリティインシデントの年次報告書
C. 世界的な情報セキュリティ侵害の動向に関する調査
D. 組織固有のリスク分析
正解: **D (**コメントを発表する**)**

A risk analysis tailored to the organization demonstrates the actual business impact and relevance of information security, helping executive management understand and support security initiatives strategically.

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 を**1193**問、３０%ディスカウント、特別な割引コード:**JPNshiken**」

質問: **17**
個人所有のモバイルデバイスを企業のメールシステムに接続する際に、最も効果的なデータ損失防止策は次のうちどれですか？
A. メールはモバイルデバイスに暗号化された形式で保存する必要があります。
B. ユーザーは生体認証による多要素認証(MFA)の使用に同意する必要があります。
C. 公衆Wi-Fiホットスポットに接続している場合は、メールの同期を防止する必要があります。
D. 各新規接続は上級管理者の承認が必要です。
正解: **(**正解を表示します**)**

質問: **18**
情報セキュリティ管理者は、組織全体でフィッシングシミュレーションを実施したいと考えています。情報セキュリティプログラムにとって、次のうちどれが最大のメリットでしょうか？
A. 従業員がフィッシングメールをクリックした場合に、管理者が措置を講じることを可能にします。
B. 従業員のサイバー意識とトレーニングニーズを継続的に評価できます。
C. 従業員の行動の記録と分析を容易にします。
D. 従業員が実際のフィッシング攻撃とシミュレーションを区別するのに役立ちます。
正解: **(**正解を表示します**)**
The greatest benefit of phishing simulations is their ability to continuously assess employee awareness and identify training needs to strengthen the organization's security posture. By analyzing employee responses, security teams can tailor awareness programs to improve detection and prevention of phishing attacks. While documentation, distinguishing real from simulated attacks, and management actions may have some value, the primary purpose is to enhance security awareness and training effectiveness.

質問: **19**
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. 復旧時間目標（RTO）
B. 保管手順
C. ステークホルダーコミュニケーション計画
D. 平均応答時間（MTTR）

正解: **(**正解を表示します**)**
Developing a stakeholder communication plan is a key preparation activity, ensuring roles, channels, and messaging are defined before an incident occurs so that information flows promptly and appropriately.

質問: **20**
最近発生した高度な持続的脅威(APT)攻撃は情報セキュリティチームによって無事対処 -封じ込められましたが、経営陣は依然として懸念を抱いています。これらの対策のうち、どれが最も確実な安心感をもたらすでしょうか？
A. 外部監査を実施し、セキュリティ体制が基準を満たしていることを確認する。
B. 攻撃からの復旧時間を短縮するために、インシデント対応計画を改訂する。
C. フォレンジックチームを投入し、攻撃が軽減されたことを確認する。
D. リスク評価を実施し、全体的なリスクが許容範囲内であることを確認します。
正解: **D (**コメントを発表する**)**
Senior management's primary concern is whether the organization's overall risk exposure remains acceptable after the APT incident. Performing a risk assessment provides assurance that residual risk is identified, evaluated, and confirmed to be within the organization's defined risk tolerance, directly addressing governance-level concerns.

質問: **21**
新任の情報セキュリティマネージャーは、組織が問題解決に短期的な解決策を用いる傾向があることに気づきました。リソースの配分と支出は効果的に追跡されておらず、コンプライアンス要件が満たされているという保証もありません。このようなボトムアップ型のセキュリティアプローチを是正するために、まず最初に何をすべきでしょうか？
A. 監査委員会を設置する。
B. 情報セキュリティ運営委員会を設置する。
C. 情報セキュリティ意識向上トレーニングプログラムを実施する。
D. 脅威分析を実施する。
正解: **(**正解を表示します**)**

質問: **22**
大規模な攻撃を受けた後、顧客への影響を最小限に抑えつつサービスを復旧させる上で、組織にとって最も重要な要素は次のうちどれでしょうか？
A. 事業影響分析(BIA)
B. 災害復旧計画(DRP)
C. インシデント管理ツール
D. 脅威インテリジェンス機能
正解: **B (**コメントを発表する**)**
Disaster recovery planning (DRP) defines the procedures, resources, roles, and technical steps required to restore systems and services after a major disruption. While a BIA determines priorities, it is the DRP that enables actual restoration of services with minimal customer impact.

質問: **23**

セキュリティレビューの結果、ファイルサーバー上の機密情報が組織内の権限のないユーザーによってアクセスされたことが判明しました。情報セキュリティマネージャーは、まず次のうちどれを行うべきでしょうか？
A. ファイルサーバーから情報を削除します。
B. ロールベースアクセス制御(RBAC)を実装する。
C. 情報へのアクセスを削除します。
D. インシデント対応計画を発動する。
正解: **(**正解を表示します**)**
The first action should be to invoke the incident response plan to ensure a structured approach to contain, investigate, and remediate the breach while preserving evidence and minimizing impact.

質問: **24**
情報セキュリティリスクを経営陣に提示する最も効果的な方法は、以下の点を強調することです。
A. ビジネスへの影響。
B. 対策。
C. 脅威インテリジェンス。
D. 時間の経過に伴うリスク軽減。
正解: **A (**コメントを発表する**)**
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/communicating-information-security-risk-simply-and-effectively-part-1

質問: **25**
インターネットに接続するアプリケーションに対してアプリケーションセキュリティテストと侵入テストを実施する主な理由は以下のとおりです。
A. アプリケーションが外部からの攻撃に対して脆弱でないことを確認する
B. アプリケーション内の実行時脆弱性を検出する
C. Webアプリケーションファイアウォール(WAF)の設定を決定する
D. インシデント対応チームの有効性をテストする
正解: **(**正解を表示します**)**
The primary reason for conducting security and penetration testing on internet-facing applications is to verify that they are resilient against external attacks, reducing the risk of exploitation by threat actors.

質問: **26**
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. テストとトレーニングにすべての関係者を参加させる
B. 定期的な内部監査と外部監査のスケジュール設定
C. 計画の見直しに取締役会と上級管理職を参加させる
D. 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
正解: **(**正解を表示します**)**

The process that is most important for the success of a business continuity plan (BCP) is involving all stakeholders in testing and training. This ensures that everyone understands their roles and responsibilities in the event of a disruption and helps identify any gaps or weaknesses in the plan through practical exercises.
While audits, plan reviews with senior management, and maintaining copies of the plan are important, regular testing and training with stakeholder involvement are crucial for ensuring that the BCP is effective and can be executed smoothly when needed.

質問: **27**
情報セキュリティ管理者が法的および規制上のコンプライアンス要件を理解する上で最も重要な理由は、次のうちどれですか？
A. コンプライアンス部門はIT関連のコンプライアンス問題を理解していない可能性があります
B. グローバルな情報セキュリティ基準では、コンプライアンス要件を考慮する必要があります。
C. コンプライアンス要件はセキュリティ戦略に制約を課す可能性がある
D. 不遵守に伴う金銭的制裁のリスクは、他の種類のリスクよりも高い。
正解: **C (**コメントを発表する**)**
Understanding legal and regulatory compliance requirements is essential because they may directly influence or limit how the information security strategy is designed and implemented, ensuring alignment with mandatory obligations.

質問: **28**
情報セキュリティ戦略を策定する際に、情報セキュリティ管理者が考慮すべき最も重要な事項は次のうちどれですか？
A. 組織目標とリスク許容度
B. 組織のネットワークとインフラストラクチャ
C. 主要関係者の役割と責任
D. 組織の管轄区域内における規制上の制約
正解: **A (**コメントを発表する**)**
Aligning the information security strategy with organizational objectives and risk appetite ensures that security efforts support business goals while staying within acceptable levels of risk.

質問: **29**
組織の事業継続計画(BCP)の有効性を確保するために、以下のうちどれが最も重要ですか？
A. 計画における重要資源の文書化
B. 上級管理職による計画の承認
C. ITの観点からの計画の監査
D. 計画の定期的なテスト
正解: **(**正解を表示します**)**
Periodic testing of the business continuity plan (BCP) is most important to ensure its effectiveness. Testing identifies gaps, validates assumptions, and ensures that employees are familiar with their roles, thereby improving the plan's reliability during actual disruptions.

質問: **30**
ある組織が最近、事業継続計画(BCP)を発動しました。従業員には事案発生時に通知されましたが、一部の従業員はコミュニケーション計画を完全に遵守しませんでした。このような事態の再発を防ぐための最善策は何でしょうか？
A. 事業影響分析(BIA)を更新する
B. 適切な従業員とともに卓上テストを実施する。
C. 計画に従った従業員にインセンティブを与える
D. BCPにおける外部コミュニケーションに関する指示を強化する
正解: **B (**コメントを発表する**)**
Tabletop testing allows employees to practice their roles and understand the communication plan in a controlled environment, helping identify and correct gaps in understanding and execution to prevent future noncompliance.

質問: **31**
情報セキュリティ管理者は、以下のインシデント管理フェーズのうち、どのフェーズで、侵害に至る一連の出来事と、開始されたインシデント対応活動を評価しようとする可能性が最も高いでしょうか？
A. 事後検証段階
B. 事案封じ込め段階
C. インシデント対応フェーズ
D. インシデント特定フェーズ
正解: **(**正解を表示します**)**
The post-incident review phase focuses on analyzing the sequence of events that led to the breach and evaluating the effectiveness of the incident response activities, with the goal of identifying lessons learned and improving future incident handling.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu ↾**193**問、３０%ディスカウント、特別な割引コード**:** **JPNshiken**」

質問: **32**
最近の監査で、組織の新規ユーザーアカウントの設定が統一されていないことが判明しました。情報セキュリティマネージャーが確認すべき最も重要な項目は次のうちどれですか？
A. ガイドライン
B. 規格
C. セキュリティポリシー
D. 自動制御

正解: (正解を表示します)

質問: **33**
サービス拒否(DoS)攻撃が失敗に終わった場合、特定された脆弱性は以下のとおりであるべきです。
A. 同様の弱点が見つかった場合は、記録して後日再検討する。
B. 最終的な解決まで追跡および報告される
C. コストを気にせず迅速に解決 -排除する
D. セキュリティ意識向上プログラムで文書化されている
正解: (正解を表示します)
https://www.byos.io/blog/denial-of-service-attack-prevention

質問: **34**
最近ランサムウェア攻撃を受けた組織の監査を実施するIS監査担当者にとって、以下のうちどれが最も懸念すべき事項でしょうか？
A. バックアップはローカルネットワーク内でのみ実行されました。
B. 従業員はサイバーセキュリティに関する方針や手順について研修を受けていなかった。
C. アンチウイルスソフトウェアは適切にアップデートされていたにもかかわらず、攻撃を防ぐことができませんでした。
D. 最新のセキュリティパッチは、実装前にテストされていませんでした。
正解: (正解を表示します)
The greatest concern is that backups were only performed within the local network, because ransomware often encrypts local and network-connected backups, making data recovery impossible without paying the ransom. Effective backup strategies should include offline or offsite backups to ensure recoverability.

質問: **35**
以下の指標のうち、情報セキュリティプログラムの成熟度について最も的確な洞察を提供するものはどれですか？
A. 対処された脆弱性の数
B. 望ましい結果を達成したコントロールの数
C. 監査指摘事項の数
D. 情報セキュリティによって阻止された攻撃の数
正解: (正解を表示します)
Maturity is best reflected by how consistently and effectively security controls operate and achieve their intended outcomes. The number of controls achieving desired results indicates process effectiveness, repeatability, and optimization -- key characteristics of a mature information security program.

質問: **36**
組織のシステムに対するサイバー攻撃を可能にするバックドアが特定された。
組織が将来同様の攻撃を軽減するために、以下のうちどれをソフトウェア開発ライフサイクルに組み込むのが最も効果的でしょうか？
A. 職務分担

B. カスタマイズされた開発者トレーニング
C. 脆弱性テスト
D. 強化されたユーザー受け入れテスト(UAT)
正解: **(**正解を表示します**)**
Integrating vulnerability testing into the software development life cycle helps detect and remediate backdoors and other security weaknesses before deployment, reducing the risk of similar attacks.

質問: **37**
事業運営を脅かす事態への対処の有効性を最も適切に測定しているのは、次のうちどれですか？
A. 復旧時間目標(RTO)
B. 解決までの平均時間
C. リスク許容度
D. 最大許容ダウンタイム
正解: **B (**コメントを発表する**)**
The best measure of the effectiveness of handling incidents that threaten business operations is mean time to resolution. This metric reflects how quickly incidents are resolved, which directly impacts the continuity and resilience of business operations.

質問: **38**
組織がデータ侵害から身を守るために最も効果的な方法はどれですか？
A. 投資意欲の高い上級管理職
B. 堅牢な情報セキュリティ戦略
C. 明確かつ周知徹底されたセキュリティポリシー
D. 十分な訓練を受けた情報セキュリティ担当者
正解: **(**正解を表示します**)**
A robust information security strategy is the best way to protect an organization from data breaches, as it ensures a comprehensive, risk-based approach to security. This strategy integrates policies, controls, employee training, and governance to proactively mitigate threats.
While senior management support, clear policies, and well-trained staff are important, they are components of an overall strategy rather than standalone solutions.

質問: **39**
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うちどれですか？
A. インシデント管理コストを監視 ･管理する能力
B. 情報資産の効果的な保護
C. リカバリリソースの最適化された割り当て
D. 混乱の影響に対する可視性の向上
正解: **(**正解を表示します**)**
Incident classification criteria enable consistent severity assessment so the organization can prioritize response efforts and allocate the right recovery resources to the most critical incidents first.

質問: **40**
情報セキュリティプログラムを更新する際に、情報セキュリティマネージャーが最初にとるべきステップは何でしょうか？
A. 組織の事業上の期待と目標を再評価する。
B. 事業目標に合致しないプログラムコンポーネントを特定する。
C. コストを見直し、業界標準と比較してベンチマークを行う。
D. 事業部門のマネージャーと主要な関係者にインタビューを行う。
正解: **(**正解を表示します**)**
Updating an information security program should begin by re-evaluating the organization's business expectations and objectives, because the program must be aligned to current business direction before identifying misaligned components, benchmarking costs, or interviewing stakeholders.

質問: **41**
脆弱性スキャンによる本番ネットワークのパフォーマンス低下を組織が補償するための最良の方法は、次のうちどれですか？
A. 営業時間外に脆弱性スキャンを実施してください。
B. 営業時間外に予告なしの侵入テストを実施する。
C. ネットワークに送信される脆弱性スキャンパケットの範囲を制限します。
D. 脆弱性スキャンを中止し、リスクの高い領域にパッチを適用します。
正解: **A (**コメントを発表する**)**
Scheduling vulnerability scanning after business hours minimizes impact on production network performance while still maintaining the vulnerability management process.

質問: **42**
組織のITシステムへの侵害の可能性がプロジェクトマネージャーから報告されました。情報セキュリティマネージャーは、まず最初に次のうちどれを行うべきでしょうか？
A. システムログを調査してください。
B. ITシステムへのアクセスを無効にする。
C. ITシステムに対してポートスキャンを実行します。
D. 事件を確認してください。
正解: **(**正解を表示します**)**
The first step the information security manager should take is to confirm whether the reported breach is actually an incident. Once the incident is confirmed, appropriate containment, investigation, and remediation steps can be taken.

質問: **43**
第三者へのアクセス権付与について、最終的な承認権限は誰が持つべきか？
A. 情報セキュリティマネージャー
B. データ管理者

C. 契約管理者
D. データ所有者
正解: **(**正解を表示します**)**
The data owner is ultimately accountable for the information and is responsible for authorizing access to it, including approving third-party access rights.

質問: **44**
セキュリティインシデントのどの段階で、インシデント対応チームが最初に投入されるべきでしょうか？
A. 根絶
B. 識別
C. 回復
D. 準備
正解: **(**正解を表示します**)**
The incident response team is initially engaged during the identification phase, when a potential security event is detected and requires analysis to determine whether it constitutes an incident.
Early engagement ensures proper validation, classification, and escalation before containment and eradication activities begin.

質問: **45**
重大なセキュリティインシデント発生後、上級管理職に報告すべき最も重要な情報は次のうちどれですか？
A. 前期間に発生した類似攻撃の一覧
B. 影響と講じられた是正措置
C. 脆弱性スキャンおよび侵入テストの結果
D. 固有リスクレベルを更新
正解: **B (**コメントを発表する**)**
After a significant security incident, the most important information to report to senior management is the impact of the incident (e.g., financial, operational, reputational damage) and the corrective actions taken to mitigate future risks. This helps leadership make informed decisions, allocate resources, and improve security posture. While historical attacks, vulnerability assessments, and risk levels are relevant, they are secondary to understanding the incident's consequences and remediation efforts.

質問: **46**
情報セキュリティフレームワークを採用する主な利点は、以下の点です。
A. 標準化されたセキュリティ管理。
B. 一般的な利用可能性指標。
C. 信頼できる新興脅威情報。
D. セキュリティおよび脆弱性報告ガイドライン。
正解: **A (**コメントを発表する**)**
https://www.cybersaint.io/blog/benefits-of-nist-cybersecurity-framework

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu ⇑**193**問、３０%ディスカウント、特別な割引コード:**JPNshiken**」

質問: **47**
ある組織で、複数のワークステーションに不正な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。そのソフトウェアにはトロイの木馬が含まれており、未知の外部組織にデータをアップロードしていました。以下のうち、不正なソフトウェアのインストールを最も効果的に防ぐことができたのはどれでしょうか？
A. ローカル管理者権限の削除
B. 侵入検知システム(IDS)の導入
C. アプリケーションのインストール前に管理者の承認が必要
D. インターネットファイアウォールで実行可能ファイルのダウンロードを禁止する
正解: **(**正解を表示します**)**
Removing local administrator rights would have best prevented the installation of unauthorized software. This would limit the ability of users to install software without proper authorization, reducing the risk of Trojan and other malicious software being installed on workstations.

質問: **48**
リスク評価プロセスにおいて脅威の優先順位付けを行う際に、最も重要な考慮事項は次のうちどれですか？
A. 組織に対する規制要件
B. 悪用された脆弱性の深刻度
C. 業界における脅威の状況
D. 業務への潜在的な影響
正解: **(**正解を表示します**)**
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/evidence-based-prioritization-of-cybersecurity-threats

質問: **49**
以下のうち、組織が法的、規制的、および契約上の要件を遵守する能力を最も効果的に示すものはどれですか？
A. 自己評価(CSA)
B. 脆弱性スキャン
C. リスク評価
D. ギャップ分析
正解: **(**正解を表示します**)**

A gap analysis compares current practices and controls against required legal, regulatory, and contractual obligations to identify where the organization does not meet requirements, directly revealing compliance capability and deficiencies.

質問: **50**
セキュリティインシデントを記録する主な理由は次のうちどれですか？
A. 報告された事件の数を追跡するため
B. インシデント対応スタッフの訓練と育成
C. 分析と調査を可能にする
D. 上級幹部に情報を提供するため
正解: **(**正解を表示します**)**
Documenting a security incident primarily supports analysis and investigation by preserving facts, timelines, actions taken, and evidence needed to understand what happened and drive appropriate response and remediation.

質問: **51**
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: **C (**コメントを発表する**)**
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.

質問: **52**
ブロックチェーンフォレンジックは、主に以下の方法でブロックチェーン関連事件の調査を支援します。
A. 分散型金融プラットフォームの規制。
B. 取引の地理的位置を特定する。
C. 所有権確認のために非代替性トークン(NFT)を実装する。
D. 記録分析を通じて不正取引の追跡を支援する。
正解: **D (**コメントを発表する**)**
Blockchain is a public, permanent record of every transaction. Forensics leverages this transparency to follow the "money trail" from one wallet to another, even if the actors are pseudonymous.
Forensic tools analyze the timing, flow, and volume of transactions to link different addresses to a single entity, which is crucial for identifying hackers or money launderers.
During an incident investigation (such as a crypto-theft), record analysis provides the documented evidence needed to prove how the assets were moved and where they currently reside.

質問: **53**
機密データを処理する顧客サービス機能を外部委託する際に、最も重要な考慮事項は次のうちどれですか？
A. 署名済みの秘密保持契約書(NDA)を入手できる能力
B. ベンダーのデータ保持および廃棄ポリシー
C. ベンダーが情報を適切に保護する能力
D. 情報拡散に関する契約上の罰則
正解: **(**正解を表示します**)**
The most important consideration when outsourcing a customer service function that processes sensitive data is ensuring that the vendor can adequately protect the information. This includes assessing their security controls, practices, and policies to ensure that sensitive data is properly safeguarded against unauthorized access, breaches, or misuse. This is critical to ensuring compliance with privacy regulations and protecting the organization's reputation.

質問: **54**
ランサムウェアやマルウェア攻撃からユーザーが復旧するのに最も役立つのは、次のうちどれですか？
A. 頻繁なシステムバックアップ
B. エンドユーザー向け意識向上トレーニング
C. インシデント対応計画
D. 定期的なウイルス対策ソフトのアップデート
正解: **(**正解を表示します**)**
The best way to enable users to recover from ransomware or malware attacks is through frequent system backups. Regular backups ensure that, in the event of an attack, users can restore their systems and data to a point before the infection, minimizing data loss and downtime.

質問: **55**
セキュリティリスクに対する意識の高い文化を構築する上で、従業員に伝えるべき最も重要なことは次のうちどれですか？
A. 情報資産の価値を理解することは、リスク管理にとって非常に重要です。
B. 従業員の業績目標には、情報セキュリティ目標が含まれます。
C. 従業員のアクセス権限は、最小権限の原則に基づいて付与されるべきである。
D. セキュリティに関する責任は、すべての従業員にあります。
正解: **(**正解を表示します**)**
Emphasizing that security is everyone's responsibility instills a shared mindset and proactive behavior across the organization, which is the foundation of a risk-aware culture.

質問: **56**
組織のシステムへの侵入が成功したことを示す最も適切な指標は次のうちどれですか？
A. 利用可能な収納スペースの減少
B. ログイン失敗回数の増加

C. 不規則な申請件数の増加
D. 内部ネットワークトラフィックの減少
正解: **(**正解を表示します**)**
The best indicator of a successful intrusion into an organization's systems is an increase in the number of irregular application requests. Unusual or irregular requests to applications can signal that an attacker has gained access and is attempting to exploit the system or exfiltrate data.

質問: **57**
組織の情報セキュリティフレームワークに沿って新技術が確実に導入されるようにするために、情報セキュリティマネージャーが取るべき最も重要な行動は次のうちどれですか？
A. 新興技術に対する継続的なセキュリティ監視およびインシデント対応計画を策定する。
B. セキュリティに関する考慮事項を開発および展開のライフサイクルに統合する。
C. 新興技術はゼロトラストの原則に従って設計および展開されることを要求する。
D. 新興技術に合わせた包括的な侵入テストを実施する。
正解: **(**正解を表示します**)**
Integrating security considerations into the development and deployment life cycle ensures emerging technologies are evaluated, designed, and implemented in line with the organization's security framework from the start, rather than relying on monitoring or testing after deployment.

質問: **58**
インシデント検知能力が未熟な組織は、次のうちどれを最優先事項とすべきでしょうか？
A. ユーザー認知度の向上
B. 新しいファイアウォールのインストール
C. 侵入テストの実施
D. セキュリティポリシーの更新
正解: **(**正解を表示します**)**
For organizations with immature incident detection capabilities, the primary focus should be on improving user awareness. Human error is a common entry point for security incidents, and in the absence of mature detection mechanisms, informed and vigilant users serve as a crucial first line of defense. Educated users are more likely to recognize and report suspicious activities, helping compensate for weak detection controls.

質問: **59**
情報セキュリティプログラムは、新興技術の導入をどのようにすれば最も効果的に支援できるでしょうか？
A. 効果的なリスクガバナンスの提供
B. 新興技術ロードマップの策定
C. 管理評価の実施
D. 許容使用ポリシーの策定
正解: **(**正解を表示します**)**

Emerging technologies introduce new security, privacy, compliance, operational, and third-party risks. The information security program best supports adoption by providing risk governance- clear accountability, risk assessment, control expectations, approval processes, and ongoing oversight.

質問: **60**
設計段階で、カスタムアプリケーションのリスク評価が実施されました。アプリケーションが稼働開始した後、以下のどの状況でリスクの再評価が最も必要になる可能性が高いでしょうか？
A. アプリケーションサーバーにパッチが適用されます
B. 手続きが変更されます
C. 追加機能が提案されています
D. 警備員が交代します
正解: **C (**コメントを発表する**)**
Introducing new functions to the application can significantly alter its risk profile, making a risk reassessment necessary to address potential new threats or vulnerabilities.

質問: **61**
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: **A (**コメントを発表する**)**
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." Other methods like penetration tests or vulnerability assessments offer snapshots of technical weaknesses, but they lack strategic depth.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu ↾**193**問、３０%ディスカウント、特別な割引コード**:** **JPNshiken**」

質問: **62**
事業部門のマネージャーが組織に影響を与える可能性のある新興技術の導入を希望する場合、情報セキュリティマネージャーにとって最適な行動は次のうちどれでしょうか？

A. 脆弱性評価を実施する。
B. ベンダーのドキュメントを確認してください。
C. 脅威分析を実施する。
D. 事業影響分析(BIA)を実施する。
正解: **(**正解を表示します**)**
The best course of action is to conduct a threat analysis. This helps assess the risks associated with adopting the emerging technology, identifying potential vulnerabilities, threats, and impacts on the organization before proceeding with implementation. Understanding the threat landscape allows for better decision-making and risk mitigation.

質問: **63**
システムやアプリケーションに重要なパッチが適用されない原因として、最も可能性が高いのは次のうちどれですか？
A. 古い構成管理データベース(CMDB)
B. リリースおよび展開ポリシーの欠如
C. ハードウェアの損傷に関する報告が不十分
D. 管理監督の不備
正解: **(**正解を表示します**)**
An outdated configuration management database (CMDB) results in incomplete or inaccurate records of systems and applications in the environment. If assets are not properly identified or tracked, they may be excluded from patch management processes, leading to critical patches being missed.

質問: **64**
生体認証は、以下の用途に最適です。
A. 承認。
B. 監査。
C. 会計。
D. 認証。
正解: **(**正解を表示します**)**

質問: **65**
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."

質問: **66**
ある組織では、災害発生時に業務上重要なアプリケーションを30分以内に復旧させることを求めています。この要件を満たすために、事業継続計画(BCP)において定義すべき指標は次のうちどれでしょうか？
A. 最大許容ダウンタイム(MTD)
B. サービスレベル契約(SLA)
C. リカバリポイント目標(RPO)
D. 復旧時間目標(RTO)
正解: **(**正解を表示します**)**
The recovery time objective (RTO) specifies the maximum allowable time to restore a business process or application after a disruption. In this case, it ensures critical applications are recovered within the required 30-minute window.

質問: **67**
以下のうち、インシデントの分類に最も大きな影響を与えるのはどれでしょうか？
A. 監査要件
B. 事件を報告する個人または部署
C. 情報の価値
D. 類似事件の履歴
正解: **(**正解を表示します**)**
Incident categorization should be driven primarily by business impact, and the value/sensitivity of the affected information is a key determinant of impact and required response priority.

質問: **68**
DevSecOpsの文脈において、ソフトウェアリリース前に脆弱性を特定することを最も効果的に可能にするのは、次のうちどれでしょうか？
A. 安全なコーディング基準に従う
B. 統合テストの実施
C. 実行可能コードのテスト
D. コードレビューの自動化
正解: **(**正解を表示します**)**
Automating code review (e.g., static analysis in the CI/CD pipeline) identifies vulnerabilities early and continuously during development, enabling fixes before release and aligning with DevSecOps' "shift left" approach.

質問: **69**
組織が重要な業務プロセスにサードパーティのクラウドコンピューティングサービスを利用することを計画している場合、情報セキュリティマネージャーはまず何をすべきでしょうか？
A. ギャップ分析を実施します。

B. ビジネス要件を分析します。
C. ホストするデータを特定します。
D. リスク評価を実施する。
正解: **(**正解を表示します**)**
The first step is to perform a risk assessment to evaluate the potential risks associated with using the third-party cloud service for a critical business process. This ensures that security, compliance, and operational risks are identified and addressed before proceeding.

質問: **70**
情報セキュリティプログラムが成功する可能性が最も高いのは、以下の要素と密接に連携している場合です。
A. 業界で認められたフレームワーク。
B. 情報セキュリティのベストプラクティス。
C. 情報セキュリティ戦略。
D. ITリスク管理フレームワーク。
正解: **(**正解を表示します**)**
An information security program is best positioned for success when it is aligned with the information security strategy, because the strategy translates business objectives and risk priorities into a clear direction that the program executes through initiatives, controls, and governance.

質問: **71**
組織は顧客をサポートするために複雑なサプライチェーンに依存しています。サプライチェーンにおけるサイバーインシデントのリスクを管理するための最善の方法は次のうちどれですか？
A. 代替サプライチェーンベンダーを評価する。
B. 追加のサイバー保険に加入する。
C. 混乱のリスクを最小限に抑えるための緊急対策を策定する。
D. すべての上流プロバイダーとの契約が締結されていることを確認してください。
正解: **(**正解を表示します**)**
For a complex supply chain, the main concern is maintaining operations when a supplier cyber incident causes disruption. Contingency plans, alternate processes, backup suppliers, recovery procedures, and communication plans best reduce business impact.

質問: **72**
組織のリスク許容度とリスク耐性を決定する主な責任者は、次のうち誰ですか？
A. 情報セキュリティマネージャー
B. 最高リスク責任者(CRO)
C. プロセスオーナー
D. 上級管理職
正解: **(**正解を表示します**)**
Senior management is primarily responsible for determining the organization's risk appetite and tolerance, as these decisions must align with strategic objectives and overall business priorities.

質問: **73**
情報セキュリティプログラムの有効性を監視するための指標を選択する際、情報セキュリティマネージャーにとって最も重要なことは以下のとおりです。
A. プログラムの戦略目標を検討する。
B. 業界ベンチマークを活用する。
C. 組織の事業戦略を検討する。
D. プログラムのリスクと補償制御を特定する。
正解: **C (**コメントを発表する**)**
Aligning security metrics with the organization's business strategy ensures that the effectiveness of the information security program supports overall business goals and objectives.

質問: **74**
新しく任命された情報セキュリティ マネージャーに、組織の既存のセキュリティ体制を最もよく把握させるタスクは次のどれですか。
A. ポリシーと手順の見直し
B. リスク評価の実行
C. 経営者と従業員へのインタビュー
D. ビジネス影響分析 (BIA) の実行
正解: **(**正解を表示します**)**
Performing a risk assessment gives a holistic and objective understanding of the threats, vulnerabilities, and controls across the organization. It reveals actual risk exposures and the effectiveness of current controls, which directly reflect the organization's security posture.
"Risk assessments identify and evaluate risk and provide the basis for determining how those risks should be managed and mitigated."

質問: **75**
パブリッククラウド、BYOD(私物端末の業務利用)、リモートワークをサポートするサイバーセキュリティ戦略に組み込むべき最も重要な要素は次のうちどれですか？
A. DevSecOpsの原則
B. 政策承認要件
C. ゼロトラスト原則
D. 役割ベースアクセス制御(RBAC)の要件
正解: **C (**コメントを発表する**)**
The most important concept to integrate into a cybersecurity strategy that supports public cloud, bring your own device (BYOD), and remote work is Zero Trust principles. Zero Trust emphasizes never trusting any user or device by default, regardless of their location, and continuously verifying identity and security posture. This is particularly critical in environments where devices and users may not be within a traditional network perimeter.
Implementing Zero Trust helps mitigate risks associated with diverse access points and users, making it essential for modern cybersecurity strategies in increasingly distributed work environments.

質問: **76**
情報セキュリティ投資に関するビジネスケースを経営陣に提示する上で、最も効果的なのは次のうちどれでしょうか ？
A. 定量的リスク評価
B. ベンダー提供の投資収益率(ROI)
C. 業界ベンチマーク
D. 運用コストの計算
正解: **A (**コメントを発表する**)**
A quantitative risk assessment provides measurable financial impact and likelihood data, allowing risk exposure and expected loss to be expressed in monetary terms. Presenting quantified risk reduction enables senior management to make informed investment decisions based on objective business impact.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu **193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **77**
IT利用規約において最も重要な目的は次のうちどれですか？
A. 組織のリソースへの第三者のアクセスを管理する
B. 組織のリソースを活用する際の期待事項を文書化する
C. 事業部門を情報セキュリティポリシーに準拠させる
D. 従業員が情報セキュリティポリシーを理解していることを示すため
正解: **(**正解を表示します**)**
The most important objective of an IT acceptable use policy is to document clear expectations for how organizational resources, such as systems, networks, and data, should be used by employees. This ensures that employees understand acceptable behaviors and the consequences of non-compliance, helping to safeguard the organization's IT environment.

質問: **78**
以下のうち、インシデント管理チームが繰り返し発生するサイバーセキュリティインシデントの根本原因分析を行う上で、最も効果的なものはどれですか？
A. デジタルフォレンジックおよびインシデント対応ツール
B. SIEMソリューション
C. 自動化されたセキュリティインシデントワークフローおよびチケットシステム
D. エンドポイント向けAI駆動型自動封じ込めソリューション

正解: (正解を表示します)
Root cause analysis of recurrent incidents requires consistent incident records, timelines, categories, ownership, remediation actions, recurrence patterns, and closure notes. An incident workflow/ticketing system best enables trend analysis and identification of repeated underlying causes.

質問: **79**
情報セキュリティ管理者が、サードパーティのSaaS(Software as a Service)プロバイダーがプライバシー規制を遵守していないことを突き止めました。次のうち、最も適切な対応策はどれですか？
A. 不遵守の影響を判断する。
B. 請負業者に特定された問題を解決するよう依頼する。
C. 契約違反に対する罰則を有効にする。
D. 一時的な補償制御を実施する。
正解: (正解を表示します)
The best first course of action is to determine the business, legal, and regulatory impact of the provider's noncompliance. This establishes severity and urgency and drives the appropriate response (e.g., require remediation, apply contractual remedies, implement compensating controls, or exit the relationship).

質問: **80**
情報セキュリティ侵害が発生した後、以下のうち測定が最も難しいものはどれですか？
A. 代替策
B. 人件費
C. 規制上の制裁
D. 評判の低下
正解: (正解を表示します)
Reputational damage is the most difficult to measure after a security breach because it involves intangible impacts on customer trust, brand perception, and future business opportunities, which are not easily quantifiable.

質問: **81**
アプリケーションセキュリティ対策は、ソフトウェア開発ライフサイクルのどの段階で最初に検討されるべきでしょうか？
A. コードレビュー
B. ソフトウェア設計
C. 要件収集
D. ソフトウェアコード開発
正解: (正解を表示します)
Application security controls should be addressed first during the requirements gathering stage of the software development life cycle (SDLC). This ensures that security is integrated from the beginning, allowing for the identification of security requirements, compliance needs, and risk considerations before design and development begin. Addressing security early helps reduce vulnerabilities and costly fixes later in the development process. While design, coding, and reviews are important, security should be a foundational requirement from the start.

質問: **82**
以下の者の中で、不正行為を防止するためのセキュリティ管理の責任を担うのに最も適任なのは誰ですか？
A. 内部監査
B. 情報所有者
C. プロセスオーナー
D. 情報セキュリティマネージャー
正解: **(**正解を表示します**)**
The process owner is best positioned to assume ownership of a security control to prevent fraudulent activity because they are responsible for the day-to-day operations and management of business processes. They understand how the process functions, where vulnerabilities may exist, and how controls can be effectively implemented without disrupting business operations.
While internal audit, information owners, and security managers play supporting roles, the process owner is directly responsible for operational integrity and fraud prevention.

質問: **83**
災害復旧計画(DRP)が策定された後、以下のどのタスクを実行すべきでしょうか？
A. 対応チームの役割を定義する。
B. 事業への影響を分析する。
C. テスト計画を作成する。
D. 復旧時間目標(RTO)を特定する。
正解: **(**正解を表示します**)**
After a disaster recovery plan is developed, the next key task is to develop the test plan to validate the DRP works as intended; BIAs, RTOs, and role definitions are inputs that should be established prior to or during DRP development.

質問: **84**
組織が機密性の高いシステムをパブリッククラウドサービスに移行する際に、最も懸念されるのは次のうちどれですか？
A. ログ記録機能の欠如
B. 認証が弱い
C. データ分離が不十分です
D. ユーザーの知識不足
正解: **(**正解を表示します**)**
In a public cloud, sensitive systems share underlying infrastructure with other tenants. The greatest concern is insufficient data separation (multi-tenancy isolation failure), which could lead to unauthorized access or leakage across tenants.

質問: **85**

情報セキュリティマネージャーは、最近明らかになった脅威に対処するため、新たなセキュリティ対策への投資を推奨しています。事業計画書に含めるべき最も重要な項目は次のうちどれですか？
A. 予想されるリスク軽減
B. 資源の入手可能性
C. 脅威インテリジェンスレポート
D. IT戦略との整合性
正解: **(**正解を表示します**)**
The most important element of a security investment business case is demonstrating how the initiative will reduce organizational risk. Senior management makes funding decisions based on risk reduction and business impact, so clearly quantifying anticipated risk reduction provides the strongest justification.

質問: **86**
組織のクラウドサービスプロバイダーが情報セキュリティリスクを適切に管理していることを最も確実に保証できるのは、次のうちどれでしょうか？
A. プロバイダーに対し、業界標準のクラウドセキュリティリスク自己評価を実施するよう求める。
B. サービス契約において、セキュリティ管理に関する監査権条項にプロバイダーが同意することを要求します。
C. ベンダーおよび製品サービス提供に関する文書の形で、セキュリティの証拠を提示するようプロバイダーに要求する。
D. プロバイダーに対し、セキュリティ管理の有効性について定期的に独立したテストを実施し、その結果を共有することを義務付ける。
正解: **(**正解を表示します**)**
The greatest assurance comes from independent validation of the provider's security controls.
Regular third-party testing and shared results give objective evidence that controls are operating effectively.

質問: **87**
組織が特定された脆弱性に対してパッチを適用することが現実的でない場合、次のうちどれが最適な導入手段でしょうか？
A. ホストベースファイアウォール
B. ホストベースの欺瞞ツール
C. ホストベースの侵入検知システム(IDS)
D. ホスト型侵入防御システム(IPS)
正解: **D (**コメントを発表する**)**
If patches cannot be applied, the organization needs a compensating control that can actively block exploitation attempts on the vulnerable host. A host-based IPS can detect and prevent malicious activity before it compromises the system.

質問: **88**
組織文化をセキュリティガイドラインに沿わせるための最も効果的な方法は、次のうちどれですか？
A. 規制要件を遵守する
B. セキュリティ意識向上プログラムを実施する

C. セキュリティ手順書を作成し配布する
D. セキュリティポリシーを伝達し、実施する
正解: **(**正解を表示します**)**
The most effective way to influence organizational culture is by clearly communicating and consistently enforcing security policies, which sets expectations, drives behavior, and embeds security into the organization's values and operations.

質問: **89**
以下のうち、業務を中断することなく災害復旧テストを最も効果的に実施できるのはどれですか？
A. 並列テスト
B. シミュレーションテスト
C. 構造化されたウォークスルー
D. 完全中断テスト
正解: **(**正解を表示します**)**
Parallel testing runs recovery systems and procedures alongside production without switching over from the live environment, allowing disaster recovery testing to be performed without interrupting business operations.

質問: **90**
ある組織は、さまざまなサービスプロバイダーと契約を結んでいます。限られたリソースの中で、各サービスプロバイダーが適切なリスク評価を受けられるようにするための最善の方法は、次のうちどれでしょうか？
A. 各サービス提供者に対する独立した評価の検討
B. 各サービスプロバイダーの相対的なリスクに基づいてデューデリジェンスを実施する
C. プロセスオーナーがサービスプロバイダーのリスク評価を独自に実施できるようにする
D. 各サービス提供者に自己評価の実施を義務付ける
正解: **(**正解を表示します**)**
Given limited resources, the most effective approach is to prioritize risk assessments based on the level of risk each service provider poses to the organization. High-risk providers (e.g., those handling sensitive data or critical operations) should receive more thorough evaluations, while lower-risk providers may undergo lighter assessments. This ensures that resources are allocated efficiently while maintaining appropriate security oversight.

質問: **91**
ソーシャルメディアポリシーに含めるべき最も重要な項目は次のうちどれですか？
A. ソーシャルメディアアカウントのプライバシー設定に関する推奨事項
B. ソーシャルメディアに関する義務研修の要件
C. 従業員によるソーシャルメディアの適切な利用
D. 従業員のソーシャルメディアアカウントの監視権限
正解: **C (**コメントを発表する**)**
The most important aspect to include in a social media policy is the acceptable use of social media by employees. This ensures that employees understand the boundaries of their online behavior, particularly when it comes to

representing the organization, protecting sensitive information, and avoiding actions that could harm the organization's reputation or security.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu ¶**193**問、３０%ディスカウント、特別な割引コード**:** **JPNshiken**」

質問**: 92**
標準的なセキュリティ構成を導入する主な目的は何ですか？
A. サポート対象外のシステムに対する潜在的なリスクを軽減するために、柔軟なアプローチを維持する。
B. サポート対象システムとサポート対象外システムの構成を比較します。
C. サポート対象外システムの管理および監視に伴う運用上の負担を最小限に抑える。
D. 脆弱性を制御し、構成変更による脅威を軽減します。
正解**: (**正解を表示します**)**

質問**: 93**
情報セキュリティインシデントを分類することによる最大のメリットは次のうちどれですか？
A. レポート機能
B. 保管管理体制の改善
C. 優先復旧
D. 包括的なドキュメント
正解**: C (**コメントを発表する**)**
Classifying information security incidents enables organizations to prioritize recovery efforts based on the severity and impact of each incident, ensuring critical issues are addressed promptly.

質問**: 94**
疑わしいインシデントを検出した後、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. 検出プロセスとツールの感度をレビューします。
B. 事業継続計画(BCP)を発動する。
C. 疑わしい事案についてトリアージを実施する。
D. 疑わしい事案を管理部門に報告してください。
正解**: (**正解を表示します**)**
After detecting a suspected incident, the next step is triage to validate the event, assess scope and severity, and prioritize response actions before escalating or invoking continuity plans.

質問: **95**
最近サイバー攻撃を受けた組織が、法執行機関への通報を検討している。インシデント対応チームにとって、以下のうち最も重要な行動はどれか？
A. デジタル証拠を暗号化する。
B. 上級管理職から意見を求める。
C. 弁護士に相談する。
D. 証拠分析のためにデジタルフォレンジックの専門家を雇う。
正解: **C (**コメントを発表する**)**
Engaging legal counsel first ensures that actions taken during the incident-especially involving law enforcement-comply with legal and regulatory requirements. Legal counsel provides guidance on evidence handling, jurisdictional issues, and communication, helping preserve admissibility and protect the organization from legal risk.

質問: **96**
プライバシー影響評価を実施する最も重要な理由は次のうちどれですか？
A. 重要な情報資産に対する補償管理策が確実に実施されるようにする
B. 上級管理職に安心感を与えるため
C. ビジネスデータ処理に伴う脅威を軽減するため
D. 業務データ処理のリスク評価が適切に行われていることを確認する
正解: **D (**コメントを発表する**)**

質問: **97**
AI関連のセキュリティインシデントに対応する際に、最も適切な初期対応手順は次のうちどれですか？
A. AIシステムからすべてのデータを削除します。
B. AIシステムを隔離する。
C. AIシステムを新しいデータで更新します。
D. AIシステムを停止します。
正解: **(**正解を表示します**)**
The initial response to an AI-related security incident should focus on containment. Isolating the AI system helps prevent further unauthorized access, data leakage, model misuse, or spread to connected systems while preserving evidence for investigation.

質問: **98**
グローバル企業がインシデント対応計画を策定しています。すべての事業部門において一貫性のある効果的なインシデント対応を確保するために、最も重要な考慮事項は次のうちどれですか？
A. 対応戦略の機密性を維持するため、地域チームなしで年次机上演習を実施する。
B. すべてのセキュリティインシデントに対応し、修復するためのインシデント対応チームを設置する
C. 全地域に適用される、事件分類のための標準化された基準の開発
D. 各地域事務所に対し、地域の規制や脅威状況を反映した独自の計画を維持することを義務付ける。
正解: **(**正解を表示します**)**

A global incident response plan needs consistent incident classification, severity levels, escalation triggers, and response priorities across all business units. Standardized criteria ensure incidents are handled uniformly, regardless of region.

質問: **99**
ある医療関連企業が、パブリッククラウド環境で開発・ホストされているAIアルゴリズムを用いて患者の健康記録をスキャンしています。情報セキュリティマネージャーが考慮すべき主要なリスク領域は次のうちどれでしょうか？
A. データ冗長性
B. データ復旧
C. データプライバシー
D. データ利用可能性
正解: **(**正解を表示します**)**
Patient health records contain highly sensitive personal and regulated information. When processed by AI in a public cloud environment, the primary concern is protecting confidentiality and ensuring compliance with privacy regulations, making data privacy the foremost risk area.

質問: **100**
新興技術に関連するセキュリティリスクを軽減する際に、最も重点的に取り組むべき分野は次のうちどれでしょうか？
A. 既存システムとの互換性
B. 変更管理統制
C. 企業強化基準の適用
D. 潜在的な脆弱性
正解: **(**正解を表示します**)**
The primary area of focus when mitigating security risks related to emerging technologies is identifying and addressing their potential vulnerabilities. Emerging technologies often introduce unknown or untested risks, so proactively analyzing and mitigating these weaknesses is essential to maintain a secure environment.

質問: **101**
侵入防御システム(IPS)は、過去1か月間でハッキング試行件数が大幅に増加したと報告したが、実際にシステムが侵害された事例はない。情報セキュリティ管理者は、まず次のうちどれを行うべきだろうか？
A. 誤検知に対処するためにIPSを調整します。
B. ハッキング未遂件数の増加を上級管理職に報告する。
C. セキュリティ意識向上トレーニングを更新する。
D. IPSによって識別されたイベントを検証します。
正解: **(**正解を表示します**)**

質問: **102**
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. 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。
C. 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。
D. オリジナルと画像のデジタル ハッシュを実行します。
正解: **(**正解を表示します**)**
Computing and comparing cryptographic hashes (e.g., MD5, SHA-1) of the original drive and the forensic image provides verifiable proof that every bit was copied exactly, ensuring integrity.

質問: **103**
リスク所有者の責任は次のうちどれですか？
A. 組織のリスク許容度を決定する
B. リスクを移転するための管理策の実施
C. 管理効果の監視を確実に行う
D. 管理体制の確立と運用
正解: **C (**コメントを発表する**)**
A risk owner is responsible for monitoring and ensuring the effectiveness of controls that mitigate the risks they own. They oversee how risks are managed within their area of responsibility, ensuring controls operate as intended and that residual risk remains within acceptable limits.

質問: **104**
セキュリティインシデント管理を提供する第三者との契約に含めるべき最も重要な要件は次のうちどれですか？
A. セキュリティインシデントは、指定された期間内にクライアント組織に報告する必要があります。
B. セキュリティインシデントの根本原因分析と是正計画を顧客組織に提供する必要があります。
C. インシデント対応チームの成熟度評価は定期的に実施する必要がある。
D. インシデント管理に関する文書化された方針は、上級管理職の承認を得なければならない。
正解: **(**正解を表示します**)**
The most critical contractual requirement is timely incident reporting to the client within a defined timeframe, because rapid notification is essential for containment, regulatory notification deadlines, coordinated response, and reducing business impact.

質問: **105**
インシデント対応計画のテストを実施することで得られる最も有益な結果は、次のうちどれですか？
A. 対応策には、上級管理職へのエスカレーションが含まれます。
B. テスト計画の結果が文書化されている。
C. インシデント対応時間が改善されました。
D. テストの結果を反映させるため、計画が強化されました。
正解: **(**正解を表示します**)**
The most beneficial outcome of testing is improving the incident response plan based on identified gaps and lessons learned, increasing future effectiveness and readiness.

質問: **106**
情報セキュリティ管理者は、組織のネットワーク全体にマルウェアが拡散していることを知らされました。次のうち、最も効果的な対応策はどれですか？
A. 従業員に対し、追って通知があるまで各自の端末の電源を切るよう指示してください。
B. ネットワーク上の感染していないマシン上のデータを暗号化します。
C. 侵入防止システム(IPS)の感度を上げる。
D. 感染したデバイスをネットワークから隔離します。
正解: **(**正解を表示します**)**
Malware spreading through the network requires immediate containment. Isolating infected devices stops further propagation while allowing investigation and remediation to continue.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu ¶**193**問、３０%ディスカウント、特別な割引コード**:** **JPNshiken**」

質問: **107**
新たな規制によりレガシーアプリケーションのアップグレードに多額の投資が必要になった場合、情報セキュリティマネージャーはまず次のうちどれを行うべきでしょうか？
A. 実装ロードマップを作成する。
B. 組織への事業上の影響を評価する。
C. リスクを軽減するための補償的対策を決定する。
D. 不遵守を是正するための費用を決定する。
正解: **(**正解を表示します**)**
The first step when facing a new regulation that requires a significant investment in upgrading a legacy application is to assess the business impact. This helps determine how noncompliance affects operations, financials, and regulatory standing, allowing for informed decision-making.
Once the impact is understood, the organization can develop an implementation roadmap, explore compensating controls, or evaluate remediation costs.

質問: **108**
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. 定期的なセキュリティ意識向上プログラムの実施
B. セキュリティイベントログ記録の定期的な分析
C. 主要リスク指標 (KRI) のしきい値設定
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**)**

The first step an information security manager should take upon learning that a competitor has experienced a ransomware attack is to update indicators of compromise in the security systems.
This action helps enhance the organization's defenses by ensuring that security systems are prepared to detect any similar threats that might target the organization.
While performing backups, conducting awareness training, and reviewing risk assessments are important actions, updating indicators of compromise directly addresses the immediate threat landscape and helps protect the organization from potential ransomware attacks.

質問: **109**
組織のエンタープライズアーキテクチャ(EA)プログラムをレビューするIS監査担当者にとって、以下の観察事項のうちどれが最も懸念すべきでしょうか？
A. 情報セキュリティ要件はEAプログラムによってレビューされます。
B. ITアプリケーションの所有者は、アーキテクチャの承認について単独で責任を負います。
C. アーキテクチャレビュー委員会はCIOが議長を務めます。
D. EAプログラムは、IT関連ではないプロジェクトを管理します。
正解: **(**正解を表示します**)**
IT application owners having sole responsibility for architecture approval is of greatest concern because it introduces the risk of inconsistent architecture decisions, lack of enterprise-wide alignment, and insufficient oversight from other key stakeholders (e.g., security, operations, compliance). Architecture approval should be collaborative and governed by a formal review board to ensure consistency and strategic alignment.

質問: **110**
以下のうち、管理責任者の役割と責任を最も適切に説明しているのはどれですか？
A. 他の部署と連携して、リスクを特定し、適切な管理策が実施されるようにする。
B. リスクを効果的に軽減するために、管理体制の継続的な監視と改善を実施する。
C. 特定されたリスクを軽減するための管理策の設計と実施を監査する。
D. 潜在的なリスクを特定し、管理の有効性について年次レビューを実施する。
正解: **B (**コメントを発表する**)**
Control owners are responsible for ensuring assigned controls are implemented, operating effectively, monitored, maintained, and improved when needed to mitigate risk.

質問: **111**
契約入札書は電子署名され、電子メールで送信されます。この目的で電子署名を使用する主な利点は何ですか？
A. 鍵が漏洩しても入札は偽造できません。
B. 契約入札プロセスを迅速化します。
C. 入札内容の変更は署名を無効にします。
D. 入札書と署名は、ある文書から別の文書にコピーできます。
正解: **C (**コメントを発表する**)**
A digital signature provides integrity and nonrepudiation. If the signed bid is changed after signing, the signature validation fails, showing that the document was altered.

質問: **112**
事故発生時に規制要件を満たすためのコミュニケーション計画について助言を行うのに最適なグループは、次のうちどれですか？
A. インシデント対応チームの責任者
B. 上級管理職
C. 情報セキュリティマネージャー
D. 法務担当者
正解: **(**正解を表示します**)**
Legal personnel are best positioned to consult on a communication plan for regulatory requirements during an incident, as they have the expertise to ensure compliance with laws, avoid legal liabilities, and address regulatory expectations appropriately.

質問: **113**
ビジネスインパクト分析(BIA)を実施する上で、最も重要な目的は次のうちどれですか？
A. 最も重要なビジネス資産を特定する
B. 災害復旧のための予算を正当化する
C. インシデント管理プロセスを構築する
D. IT復旧要件を確立する
正解: **A (**コメントを発表する**)**
The most important objective of conducting a business impact analysis (BIA) is to identify the most critical business assets. This helps prioritize recovery efforts and ensures that the organization can focus on protecting the most essential resources and processes in the event of a disruption.

質問: **114**
インシデント対応の机上演習を実施する主な理由は次のうちどれですか？
A. 組織の情報セキュリティプログラムを成熟させる
B. インシデント対応準備状況をリーダーシップ層に報告する
C. 実際の事件発生に備えて、インシデント対応チームを準備する
D. インシデント対応に必要なリソースを定義する
正解: **(**正解を表示します**)**
The primary reason for conducting a tabletop exercise is to prepare the incident response team to effectively handle real-world incidents by practicing roles, decision-making, and coordination in a simulated environment.

質問: **115**
新しいプライバシー規制では、違反に対して多額の罰金が科せられます。情報セキュリティマネージャーが、この規制が組織に与える影響をより深く理解するために、次のうちどれが最も効果的でしょうか？
A. 定性的リスク評価
B. 費用便益分析
C. 事業影響分析(BIA)

D. 管理ギャップ評価
正解: **(**正解を表示します**)**
A business impact analysis (BIA) helps determine the potential consequences of privacy breaches, including financial penalties, on the organization, providing a clear understanding of the regulation's impact.

質問: **116**
ある部署から、セキュリティ対策がもはや有効ではないとの報告がありました。情報セキュリティマネージャーにとって、次のうちどれが最善の対応策でしょうか？
A. コントロールを交換してください。
B. 管理者に不具合を報告する。
C. 多層防御を確認する。
D. 制御状態を評価する。
正解: **(**正解を表示します**)**
Assessing the control state allows the information security manager to determine the nature and extent of the issue, so appropriate corrective action can be taken based on actual findings.

質問: **117**
ITセキュリティプログラムの目標達成を促進する上で、最も効果的な方法はどれですか？
A. ヘルプデスクと変更管理プラットフォームの構築
B. 職務記述書にセキュリティに関する責任を含める
C. 全従業員を対象とした必須のITセキュリティ研修プログラムの設計
D. 経営陣と事業部門が関与する運営委員会の設置
正解: **(**正解を表示します**)**
IT security program objectives are implemented most effectively when there is governance support, executive sponsorship, business involvement, and prioritization. A steering committee helps align objectives with business needs and ensures resources, accountability, and cross- functional cooperation.

質問: **118**
技術的な対策がない場合、会社支給の携帯端末における不正なテキストメッセージの送受信を減らすための最善の方法は何でしょうか？
A. 組織が管理策を実施できるようになるまで、モバイルデバイスの提供を停止してください。
B. セキュリティ意識向上トレーニングに、禁止されているテキストメッセージの送信に関するトピックを含める。
C. 利用規約について定期的にリマインダーを伝達する。
D. 事業影響分析(BIA)を実施し、その報告書を経営陣に提出する。
正解: **(**正解を表示します**)**
In the absence of technical controls, regularly communicating reminders of the acceptable use policy is the most effective way to reinforce expected behavior and deter unauthorized text messaging on company-supplied mobile devices.

質問: **119**

高い可用性が求められるeビジネスにとって、以下の設計原則のうちどれが最適でしょうか？
A. 取引を迅速に受け付け、処理できる単一のエントリーポイント
B. ユーザーのニーズを満たす別のeコマースサイトへの手動フェイルオーバー
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転送するインテリジェントなミドルウェア
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 real-time, automated redirection of transactions to alternative systems without manual intervention, supporting high availability requirements for e-business operations.

質問: **120**
以下の指標のうち、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の整合性を示す最良の証拠となるのはどれですか？
A. 事業部門ごとのセキュリティインシデントの平均件数
B. セキュリティ対策に関連する平均投資収益率(ROI)
C. 企業全体のセキュリティインシデントの平均解決時間(MTTR)
D. 高リスク情報資産について特定された脆弱性の数
正解: **A (**コメントを発表する**)**
Governance Alignment is specifically about how well security is integrated into the business. If security governance is aligned, you should see a consistent or decreasing level of risk/incidents across all business units, proving the strategy is working globally, not just on a per-project financial basis.

質問: **121**
組織の情報セキュリティ管理者は、主に以下の目的で内部監査機能を活用するべきである。
A. 方針と手順を見直す。
B. 管理上のギャップを特定する。
C. セキュリティ予算の正当性を説明する。
D. セキュリティ認証を取得する。
正解: **B (**コメントを発表する**)**
Internal audit is primarily leveraged to provide independent assurance by evaluating controls and identifying gaps or weaknesses, enabling management to address deficiencies and strengthen the control environment.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu ¶**193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **122**

10年以上前に導入されたレガシーシステムの継続性計画を作成する際に、以下のうちどれを最も重視すべきでしょうか？
A. システムメーカーはシステムのサポートを提供していません。
B. システム復旧にかかる時間が、業務上許容できる期間よりも長い。
C. インシデント対応チームは、システムの技術文書を保有していません。
D. 最新のセキュリティパッチがシステムに適用されていません。
正解: **B (**コメントを発表する**)**
The greatest concern when creating a continuity plan for a legacy system is the duration for system restoration. If the recovery time exceeds what the business can accept, it can severely disrupt operations, making it a critical factor to address in the continuity plan.

質問: **123**
クラウドプロバイダーと連携してインシデント対応計画を策定する際に、最も重要なセキュリティ上の考慮事項は次のうちどれですか？
A. クラウドセキュリティ監査レポート
B. エスカレーションプロセス
C. クラウドプロバイダースタッフの経験
D. リカバリポイント目標(RPO)
正解: **(**正解を表示します**)**
In a cloud environment, incident response depends on rapid coordination between the organization and the cloud provider. Clear escalation processes define who to contact, when to escalate, required response times, responsibilities, and communication paths during an incident.

質問: **124**
取締役会が求める、事業が直面する情報セキュリティリスクの簡潔な概要を最も適切に満たすのは、次のうちどれでしょうか？
A. リスクヒートマップ
B. バランススコアカード
C. リスクシナリオの概要
D. 事業影響分析(BIA)
正解: **(**正解を表示します**)**

質問: **125**
事業継続計画(BCP)の策定においてリスク評価を実施する主な利点は、以下の点が促進されることです。
A. 現在のバックアップ手順の完全性と堅牢性の評価。
B. 業務プロセスの中断に対する効果的な緩和戦略。
C. 冗長性を判断するためのネットワークアーキテクチャ設計の評価。
D. 主要プロセスの中断が事業に及ぼす影響と可能性の理解。
正解: **(**正解を表示します**)**

A risk assessment for BCP identifies threats, vulnerabilities, likelihood, and potential impact to critical business processes. This helps the organization understand which interruptions are most likely and most damaging.

質問: **126**
事業継続計画(BCP)を策定する組織にとって、以下のうち最も重要な考慮事項はどれでしょうか？
A. 代替処理拠点の設置
B. 復旧時間目標(RTO)の達成
C. データバックアップ頻度の決定
D. 耐障害性システムの維持
正解: **(**正解を表示します**)**
A BCP is designed to keep critical business functions operating or restore them within acceptable timeframes. The RTO defines how quickly processes, systems, and services must be recovered after disruption, so meeting RTOs is the most important consideration.

質問: **127**
小規模組織が業務目標を達成するために、サポート対象外のソリューションを使用する必要がある。情報セキュリティマネージャーが関連するリスクを管理するために取るべき最善の行動は次のうちどれか？
A. 事業部門にシステム変更を勧める。
B. 経営陣にリスクを受け入れるよう勧める。
C. 定期的に脆弱性スキャンを実行する。
D. 補償的なセキュリティ対策を実施する。
正解: **(**正解を表示します**)**
When a solution must be used despite being out of support, the best course of action is to implement compensating controls to mitigate the associated risks and maintain an acceptable security posture.

質問: **128**
ゼロトラストの原則に沿うために、外部関係者とやり取りする際に最も重要な行動は次のうちどれですか？
A. 外部関係者のアクセス管理慣行について、定期的な包括的監査を実施することを徹底する。
B. 外部関係者に対し、保存データおよび転送データに特定の種類の暗号化方式を使用することを義務付ける
C. 外部機関に対し、従業員への年次セキュリティ研修の実施を義務付ける
D. 外部関係者との契約において、継続的な検証と最小権限アクセスを義務付けることを確実にする。
正解: **D (**コメントを発表する**)**
Zero Trust is built on continuous verification and enforcing least privilege for every access request. Ensuring contracts require these principles for external parties is the most important action because it establishes enforceable expectations for how third parties will access and use the organization's resources.

質問: **129**
組織内にセキュリティ文化を構築するための主要な目標として、次のうちどれが適切でしょうか？
A. リスクを許容レベルまで低減する
B. 上級管理職に対し、統制の有効性を示すため

C. 組織内のセキュリティを最優先事項とする
D. 情報セキュリティ対策のためのリソースを確保する
正解: **A (**コメントを発表する**)**

質問: **130**
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要な権限は誰にありますか？
A. リスク所有者
B. ITリスクマネージャー
C. 情報セキュリティマネージャー
D. 内部監査員
正解: **(**正解を表示します**)**
The risk owner has primary authority and accountability for making decisions about risk treatment, including whether additional measures are needed to mitigate the identified risk.

質問: **131**
新たな情報セキュリティ報告要件がまもなく発効します。情報セキュリティ管理者が最初に行うべき行動は次のうちどれですか？
A. 新しい要件への非準拠に関連する費用便益分析を実施します。
B. 新しい要件に対するギャップ評価を実行します。
C. 新しい要件がビジネスに適用されるかどうかを調査します。
D. 新しい要件を上級管理職に通知します。
正解: **C (**コメントを発表する**)**
Before taking any compliance steps, the information security manager must first assess whether the regulation is applicable to the organization. This ensures resources are not spent unnecessarily. "The applicability of legal, regulatory, and contractual requirements must be determined before initiating compliance activities."

質問: **132**
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、最も適切な方法は次のうちどれですか？
A. IDM(アイデンティティおよびアクセス管理)ツールを導入する。
B. ベンダーが推奨するユーザーアカウント設定を採用する。
C. ユーザーのアクセス権限のリスク評価を実施する。
D. ユーザーの役割に基づいてアクセス権限を定義します。
正解: **(**正解を表示します**)**
https://www.zendata.dev/post/data-access-controls-101-restricting-data-access-to-authorised-users-only

質問: **133**
買収したばかりの企業のセキュリティ体制を評価する際、情報セキュリティマネージャーが最初に行うべき手順は次のうちどれでしょうか？
A. 買収した企業のセキュリティ戦略をレビューする。
B. 買収した企業のセキュリティポリシーのコンプライアンスレビューを実施する。

C. 現在のセキュリティポリシーを実施する。
D. 買収した企業の過去のセキュリティインシデントをレビューする。
正解: **(**正解を表示します**)**
Assessing security posture starts at a strategic level:
- Objectives
- Governance model
- Risk alignment
Reviewing the security strategy establishes context for:
- Policies
- Controls
- Incident history

質問: **134**
情報セキュリティ運営委員会の主な目的は次のうちどれですか？
A. 長期的な情報セキュリティ対策を承認する
B. 情報セキュリティが事業目標達成に確実に貢献するようにする
C. 情報セキュリティプログラムの優先順位を設定する
D. 情報セキュリティポリシーが承認されていることを確認する
正解: **C (**コメントを発表する**)**
The security steering committee provides governance direction by aligning security activities with business needs and setting priorities for the information security program.

質問: **135**
セキュリティ構成のベースラインを定義する際に、最も重要な考慮事項は次のうちどれですか？
A. 基準値はリスクに比例します。
B. 基準値は事業分野と一致しています。
C. ベースラインは既知のシステム脆弱性に対処します。
D. 基準値は、適用される規制基準に対応しています。
正解: **(**正解を表示します**)**
Security configuration baselines must be proportionate to risk to ensure controls are appropriate and cost-effective. Overly strict or insufficient baselines can either hinder operations or leave systems exposed, making risk proportionality the most important consideration.

質問: **136**
組織がセキュリティインシデントを特定し、封じ込めるために最も効果的な方法はどれですか？
A. 脅威モデリング
B. 卓上運動
C. リスク評価
D. 継続的なモニタリング
正解: **D (**コメントを発表する**)**

Continuous monitoring provides real-time visibility into systems and networks, enabling the organization to promptly identify and contain security incidents as they occur.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu **1193**問、３０%ディスカウント、特別な割引コード**:** **JPNshiken**」

質問**: 137**
ある組織がセキュリティパフォーマンスを測定するためのセキュリティ指標を選定しており、ファイアウォールの専門家はファイアウォールによってブロックされた外部攻撃の数を追跡することを提案しています。この指標を使用する上で、最も懸念される点は次のうちどれですか？
A. ブロックされた外部攻撃の数は、真の脅威プロファイルを表すものではありません。
B. ブロックされた外部攻撃の数は、組織の人気度を示す指標です。
C. 時間経過に伴うブロックされた外部攻撃の数は、攻撃者の動機を説明するものではありません。
D. ブロックされた外部攻撃の数は月によって変動するため、グラフに一貫性がなくなります。
正解**: (**正解を表示します**)**
The greatest concern with using the number of blocked external attacks as a metric is that it may not accurately represent the true threat profile. A large number of blocked attacks could indicate an effective firewall but might not reflect the full scope or sophistication of potential threats. It is important to measure metrics that better reflect the overall security posture, including the nature of attacks and vulnerabilities.

質問**: 138**
事件への対応を評価する最良の方法はどれですか？
A. インシデント対応のタイムラインを分析します。
B. インシデント後の対応レビューを実施する。
C. 卓上演習を実施する。
D. 検出までの平均時間を評価します。
正解**: (**正解を表示します**)**
A post-incident response review provides a comprehensive evaluation of how the incident was handled, including effectiveness of controls, communication, decision-making, and areas for improvement. It ensures lessons learned are formally documented and integrated into process improvements, making it the most effective method to evaluate the overall response.

質問**: 139**
情報セキュリティプログラムの主な目標は次のうちどれですか？
A. 情報セキュリティリスクを最小限に抑えるため

B. 組織の情報インフラを脅威から保護する
C. 組織の法的および規制上の要件に対応するため
D. 情報資産に適切な保護を提供する
正解: **(**正解を表示します**)**
The primary goal of an information security program is to provide appropriate protection for the organization's information assets. This involves ensuring confidentiality, integrity, and availability of data, as well as mitigating risks to the information infrastructure, in line with legal and regulatory requirements.

質問: **140**
インシデント分類アプローチを策定する際に、最も重要な考慮事項は次のうちどれですか？
A. 分類レベルが組織のリスクと整合していることを確認する
B. 自動化ツールを活用して基準を策定する
C. 分類における業界のベストプラクティスの採用
D. 上級管理職の承認を得る
正解: **(**正解を表示します**)**
Aligning classification levels to organizational risk ensures that incidents are prioritized and handled according to their potential impact, enabling an effective and risk-based incident response strategy.

質問: **141**
組織の情報セキュリティ意識向上プログラムの効果を最もよく示す指標は次のとおりです。
A. 上級管理職の満足度。
B. ヘルプデスクに報告されたインシデント。
C. 侵入検知システム(IDS)アラート。
D. 稼働停止時間(時間)。
正解: **(**正解を表示します**)**
An effective security awareness program increases employees' ability to recognize and report suspicious activity. A meaningful indicator is the number and quality of incidents reported to the help desk, as this reflects improved awareness and proactive behavior by staff.

質問: **142**
災害復旧計画(DRP)を策定する際に、最も重要な考慮事項は次のうちどれですか？
A. リスク管理計画
B. 事業継続計画(BCP)
C. 事業影響分析(BIA)
D. 費用便益分析
正解: **(**正解を表示します**)**
The most important factor to consider when developing a disaster recovery plan (DRP) is the business impact analysis (BIA). The BIA helps identify and prioritize critical business functions and the potential impact of disruptions, which directly informs the development of an effective disaster recovery plan.

質問: **143**
取締役会への情報セキュリティプログラム報告に含めるべき最も重要な項目は次のうちどれですか？
A. 指標
B. コスト削減
C. 技術リスク
D. 詳細なセキュリティインシデント
正解: **(**正解を表示します**)**
The board of directors focuses on strategic decision-making and risk management, so the most important aspect of security program reporting is technology risk and its potential impact on business objectives. This helps the board understand cybersecurity threats, regulatory concerns, and investment needs at a high level. While metrics, cost savings, and incident details are useful, they are tactical rather than strategic and do not provide the broad risk perspective that boards require.

質問: **144**
ある組織が、内部ネットワークに対するサイバー攻撃が活発に行われていることを確認しました。インシデント対応の成功にとって、以下の考慮事項のうちどれが最も重要ですか？
A. データ損失防止(DLP)ツールは正常に機能しています。
B. 鑑識サポートの連絡先はすぐに入手可能です。
C. 復旧時間目標(RTO)を達成できます。
D. ステークホルダーへのコミュニケーションは別のチャネルを通じて行われます。
正解: **D (**コメントを発表する**)**
During an active attack, the organization must assume normal communication channels (email, chat, internal voice) may be monitored or disrupted by the attacker. Using a separate, out-of-band channel is most critical to coordinate response securely and effectively.

質問: **145**
情報セキュリティマネージャーは、リスクオーナーがプロセス効率を向上させるために、主要な制御をより弱い代替制御に置き換える例外を承認したことを知ります。以下のうち、最も懸念すべき事項はどれでしょうか？
A. 補償制御は自動化されていません
B. 経営陣へのリスク報告は不正確である可能性がある
C. リスクレベルが許容限度を超える可能性があります
D. 規制要件を遵守しない場合、以下の結果を招く可能性があります。
正解: **C (**コメントを発表する**)**
The greatest concern is that replacing key controls with weaker ones may raise risk levels beyond the organization's acceptable limits, potentially exposing it to significant threats and undermining its risk management strategy.

質問: **146**
セキュリティ標準が特定されたビジネス目標の達成を妨げている場合、情報セキュリティマネージャーはまず次のうちどれを行うべきでしょうか？

A. リスク受容を推奨します。
B. 事業目標を再検討する。
C. 事業影響分析(BIA)を実施する。
D. 費用対効果分析を実施する。
正解: **(**正解を表示します**)**
The first step an information security manager should take is to revisit the business objective.
This ensures that the objective remains aligned with organizational goals and that any constraints imposed by the security standard are properly evaluated against the business needs.
Adjustments may then be made to the objective or security standard as needed.

質問: **147**
組織のWebアプリケーションプラットフォームへの不正侵入がSIEMプラットフォームで検知され、ログに記録されましたが、大量のアラートが発生していたことと、週末に発生したため、セキュリティチームはこの事象に気づきませんでした。このような事象への対応を改善するための最善の方法は次のうちどれですか？
A. 侵入検知 防御ソリューションを導入する。
B. SIEMが利用可能なすべてのログを取り込むように設定します。
C. ファイアウォールとSIEMイベントをレビューするセキュリティスタッフを増員します。
D. 24時間365日稼働する自動検知および通知プロセスを確立する。
正解: **D (**コメントを発表する**)**
Establishing a 24/7 automated detection and notification process is the best way to ensure critical events are detected and acted upon promptly, even during off-hours or when alert volumes are high. Automation helps reduce reliance on manual monitoring and improves response time to high-priority incidents.

質問: **148**
以下のうち、インシデント対応チームの準備態勢にとって最も大きなリスクとなるのはどれですか？
A. 情報セキュリティ管理の変化
B. ハッカーが使用する新たな攻撃手法
C. 正式なインシデント対応シナリオの欠如
D. 時代遅れのインシデント対応計画
正解: **(**正解を表示します**)**
Outdated incident response plans mean procedures, contacts, roles, technologies, and escalation paths may no longer reflect the current environment. If plans are not current, the team may respond incorrectly or inefficiently during an incident, directly undermining preparedness and effectiveness.

質問: **149**
ビジネスパートナーと情報を共有する組織のセキュリティ要件を最も適切に定義しているのは、次のうちどれですか？
A. ビジネスパートナーのプライバシー保護要件を規定する規制指令
B. 組織とビジネスパートナー間の契約上の合意
C. 組織とビジネスパートナーが合意したITガバナンスガイドライン

D. 取引先の確立された情報セキュリティポリシー
正解: **(**正解を表示します**)**
The best way to define security requirements for an organization that shares information with a business partner is through contractual agreements between the organization and the business partner. These agreements (such as service-level agreements or data-sharing agreements) explicitly outline the security expectations, responsibilities, and controls to ensure both parties are aligned on protecting shared information.

質問: **150**
以下のうち、効果的なセキュリティ文化を最もよく示しているのはどれですか？
A. セキュリティ基準とポリシーはスタッフに周知され、遵守されている。
B. 経営陣は従業員に対し、セキュリティインシデントを報告するよう奨励している。
C. セキュリティリスクは許容範囲内で管理 維持されている。
D. 情報セキュリティは重要なビジネスパートナーおよびイネーブラーと見なされています。
正解: **(**正解を表示します**)**
An effective security culture is best indicated when information security is viewed as a strategic business partner and enabler, reflecting deep integration into decision-making and organizational values beyond mere compliance.

質問: **151**
外国でホストされるIaaS(Infrastructure as a Service)モデルにIT運用を移行する際に、最も重要な考慮事項は次のうちどれですか？
A. 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ることを保証するのに役立ちます。
B. 原産国の法律や規制は適用されない場合があります。
C. セキュリティ侵害が発生した場合、法的責任や罰則が発生する可能性があります。
D. データは不明な場所に保存されている可能性があり、容易に取得できない可能性があります。
正解: **(**正解を表示します**)**
The most critical consideration when shifting IT operations to an Infrastructure as a Service (IaaS) model hosted in a foreign country is that laws and regulations of the origin country may not be applicable. Different countries have varying laws regarding data protection, privacy, and compliance, and relying on the laws of the hosting country can lead to significant legal and regulatory risks.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu ↟**193**問、３０%ディスカウント、特別な割引コード**:** **JPNshiken**」

質問: **152**

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

質問: **153**
組織活動を導くための情報セキュリティガバナンスフレームワークの導入を最も効果的にサポートするのは、次のうちどれですか？
A. セキュリティ管理ギャップ分析の結果
B. リスク管理監査の結果
C. ビジネスリーダーからの客観的な意見
D. セキュリティ技術の動向分析
正解: **(**正解を表示します**)**
Objective input from business leaders best supports implementation because governance must align with business objectives and risk appetite, and leadership involvement drives authority, adoption, and integration into organizational decision-making.

質問: **154**
業務アプリケーションに、外部攻撃者が悪用してシステムを侵害する可能性のある重大な脆弱性が発見されました。情報セキュリティ管理者が取るべき最善の行動は何でしょうか？
A. 一時的な対策を実施する。
B. 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に依頼してください。
C. 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。
D. アプリケーションを直ちに終了してください。
正解: **(**正解を表示します**)**
The information security manager's best course of action is to report the risk to the business application owner, who is responsible for deciding on the appropriate treatment (e.g., patching, mitigation, or acceptance). This ensures accountability and aligns the response with business priorities and risk tolerance.

質問: **155**
主要プロジェクトのマネージャーは、プロジェクトを期日通りに完了させるために追加のリソースを確保する目的で、通常の請負業者オンボーディングプロセスを省略しました。契約はオフラインで締結され、請負業者には通常のデューデリジェンスプロセスを経ずに組織へのアクセス権が付与されました。以下のうち、最も懸念すべき事項はどれでしょうか？
A. 事故が報告された場合、プロジェクトがさらに遅れる可能性があります。
B. 請負業者が業務機能を不適切に第四者サプライヤーにアウトソーシングする可能性がある。
C. 請負業者は業界基準に沿って業務を行っていない可能性があります。

D. 第三者との契約を規定する契約上の要件が不十分です。
正解: **(**正解を表示します**)**
Bypassing the standard onboarding and due diligence process means contractual terms, security requirements, and accountability may be missing or inadequate. This creates unmanaged third- party risk, making the lack of sufficient contractual requirements the primary concern.

質問: **156**
災害発生時に組織が業務を継続するために、以下のうちどれを発動すべきでしょうか？
A. 事業継続計画(BCP)
B. 危機コミュニケーション計画
C. IT緊急時対応計画
D. 災害復旧計画(DRP)
正解: **(**正解を表示します**)**
The BCP is designed to ensure that critical business processes continue to function during and after a disaster. It focuses on the business as a whole, including people, workspace, and manual workarounds.
While other plans focus on fixing what broke, the BCP focuses on how the organization keeps serving customers and meeting obligations while the systems are down.
The BCP sits at the top of the hierarchy. It encompasses all the steps needed to maintain business "uptime," whereas technical plans are subsets of this larger goal.

質問: **157**
重大なセキュリティ侵害への対応において、最初に考慮すべき事項は次のうちどれですか？
A. 封じ込め
B. 鑑識
C. 根絶
D. ドキュメント
正解: **(**正解を表示します**)**
The first action to consider when responding to a major security breach is containment.
Containment helps to prevent further damage or spread of the breach, ensuring the issue is controlled before moving on to further steps like forensics or eradication.
Once the breach is contained, the organization can then proceed with forensics to investigate the cause, eradication to remove the threat, and documentation for reporting and analysis.

質問: **158**
セキュリティ対策の有効性を監視するための最良の方法はどれですか？
A. 定期的に脅威評価を実施する。
B. セキュリティ指標を確立し、報告する。
C. 類似組織と比較してセキュリティ対策をベンチマークする。
D. アプリケーションおよびシステム監査ログを確認する。
正解: **B (**コメントを発表する**)**

Establishing and reporting security metrics provides ongoing, repeatable measurement of whether controls are performing as intended over time, making it the best way to monitor control effectiveness.

質問: **159**
クラウドデータベースの暗号化を実装する際のベストプラクティスは、次のうちどれですか？
A. ベンダーは公開鍵暗号をサポートしています。
B. ベンダーはプライマリキーとインデックス付き列を暗号化します。
C. 組織は独自の暗号化アルゴリズムを実装しています。
D. 組織は独自の暗号化キーを保持しています。
正解: **(**正解を表示します**)**
Best practice is for the organization to maintain control of its encryption keys (customer-managed keys) to reduce vendor dependency and insider risk, and to retain the ability to revoke access and meet compliance requirements.

質問: **160**
組織のインシデント対応能力を最も効果的に向上させるには、次のうちどれが最適でしょうか？
A. 事件の封じ込めに追加の財源を割り当てる
B. 事業影響分析(BIA)の実施を確実にする
C. 分散型インシデント対応監視機能の実装
D. インシデント分類プロセスの改善
正解: **(**正解を表示します**)**
A well-defined and refined incident classification process improves prioritization, escalation, and resource allocation during incident handling. Accurate classification enables consistent response, better trend analysis, and more effective management of incidents, directly maturing overall incident response capability.

質問: **161**
インシデント管理チームはサイバー攻撃を確認し、影響を受けたコンピュータを特定しました。次に取るべき行動は次のうちどれですか？
A. 影響を受けているコンピュータをネットワークから隔離します。
B. 影響を受けているコンピュータの電源を切断します。
C. ドライブ上のすべてのデータのビットレベルイメージを取得します。
D. 調査結果を上級管理職に報告する。
正解: **A (**コメントを発表する**)**
After confirming the attack and identifying affected systems, the next priority is containment to prevent further spread or damage. Isolating the affected computers from the network limits lateral movement, data exfiltration, and additional compromise while preserving system state for further investigation.

質問: **162**
AIシステムのインシデント対応計画の検出フェーズで実行される可能性が最も高いのは、次のうちどれですか？
A. AI対応計画を見直し、改善点を特定するための机上演習を実施する。
B. AI関連のインシデントが検知された場合、さらなる影響を防ぐための即時措置を開始する

C. 異常検知アルゴリズムや行動分析などのAI駆動型セキュリティソリューションを活用する
D. AI関連のインシデントに対応したインシデント対応ポリシー、手順、およびプレイブックの開発
正解: **(**正解を表示します**)**
The detection phase focuses on identifying suspicious or abnormal activity. For an AI system, anomaly detection and behavioral analytics can help detect model misuse, abnormal inputs/outputs, data poisoning indicators, unauthorized access, or unexpected system behavior.

質問: **163**
セキュリティ基準を確立する上で、以下のうちどれが最も重要ですか？
A. ガイドライン
B. 手順
C. 規格
D. ポリシー
正解: **(**正解を表示します**)**
Security baselines are built from mandatory technical requirements, such as secure configuration settings, patch levels, logging requirements, password parameters, and hardening rules. These are defined in standards.

質問: **164**
ユーザーが、機密性の高い企業データが保存されている個人用モバイル端末の盗難を報告しました。データ漏洩のリスクを最も効果的に最小限に抑えるには、次のうちどれが最適でしょうか？
A. ユーザーの企業データへのアクセス権を削除する
B. 事件を警察に通報する
C. デバイスを遠隔で消去する
D. ユーザーが個人のモバイルデバイスを使用することを禁止する
正解: **(**正解を表示します**)**

質問: **165**
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. 関係する関係者に通知します。
B. フォレンジック分析を実施します。
C. 学んだ教訓を実行します。
D. 影響を受けたシステムを復元します。
正解: **B (**コメントを発表する**)**
Once containment is achieved, the priority is to conduct forensic analysis to preserve evidence, determine the scope and root cause of the attack, and inform subsequent recovery efforts before restoring systems or drawing broader lessons.

質問: **166**
インシデント撲滅フェーズの主要目標は以下のとおりです。
A. 侵害の原因を軽減する。

B. 証拠を確保し、保全する。
C. 学んだ教訓を実践する。
D. 事業への影響を評価する
正解: **(**正解を表示します**)**
The primary goal of the incident eradication phase is to eliminate the root cause of the security incident to prevent further damage or recurrence. This may involve removing malware, closing exploited vulnerabilities, revoking compromised credentials, or restoring affected systems. While securing evidence, lessons learned, and impact assessments are important, they are not the main focus of the eradication phase.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu ¶**193**問、３０%ディスカウント、特別な割引コード**:** **JPNshiken**」

質問**: 167**
以下の機器のうち、非武装地帯(DMZ)に設置された場合、最も重大な暴露要因となるのはどれでしょうか？
A. データベースサーバー
B. メールリレーサーバー
C. アプリケーションサーバー
D. プロキシサーバー
正解**: A (**コメントを発表する**)**
A database server placed in a demilitarized zone (DMZ) would be the most significant exposure.
The DMZ is typically used for servers that need to be accessible from external networks, such as web or mail servers. A database server, which often contains sensitive business data, is typically kept in a more secure internal network to prevent unauthorized access. Placing it in the DMZ exposes it to greater risk.

質問**: 168**
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. 避ける
C. 転送
D. 受け入れる
正解**: (**正解を表示します**)**
When a risk's potential impact is negligible and its likelihood is very low, the most cost-effective approach is to accept it rather than expend resources on mitigation, avoidance, or transfer.

質問**: 169**

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." This ensures security, compliance, and operational continuity.

質問: **170**
行動分析ツールは、主に組織内のリスク管理に使用されます。
A. エンドポイントにおけるセキュリティベースラインの確立。
B. 外部ユーザーからの通信を分析し、マルウェアを検出する。
C. 異常なユーザーアクティビティの検出。
D. 機密データの流出を防止する。
正解: **C (**コメントを発表する**)**
Behavioral analytics tools primarily manage risk by detecting anomalous user activities that deviate from established patterns, enabling early identification of insider threats, compromised accounts, or misuse.

質問: **171**
システム開発プロジェクトに情報セキュリティを確実に組み込むために、最初に行うべきことはどれですか？
A. セキュリティポリシーを確認してください。
B. 各プロジェクトチームにセキュリティ担当者を配置する。
C. ビジネスへの影響に基づいてリソースを割り当てる。
D. セキュリティ要件を定義する。
正解: **(**正解を表示します**)**
Defining security requirements first establishes what must be built into the system (controls, data handling, authentication, logging, etc.) so security can be incorporated from the start and validated throughout the project lifecycle.

質問: **172**
職務分掌を確実にするために、システム管理者以外の者が行うのが最適な活動は次のうちどれですか？
A. システムログの削除
B. システムユーティリティの使用
C. システム復旧手順の定義
D. 監視システム利用状況

正解: **D** (コメントを発表する)
Monitoring system utilization is an audit function that should be kept independent of the system administrator's duties, ensuring oversight and preventing the administrator from hiding misuse of resources.

質問: **173**
ある組織が、新たな先端技術への投資を検討しています。情報セキュリティマネージャーがその影響を評価する際に、最も重要な考慮事項は次のうちどれでしょうか？
A. システム互換性
B. 安全な構成
C. 業界における当該技術のピアレビュー
D. 技術の脆弱性
正解: (正解を表示します)
The most important consideration when evaluating the impact of a new emerging technology is its vulnerabilities. Understanding potential security weaknesses in the technology ensures that appropriate safeguards are put in place to protect the organization from any risks associated with its adoption.

質問: **174**
情報セキュリティプログラムがビジネス戦略と整合していることを示す最良の証拠は、次のうちどれですか？
A. 情報セキュリティ対策は、ビジネスプロセスと直接的に関連しています。
B. 情報セキュリティプログラムには、明確に定義されたリスク許容度が必要です。
C. 情報セキュリティプログラムは、最高情報セキュリティ責任者(CISO)の期待を満たしています。
D. 情報セキュリティチームは、上級管理職に主要業績指標(KPI)を提供することができます。
正解: **A** (コメントを発表する)
The best evidence that the information security program is aligned to the business strategy is that information security initiatives are directly correlated to business processes. This shows that security efforts are focused on protecting and supporting critical business functions, ensuring that security aligns with and enables business objectives.
While risk tolerance, meeting the CISO's expectations, and providing KPIs are important, the direct alignment of security initiatives with business processes is the clearest indication that the security program is supporting the overall business strategy.

質問: **175**
以下のうち、情報セキュリティに関する問題の報告を従業員に最も促すものはどれですか？
A. 卓上運動は定期的に行われます。
B. リーダーたちは前向きなセキュリティ文化を築いている。
C. セキュリティスキル研修に対してインセンティブが提供されます。
D. 正式なインシデント対応プロセスが整備されています。
正解: (正解を表示します)

A positive security culture established by leadership fosters trust, openness, and psychological safety, encouraging staff to report issues without fear of blame or retaliation. Tone at the top directly influences employee behavior, making leadership-driven culture the most effective way to promote proactive reporting.

質問: **176**
同じデジタル署名証明書が2人以上のユーザーによって使用される可能性がある場合、情報セキュリティ管理者が最も懸念すべき事項は次のうちどれでしょうか？
A. 職務分担
B. 証明書の改ざん
C. データ暗号化が弱体化している
D. 送信者の身元を検証できない
正解: **(**正解を表示します**)**
A digital signing certificate is used to uniquely bind an individual's identity to their cryptographic signature. If the same certificate can be used by multiple users, the information security manager's primary concern is that the true sender of a digitally signed message cannot be reliably identified, undermining nonrepudiation and trust in the signature.

質問: **177**
アプリケーションの復旧優先順位を決定するための最適なリソースは次のうちどれですか？
A. 費用便益分析
B. リスク評価
C. 事業影響分析(BIA)
D. インシデント対応計画
正解: **C (**コメントを発表する**)**
A business impact analysis (BIA) identifies critical business processes, acceptable downtime, and dependencies, which directly determines the priority order for recovering applications.

質問: **178**
事案対応の封じ込め段階で最も起こりやすいのは次のうちどれですか？
A. 根本原因分析レポートの提示
B. 重要システムの復旧
C. 事件の確認
D. 事件の影響を受けた関係者への通知
正解: **D (**コメントを発表する**)**
During the containment phase of incident response, the primary focus is to limit the spread of the incident and prevent further damage. This often includes notifying stakeholders affected by the incident, ensuring they are aware of the situation and can take necessary actions, such as following specific protocols or staying informed.

質問: **179**
組織の技術インフラへの変更によって生じる脆弱性を特定するのに最も役立つのは、次のうちどれですか？

A. 確立されたセキュリティ基準
B. 脅威分析
C. 侵入テスト
D. 侵入検知システム(IDS)
正解: **C (**コメントを発表する**)**
Penetration testing is best for identifying exploitable vulnerabilities introduced by infrastructure changes. It validates whether new configurations, systems, integrations, or network paths can be abused by attackers.

質問: **180**
情報セキュリティガバナンスフレームワークを導入する際に、最初に確立すべき事項は次のうちどれですか？
A. セキュリティポリシー
B. セキュリティインシデント管理チーム
C. セキュリティアーキテクチャ
D. セキュリティ意識向上トレーニングプログラム
正解: **(**正解を表示します**)**
Security policies provide the foundation and direction for all other components of an information security governance framework and should be established first.

質問: **181**
認定を受けた第三者機関によって侵入テストが実施されました。情報セキュリティマネージャーが最初にとるべき行動は次のうちどれでしょうか？
A. 特定された問題を解決するためのビジネスケースを作成する。
B. 調査結果を評価するためにリスク評価を実施する。
C. 侵入防御システム(IPS)の設定を更新します。
D. 発見された脆弱性が許容可能な時間枠内で解決されるようにする。
正解: **B (**コメントを発表する**)**
The information security manager's first course of action after a penetration test should be to ensure a risk assessment is performed to evaluate the findings. This helps prioritize the vulnerabilities based on their risk level and potential impact, allowing the organization to address the most critical issues first.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu ↥**193**問、３０%ディスカウント、特別な割引コード**:** **JPNshiken**」

質問: **182**

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入社し、まずすべての主要なITプロセスの監査を実施します。脆弱性管理プログラムに関する以下の調査結果のうち、最も懸念すべきものはどれでしょうか？
A. 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。
B. 特定された脆弱性が記録されず、タイムリーに解決されない。
C. 発見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。
D. 特定された脆弱性は公開されておらず、啓発プログラムでも周知されていない。
正解: **(**正解を表示します**)**
The finding that should be of greatest concern in a vulnerability management program is that identified vulnerabilities are not logged and resolved in a timely manner. Timely logging and remediation of vulnerabilities are critical to reducing the organization's exposure to security risks.

質問: **183**
情報セキュリティポリシーは、主に以下の点との整合性を反映するべきである。
A. データセキュリティ基準。
B. 業界のベストプラクティス。
C. 情報セキュリティフレームワーク。
D. 経営陣の意図。
正解: **(**正解を表示します**)**
Information security policies should primarily reflect senior management's intent because they set the strategic direction and priorities for security within the organization. This ensures that the policies align with the organization's goals and receive the necessary support and enforcement.

質問: **184**
特定のアプリケーション要件により、プロジェクトチームに管理者権限が付与されました。これらのユーザーに明確に定義された役割と責任を伝える主な理由は何ですか？
A. 管理監督要件の改善
B. 説明責任に対する理解の向上
C. 職務分担の明確化
D. より明確な研修要件
正解: **B (**コメントを発表する**)**
When users are granted administrative privileges, clearly defining roles and responsibilities primarily ensures they understand their accountability for how privileged access is used, supporting proper governance and reducing misuse risk.

質問: **185**
情報セキュリティインシデント分類における重大度階層の主要な基準として、以下のうちどれを用いるべきでしょうか？
A. 事業への悪影響
B. 根本原因分析結果
C. 資源の入手可能性

D. 法的および規制上の要件
正解: **(**正解を表示します**)**
The severity of a security incident is fundamentally determined by its potential or actual impact on the organization's operations, assets, and overall business objectives. Classifying incidents based on the adverse effects they impose ensures that the organization can prioritize its response efforts effectively, allocating resources to incidents that pose the greatest threat to business continuity and integrity.

質問: **186**
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. データ セットに匿名化を適用してリスクを軽減します。
C. 保険を購入することでリスクを移転します。
D. 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。
正解: **(**正解を表示します**)**
https://www.imperva.com/learn/data-security/anonymization/

質問: **187**
組織が情報セキュリティ関連のコンプライアンス要件を満たすために最も効果的な方法はどれですか？
A. 経営幹部会議および取締役会において、コンプライアンス要件を議題項目に含めること
B. 組織のセキュリティプログラムを策定する際に、コンプライアンス要件を考慮する
C. セキュリティコンプライアンスに関する責任を最高情報セキュリティ責任者(CISO)に割り当てる
D. 内部監査機能において、コンプライアンス監査を年次セキュリティ監査計画に含めること
正解: **(**正解を表示します**)**
The best way to ensure an organization meets information security-related compliance requirements is to consider these requirements when developing the organization's security program. This ensures that compliance is built into security controls and processes from the outset, making it easier to meet ongoing regulatory obligations.

質問: **188**
クラウドに保存されている顧客の個人情報を保護するための最適な対策は、次のうちどれですか？
A. 強力な暗号化方式
B. 適切なデータ匿名化
C. 強力な物理的アクセス制御
D. デジタル記録の適時削除
正解: **(**正解を表示します**)**
https://www.paloaltonetworks.com/blog/prisma-cloud/cloud-data-security-protection-everything-you-need-to-know/

質問: **189**

規制機関が顧客決済取引処理に関する新しいガイドラインを発行した場合、情報セキュリティ管理者はまず次のうちどれを行うべきでしょうか？
A. 既存の管理体制がガイドラインを満たしているかどうかを評価する。
B. 新しい管理策を導入するコストを決定する。
C. 規制不遵守に伴うリスクを評価する。
D. 新しいガイドラインを実施するための戦略を準備する。
正解: **(**正解を表示します**)**
The first step is to evaluate whether existing controls already meet the new regulatory guideline.
Understanding the current control environment against the new requirements establishes the baseline and determines whether gaps exist before assessing cost, risk, or implementation strategy.

質問: **190**
情報セキュリティ管理者が、適用される法律および規制に従ってデータが適切な期間保持されたことを証明する最良の方法は、次のうちどれですか？
A. データインベントリの実施
B. 保持構成のコピーを取得する
C. 規制からマッピングされた要件に関するレポートを提供する
D. 情報管理方針における保存期間の公表
正解: **(**正解を表示します**)**
Copies of the retention configurations (e.g., system settings, retention rules) provide concrete, verifiable evidence that retention controls are implemented to enforce the required retention periods, rather than merely documenting intent or requirements.

質問: **191**
情報セキュリティプログラムにおいて、最も重要な要素は次のうちどれですか？
A. プログラム開発に機能別マネージャーを参加させる
B. 利用可能なリソースに基づいてプログラムの成果物の優先順位付けを行う
C. 企業が採用しているプロジェクト管理手法を適用する
D. プログラムの関連性をグローバルスタンダードと比較評価する
正解: **(**正解を表示します**)**

質問: **192**
多層防御の設計において考慮すべき最も重要な属性は以下のとおりです。
A. ある層の故障が次の層の故障を引き起こすことはありません。
B. 最も強力な制御は、複数の制御層を置き換えることができます。
C. 各層における制御コストは、保護全体のコストに寄与します。
D. 各層に対して一貫したアプローチが用いられています。
正解: **(**正解を表示します**)**
Defense-in-depth relies on independent, layered controls so that if one layer is bypassed or fails, other layers still function and continue to protect - preventing a single point of failure from collapsing the entire defense.

質問: **193**
組織がアウトソーシングされたサービスに対して適切なセキュリティ管理を確実に実施するための最も効果的な方法は、次のうちどれですか？
A. サービスプロバイダーのセキュリティポリシーとプロセスを定期的に見直すことを要求する。
B. サービス提供者が業界のベストプラクティスを実施することを義務付ける署名済みの契約を要求する。
C. 合意された独立した第三者による定期的なセキュリティコンプライアンス監査を要求する。
D. サービスプロバイダーに組織のセキュリティポリシーと基準を使用するよう要求する。
正解: **(**正解を表示します**)**
Regular security compliance audits by an independent third party are the most effective method to ensure that outsourced service providers maintain adequate security controls. These audits provide an unbiased assessment of compliance and the effectiveness of implemented controls.

質問: **194**
組織のフィッシング対策研修が成功したことを示す最良の指標は、次のうちどれですか？
A. トレーニング後、ユーザーからの報告が大幅に増加
B. フィッシング攻撃の試行回数が時間とともに減少する
C. 外部監査チームが全スタッフが研修を修了したことを確認しました。
D. 研修終了時のクイズの点数が過去よりも高い
正解: **(**正解を表示します**)**
The best indication of phishing awareness training success is a significant increase in reporting by users. This shows that employees are more vigilant and aware of phishing attempts, indicating they are actively applying what they learned during the training.

質問: **195**
組織の情報セキュリティ体制を最もよく示しているのは、次のうちどれですか？
A. 脅威分析結果
B. 定期的な政策見直し
C. 脆弱性スキャン結果
D. 内部統制監査報告書
正解: **(**正解を表示します**)**
A controls audit report best indicates an organization's information security posture because it provides a comprehensive evaluation of the effectiveness and implementation of security controls, helping to assess how well security measures are protecting the organization.

質問: **196**
ランサムウェア攻撃後にクリーンなデータを復元できる能力を確保するための最良の方法は、次のうちどれですか？
A. 複数のオフラインバックアップを維持する。
B. データをステージングサーバーに復元します。

C. 鑑識チームを招集する。
D. 機密性の高い生産データを暗号化する。
正解: **A (**コメントを発表する**)**
The best way to ensure the ability to restore clean data after a ransomware attack is to maintain multiple offline backups. Offline (air-gapped) backups prevent ransomware from encrypting or corrupting backup data, ensuring that the organization can recover critical information without paying the ransom. While restoring data to a staging server, engaging forensics, and encrypting production data are useful, they do not guarantee the availability of clean, restorable data like offline backups do.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu ↑**193**問、３０%ディスカウント、特別な割引コード**:** **JPNshiken**」

質問**: 197**
規制の厳しい市場で事業を展開している組織にとって、ビジネスに大きな影響を与える新しい規制要件を実装する必要がある場合、最も重要な考慮事項は何ですか?
A. 外部監査の実施
B. 補償制御の確立
C. 強力な監視制御の実施
D. ギャップ分析の実施
正解: **(**正解を表示します**)**
Conducting a gap analysis is critical to understand where current controls fall short of the new requirements, allowing the organization to prioritize remediation and allocate resources effectively.

質問**: 198**
本国を拠点とする電子商取引事業を展開する組織が、厳格なセキュリティ法を持つ別の国に新たなオフィスを開設した。このような状況において、全体的なセキュリティ戦略は以下の点に基づいて策定されるべきである。
A. 最も厳しい要件。
B. セキュリティ組織構造。
C. リスク評価結果。
D. 国際セキュリティ基準。
正解: **(**正解を表示します**)**
By adopting the most stringent requirements, the organization ensures compliance with the stricter local laws while inherently satisfying the less rigorous home-country standards. This "highest-common-denominator" approach minimizes regulatory risk and provides a uniform security baseline across all locations.

質問: **199**
システムの補償制御を推奨する際に、次のうちどれが最も有用な入力情報でしょうか？
A. 経営上の推奨事項
B. リスク評価結果
C. セキュア構成に関するベンダーのドキュメント
D. 費用便益分析
正解: **(**正解を表示します**)**
Compensating controls are implemented to address identified risks when primary controls cannot be applied. Risk assessment results provide the necessary insight into threat likelihood, impact, and residual risk, making them the most useful input when determining appropriate compensating controls.

質問: **200**
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ことを確実にするために、以下のうちどれが重要ですか？
A. 最新のリスク登録簿
B. ステークホルダーコミュニケーション計画
C. エスカレーション計画
D. 資産分類
正解: **(**正解を表示します**)**
A stakeholder communication plan is critical to ensure that the right stakeholders are informed and can make timely decisions during a cybersecurity incident. It helps outline who needs to be contacted, what information needs to be shared, and when, ensuring coordinated and effective response actions.

質問: **201**
情報セキュリティプログラムの有効性を示す最良の証拠となるのは、次のうちどれですか？
A. 規制要件への準拠に関するギャップ分析
B. 主要業績評価指標(KPI)
C. 主要リスク指標(KRI)
D. 第三者による侵入テスト
正解: **B (**コメントを発表する**)**
KPIs measure how well the information security program is performing against defined objectives.
They provide ongoing evidence of program effectiveness, such as control implementation, training completion, incident response performance, patching performance, and policy compliance.

質問: **202**
ビジネスインパクト分析(BIA)の主な成果は次のうちどれですか？
A. イベントトリアージの効率化とインシデント対応手順の実施
B. 技術的なセキュリティ対策およびセキュリティ文化の強化のための予算配分
C. 業界固有の規制への準拠の保証と業務プロセスの改善

D. 重要な業務機能の特定と復旧活動の優先順位付け
正解: **(**正解を表示します**)**
The primary outcome of a Business Impact Analysis (BIA) is the identification of critical business functions and the prioritization of recovery efforts based on the potential impact of disruptions.
This enables informed decisions for continuity planning and resource allocation to minimize operational and financial impacts during incidents.

質問: **203**
事業継続計画(BCP)のテストを実施する最大のメリットは次のうちどれですか？
A. 回復期におけるチームの関与を確保する
B. 復旧責任の割り当ての確認
C. 回復成功の可能性を高める
D. 復旧プロセスにおける技術の信頼性向上
正解: **C (**コメントを発表する**)**
The greatest benefit of business continuity plan (BCP) testing is ensuring that the organization can successfully recover operations in the event of a disruption. Testing identifies gaps, weaknesses, and areas for improvement, leading to a more effective and reliable recovery process. While team engagement, responsibility assignment, and technology reliability are important, they are secondary benefits that contribute to the primary goal of ensuring successful recovery.

質問: **204**
企業向け暗号化インフラストラクチャを構築またはアップグレードする際、成長するビジネス環境にとって最も重要な要件は次のうちどれですか？
A. スケーラブルなアーキテクチャとシステム
B. サービスディスカバリ
C. ネットワークスロットリング
D. バックアップおよび復元機能
正解: **(**正解を表示します**)**
In growing business environments, the most critical requirement for cryptographic infrastructure is having scalable architectures and systems. As the organization expands, the infrastructure must efficiently support increased encryption demands, certificate management, and key lifecycle operations without degrading performance.

質問: **205**
情報セキュリティ戦略を策定する際の最初のステップとして、次のうちどれを行うべきでしょうか？
A. 現状に基づいてギャップ分析を実施する。
B. 情報セキュリティを推進する主要な関係者を特定する。
C. 情報セキュリティリスクの許容レベルを決定する。
D. セキュリティの基準と制御を特定するためのロードマップを作成する。
正解: **C (**コメントを発表する**)**
An information security strategy must be driven by the organization's risk appetite/tolerance.

Before defining controls, roadmaps, or gap remediation, the organization must know what level of information security risk is acceptable in relation to business objectives.

質問: **206**
効果的な情報セキュリティ意識向上プログラムの最大のメリットは、組織が以下のことができるようになることです。
A. コンプライアンス要件を満たしている。
B. 有意義な指標を開発する。
C. 説明責任を確立する。
D. セキュリティインシデントを削減する。
正解: **(**正解を表示します**)**
The greatest benefit of an effective information security awareness program is its ability to reduce security incidents. By educating employees on security risks and best practices, the organization minimizes human error and improves the overall security posture.

質問: **207**
ランサムウェア攻撃への対応として、最初にとるべき行動は次のうちどれですか？
A. 鑑識チームに連絡してください。
B. バックアップの可用性を確認してください。
C. 影響を受けているデバイスをネットワークから切断します。
D. 上級管理職にこの出来事を報告する。
正解: **C (**コメントを発表する**)**
The first action in response to a ransomware attack should be to disconnect the impacted devices from the network. This helps contain the spread of the ransomware and prevents it from affecting other systems, allowing for further investigation and mitigation steps to be taken.

質問: **208**
情報セキュリティ管理者は、パッチを適用できないWeb接続型のレガシーアプリケーション上のデータを保護するための選択肢を検討しています。以下のうち、補償制御の有効性について最も適切な情報を提供するものはどれでしょうか？
A. ファイアウォールルール
B. 脅威評価
C. 侵入検知システム(IDS)ログ
D. 侵入テスト
正解: **(**正解を表示します**)**
The option that would provide the best information about the effectiveness of compensating controls for protecting a web-facing legacy application that cannot be patched is penetration testing. Penetration testing simulates real-world attacks to evaluate whether the compensating controls effectively protect the application from potential threats and vulnerabilities.

質問: **209**
事業継続計画(BCP)を作成する主な理由は、インシデント発生時の対応です。
A. エスカレーションとトリアージ。
B. 識別とコミュニケーション。
C. 予防と緩和。
D. 報告と対応の開始。
正解: **(**正解を表示します**)**
A business continuity plan is primarily created to ensure critical business functions can continue (or be restored quickly) during disruptive events, which is focused on mitigating the business impact of incidents rather than incident handling steps like triage or reporting.

質問: **210**
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. 戦略。
B. リスク評価。
C. 主要業績評価指標 (KPI)。
D. 標準。
正解: **(**正解を表示します**)**
Business objectives and organizational risk appetite are most useful inputs to the development of information security strategy. Understanding these elements ensures that the information security strategy aligns with the overall goals of the organization and addresses the level of risk that the organization is willing to accept.

質問: **211**
社内開発アプリケーションに新たな脆弱性が出現する傾向に対処するために、情報セキュリティマネージャーが最初にとるべきステップは次のうちどれでしょうか？
A. 開発者の参加を義務付けたセキュリティ委員会を設置する。
B. 開発者の求人情報にセキュリティ要件を追加する。
C. 本番環境のアプリケーションに対して侵入テストを実施します。
D. 既存の変更管理プロセスの有効性を評価する。
正解: **(**正解を表示します**)**
The first step should be to evaluate the change management process to determine if security controls are being properly integrated into the development lifecycle. If vulnerabilities are consistently emerging, there may be gaps in secure coding practices, testing, or review processes. Identifying weaknesses in change management helps ensure that security is embedded in development and deployment processes, reducing future vulnerabilities.

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

ス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu 1193問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **212**
サイバー攻撃の撲滅計画を立てる際に、最も重要な考慮事項は次のうちどれですか？
A. 根絶チームのスキルと能力
B. プロセスに必要なツールと労力のコスト
C. 脅威の種類と発生源に関する知識
D. オペレーティングシステムのクリーンなバックアップを取得する
正解: **C** (コメントを発表する)

質問: **213**
オンライン銀行がネットワークへの不正侵入を検知した場合、まず最初に何をすべきでしょうか？
A. 影響を受けたネットワークセグメントを隔離する
B. インシデント対応計画を発動する
C. 機密情報が漏洩していないか評価する
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)
Once a successful intrusion is identified, the first step is to activate the formal incident response plan so containment, investigation, escalation, evidence handling, communication, and regulatory steps are coordinated properly.

質問: **214**
上級管理職は最近、業界のベスト プラクティスに反するモバイル アクセス ポリシーを承認しました。組織のネットワークへのモバイル アクセスに関するセキュリティ標準を開発する場合、情報セキュリティ マネージャーにとって最善の行動方針は次のどれですか。
A. 標準を組織のポリシーに合わせます。
B. 標準を業界のベストプラクティスに合わせます。
C. 標準を開発する前に矛盾を解決します。
D. 標準をポリシーに適合させることの費用対効果分析を実行します。
正解: **B** (コメントを発表する)
The information security manager's best course of action when developing security standards for mobile access to the organization's network is to align the standards with industry best practices.
This approach ensures that the standards incorporate proven security measures that help protect the organization's assets and data, even if they conflict with the organizational policy approved by senior management.
While it's important to be aware of the organizational policy, prioritizing industry best practices helps mitigate risks and ensures that the organization's security posture remains robust and compliant with recognized standards, which can be critical for regulatory and operational success.

質問: **215**

ある組織が、自社開発のアプリケーションを、Platform as a Service(PaaS)モデルを使用するサードパーティのクラウドホスティングプロバイダーに移行したいと考えています。クラウドプロバイダーを選定する前に、組織にとって最も重要な確認事項は何でしょうか？
A. クラウドプロバイダーは、復旧目標時点(RPO)を満たすことができます。
B. クラウドプロバイダーは適用される規制を遵守します
C. ホスティング契約には解約条項があります
D. クラウドプロバイダーのサービスレベル契約(SLA)には可用性要件が含まれています
正解: **B** (コメントを発表する)
Before selecting a PaaS cloud provider, it is most important to ensure regulatory compliance.
Hosting sensitive or proprietary data with a provider that does not adhere to relevant laws and regulations can expose the organization to legal, financial, and operational risks.

質問: **216**
提供されるサービスのセキュリティに対処するために、ベンダー選定プロセスを改善するための最良の方法は次のうちどれですか？
A. 侵入テストを実施して、制御上の欠陥を特定する
B. セキュリティ上の欠陥を特定するためのリスク評価の実施
C. 定期的なセキュリティ監査を実施し、管理上の不備を特定する
D. ベンダーにセキュリティ上の欠陥を報告することを契約で義務付ける
正解: (正解を表示します)
Performing risk assessments during vendor selection systematically identifies security deficiencies before engagement and ensures decisions are based on risk exposure. This proactive evaluation directly strengthens the selection process by integrating security risk analysis into procurement decisions.

質問: **217**
CI/CDパイプラインにおけるセキュリティインシデントを封じ込めるための最善の対策は、次のうちどれですか？
A. ビルドを変更せずにログ記録を増やす。
B. 本番環境を無効にします。
C. 最後に確認された安全なビルドに戻します。
D. すべての開発者アカウントを直ちに無効にします。
正解: (正解を表示します)
In a CI/CD pipeline incident, the best containment action is to stop the unsafe change from continuing and restore a trusted build state. Reverting to the last known secure build limits exposure while preserving service availability.

質問: **218**
ウェブサーバーの重大な脆弱性に起因する不正なネットワークアクセスを伴うサイバーインシデントの根本原因を最も効果的に解決できる対策は、次のうちどれですか？
A. パッチ適用プロセスの改善
B. 不正アクセスによりアカウントをロックする
C. 影響を受けるシステムの隔離

D. 悪意のあるネットワーク接続の終了
正解: **(**正解を表示します**)**
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a

質問: **219**
以下のうち、取締役会および経営陣に対し、情報セキュリティプログラムの現状に関する最も重要な情報を伝えるのはどれですか？
A. 業界競合他社のリスクプロファイル
B. 過去のインシデント管理指標
C. 新たな脅威の状況
D. 組織の現在のリスクプロファイル
正解: **D (**コメントを発表する**)**
The current risk profile of the organization provides board members and executives with the most meaningful insight into the organization's security posture, key risks, and potential impact on business objectives. This information helps in strategic decision-making, resource allocation, and risk management. While industry risk profiles, historical metrics, and emerging threats are useful, they do not provide a direct view of the organization's specific security risks.

質問: **220**
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. 情報セキュリティ管理者
B. 上級管理職
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**)**
The person best suited to own the risk discovered in an application is the system owner. The system owner is responsible for the application and its operations, including managing risks associated with it. They are best positioned to make decisions about how to address or mitigate the risk based on business priorities and resource availability.

質問: **221**
情報セキュリティ対策の有効性を経営陣に示すために、最も適切な指標は次のうちどれですか？
A. パッチ適用済みのサーバーの割合
B. マルウェア感染によるシステム停止
C. セキュリティインシデントに起因する年間損失
D. ネットワークスキャンで発見されたセキュリティ脆弱性の数
正解: **(**正解を表示します**)**

質問: **222**

第三者との既存の契約において、組織の顧客データを保護するための要件が明確に規定されていない場合、次のうちどれが最善の対応策でしょうか？
A. 許容できないリスクのため、アウトソーシング契約を解除する。
B. 監査権条項を発動して、要件と管理をレビューする。
C. 契約および組織の要件に対するギャップ分析を実施する。
D. セキュリティパフォーマンスを見直して契約を再交渉する。
正解: **C** (コメントを発表する)
The first step is to identify exactly what is missing by comparing the current contract against the organization's customer data protection requirements. This provides a factual basis for remediation, such as contract amendment or renegotiation.

質問: **223**
組織全体の新しい情報セキュリティプログラムへの支持を得るための最良の方法は、次のうちどれですか？
A. 情報セキュリティ戦略委員会を設置する。
B. 類似の業界組織とのベンチマーク。
C. 組織全体を対象としたフィッシングキャンペーンを実施する。
D. 情報セキュリティRACIチャートを公開する。
正解: (正解を表示します)
A Strategy Committee (consisting of senior executives from across the business) ensures that the program is aligned with business goals. When the business leaders help build the strategy, they naturally support it.

質問: **224**
アプリケーションの脆弱性を防止するために、DevSecOps環境において最も重要なセキュリティ対策は次のうちどれですか？
A. 継続的インテグレーション／継続的デプロイメント(CI/CD)パイプラインへのセキュリティテストの統合
B. 開発者によるセキュリティログおよび機密性の高いシステムテレメトリへのアクセスを制限し、不正使用を防止する。
C. 静的アプリケーションセキュリティテスト(SAST)を使用して、本番環境のアプリケーションに対する年次コードレビューを実施する
D. モノリシックアーキテクチャを採用することで、本番環境における攻撃対象領域の複雑さを軽減する。
正解: (正解を表示します)
DevSecOps requires security to be embedded early and continuously in the development lifecycle. Integrating security testing into the CI/CD pipeline helps detect vulnerabilities before code reaches production.

質問: **225**
最高情報セキュリティ責任者(CISO)は、財務、運用、評判に様々な影響を与える複数の重大なリスクを特定しました。組織のリスク許容度に見合ったリスク対策を選択する上で、最も効果的なアプローチは次のうちどれでしょうか？
A. 特定されたすべての重大なリスクに対処するために、均等な予算を割り当てる。
B. 最短時間で実施できる対策を優先する。

C. 組織のリスク基準を、リスク対策戦略を選択する際の重要な要素として使用する。
D. リスク対策費用を含め、財務上の影響が最も大きいリスクのみに焦点を当てます。
正解: **(**正解を表示します**)**
The most effective approach is to use the organization's risk criteria, which includes the organization's risk appetite, to guide the selection of appropriate risk treatment strategies. This ensures that the treatment decisions align with the organization's capacity to absorb and manage risks, considering factors such as financial impact, operational impact, and reputational risk. By considering these criteria, the organization can make well-informed decisions that balance risk reduction with cost, resources, and strategic objectives. While prioritizing time or focusing only on financial impacts may be short-sighted, using the overall risk criteria provides a holistic approach to risk management.

質問: **226**
組織内で情報セキュリティ文化を確立するために最も貢献するのは、次のうちどれですか？
A. 情報セキュリティに関する業界のベストプラクティスに従う
B. 定期的な情報セキュリティ意識向上活動の実施
C. 情報セキュリティポリシーの経営陣の承認を得る
D. ソフトウェア開発ライフサイクルに情報セキュリティ要件を組み込む
正解: **(**正解を表示します**)**
Regular awareness initiatives educate and engage employees at all levels, reinforcing secure behavior and integrating information security into daily practices, which is essential for building and sustaining a strong security culture.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu ↾**193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **227**
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."
Even if some findings are unfixed or reclassified, the lack of any classification process undermines the whole risk management effort.

質問: **228**
経営陣は、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ことを懸念している。情報セキュリティマネージャーがこの懸念に対処するためにシステムを調整したことを最もよく示しているのは、次のうちどれか？
A. 偽陽性の減少
B. 偽陽性の増加
C. 偽陰性の増加
D. 偽陰性率の低下
正解: **(**正解を表示します**)**
Disruptions from an IPS are most commonly caused by false positives blocking legitimate traffic.
Tuning the IPS to decrease false positives reduces unnecessary business interruptions while maintaining effective prevention.

質問: **229**
組織の災害復旧準備として最も効果的なのは次のうちどれですか？
A. フェイルオーバーテスト
B. インシデント対応ポリシー
C. 事業継続計画(BCP)
D. セキュリティ意識向上トレーニング
正解: **(**正解を表示します**)**
A business continuity plan (BCP) best prepares an organization for disaster recovery by defining how critical business functions will continue during and after a disruption, including recovery priorities and coordination needed to support disaster recovery activities.

質問: **230**
情報セキュリティ意識向上プログラムが効果的であることを示す最良の指標は、次のうちどれですか？
A. 情報セキュリティプログラムの維持コストの削減
B. 報告された情報セキュリティインシデント数の減少
C. ソーシャルエンジニアリング攻撃の成功率の低下
D. 情報セキュリティ攻撃の件数の減少
正解: **(**正解を表示します**)**

A reduction in the success rate of social engineering attacks is the best indication of an effective security awareness program because it directly reflects user behavior change and increased vigilance - which are core goals of awareness efforts.

質問: **231**
組織内で強固な情報セキュリティ文化を構築するために、以下のうちどれが最も重要ですか？
A. 従業員による組織のセキュリティポリシーの遵守を厳格に徹底する
B. 情報セキュリティポリシーに対する上級管理職の承認
C. IT環境の開発および運用に組み込まれたセキュリティ制御
D. 組織全体における成熟した情報セキュリティ意識向上トレーニング
正解: **(**正解を表示します**)**

質問: **232**
ログ分析の実施は、インシデント管理ライフサイクルのどの段階に該当しますか？
A. 事件後
B. 計画
C. 封じ込め
D. 検出
正解: **(**正解を表示します**)**
Log analysis is primarily used during the detection phase to identify and confirm the presence of incidents or suspicious activities within the environment.

質問: **233**
組織がソーシャルメディアポリシーを策定する最も重要な理由は以下のとおりです。
A. マルウェアの拡散を防ぐ。
B. 従業員の生産性を向上させる。
C. 会社のブランドを守る。
D. 従業員のインターネット上の活動を監視する。
正解: **(**正解を表示します**)**
The most important reason for an organization to establish a social media policy is to protect the company brand. A clear policy helps ensure that employees represent the organization appropriately online, preventing potential damage to the company's reputation, brand image, or legal standing.

質問: **234**
サービス契約の以下の要素のうち、組織がクラウドサービスプロバイダーに関連する情報セキュリティリスクを監視するのに最も適しているのはどれですか？
A. 補償条項
B. コンプライアンス状況報告
C. サービス提供者の施設への物理的なアクセス
D. 侵害検知および通知

正解: **B** (コメントを発表する)
Cloud providers rarely allow physical access or custom audits. Regular compliance reports (like SOC 2 Type II or ISO 27001 certificates) provide the Information Security Manager with independent verification that the provider's controls are functioning correctly.
Unlike a "breach notification" (which only tells you after a failure has occurred), compliance reporting allows for the proactive monitoring of the provider's adherence to agreed-upon security standards.
These reports serve as the primary data source for the organization's ongoing risk assessments, ensuring the provider remains within the organization's risk appetite.

質問: **235**
セキュリティインシデントを効果的に封じ込めるためのアプローチを策定する際に、最も重要な考慮事項は次のうちどれですか？
A. インシデント封じ込めに対する上級管理職の責任の割り当て
B. インシデントの影響を受けたシステムを本番環境から隔離する
C. 事業に影響を与える可能性のある評判の損害を軽減する
D. 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
正解: **B** (コメントを発表する)
The most important consideration for effective incident containment is isolating affected systems to prevent the spread of the threat and limit further damage to the production environment.

質問: **236**
上級管理職は、ミッションクリティカルなシステムの災害復旧計画 (DRP) を徹底的にテストしたいと考えています。
次のどれが最も信頼性の高い結果をもたらすでしょうか?
A. 完全中断テスト
B. 並列テスト
C. シミュレーションテスト
D. 構造化されたウォークスルー
正解: (正解を表示します)
A full interruption test provides the most reliable results because it involves shutting down the mission-critical system and actually testing the recovery procedures in a real-world scenario. This type of test validates the effectiveness and readiness of the disaster recovery plan under actual operational conditions, ensuring that all systems, processes, and teams are prepared to respond to a true disaster. While parallel, simulation, and walk-through tests are valuable for assessing aspects of the DRP, they do not offer the same level of assurance as a full interruption test.

質問: **237**
組織にセキュリティリスク管理を導入する際に最も重要なことは、以下の点を確実にすることです。
A. リスク管理手法は確立されたフレームワークに従います。
B. 情報セキュリティポリシーが文書化され、理解されている。

C. リスク処理プロセスが定義されています。
D. 事業部門がリスク管理手法を承認する。
正解: **D (**コメントを発表する**)**

質問: **238**
新しいセキュリティ対策のビジネスケースを作成する際、情報セキュリティマネージャーはまず最初に以下の点に留意する必要があります。
A. 実現可能性調査を実施する。
B. 総所有コスト(TCO)を計算します。
C. 費用対効果分析を実施する。
D. 対処すべき課題を定義する。
正解: **D (**コメントを発表する**)**
https://www.cisa.gov/sites/default/files/2023-02/ISC_making_a_business_case_for_security_2023_edition_508c.pdf?es_id=f3da987c27

質問: **239**
情報セキュリティ運営委員会の有効性にとって、以下のうちどれが最も重要ですか？
A. 委員会はリスク管理フレームワークを使用しています。
B. 委員会は規制に関する豊富な知識を有している。
C. 委員会は上級管理職の代表者で構成されています。
D. 委員会は複数の組織から代表者を選出しています。
正解: **(**正解を表示します**)**
The most important factor for the effectiveness of an information security steering committee is that the committee has cross-organizational representation. This ensures that the perspectives and needs of different departments and business units are considered, allowing for comprehensive decision-making and alignment of security strategies with overall business objectives.

質問: **240**
災害復旧戦略を策定する際に考慮すべき最も重要な要素は次のうちどれですか？
A. ベンダーの能力と代替復旧拠点の近接性
B. 最大許容ダウンタイム(MTD)および許容データ損失
C. 年間損失期待値(ALE)およびリスクエクスポージャー
D. 復元するデータ量と復旧するストレージメディアの容量
正解: **(**正解を表示します**)**
Disaster recovery strategies must align with business requirements for service availability and data protection. Maximum tolerable downtime (MTD) defines how long a system can be unavailable, and acceptable data loss defines recovery point objectives. These business-driven thresholds are the primary determinants of the recovery strategy.

質問: **241**

新しいセキュリティソリューションを導入する上で、最も適切な正当化理由となるのはどれでしょうか？
A. 内部監査結果
B. ビジネスケース
C. インシデント管理レポート
D. リスク分析レポート
正解: **B** (コメントを発表する)
A business case offers a comprehensive evaluation of a proposed security solution, detailing its benefits, costs, risks, and alignment with organizational objectives. It serves as a decision-making tool, enabling stakeholders to assess the value and feasibility of the investment. By presenting a clear rationale, a business case facilitates informed decisions regarding the allocation of resources for security initiatives.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu ↾**193**問、３０%ディスカウント、特別な割引コード:**JPNshiken**」

質問: **242**
組織にとって、脆弱性スキャンツールの主な利点は次のうちどれですか？
A. 組織プロセスにおける脆弱性の特定
B. ネットワーク上のデバイスがもたらす潜在的なリスクを特定する
C. 複雑な脆弱性を見逃さないようにする
D. 情報セキュリティリスク分析プログラムの自動化
正解: (正解を表示します)
The primary benefit of a vulnerability scanning tool is its ability to identify potential security weaknesses in devices on the network, enabling timely remediation to reduce exposure to threats.

質問: **243**
セキュリティ対策の有効性を最も確実に保証できるのは、次のうちどれですか？
A. 内部監査結果
B. リスク評価
C. 自己評価
D. 独立試験
正解: (正解を表示します)
Independent testing provides the best assurance of a security control's effectiveness because it offers an unbiased, external evaluation of how well the control functions in practice, without internal bias or conflicts of interest.

質問: **244**

情報セキュリティマネージャーが作成した、複数のコンポーネントからなるIDおよびアクセス管理(IAM)イニシアチブのコスト見積もりは、単一の実装では費用がかかりすぎ、複雑すぎる。コンポーネントの優先順位付けに最適な方法は何か？

A. 金銭的な利益に基づいて評価してください。
B. 導入コストに基づいて評価します。
C. 実装の容易さに基づいて評価してください。
D. 残存リスクの低減度合いに応じて評価します。

正解: **D** (コメントを発表する)

The best way to prioritize the components of an IAM initiative is by rating them according to the reduction in residual risk. This approach ensures that the components that address the most critical security risks are implemented first, improving the organization's overall security posture. It aligns the implementation with the organization's risk management priorities.

質問: **245**

効果的なサイバーセキュリティインシデント管理において、以下のうち最も重要なものはどれですか？

A. 早期発見と対応
B. 定期的な卓上運動
C. 根本原因分析
D. 捜査および鑑識

正解: **A** (コメントを発表する)

https://www.nextdlp.com/resources/blog/cyber-security-incident-management-guide

質問: **246**

新しい規制では、組織は1年以内にすべてのモバイルデバイス上の機密性の高い顧客情報を暗号化することが義務付けられています。コンプライアンスへの準備として、最初に行うべき手順は次のうちどれでしょうか？

A. 既存の管理策と新しい要件との間のギャップを特定する。
B. 要件を満たす暗号化ソリューションを実装するための計画を策定する。
C. モバイルデバイス暗号化ソリューションのビジネスケースを作成する。
D. リスク評価を実施して、補償制御を決定する。

正解: (正解を表示します)

The first step is to perform a gap analysis to determine the difference between current mobile device security controls and the new regulatory encryption requirement. Understanding the current state versus required state establishes the baseline necessary to plan remediation, allocate resources, and ensure timely compliance.

質問: **247**

以下のうち、情報セキュリティプログラムに対する経営陣の支持を最もよく示しているのはどれですか？

A. セキュリティポリシーと手順の実施
B. 組織全体でのセキュリティ意識向上トレーニングの実施を義務付ける
C. 十分なセキュリティ資源と資金の提供
D. セキュリティニーズに関して各事業部門からフィードバックを募る

正解: (正解を表示します)
Providing adequate resources and funding is the clearest demonstration of senior management support because it reflects executive commitment to enable the security program to meet business objectives and manage risk effectively.

質問: **248**
以下のうち、Webベースのアプリケーション攻撃を最も効果的に軽減できるのはどれですか？
A. 侵入検知システム(IDS)の導入
B. データ入力の検証
C. トランスポート層セキュリティ(TLS)の利用
D. 境界にステートフル検査ファイアウォールを採用する
正解: **B** (コメントを発表する)
Validating data input is the best way to mitigate web-based application attacks, such as SQL injection, cross-site scripting (XSS), and buffer overflows. Proper input validation ensures that malicious or unexpected data is rejected before it can exploit vulnerabilities in the application.
While IDS, TLS, and firewalls provide important security measures, they do not directly prevent application-layer attacks caused by unvalidated input.

質問: **249**
情報セキュリティ ポリシーを策定する際に、さまざまな事業部門の関係者を関与させる主な理由は何ですか。
A. セキュリティ侵害への対処責任を共有する
B. 組織全体でポリシーの受け入れを得る
C. IT部門の作業負荷を軽減する
D. 政策開発の全体的なコストを削減する
正解: (正解を表示します)
Involving stakeholders from various business units promotes buy-in, relevance, and adherence.
When users feel they've had input in shaping the policy, they're more likely to support and follow it. Stakeholders also provide insights into business processes that help ensure policies are practical and tailored. This collaboration enhances organizational alignment and ensures policies do not create unintended operational friction.
"Stakeholder involvement is key to ensuring that policies are practical, aligned with operations, and accepted throughout the organization."

質問: **250**
事業継続計画のどの段階でリスク特定が行われるのか？
A. 開発
B. 影響分析
C. プロジェクト計画
D. 関係者会議
正解: (正解を表示します)

質問: **251**
ランサムウェア攻撃に対する最も効果的な対策はどれですか？
A. システムの自動隔離
B. 徹底したコミュニケーション計画
C. 強力なパスワード要件
D. 効果的なバックアップ計画とプロセス
正解: **(**正解を表示します**)**
The most effective response against ransomware attacks is having strong backup plans and processes. Regular, secure backups ensure that an organization can recover its critical data if it becomes encrypted by ransomware, reducing the impact and minimizing downtime without paying the ransom.

質問: **252**
火災関連災害に対して実施された物理的および環境的セキュリティ対策の有効性を評価するための最良の方法は、次のうちどれですか？
A. 災害復旧計画(DRP)を確認する。
B. 避難訓練を実施する。
C. 啓発セッションを実施する。
D. 緊急時対応チームの手順を確認する。
正解: **(**正解を表示します**)**
Evacuation exercises directly test the effectiveness of physical and environmental security controls in real-world scenarios, revealing gaps and ensuring preparedness for fire-related disasters.

質問: **253**
情報セキュリティマネージャーが、組織のセキュリティ意識向上プログラムを更新し、ランサムウェアに関するトレーニングを追加する予定です。関連資料を作成する際に、最も重要な考慮事項は次のうちどれですか？
A. 研修実施までの期間
B. 過去のランサムウェア事件に関する統計
C. 1日あたりに受信するフィッシングメールの数
D. 研修の対象者
正解: **(**正解を表示します**)**
Security awareness content must be tailored to the intended audience to ensure relevance, comprehension, and behavioral impact. Different roles have different risk exposures and responsibilities, so aligning the material with the audience is most critical for effectiveness.

質問: **254**
情報セキュリティ管理指標を作成する際に、定義することが最も重要な項目は次のうちどれですか？
A. 予算
B. 目的
C. ポリシー
D. ベンチマーク

正解: **(**正解を表示します**)**
https://secureframe.com/blog/cybersecurity-metrics-and-kpis

質問: **255**
以下のうち、脆弱性管理プロセスの有効性を最もよく示しているのはどれですか？
A. 第三者機関による監査結果
B. 内部脆弱性スキャンの結果
C. 脆弱性管理のための予算配分
D. 展開前にパッチをテストするのに必要な時間
正解: **(**正解を表示します**)**
The best indicator of the effectiveness of the vulnerability management process is the results from internal vulnerability scans. These scans help identify weaknesses in the system, track the resolution of vulnerabilities over time, and assess how well the organization is addressing security gaps. Regular vulnerability scans provide direct, actionable data to evaluate the success of the vulnerability management program. While third-party audits, budget allocation, and patch testing times are relevant, they do not provide the same continuous and detailed feedback as internal vulnerability scans.

質問: **256**
外部ソースから報告されたソフトウェアのバグは、影響を受けるアプリケーションを評価するために、次のうちどのプロセスをトリガーするべきでしょうか？
A. 継続的な改善
B. 根本原因分析
C. 脆弱性管理
D. 問題管理
正解: **C (**コメントを発表する**)**
When a software bug is reported by external sources, it should trigger the vulnerability management process, which involves identifying, assessing, prioritizing, and remediating vulnerabilities in affected applications. This ensures that security risks are properly managed and mitigated. While root cause analysis and problem management help in identifying underlying issues, vulnerability management is the most relevant process for assessing security risks related to software bugs.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu ↑**193**問、３０%ディスカウント、特別な割引コード**:** **JPNshiken**」

質問: **257**

セキュリティインシデントが確認された後、情報セキュリティマネージャーが最初に考慮すべき事項は次のうちどれですか？
A. インシデント報告基準の策定
B. 封じ込め手順の実行
C. 事業運営の復旧
D. 根本原因の特定
正解: **(**正解を表示します**)**
https://insecurityinsight.org/wp-content/uploads/2020/02/2018_08_24_ECHO_SIIM-User-Guide-Eng.pdf

質問: **258**
量子コンピューティング技術が情報セキュリティにもたらす最大の脅威は、次のうちどれですか？
A. 量子コンピュータは、データの機密性を保護する現在のいくつかの暗号化方式を破ることができます。
B. 量子コンピュータは安全な通信を可能にするが、それを利用できるごく一部の人だけが恩恵を受ける。
C. 量子コンピュータは、大規模なデータセットを極めて高速に処理することで、可用性を損なう可能性があります。
D. 量子コンピュータは、従来のコンピュータでは処理できない複雑な物理システムをシミュレートできます。
正解: **(**正解を表示します**)**
The greatest threat posed by quantum computing to information security is its potential to break widely used encryption algorithms, such as RSA and ECC, which are foundational to data confidentiality. Quantum algorithms like Shor's algorithm can factor large integers efficiently, undermining the security of current public-key cryptosystems.

質問: **259**
情報セキュリティ管理者が、新興技術による脅威状況の変化を特定するのに最も役立つのは、次のうちどれですか？
A. 脅威インテリジェンスフィード
B. 定期的なリスク評価
C. 業界他社とのベンチマーク
D. 年次セキュリティ脅威評価
正解: **(**正解を表示します**)**
Threat intelligence feeds provide timely, continuously updated information on new threats, tactics, and vulnerabilities - making them the best way to identify changes in the threat landscape driven by emerging technologies.

質問: **260**
従業員が電子メールで送信された疑わしいリンクをクリックしたと報告した場合、情報セキュリティ管理者はまず次のうちどれを行うべきでしょうか？
A. 必須のセキュリティ意識向上トレーニングをスケジュールしてください。
B. ユーザーのアカウントをロックします。
C. 事件を調査し、確認する。

D. ユーザーのコンピュータを無効化し、隔離します。
正解: **(**正解を表示します**)**
The first step is to investigate and confirm whether an incident has occurred (e.g., analyze the email/link, check endpoint and network indicators). This ensures actions like account lock or device quarantine are appropriate and proportionate, avoiding unnecessary disruption.

質問: **261**
情報セキュリティマネージャーが、インシデント対応計画に含めるデジタルフォレンジック調査を支援するための手順書を作成しています。関連する要件について、次のうちどれが最適な情報源となるでしょうか？
A. 上級管理職
B. 情報セキュリティ運営委員会
C. 法律顧問
D. リスク所有者
正解: **(**正解を表示します**)**
Digital forensic procedures must ensure evidence is collected, preserved, and handled in a manner that maintains legal admissibility and complies with applicable laws and regulations.
Legal counsel provides the most critical input regarding chain of custody, privacy considerations, regulatory obligations, and potential litigation requirements.

質問: **262**
情報セキュリティフレームワークを採用する際に最も重要なのは、以下の制御策を選択することです。
A. 組織に対するあらゆるリスクを排除する。
B. 組織のビジネスモデルに適用する。
C. 最低限の規制要件を満たしている。
D. 業界標準に準拠しています。
正解: **(**正解を表示します**)**
When adopting an information security framework, it is most important to select controls that apply to the organization's business model. This ensures that the security measures are relevant to the specific needs, operations, and risks faced by the organization, rather than just meeting generic standards or regulatory requirements.

質問: **263**
あるグローバル企業が、本社所在地国よりもデータ保護規制が厳しい国へ事業を拡大する計画を立てています。これらの新たな要件に対応するための最適なアプローチは次のうちどれでしょうか？
A. 新しい国での潜在的な侵害やインシデントをカバーするサイバーセキュリティ保険に加入してください。
B. 現地の事業運営が本社の地理データ保護法に準拠していることを確認する。
C. 法務部門と協力して、現地の規制要件を解釈し、適用可能な管理策を実施する。
D. 新しい国の規制に合わせて、組織全体のセキュリティポリシーを調整する。
正解: **(**正解を表示します**)**

The best approach is to work with legal experts to interpret the local regulatory requirements and implement applicable controls. This ensures that the organization complies with the stricter data protection laws of the new country while maintaining alignment with business objectives and mitigating potential legal and regulatory risks.

質問: **264**
インシデント対応活動の一環として、復旧プロセスを開始する最適なタイミングは、以下の後です。
A. インシデント対応チームが設立されました
B. 根本原因が特定されました
C. インシデントマネージャーがインシデントを宣言しました
D. 根絶段階が完了しました
正解: **(**正解を表示します**)**
Recovery should begin only after the eradication phase is completed to ensure that all malicious components have been fully removed and the environment is safe to restore and resume normal operations.

質問: **265**
効果的なインシデント管理プログラムを示す最良の指標は次のうちどれですか？
A. 事件発生時の迅速な検知と対応の改善
B. 報告されたセキュリティインシデント数の減少
C. 報告されたセキュリティインシデント数の増加
D. インシデント対応のための資金とリソースの強化
正解: **(**正解を表示します**)**
The best indicator of an effective incident management program is improved speed and efficiency in detecting and responding to incidents, demonstrating that the program is functioning as intended.

質問: **266**
ある組織が、重要なシステムに影響を与える大規模なセキュリティインシデントに見舞われた。
システムを別の場所に復旧するという決定が下された場合、どの計画を実行すべきでしょうか？
A. インシデント対応計画
B. コミュニケーションプラン
C. 災害復旧計画(DRP)
D. 事業継続計画(BCP)
正解: **(**正解を表示します**)**
In the case of a large-scale security event impacting a critical system, and the decision to restore the system at an alternate location, the appropriate plan to invoke is the Disaster Recovery Plan (DRP). The DRP focuses on restoring systems, data, and IT services after a major disruption, including relocating operations to an alternate site.

質問: **267**
セキュリティの観点から、SaaS(Software as a Service)プロバイダーを活用する計画を立てる際に、最も重要な考慮事項は何ですか？
A. 定期的な侵入テストの実施

B. 上級管理職の意見を得る
C. デューデリジェンスの実施
D. データ所有者からの承認を得る
正解: **(**正解を表示します**)**
The most important security consideration when leveraging a SaaS provider is performing due diligence to verify the provider's security controls, compliance posture, and ability to protect the organization's data before onboarding.

質問: **268**
情報セキュリティマネージャーが、失敗したセキュリティプログラムの修復のために採用されました。経営陣向けの情報セキュリティ計画を作成する際の最初のステップは何ですか？
A. 現在のセキュリティ状態を判断します。
B. 具体的なセキュリティソリューションを開発する。
C. コントロールを特定する。
D. 新規イニシアチブのセキュリティ要件を特定する
正解: **(**正解を表示します**)**
Before creating an effective security plan, the information security manager must first assess the current state of security within the organization. This includes evaluating existing security controls, identifying gaps, reviewing past incidents, and understanding the organization's risk posture. This assessment serves as the foundation for developing a strategic security plan that aligns with business objectives and effectively addresses security weaknesses.

質問: **269**
フィッシング攻撃が成功し、機密情報を含む複数のデータベースが侵害されたことが判明した場合、最初に行うべきことは次のうちどれですか？
A. ファイアウォールのポートを閉じます。
B. 上級管理職に警告する。
C. データベースへのアクセスを無効にします。
D. インシデント対応計画を発動する。
正解: **(**正解を表示します**)**
Activating the incident response plan ensures a structured, coordinated, and authorized response aligned with predefined procedures. It initiates proper containment, communication, investigation, and escalation processes in the correct order, preventing ad hoc or uncoordinated actions that could worsen the situation.

質問: **270**
事業影響分析(BIA)は、主に以下の目的で定期的に実施されるべきである。
A. 環境変化に対する脆弱性を検証する。
B. 規制への準拠を確認する。
C. 資産の重要性を分析する。
D. 制御の有効性を検証する。
正解: **(**正解を表示します**)**

A BIA is performed periodically to reassess which business processes and supporting assets are most critical and to confirm impact and recovery priorities as the business changes.

質問: **271**
事業継続計画(BCP)を策定する際に、最初に行うべきことは次のうちどれですか？
A. 現在の復旧政策を見直す。
B. 組織戦略を定義する。
C. 既存のサイバー保険の補償内容を確認する。
D. 重要なプロセスを優先する。
正解: **(**正解を表示します**)**
The first step when developing a business continuity plan (BCP) is to define the organizational strategy. This ensures that the BCP aligns with the overall business objectives and provides a clear direction for recovery efforts in the event of a disruption.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu ↾**193**問、３０%ディスカウント、特別な割引コード**:** **JPNshiken**」

質問: **272**
特定されたリスクに対し、事象の発生確率や影響を軽減するための技術的解決策を適用することで対処しました。適用されたリスク対応策はどれですか？
A. 緩和する
B. 避ける
C. 承認
D. シェア
正解: **A (**コメントを発表する**)**
Applying a technical solution to reduce the likelihood or impact of a risk is an example of risk mitigation. This response involves implementing controls or measures to lower the risk to an acceptable level while still continuing the associated activity.

質問: **273**
情報セキュリティ投資を正当化するためのビジネスケースを作成する際、経営陣が十分な情報に基づいた意思決定を行うために最も役立つのは次のうちどれでしょうか？
A. 情報セキュリティ戦略
B. 業界における証券投資の動向
C. セキュリティインシデントによる損失

D. リスク評価の結果
正解: **D** (コメントを発表する)
https://www.sciencedirect.com/topics/computer-science/risk-assessment-result

質問: **274**
新しいサイバーセキュリティ規制が公布された際に、情報セキュリティ管理者が取るべき最善の行動は次のうちどれでしょうか？
A. セキュリティ戦略を更新する。
B. セキュリティ運用プロジェクト計画をレビューする。
C. セキュリティリスク評価を実施する。
D. セキュリティ指標ダッシュボードを調整します。
正解: **C** (コメントを発表する)
The best course of action is to conduct a security risk assessment to understand how the new regulation affects the organization's risk exposure and obligations, which then drives appropriate updates to strategy, plans, and metrics.

質問: **275**
ある組織は、重要なアプリケーションのセキュリティ脆弱性を修正するには費用がかかりすぎるため現実的ではないと判断したが、その影響は事業にとって重大である。次のうち、最も適切なリスク対策はどれか？
A. アプリケーションの使用を中止してください。
B. アプリケーションの継続使用に伴うリスクを受け入れる。
C. アプリケーションに対する補償制御を実装します。
D. サイバーセキュリティ保険に加入する。
正解: (正解を表示します)
Implementing compensating controls is the most appropriate risk treatment in this scenario. If fixing the vulnerability is too costly, compensating controls can help mitigate the impact of the vulnerability, such as additional monitoring, access restrictions, or network segmentation, to reduce the risk to acceptable levels while still allowing the application to be used.

質問: **276**
ある組織は情報セキュリティインシデントに適切に対応しました。しかし、情報セキュリティマネージャーは、インシデント管理手順に規定されている手順の一部が対応チームによって実行されていなかったことを知りました。情報セキュリティマネージャーが最初にとるべき行動は何でしょうか？
A. インシデント対応チームにインタビューする。
B. インシデント管理手順を確認する。
C. インシデント対応チームに追加のトレーニングを提供する。
D. インシデント管理手順から該当の手順を削除します。
正解: (正解を表示します)
The first step should be to review the incident management procedures to determine if they were unclear, outdated, or impractical. This ensures that the procedures are relevant and actionable, allowing for updates or clarifications before addressing other areas such as training or team actions.

質問: **277**
情報セキュリティ管理者が、組織の脆弱性管理プログラムに欠陥があることを特定しました。関連プロセスの更新を準備する際に、最も重要な考慮事項は次のうちどれですか？
A. 資産管理ツールに不足しているシステムを特定し、更新する。
B. 脆弱性管理研修の義務化。
C. 業界標準フレームワークに基づいた新しい脆弱性管理ポリシーの開発。
D. 主要な関係者からフィードバックを得る。
正解: **(**正解を表示します**)**
The most important consideration when preparing to update vulnerability management processes is engaging key stakeholders for feedback. This ensures that the updated processes align with business needs, address relevant concerns, and have the necessary support from those responsible for execution and decision-making.

質問: **278**
段階的なインシデント復旧アプローチを採用する主な理由は次のうちどれですか？
A. 経営陣の賛同を得るため
B. 修復手順の優先順位付け
C. 重要なシステムが最初に復旧されるようにする
D. 対応チームが事件を分析する時間を与えるため
正解: **(**正解を表示します**)**
The primary reason to use a phased incident recovery approach is to ensure that critical systems are recovered first. This approach helps prioritize recovery efforts based on the importance of systems to business operations, ensuring that the most essential functions are restored as quickly as possible.

質問: **279**
リスクを認識する文化を構築するための最良の方法はどれですか?
A. セキュリティ制御への準拠を定期的にテストします。
B. リスク認識メッセージを定期的に変更します。
C. スタッフがリスクを報告するためのチャネルを確立します。
D. 脅威が文書化され、タイムリーに伝達されるようにします。
正解: **(**正解を表示します**)**

質問: **280**
ある組織が業務機能を外部ベンダーにアウトソーシングする場合、ベンダーがマスター契約に記載されているセキュリティ要件を継続的に遵守していることを経営陣が確実に確認するために、次のうちどれが最も効果的でしょうか？
A. ベンダーの第三者認定評価を定期的にレビューする。
B. ベンダー向けに、組織のセキュリティ要件に関するトレーニングプログラムを企画する。
C. ベンダーサイトで監査権限セキュリティ管理を確立する。
D. 基本契約におけるセキュリティ条項の定期的な再承認を実施する。

正解: (正解を表示します)
Periodic reviews of independent, third-party accredited assessments (e.g., SOC reports, ISO certifications) provide recurring, objective evidence that the vendor's controls continue to operate in line with the contract's security requirements.

質問: **281**
以下のうち、情報セキュリティプログラムに対する経営陣の支持を最もよく示しているのはどれですか？
A. トップダウンコミュニケーション
B. 運営委員会の関与
C. 認定プログラムへの参加
D. 定期的なセキュリティ意識向上トレーニング
正解: (正解を表示します)
Senior management support is best evidenced by active governance participation, not just messaging. Steering committee involvement shows ongoing oversight, decision-making authority, and resource commitment.

質問: **282**
情報セキュリティマネージャーが、組織のワークステーションを新しいオペレーティングシステムバージョンにアップグレードしたいと考えています。アップグレードに対する上級管理職の支持を得るために、次のうちどれが最も役立つでしょうか？
A. ユーザー調査の結果、現在のオペレーティングシステムに問題があることが判明しました。
B. 新しいオペレーティングシステムの最新セキュリティ機能一覧
C. 新オペレーティングシステムにおけるパフォーマンス改善点の概要
D. リスクに基づいた現行オペレーティングシステムの評価
正解: **D** (コメントを発表する)
https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/how-the-ciso-can-build-support-from-senior-management

質問: **283**
新興技術が組織にとって重大なリスクとなる理由を最もよく説明しているのは、次のうちどれですか？
A. 新興技術は偏りが生じやすく、不正確な結果を生み出す可能性があります。
B. リスクが適切に評価されていない可能性があります。
C. 新興技術には規制基準が含まれていない場合があります。
D. 技術的な課題や信頼性のリスクが存在する可能性があります。
正解: (正解を表示します)
Emerging technologies often introduce new, poorly understood risks, and organizations may adopt them before fully assessing security, privacy, regulatory, operational, and third-party impacts.

質問: **284**
以下の活動のうち、災害復旧計画(DRP)が組織の要件を満たしていることを最も確実に保証できるのはどれですか？

A. 組織の事業目標をDRPにマッピングする
B. DRP卓上演習の実施
C. DRPの主要関係者へのインタビューを実施する
D. DRPを業界の同業他社と比較する
正解: **(**正解を表示します**)**
Tabletop exercises simulate disaster scenarios and test the actual response procedures, providing the most assurance that the DRP is practical, effective, and aligned with organizational requirements.

質問: **285**
予告なしに実施される災害復旧訓練の主な目的は何ですか？
A. 目標復旧時間(RTO)を推定する
B. 上級管理職に指標を提供する
C. 職員が状況にどのように反応するかを評価する
D. サービスレベル契約(SLA)を評価する
正解: **C (**コメントを発表する**)**
An unannounced disaster recovery exercise primarily tests real-world readiness by evaluating how personnel respond under realistic conditions (decision-making, communication, execution), rather than measuring RTOs or producing management metrics.

質問: **286**
経営陣が承認したセキュリティポリシーの例外規定により、組織のネットワーク上で不審なインターネットトラフィックに関する警告が予想外に増加している。
以下のうち、最も適切な行動はどれですか？
A. アラートの増加を引き起こすルールを削除します。
B. リスク分析と提言を上級管理職に提示する。
C. 情報セキュリティポリシーを更新する。
D. 経営陣に交通分析結果を提示する。
正解: **(**正解を表示します**)**
The exception was approved by senior management, but it is now creating unexpected security risk indicators. The information security manager should analyze the risk, assess the impact of the suspicious traffic, and present recommendations so management can decide whether to modify, revoke, or formally accept the increased risk.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu ↾**193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **287**
すべての重要な本番サーバーが最新のマルウェア署名ファイルを使用していることを確認する最善の方法は次のとおりです。
A. サーバーの署名ステータスのレポートを生成します。
B. 最近特定された無害なウイルスを使用して、それが隔離されているかどうかをテストします。
C. 最新の署名ファイルを調べて、コンソールと比較します。
D. 署名ファイルが最後に公開された日付を確認します。
正解: **(**正解を表示します**)**
To verify that all critical production servers are using up-to-date malware signatures, the best evidence is a centralized status report showing each server's current signature version/date and update state.

質問: **288**
ある組織は、市場での競争力を維持するために、モノのインターネット（IoT）ソリューションの導入を決定しました。情報セキュリティ対策として、まず最初に取り組むべきものは何でしょうか？
A. リスクプロファイルを再計算する
B. 補償制御を実装する
C. リスク許容度を再評価する
D. セキュリティアーキテクチャを更新する
正解: **(**正解を表示します**)**
When introducing new technologies, the first step is to recalculate the risk profile to identify any new or changed risks.
"The implementation of new technologies should trigger a review of the risk profile to identify and address new exposures."

質問: **289**
特定の個人に管理権を割り当てることの主な利点は次のうちどれですか？
A. 緩和策の実施と維持を支援する
B. セキュリティ意識向上トレーニングの必要性を排除する
C. セキュリティポリシーと手順の必要性を軽減する
D. コントロールテストとレポート作成の効率化
正解: **(**正解を表示します**)**
Assigning control ownership to specific individuals ensures accountability for implementing, monitoring, and maintaining security controls. This improves compliance, risk management, and security posture by ensuring that controls are properly managed over time. While streamlining testing, reducing training needs, or eliminating policies might be secondary effects, the primary benefit is ensuring that mitigation efforts are consistently applied and maintained.

質問: **290**
現在の情報セキュリティ管理に影響を与える新しい規制要件に対応するために、最初に更新する必要があるのは次のどれですか?

A. コントロールマトリックス
B. ビジネス影響分析 (BIA)
C. リスクレジスタ
D. 情報セキュリティポリシー
正解: **D (**コメントを発表する**)**
The document that should be updated first to account for new regulatory requirements impacting current information security controls is the information security policy. The information security policy provides the overarching framework and guidelines for security controls and practices within the organization. Updating it ensures that all subsequent documents, including control matrices, risk registers, and BIAs, align with the new regulatory requirements.

質問: **291**
自動化されたIDおよびアクセス管理(IAM)システムを使用する大規模な多国籍企業にとって、以下のうちどれが最大の課題となるでしょうか？
A. 人事部(HR)からの不正確な従業員データ
B. 組織内での多数のアプリケーション
C. 雇用期間中のユーザーロールの頻繁な変更
D. 業界平均を大幅に上回る従業員離職率
正解: **(**正解を表示します**)**
The greatest challenge to a large multinational organization using an automated identity and access management (IAM) system is inaccurate workforce data from human resources (HR).
Since IAM systems rely on accurate HR data to assign roles and access rights, inaccuracies can lead to improper access permissions, posing security risks and compliance issues.

質問: **292**
組織がチームや個人による優れたセキュリティ行動を特定し、認識するのに最も役立つのは、次のうちどれでしょうか？
A. 仲間からの評価
B. マネージャーのレビュー
C. 内部監査
D. セキュリティトレーニング指標
正解: **(**正解を表示します**)**
Peer recognition is best for identifying and reinforcing positive security behaviors in day-to-day work. It helps make secure behavior visible, valued, and culturally accepted across teams.

質問: **293**
事後検証を実施する上で最も重要な目標は次のうちどれですか？
A. インシデントの総コストを計算する
B. コンプライアンス要件を満たす
C. 事件発生件数の月間傾向の把握

D. 類似事件の影響を軽減する
正解: **D (**コメントを発表する**)**
The primary objective of a post-incident review is to identify lessons learned and improve controls, processes, and response capabilities. By addressing root causes and strengthening preventive and detective measures, the organization reduces the likelihood and impact of similar future incidents.

質問: **294**
新しい情報資産を導入する際、資産所有者の最も重要な責任は何でしょうか？
A. 情報バックアップ
B. 情報アクセス管理
C. 情報廃棄
D. 情報分類
正解: **D (**コメントを発表する**)**
https://bls-staycompliant.co.uk/news/what-is-an-information-asset-owner/

質問: **295**
ビジネス影響分析 (BIA) を実施する主な目的は、次のことを決定することです。
A. 事業継続プログラムの範囲。
B. ビジネスの回復に必要なリソース。
C. 回復時間目標 (RTO)。
D. インシデント対応計画の範囲。
正解: **(**正解を表示します**)**
The primary purpose of conducting a business impact analysis (BIA) is to determine the resources needed for business recovery. A BIA helps identify critical business functions and the impact of disruptions on these functions, allowing organizations to prioritize recovery efforts and allocate the necessary resources effectively.

質問: **296**
以下のうち、インシデント対応計画のテスト実施を保証する責任を負うのは誰ですか？
A. ビジネスプロセスオーナー
B. 事業継続マネージャー
C. インシデント対応チームのメンバー
D. 情報セキュリティマネージャー
正解: **D (**コメントを発表する**)**
The information security manager is accountable for ensuring the incident response plan is tested because incident response falls under the information security program's governance and oversight responsibilities, including validating readiness through exercises and tests.

質問: **297**
情報セキュリティ管理者が、セキュリティ対策が新たな脆弱性に効果的に対処できるようにするための最善の方法は、次のうちどれですか？

A. 定期検査
B. 第三者監査レビュー
C. 管理ギャップ分析
D. 脆弱性管理計画の更新
正解: **A (**コメントを発表する**)**
Conducting periodic control reviews ensures that security controls remain effective in addressing new and emerging vulnerabilities. Regular assessments help identify weaknesses, ensure compliance with security policies, and allow for timely adjustments to security measures. While third-party audits, gap analysis, and vulnerability management updates are useful, they do not provide the ongoing validation of control effectiveness that periodic reviews do.

質問: **298**
災害を適時に宣言する主な目的は以下のとおりです。
A. 事業経営陣が復旧プロセスに関与することを確実にする。
B. 組織の重要なサービスの継続性を確保する。
C. 災害復旧プロセスの欠陥を評価し、修正する。
D. 重要な物理的資産をさらなる損失から保護する。
正解: **(**正解を表示します**)**

質問: **299**
ビジネスインパクト分析(BIA)の主な目的は次のうちどれですか？
A. 情報資産の重要度を判断する
B. 投資収益率(ROI)を算出する
C. インシデントの深刻度レベルを設定する
D. セキュリティの役割と責任を明確にする
正解: **(**正解を表示します**)**

質問: **300**
グローバル組織がインシデント対応チームを編成しています。組織は、すべてのインシデントについて本部に情報を提供し、広範囲に分散した事象に対して統一的な対応ができるようにしたいと考えています。これらの目的を最も効果的にサポートするのは次のうちどれですか？
A. 仮想インシデント対応チーム
B. 外部委託のインシデント対応チーム
C. 中央集中型インシデント対応チーム
D. 分散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 that all incidents are reported to and coordinated through headquarters, supporting unified communication and consistent response across global locations. This approach aligns with the organization's objectives to keep headquarters informed and maintain a unified response to incidents worldwide.

質問: **301**
モバイルデバイスの増加と柔軟性の向上によって生じる最も重大なセキュリティ問題は以下のとおりです。
A. サポートの複雑さ。
B. 脅威への曝露度が高い。
C. 説明責任の欠如。
D. オペレーティングシステムの多様性。
正解: **(**正解を表示します**)**
The rapid growth and flexibility of mobile devices most significantly increases exposure to threats (more endpoints, varied networks, higher likelihood of loss/theft, and expanded attack surface), which drives overall risk upward.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu 「**193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **302**
ある組織が脆弱性評価を実施したところ、多数のサーバーで古いバージョンのソフトウェアが稼働していることが分かりました。この脆弱性を引き起こす可能性が最も高いのは、次のうちどの制御上の不備でしょうか？
A. パッチ管理の不備
B. 未成熟な脆弱性監視
C. 侵入テストが不十分
D. ネットワークアクセスの設定ミス
正解: **(**正解を表示します**)**
Numerous servers running outdated software most directly indicates that patches and updates are not being applied in a timely and consistent manner. This is a classic patch management control deficiency.

質問: **303**
第三者ベンダーが、組織の顧客向けモバイルアプリを開発しています。情報セキュリティマネージャーにとって、以下の問題のうちどれが最も懸念すべきでしょうか？
A. 導入後のサービスレベル契約(SLA)は定義されていません。
B. このモバイルアプリのプログラマーは全員、海外の請負業者です。
C. ベンダーは情報セキュリティ機能を外部委託しています。
D. この契約にはデータセキュリティに関する要件はありません。
正解: **(**正解を表示します**)**
Without data security requirements in the contract, the organization has no enforceable obligations for how customer data will be protected (controls, breach notification, privacy requirements, testing, retention, etc.), creating the greatest and most immediate third-party risk.

質問: **304**
従業員がセキュリティ責任を果たすよう動機づけるには、以下の方法が最も効果的です。
A. 職務記述書内で役割を明確に定義する
B. 方針と手順。
C. コミュニケーションとトレーニング。
D. 監視と対応。
正解: **C (**コメントを発表する**)**
Motivating employees to fulfill their security responsibilities is best accomplished through effective communication and training. These practices help raise awareness, ensure employees understand their security roles, and reinforce the importance of security practices in their day-to- day work.

質問: **305**
次のうち、抑止力による統制の例はどれですか？
A. 侵入検知システム(IDS)
B. 定期的なデータ復元
C. 責任の分離
D. 警告バナー
正解: **(**正解を表示します**)**
A warning banner is a deterrent control because it discourages unauthorized activity by notifying users of monitoring, permitted use, and potential consequences.

質問: **306**
データ損失防止(DLP)ソリューションを選択する際に、最も重要な考慮事項は次のうちどれですか？
A. このソリューションは例外処理の監査証跡を提供します
B. データ損失時にデータを復旧できます
C. ソリューションはリスクプロファイルに合致しています
D. 情報分類ポリシーが策定されました
正解: **D (**コメントを発表する**)**
A data loss prevention (DLP) solution depends on clearly defined data classification to determine what data is sensitive and how it should be protected. Without an established information classification policy, the organization cannot effectively configure or enforce DLP controls, making classification the foundational requirement.

質問: **307**
マーケティングチームによるコンテンツ作成のための生成型AIの利用を評価する情報セキュリティマネージャーにとって、以下のうちどれが最も懸念すべき事項でしょうか？
A. 生成型AIプラットフォーム上での機密性の高い企業マーケティングデータの漏洩
B. 社内マーケティング調査および非機密活動における生成型AIの利用拡大
C. マーケティングチームが企業メールアドレスを使用して生成型AIサービスに登録する
D. 生成型AIプラットフォームにおけるログ記録機能の不足

正解: **A** (コメントを発表する)
The greatest concern is the potential exposure of sensitive corporate marketing data, which can lead to data leakage, loss of competitive advantage, or regulatory non-compliance if the data is processed or stored insecurely on external AI platforms.

質問: **308**
組織全体でセキュリティに関する期待値を設定するために、情報セキュリティポリシーが定期的に承認されることが最も重要です。
A. 最高情報セキュリティ責任者(CISO)
B. コンプライアンス管理。
C. 最高技術責任者(CTO)。
D. 上級管理職。
正解: **D** (コメントを発表する)
An information security policy sets organization-wide expectations and requires authority, visibility, and commitment from the top. Regular endorsement by senior management demonstrates governance support and makes the policy enforceable across all business units.

質問: **309**
ネットワーク上の重要データをセグメント化した後、リスク評価の結果、データ漏洩のリスクが依然として許容レベルを超えていることが判明しました。さらなるリスクを軽減するために、どの追加対策が最も効果的でしょうか？
A. エンドユーザーのデータアクセス権限の見直し
B. ゼロトラストモデルの実装
C. データ処理に重点を置いたトレーニングを実施する
D. 外部ネットワークを積極的に監視する
正解: (正解を表示します)
After network segmentation, the remaining exposure risk is most directly reduced by validating and tightening who can access the critical data. Reviewing access rights supports least privilege and can remove excessive or inappropriate permissions.

質問: **310**
イベント ログがインシデント調査に受け入れられるためには、証拠の連鎖を確立するために考慮すべき最も重要な事項は次のどれですか。
A. 集中ログ
B. タイムクロックの同期
C. 利用可能なフォレンジックツール
D. 管理者ログアクセス
正解: (正解を表示します)
The most important consideration to establish chain of evidence for event logs to be acceptable for incident investigation is time clock synchronization. Ensuring that all systems' clocks are synchronized is crucial because it

helps maintain a reliable timeline of events, which is essential for accurately understanding the sequence of actions during an incident.
While centralized logging, available forensic tools, and restricted administrator log access are important for overall log management and security, synchronized timestamps are critical for establishing the integrity and reliability of the evidence collected during an investigation.

質問: **311**
評価されたリスクに対するリスク対応策の選択について、主に誰が責任を負うのでしょうか？
A. リスク管理専門家
B. 情報セキュリティマネージャー
C. リスク所有者
D. 資産所有者
正解: **C (**コメントを発表する**)**
The risk owner is accountable for managing the specific risk and has the authority to decide how it will be treated (accept, mitigate, transfer, or avoid). Selecting the risk response requires business decision-making authority, which resides with the risk owner, not advisory or support roles.

質問: **312**
情報セキュリティ意識向上プログラムの効果を最もよく示しているのは、次のうちどれですか？
A. データ損失防止(DLP)インシデント報告件数の減少
B. セキュリティトレーニングに関するエンドユーザーからのフィードバックの改善
C. フィッシング事件の減少
D. ユーザーから報告された情報セキュリティインシデントの増加
正解: **(**正解を表示します**)**
An effective security awareness program results in increased user awareness and a higher number of reported security incidents, as employees recognize and report potential threats before they escalate. This indicates that users are more engaged and proactive in identifying risks. While fewer DLP or phishing incidents may suggest improved security, they could also mean that users are unaware of incidents. Positive training feedback is useful but does not directly measure awareness effectiveness like increased reporting does.

質問: **313**
次のうち、新たに出現する高度な持続的脅威(APT)攻撃者から最も効果的に保護できるのはどれですか？
A. セキュリティ意識向上資料を更新しました
B. プロアクティブなモニタリング
C. ハニーポット環境
D. 継続的なインシデント対応訓練
正解: **B (**コメントを発表する**)**
Proactive monitoring enables early detection of suspicious activities and advanced persistent threats (APTs), allowing an organization to respond quickly to sophisticated and evolving attacks.

質問: **314**
以下のうち、効果的かつ迅速なインシデント対応を最も効果的にサポートするのはどれですか？
A. 文書化されたインシデント対応計画を策定しておくこと
B. 内部および外部のステークホルダーの関与
C. 法医学的インシデント対応専門家の任命
D. SIEMソリューションの維持管理
正解: **A (**コメントを発表する**)**
A documented incident response plan most directly enables effective and timely response by defining roles, procedures, escalation paths, and required actions in advance, reducing confusion and delays during an incident.

質問: **315**
ある組織が、BYOD(Bring Your Own Device)環境で使用するモバイルデバイス管理(MDM)ソフトウェアを評価しています。MDMソフトウェアの最も重要な機能は、以下のとおりです。
A. ネットワークアクセスをブロックします。
B. リモートワイプを有効にする。
C. 追跡装置の位置。
D. テキストメッセージを保持する。
正解: **(**正解を表示します**)**
In a BYOD environment, the most important feature of MDM software is the ability to enable remote wipe. This allows the organization to remotely erase sensitive data from a lost or stolen device, ensuring that confidential information is not exposed.

質問: **316**
情報セキュリティインシデントの影響を受けた顧客への連絡において、以下のうちどれを最も重要に含めるべきでしょうか？
A. 漏洩したデータの種類の詳細
B. 組織にとってのインシデントによるコスト
C. 事件に関する技術情報
D. 攻撃者の身元
正解: **A (**コメントを発表する**)**
Customers need to understand what type of their data was exposed so they can assess personal impact and take appropriate protective actions (e.g., monitoring accounts, resetting credentials).

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

ス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu 1193問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **317**
以下のうち、データ所有者の主要な責任はどれですか？
A. データ品質
B. データストレージ
C. データバックアップ
D. データ分類
正解: **D** (コメントを発表する)

質問: **318**
ある金融機関が、顧客データが侵害されるサイバーセキュリティインシデントに見舞われた。
この事件に関する外部向け広報を準備する際に、最も重要な考慮事項は次のうちどれですか？
A. 情報漏洩に関する情報提供を顧客から求められた場合にのみ、顧客に通知します。
B. 事件の詳細がすべて確認されるまで通知を延期する
C. 関連する利害関係者グループに合わせたコミュニケーション
D. 法的 規制当局とのコミュニケーションを限定する
正解: (正解を表示します)
External communication after a customer data compromise must be clear, accurate, timely, and appropriate for each audience, such as customers, regulators, partners, media, and possibly law enforcement.

質問: **319**
ある組織は技術的および物理的な対策に多額の投資を行ってきたにもかかわらず、依然として容認できないレベルのインシデントが発生している。この問題を改善する可能性が最も高いのは次のうちどれか？
A. 採用時およびその後定期的にセキュリティ意識向上トレーニングを義務付ける
B. 既存の統制を監査し、不備を特定する
C. 従業員にセキュリティポリシーの確認と承認を求める
D. インシデントに対処するための管理責任者への研修を義務付ける
正解: (正解を表示します)
Human error is a leading cause of security incidents. Mandating regular security awareness training helps improve employee behavior and reduces the likelihood of incidents that bypass technical and physical controls.

質問: **320**
クライアントが使用する本番環境のウェブサーバーに重大な脆弱性があることが判明した場合、最初に行うべきことは次のうちどれですか？
A. 業務システム所有者に連絡してください。
B. 調査結果を検証する。
C. 補償制御を実施する。
D. ギャップ分析を実施する。

正解: (正解を表示します)
The first step upon learning that a production web server used by clients has a critical vulnerability is to validate the finding. This ensures that the vulnerability is real, accurately assessed, and not a false positive before taking further action.

質問: **321**
ビジネスインパクト分析(BIA)を実施する準備をする際に、情報セキュリティマネージャーが最初に考慮すべき事項は次のうちどれですか？
A. 重要と分類される機能間の相互依存関係
B. 事業上の脅威に関する定量的情報
C. 事業機能に影響を与える混乱に関する上級管理職の意見
D. 事業主の意見が重要度を確立するのに役立つ
正解: (正解を表示します)
A BIA depends on understanding which business processes are critical and what impact disruptions would have. Business owners are the best source for defining process criticality, acceptable downtime, recovery priorities, and operational impact.

質問: **322**
インシデント対応計画にインシデント分類スキームを含めるべき最も適切な理由は次のうちどれですか？
A. インシデント対応の優先順位付けを支援するため
B. インシデント報告書の作成を容易にするため
C. 事業継続計画(BCP)の作成を支援する
D. 通知およびエスカレーションプロセスを特定する
正解: (正解を表示します)
An incident classification scheme enables the organization to prioritize incident responses based on severity and impact, ensuring the most critical incidents are addressed promptly.

質問: **323**
新たなリスクが特定された後に、更新された情報セキュリティ戦略に対する上級管理職のコミットメントを得るために、以下のうちどれが最も重要ですか？
A. リスク登録簿にリスクを記録する
B. 組織への影響を示す
C. リスク評価プロセスの更新
D. 業界における最近の事件一覧を提示する
正解: (正解を表示します)
To obtain senior management commitment for an updated information security strategy, it is crucial to demonstrate the impact that newly identified risks pose to the organization. Senior management prioritizes decisions based on business impact, so clearly showing how these risks affect financials, operations, reputation, or compliance will justify the need for strategic updates.

While capturing risks in a register and updating risk assessments are important, they do not directly drive executive-level commitment as effectively as demonstrating impact.

質問: **324**
セキュリティフレームワークが推奨するすべての制御策を実装する上で、最も大きな懸念事項は次のうちどれですか？
A. 上級管理職からの承認が得られない
B. 投資収益率(ROI)がマイナス
C. リスクレベルの上昇
D. 実施期間の延長
正解: **(**正解を表示します**)**
Implementing every recommended control can create unnecessary cost and complexity beyond what the organization's risk profile and business needs justify, leading to a negative ROI from over-control rather than risk-based, targeted implementation.

質問: **325**
組織は、ITアプリケーションの社内ホスティングとサポートを置き換えるために、SaaS(Software as a Service)の利用をますます増やしています。調達決定において情報セキュリティ上の懸念事項が考慮されるようにするための最も効果的な方法は、次のうちどれでしょうか？
A. 情報セキュリティリスク評価を調達プロセスに組み込む。
B. 調達チームに定期的な情報セキュリティ研修を実施する。
C. SaaSベンダーとの調達契約において監査権を行使する。
D. IT部門のメンバーを定期的な調達チーム会議に招待し、ベストプラクティスに影響を与えてもらう。
正解: **A (**コメントを発表する**)**
SaaS procurement introduces third-party, data protection, access control, compliance, availability, and vendor lock-in risks. Integrating security risk assessments directly into procurement ensures these risks are evaluated before vendor selection and contract approval.

質問: **326**
情報セキュリティ戦略策定におけるビジネスステークホルダーの関与において、最も重要な目的は次のうちどれですか？
A. 情報セキュリティ資金の獲得
B. 組織的な整合性の確保
C. 組織のリスク許容度を定義する
D. 部門長の承認を申請する
正解: **(**正解を表示します**)**
The most important objective of business stakeholder involvement during information security strategy development is ensuring organizational alignment. Engaging stakeholders helps ensure that the security strategy aligns with the organization's goals, priorities, and overall risk management approach, making it more effective and integrated into business processes.

質問: **327**
事業継続計画(BCP)において復旧戦略を策定する際に、最も重要な考慮事項は次のうちどれですか？
A. 法的要件
B. バックアップサイトの地理的位置
C. サービス中断に対する組織の許容度
D. 災害発生の可能性
正解: **(**正解を表示します**)**
The most important consideration when defining a recovery strategy in a business continuity plan (BCP) is understanding the organization's tolerance to service interruption, which is typically defined by Recovery Time Objective (RTO) and Recovery Point Objective (RPO). These factors determine how quickly services must be restored and how much data loss is acceptable, directly influencing recovery strategies. While legal requirements, backup site location, and disaster likelihood are important, they are secondary to ensuring the recovery strategy aligns with business continuity needs.

質問: **328**
セキュリティ意識の高い文化を構築する際に、以下のうち最も重要なものはどれですか？
A. セキュリティミッションステートメント
B. 従業員の信念
C. 上級管理職の行動
D. 組織の価値観
正解: **(**正解を表示します**)**
Senior management conduct is crucial in building a security-aware culture because leadership behavior sets the tone for the organization's priorities and influences employees to align with security practices. Management's active participation and commitment to security demonstrate its importance to the entire organization.

質問: **329**
効果的なリスク意思決定を支援するために、以下のうちどれを整備しておくことが最も重要ですか？
A. 明確に定義され承認された管理
B. 中堅管理職で構成される監査委員会
C. 確立されたリスク領域
D. リスク報告手順
正解: **(**正解を表示します**)**
Effective risk decisions require timely, consistent, and actionable information. Risk reporting procedures ensure risks are identified, communicated, escalated, and tracked in a structured way so decision-makers have what they need to accept, mitigate, transfer, or avoid risk.

質問: **330**
デジタルシステムの信頼性と回復力を最も適切に測定できる指標は次のうちどれですか？
A. 平均故障間隔(MTBF)

B. 平均応答時間
C. 平均復旧時間(MTTR)
D. 平均故障時間(MTTF)
正解: **(**正解を表示します**)**
MTBF measures the average time between system failures, making it the best metric for assessing the reliability and resilience of digital systems over time.

質問: **331**
組織の情報セキュリティマネージャーは、システム侵入に関連するセキュリティインシデントの可能性について警告を受けました。情報セキュリティマネージャーが最初にとるべき行動は次のうちどれでしょうか？
A. 状況を上級管理職に報告してください。
B. 資源を動員して被害を最小限に抑える。
C. インシデント対応計画を発動する。
D. インシデントが発生したことを確認します。
正解: **(**正解を表示します**)**
The first step in responding to a possible security incident is to verify whether an actual incident has occurred. This helps avoid unnecessary actions and ensures resources are used appropriately. Once verified, further steps such as activating the incident response plan or mobilizing resources can be taken.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu 「**193**問、３０%ディスカウント、特別な割引コード**:** **JPNshiken**」

質問: **332**
新しい生産システムの導入に伴うリスクを最も効果的に軽減できるのは、次のうちどれですか？
A. 構成管理
B. 問題管理
C. インシデント管理
D. リリース管理
正解: **D (**コメントを発表する**)**
Release management is responsible for planning, scheduling, and controlling the movement of releases to test and production environments. It ensures that new systems are deployed in a controlled and tested manner, thereby best mitigating risks associated with production deployments.

質問: **333**

電子商取引アプリケーションにおける不正アクセスが疑われる事案が発生した場合、最初に行うべき対応は次のうちどれですか？
A. アプリケーションを再インストールしてください。
B. アプリケーションへのアクセス権を取り消す。
C. 影響を受けた資産を隔離します。
D. アクセスログを確認する。
正解: **(**正解を表示します**)**
The question uses the word "suspected." In CISM-speak, "suspected" means you are still in the Identification/Analysis phase, not yet in the Containment or Eradication phases.
Before you take any disruptive action (like shutting down a revenue-generating e-commerce site), you must confirm that an incident is actually occurring. You cannot respond to a ghost.
Reviewing the access logs is the most immediate way to validate the suspicion. It allows you to see if the access was indeed unauthorized, identify the source, and understand the scope without crashing the business process.
In an e-commerce environment, "Isolating assets" or "Revoking access" causes immediate downtime and loss of revenue. A Manager does not pull the plug until the threat is verified.

質問: **334**
ある事業部門は、生産性向上を目的とした情報管理システムのアップグレードを盛り込むため、長期事業計画を更新しました。この取り組みを支援するために、対応する情報セキュリティ戦略を更新する際の主要な根拠は何であるべきでしょうか？
A. ビジネス戦略
B. 能力成熟度モデル
C. 情報セキュリティフレームワーク
D. 生産性に関する主要業績評価指標(KPI)
正解: **(**正解を表示します**)**
The primary basis for updating the corresponding information security strategy should be the business strategy. The security strategy must align with and support the business objectives, ensuring that information security efforts are focused on enabling business goals such as increased productivity and the successful upgrading of information management systems.

質問: **335**
情報セキュリティフレームワークの設計において、最も適切な情報源となるのは次のうちどれですか？
A. 利用可能なスキル
B. 導入コスト
C. 最近の監査結果
D. リスク許容度
正解: **D (**コメントを発表する**)**
Risk appetite defines the level of risk an organization is willing to accept and serves as the foundational input for designing an information security framework that aligns with business objectives and tolerance for risk.

質問: **336**
組織内のセキュリティ文化に最も大きな影響を与えることができる役割は、次のうちどれですか？
A. 最高執行責任者(COO)
B. 最高情報セキュリティ責任者(CISO)
C. 最高情報責任者(CIO)
D. 最高経営責任者(CEO)
正解: **(**正解を表示します**)**

質問: **337**
情報セキュリティプログラムのパフォーマンスを上級管理職に報告する際に、情報セキュリティマネージャーにとって最も役立つのは次のうちどれですか？
A. システム脆弱性スキャン結果
B. 特定され、対処されたインシデントの数
C. ポリシー例外の数
D. 独立セキュリティ監査の結果
正解: **(**正解を表示します**)**
The number of incidents identified and remediated is a business-relevant performance indicator that shows operational effectiveness and trend over time, making it most useful for communicating program performance to senior management.

質問: **338**
情報セキュリティ管理者が、セキュリティポリシーを繰り返し遵守していない部署を特定した場合、次に取るべき行動は何でしょうか？
A. 部門の利用者に対し、セキュリティ意識向上トレーニングを再度受講させる。
B. 部署内のシステムに対する脆弱性評価を実施する。
C. ポリシー遵守を強制するための追加的な管理策を導入する。
D. ポリシー違反を上級管理職に報告する。
正解: **(**正解を表示します**)**
The next course of action when an information security manager has identified a department that is repeatedly not following the security policy should be to report the policy violation to senior management. Senior management needs to be informed of the repeated non-compliance so they can address the issue at the appropriate level and ensure the department takes corrective actions.

質問: **339**
新しいセキュリティ イニシアチブの成功を促進するには何が最適でしょうか?
A. IT セキュリティ運営委員会を設立します。
B. セキュリティに関する意思決定にビジネスを組み込む。
C. セキュリティポリシーを定期的に更新する
D. 実装後のセキュリティ メトリックを監視します。
正解: **(**正解を表示します**)**

Involving the business in security decision making secures executive sponsorship, aligns initiatives with organizational objectives, and ensures the resources and buy-in needed for success.

質問: **340**
情報セキュリティプログラムの成功にとって、次のうちどれが最も重要ですか？
A. 世界的に認められた枠組みとの整合性
B. 適用される規制の遵守
C. 既存の業務プロセスとの統合
D. 運営委員会による政策承認
正解: **(**正解を表示します**)**
Integrating security into existing business processes is most crucial because it embeds security into day-to-day operations, driving consistent adoption and sustained effectiveness beyond formal frameworks, compliance, or governance approvals alone.

質問: **341**
インシデント修復の主な目的は次のうちどれですか？
A. インシデント対応計画の改訂
B. システム整合性の回復
C. インシデント対応の有効性の評価
D. エンドポイントセキュリティの復旧
正解: **(**正解を表示します**)**
The primary objective of incident remediation is to restore system integrity by eliminating vulnerabilities, correcting configurations, and ensuring systems are secure and fully functional after an incident.

質問: **342**
ベンダーのセキュリティアップデートが提供されなくなった旧式のクライアントWebアプリケーションサーバーをサイバー攻撃者が悪用するリスクを最も効果的に低減する対策は、次のうちどれですか？
A. 脆弱性対策
B. ネットワーク分割
C. 年間ユーザーアカウント再認証
D. 生体認証アクセス制御
正解: **B (**コメントを発表する**)**
If a legacy web application server no longer receives vendor security updates, vulnerabilities may remain unpatched. Network segmentation is the most effective compensating control because it limits exposure, restricts access paths, and reduces the chance that threat actors can reach or move from the vulnerable server.

質問: **343**
IT調査におけるデジタルフォレンジックの主な役割は次のうちどれですか？
A. 事件の詳細に関するシステム証拠を分析する
B. 関係者に対する法的罰則を決定する

C. 将来のインシデントを防止するための新しいソフトウェアツールを開発する
D. 組織に対する事件の財務的影響を評価する
正解: **(**正解を表示します**)**
The primary role of digital forensics during an IT investigation is to analyze system evidence to uncover incident details, such as how the breach occurred, what was affected, and who was responsible. This supports legal, regulatory, and remediation efforts.

質問: **344**
サイバーセキュリティリスク評価を実施する主な目的は以下のとおりです。
A. 上級管理職へのセキュリティ報告を支援する。
B. 複数のセクターにわたるコンプライアンスを検証する。
C. 組織の現在のセキュリティ体制を理解する。
D. サイバーセキュリティプログラムの有効性を示す指標を提供する。
正解: **(**正解を表示します**)**
The primary purpose of a cybersecurity risk assessment is to identify and understand the organization's current security posture, including vulnerabilities and threats, to inform effective risk management.

質問: **345**
情報セキュリティ管理者が上級管理職に情報セキュリティプログラムの状況報告を行う際、主な焦点は以下のとおりであるべきです。
A. 主要業績評価指標(KPI)。
B. 正味現在価値(NPV)。
C. 主要管理策の評価。
D. セキュリティ投資収益率(ROI)。
正解: **(**正解を表示します**)**
Explanation: Program status reporting to senior management should primarily use KPIs to communicate progress and performance against objectives in business-relevant terms (e.g., trends, targets, and effectiveness of key activities).

質問: **346**
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."

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu ↥**193**問、３０%ディスカウント、特別な割引コード:**JPNshiken**」

質問: **347**
以下の情報のうち、経営陣が新たな規制への準拠の価値を評価する上で最も役立つのはどれですか？
A. 主要業績評価指標(KPI)の状況
B. 主要リスク指標(KRI)の状況
C. 法令遵守違反の影響
D. 法令遵守違反による評判リスク
正解: (正解を表示します)
Senior management can best assess the value of compliance with new regulations by understanding the impact of noncompliance. This provides insight into potential legal, financial, and operational consequences, which are crucial for making informed decisions about compliance efforts.

質問: **348**
組織全体で効果的な情報セキュリティ対策の導入を最も効果的に支援するのは、次のうちどれですか？
A. 事業継続対策
B. セキュリティ意識の高い文化
C. 最新のセキュリティ技術
D. 情報セキュリティ指標
正解: (正解を表示します)
A security-aware culture ensures that employees consistently follow security policies and practices in their daily activities. This widespread behavioral alignment is the most effective way to embed and sustain strong information security practices across the organization.

質問: **349**
情報セキュリティインシデントの深刻度を分類する際に考慮すべき最も重要な要素は次のうちどれですか？
A. 影響を受けた組織のブランド評判
B. 事件発生場所(地理的位置)
C. トリアージに必要なリソース
D. 事業運営への影響
正解: (正解を表示します)
The most important factor when categorizing the severity of information security incidents is the impact on business operations. An incident's severity is often determined by how much it disrupts the organization's ability to function and deliver its critical services. This helps prioritize responses and allocate resources effectively.

質問: **350**
情報セキュリティマネージャーは、複数の地域を対象とした情報漏洩通知手順を策定しています。組織の顧客の居住地を把握した後、情報セキュリティマネージャーは次に何をすべきでしょうか？
A. 各地域における通知のタイミングと必要な対応を決定する。
B. 通知のタイミングとアクションをグローバルに標準化する
C. 各地域に広報担当者を任命する。
D. 既存プロセスのギャップ分析を実施する
正解: **(**正解を表示します**)**
After identifying where customers reside, the next logical step is to understand and comply with the specific data breach notification requirements of each jurisdiction. Different geographic regions have varying laws regarding how quickly affected parties must be notified, what information needs to be included, and whether regulators or other authorities must also be informed. Compliance with these laws is critical to avoid legal penalties and maintain customer trust.

質問: **351**
最高情報責任者(CIO)は最近、システム管理者の自宅からのリモートアクセスをセキュリティポリシーの例外として承認しました。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何でしょうか？
A. 関連するリスクを経営陣に報告し、管理者のアクセスを無効にします。
B. システム管理者がリスクを認識し、リモートアクセスを監視するようにしてください。
C. リモートアクセスセキュリティに関するポリシーを見直し、変更を提案する。
D. 正式なセキュリティインシデントを登録し、運営委員会にエスカレーションする。
正解: **(**正解を表示します**)**
The information security manager's best course of action would be to review the policy on remote access security and recommend changes. This approach allows for a reassessment of the current security policy in light of the exception, ensuring that appropriate controls are in place to mitigate any associated risks while aligning with the new operational needs.

質問: **352**
以下のユーザータイプのうち、管理者権限を持つ可能性が最も高いのはどれですか？
A. プロセスオーナー
B. データ管理者
C. データアーキテクト
D. データ所有者
正解: **(**正解を表示します**)**
Data custodians are usually responsible for the technical administration, storage, backup, protection, and operation of data systems. Because they manage the systems that hold the data, they are the users most likely to have administrator rights.

質問: **353**

リスク許容度を決定する際の主要な基準として、次のうちどれを用いるべきでしょうか？
A. 独立監査結果
B. 残存リスクレベル
C. リスク評価結果
D. 組織目標
正解: **D** (コメントを発表する)
The primary basis for determining risk appetite should be organizational objectives. The organization's goals and strategy influence its tolerance for risk. Risk appetite is aligned with the objectives and priorities of the organization, ensuring that risks taken are in line with its mission, values, and overall business direction.

質問: **354**
リスク評価の結果を上級管理職に報告する際に、最も重要な考慮事項は次のうちどれですか？
A. 報告書には、業界ベンチマークとの比較を含めるべきです。
B. 報告書には推奨される管理策を含める必要があります。
C. 報告書はビジネス用語で記述する必要があります。
D. 報告書は正式な方法論を用いるべきである。
正解: (正解を表示します)
Senior management makes decisions based on business impact, financial exposure, and strategic objectives. Presenting risk assessment results in business terms (e.g., operational impact, financial loss, reputational damage) ensures the information is understandable, actionable, and aligned with executive decision-making.

質問: **355**
セキュリティプログラムの重要性を経営陣に伝えるための最良の方法は、次のうちどれですか？
A. 新たな脅威や進化する脅威に対する重大な脆弱性のリストと修復スケジュールを伝達する。
B. 定義されたセキュリティキーコントロール指標(KCI)および責任を負うコントロールオーナーのステータス更新情報を提供します。
C. 最近のセキュリティインシデントとインシデント対応プロセスの有効性に関する報告。
D. セキュリティ戦略と主要なビジネスイニシアチブとの関連性を説明する。
正解: (正解を表示します)
Demonstrating how the security strategy supports and enables key business initiatives is the best way to gain executive leadership's attention and support, as it aligns security with business value and objectives.

質問: **356**
組織に重大な影響を及ぼすインシデントが発生した後、情報セキュリティマネージャーは、将来同様のインシデントを防ぐための適切な対策を確立する任務を負っています。最初に行うべきことは次のうちどれですか？
A. 根本原因分析を実施する
B. インシデント対応手順の改善
C. 事業影響分析(BIA)の見直し
D. 教訓を学ぶ演習を実施する
正解: (正解を表示します)

Conducting an RCA allows for the identification of the fundamental issues that led to the incident.
By systematically examining the underlying causes, organizations can develop targeted controls to address these specific vulnerabilities, thereby reducing the likelihood of recurrence. This approach ensures that corrective measures are both effective and efficient.

質問: **357**
インシデント対応トレーニング計画に含まれる以下のトピックのうち、チームが対応プロセスの全体的な有効性を向上させるために最も役立つのはどれですか？
A. シナリオレビュー
B. 事件後の検証
C. 根本原因分析
D. インシデントギャップ分析
正解: **(**正解を表示します**)**
Post-incident reviews evaluate what worked, what failed, and what should be improved after real incidents or exercises. They directly support continuous improvement of the overall incident response process.

質問: **358**
情報セキュリティ管理者は、従業員が会議中にメモを取るために公開されているAIサービスアプリケーションをインストールしていることを知りました。このサービスは会議の議論をオンラインリポジトリに保存しています。次のうち、最も適切な対応策はどれですか？
A. インシデント対応チームを招集する。
B. アプリケーションのリスク評価を実施する。
C. アプリケーションへのアクセスをブロックします。
D. 問題を管理者に報告してください。
正解: **(**正解を表示します**)**
The best first course of action is to assess the risk of the public AI note-taking application, including what data is stored, where it is stored, access controls, retention, confidentiality, privacy, contractual terms, and regulatory exposure.

質問: **359**
経営陣に報告される平均解決時間(MTTR)指標は、次のうちどれに該当するか？
A. 復旧時間目標(RTO)
B. リカバリポイント目標(RPO)
C. 主要業績評価指標(KPI)
D. 主要リスク指標(KRI)
正解: **(**正解を表示します**)**
MTTR measures how efficiently the organization resolves incidents or service issues. Since it measures operational performance against response/recovery objectives, it is a KPI.

質問: **360**

インシデント対応における復旧フェーズの主な目的は以下のとおりです。
A. インシデントの根本原因を特定し、取り除く。
B. インシデントから得られた教訓を特定し、文書化する。
C. 組織の事業継続計画(BCP)で定義された時点までサービスを復旧する。
D. 業界をリードする制御フレームワークで定義された時点までサービスを復旧する。
正解: (正解を表示します)
The primary purpose of the recovery phase in incident response is to restore services to the point defined in the organization's business continuity plan (BCP). The BCP outlines the required recovery point and time objectives to ensure critical operations are resumed after an incident.

質問: **361**
上級幹部が業務上の必要性から、組織のインターネットトラフィックフィルタを回避するよう情報セキュリティマネージャーに依頼しました。情報セキュリティマネージャーが次に取るべき行動は次のうちどれでしょうか？
A. ポリシーに準拠していないため、リクエストを却下します。
B. 例外要求を実装します。
C. ITネットワークマネージャーに通知し、共同で承認決定を行う。
D. 制御例外処理プロセスに従ってください。
正解: (正解を表示します)
The appropriate next step is to follow the established controls exception process so the request is formally risk-assessed, documented, approved by the proper authority, time-bound, and monitored rather than handled ad hoc.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu 「**193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **362**
組織のセキュリティ文化を確立する上で、以下の内部要因のうちどれが最も大きな影響を与えるでしょうか？
A. ビジネスリーダーの支援
B. 組織のリスク許容度
C. 組織のセキュリティ意識
D. 従業員のスキルと資格
正解: (正解を表示します)
The support of business leaders has the greatest impact on establishing an organization's security culture. Leadership sets the tone for prioritizing security, influences employee behavior, and ensures resources and attention are allocated to security initiatives, making it a critical internal factor.

質問: **363**
重要な業務プロセスをサポートするために、SaaS(Software as a Service)アプリケーションが導入されました。アプリケーションに影響を与えるインシデントに迅速に対応するために、サービスレベル契約(SLA)に含めるべき最も重要な項目は次のうちどれですか？
A. 販売業者の宣言および保証
B. 対象システムの監視強化
C. インシデント対応における役割と責任を明確に定義する
D. 確立されたインシデント対応手順
正解: **(**正解を表示します**)**
https://hallellis.co.uk/saas-service-level-agreements-best-practices/

質問: **364**
以下のうち、成熟した情報セキュリティプログラムを示す最良の証拠はどれですか？
A. 経営陣は情報セキュリティポリシーを承認しました。
B. 組織にはセキュリティ意識向上とトレーニングプログラムがあります。
C. セキュリティ指標が定義され、測定されます。
D. ITセキュリティ担当者は厳格な技術的セキュリティ管理を実施しました。
正解: **C (**コメントを発表する**)**
According to maturity models (like CMMI), a "mature" process is one that is quantitatively managed. You cannot improve what you do not measure.
While policies and training are necessary, they only show that a program exists. Metrics provide the evidence that the program is actually achieving its objectives and reducing risk.
A mature program uses data to drive decision-making. Measuring metrics allows the Information Security Manager to demonstrate "value delivery" to the board and adjust the strategy based on real-world performance.

質問: **365**
組織がインシデント管理の優先順位付けを改善するために最も効果的な方法はどれでしょうか？
A. システムの資産価値を定量化する
B. ユーザーの重要度ランキング
C. 影響を受けるユーザー数の定量化
D. ITシステムをビジネスプロセスにマッピングする
正解: **D (**コメントを発表する**)**
Mapping IT systems to business processes helps the organization understand the business impact of incidents, enabling better prioritization based on critical business functions.

質問: **366**
インシデント管理プロセスのどの段階で、脅威の除去と影響を受けたシステムの以前の状態への復元が行われますか？
A. 学んだ教訓
B. 検出と分析

C. 封じ込め
D. 根絶
正解: **(**正解を表示します**)**
The eradication phase focuses on removing the threat (malware, attacker persistence, compromised accounts) and restoring systems to a known-good state so normal operations can safely resume.

質問: **367**
以下のうち、アプリケーションデータへの不正アクセスに伴うリスクは誰が負うべきでしょうか？
A. アクセス管理者
B. アプリケーション所有者
C. データ管理者
D. アプリケーション開発者
正解: **B (**コメントを発表する**)**

質問: **368**
国内企業の経営陣が、事業を複数の海外拠点に拡大する計画を発表しました。この計画を知った情報セキュリティマネージャーが最初にとるべき行動は次のうちどれでしょうか？
A. 各新規拠点ごとに、地域に合わせた情報セキュリティポリシーを作成する。
B. 国際的な情報セキュリティ基準に対するギャップ分析を実施する。
C. セキュリティ研修および啓発資料を適切に更新する。
D. 新しい拠点に影響を与える法的および規制上の要件を調査する。
正解: **(**正解を表示します**)**
Understanding the legal and regulatory requirements in new international locations is the first critical step, as these requirements directly influence the design and implementation of compliant security controls and policies.

質問: **369**
BYOD(Bring Your Own Device)プログラムを導入する企業にとって、セキュリティ対策が施されていないモバイルデバイスに保存されている企業データのセキュリティを最も効果的に確保できるのは、次のうちどれでしょうか？
A. データ損失防止(DLP)
B. 利用規約
C. コンテナ化ソリューション
D. 機器認証プロセス
正解: **(**正解を表示します**)**
Containerization isolates corporate data and applications from personal content on the device and allows enforcing encryption, access controls, and remote wipe for only the corporate container, providing the best protection of corporate data on otherwise unsecured BYOD devices.

質問: **370**
組織の情報セキュリティ戦略が組織目標と整合していることを確実にするために、次のうちどれが最も役立ちますか？

A. 情報セキュリティ戦略の継続的な更新のための変更管理プロセスを確立する
B. リスク登録簿が継続的に更新され、見直されていることを確認する
C. 情報セキュリティプロセスを監視するための自動化ソリューションの実装
D. 情報セキュリティ戦略の策定にビジネス関係者を参加させる
正解: **(**正解を表示します**)**
Security strategy must support business goals, risk appetite, priorities, and operating needs.
Involving business stakeholders ensures the strategy is built around organizational objectives rather than only technical security concerns.

質問: **371**
サイバーセキュリティ侵害の最も一般的な原因は次のうちどれですか？
A. 人的ミス
B. 特権アカウントの悪用
C. コントロール基準値の欠如
D. パスワードのローテーションが不十分
正解: **(**正解を表示します**)**
Human error is the most common contributor to cybersecurity breaches. Mistakes such as misconfigurations, falling for phishing attacks, or mishandling sensitive data often lead to vulnerabilities that are exploited by attackers. Addressing human error through training, awareness, and user-friendly controls is critical for reducing risk.

質問: **372**
組織文化が情報セキュリティプログラムの有効性に及ぼす主な影響は、次のうちどれですか？
A. 情報セキュリティ管理が遵守されている限り、文化の影響は最小限です。
B. 文化は情報セキュリティに対する行動を形成する。
C. 文化は、プログラム実施に必要な責任を定義します。
D. 文化は情報セキュリティ対策の予算を決定するのに役立ちます。
正解: **(**正解を表示します**)**
Organizational culture primarily influences how employees behave regarding information security, directly affecting the effectiveness of the security program.

質問: **373**
分散型サービス拒否(DDoS)攻撃に対する有効な封じ込め戦略として、次のうちどれが適切でしょうか？
A. 攻撃者が悪用しているファイアウォールポートを無効にします。
B. 影響を受けるサーバーの電源を切ります。
C. 攻撃者のトラフィックをリダイレクトします。
D. 攻撃者が使用するIPアドレスをブロックします。
正解: **(**正解を表示します**)**
Redirecting the attacker's traffic (for example, to a scrubbing service) helps mitigate the impact of a DDoS attack while allowing legitimate traffic to continue, making it an effective containment strategy.

質問: **374**
サイバーインシデントをその影響に基づいて監視し、解決するまで追跡するのに最も効果的なシステムの種類はどれですか?
A. エンドポイント検出と応答 (EDR)
B. ネットワーク侵入検知システム（NIDS）
C. 拡張検出および応答 (XDR)
D. セキュリティ情報イベント管理 (SIEM)
正解: **(正解を表示します)**
SIEM systems collect and analyze log data from across the organization, allowing for real-time monitoring, incident correlation, and end-to-end tracking of response activities - including severity classification and closure.
"SIEM tools enable centralized management, prioritization, and documentation of incidents, making them essential for impact tracking and incident lifecycle management." While EDR and XDR help detect threats, SIEMs offer the full scope for impact-based tracking.

質問: **375**
有意義な情報セキュリティ指標を作成する上で、以下のうち最も重要なものはどれですか？
A. 指標には主要なビジネスシステムを含める必要があります。
B. 指標は上級管理職の承認を得なければなりません。
C. 指標は、認められた業界標準に準拠する必要があります。
D. 指標はビジネス目標と一致していなければなりません。
正解: **(正解を表示します)**
Metrics are only meaningful if they reflect what the business is trying to achieve and what risks matter most. Aligning metrics with business objectives ensures they drive the right decisions and demonstrate security's value in business terms.

質問: **376**
ウェブ開発者がウェブアプリケーションのセキュリティリスクの深刻化を確実に理解できるようにするための最も効果的な方法は、次のうちどれですか？
A. 開発ライフサイクルの初期段階からセキュリティを組み込む。
B. セキュリティ要件を職務記述書に組み込む。
C. カスタマイズされたセキュリティ意識向上トレーニングプログラムを実施する。
D. 安全なウェブ開発手法を標準化する。
正解: **(正解を表示します)**
A tailored security awareness training program for web developers most effectively builds understanding of current and evolving web application threats by making the risks concrete and relevant to their daily work, improving security-minded behavior and decisions.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu ↾**193**問、３０%ディスカウント、特別な割引コード:**JPNshiken**」

質問: **377**
データ分類プロジェクトを実施する際、情報セキュリティ管理者は以下のことを行うべきです。
A. 情報所有者を特定する。
B. 情報アクセス権限を割り当てる。
C. 情報管理者を特定する。
D. 情報の重要度と機密性を割り当てる。
正解: **(**正解を表示します**)**
The first step in a data classification project is to identify information owners, as they are responsible for determining the classification level (e.g., public, confidential) of the data they own.
Only after owners are identified can the classification, access privileges, and custodianship be properly assigned.

質問: **378**
情報セキュリティロードマップにおいて、短期計画と長期計画を分離する最も適切な理由は次のうちどれですか？
A. ビジネス関係者の関与を促進するため
B. 経営陣への事業計画報告を円滑にするため
C. 規制要件を満たすため
D. イニシアチブにリソースを割り当てる
正解: **(**正解を表示します**)**
Separating short-term from long-term plans within an information security roadmap is essential to allocate resources effectively. This ensures that immediate priorities are addressed promptly while aligning resources for future strategic initiatives, maintaining a balance between current and long-term security needs.

質問: **379**
効果的な情報セキュリティプログラムを示す最良の指標は、次のうちどれですか？
A. リスクは許容できるレベルに抑えられています。
B. 方針は上級管理職によって審査および承認されます。
C. 主要リスク指標(KRI)が設定される。
D. 従業員から報告されたセキュリティインシデントの件数が増加しました。
正解: **(**正解を表示します**)**
The best indication of an effective information security program is that risks are managed to an acceptable level based on the organization's risk appetite. This ensures that security efforts are aligned with business objectives, compliance requirements, and threat landscapes. While policy reviews, KRIs, and increased incident reporting are

valuable, they do not directly measure the overall effectiveness of the security program like proper risk treatment does.

質問: **380**
組織のネットワークの一部でマルウェア攻撃が成功し、封じ込められた後、次に起こるべきことは次のうちどれですか？
A. 回復
B. 事件の報告
C. 教訓の振り返り
D. 根絶
正解: **D (**コメントを発表する**)**
After a successful malware attack has been confirmed and contained, the next step is eradication. This involves removing the malware from the affected system and ensuring that all traces of the attack are eliminated to prevent reinfection. Once eradication is complete, recovery and other post-incident activities can proceed.

質問: **381**
サービスプロバイダーが顧客データを保護するための適切な管理体制を維持していることを確認する最も効果的な方法は、次のうちどれですか？
A. 第三者サービスレベル契約(SLA)を確認する。
B. サービスプロバイダーに対して侵入テストを実施する。
C. サービス提供者の年次独立統制報告書をレビューする。
D. サービスプロバイダーにデータを保護するための基準を提供する。
正解: **(**正解を表示します**)**
The most effective way to verify that a service provider is maintaining adequate security controls is to review independent third-party audit reports, such as SOC 2, ISO 27001 certifications, or other compliance assessments. These reports provide an objective evaluation of the provider's security posture and control effectiveness. While SLAs, penetration tests, and security standards are useful, independent control reports offer the most reliable and comprehensive verification.

質問: **382**
新たなリスクと脅威の状況を分析する際、情報セキュリティ管理者はまず最初に以下のことを行うべきです。
A. 新たな脅威の発生源を特定する。
B. ビジネス資産に対する脅威をマッピングする。
C. 業界内の過去の脅威をレビューする。
D. 脅威が現実化した場合の影響を判断する。
正解: **(**正解を表示します**)**
When analyzing the emerging risk and threat landscape, an information security manager should first map threats to business assets. This helps ensure that the analysis is focused on understanding how emerging threats could impact the organization's critical assets, enabling a more targeted and relevant risk management approach.

質問: **383**
あるグローバル企業が、顧客関係管理(CRM)システムをクラウドプラットフォームに移行しようとしています。法的および規制上のコンプライアンスに関して、最も重要な考慮事項は次のうちどれですか？
A. 職務分担
B. データ保存場所
C. セキュリティインシデントの分類
D. サービスレベル契約(SLA)の指標
正解: **(**正解を表示します**)**
Data storage location is critical for legal and regulatory compliance, especially in a global organization, due to data sovereignty and privacy laws that govern where and how personal data can be stored and processed.

質問: **384**
組織の情報セキュリティプログラムにとって、最も適切なビジネス上の正当化理由となるのは、次のうちどれですか？
A. 事業影響分析(BIA)の結果
B. 主要リスク指標(KRI)
C. 独立系セキュリティ監査結果
D. 投資収益率(ROI)予測
正解: **(**正解を表示します**)**
A BIA shows the potential business impact of disruptions, data loss, system outages, and security failures. This provides the strongest business justification for funding and supporting the information security program because it links security needs directly to business consequences.

質問: **385**
組織のセキュリティ意識向上プログラムが効果的であることを最もよく示すのは、次のうちどれですか？
A. 報告されたセキュリティインシデントが大幅に減少
B. すべてのセキュリティ意識向上トレーニングプログラムにおいて出席率100%を達成
C. サイバー関連の不審な活動に関する報告が大幅に増加
D. フィッシングシミュレーションのクリック率は業界平均を下回っています
正解: **(**正解を表示します**)**
An increase in reports of suspicious cyber-related activities indicates that employees are more aware, vigilant, and proactive in identifying potential threats. Effective awareness programs change behavior, and proactive reporting demonstrates improved security culture and engagement rather than simply reduced incident visibility.

質問: **386**
ある医療関連企業が、自社製品の顧客向けトレーニングソリューションを提供するために、仮想現実(VR)ベンダーと提携しています。契約書に含めるべき最も重要な項目は次のうちどれですか？
A. 組織のデータを暗号化する要件
B. 組織のデータの再利用を禁止する条項
C. ベンダーを監査する権利を定める条項

D. 稼働時間に関するサービスレベル契約(SLA)
正解: **(**正解を表示します**)**
Establishing the right to audit ensures the organization can verify that the VR vendor is complying with agreed-upon security, privacy, and regulatory requirements. Ongoing oversight and the ability to independently assess controls provide stronger assurance than relying solely on contractual promises or technical requirements.

質問: **387**
組織内の残存リスクを最もよく表しているのは、次のうちどれですか？
A. リスク管理フレームワーク
B. バランススコアカード
C. ヒートマップ
D. 事業影響分析(BIA)
正解: **(**正解を表示します**)**

質問: **388**
情報セキュリティ運営委員会の最も重要な機能は、次のうちどれですか？
A. 組織的リスク評価プロセスの開発
B. ビジネスから複数の視点を得る
C. 組織資産へのデータ分類の割り当て
D. 論理アクセス制御のセキュリティ標準の定義
正解: **B (**コメントを発表する**)**

質問: **389**
情報セキュリティリスク管理プロセスを企業リスク管理に統合することで、おそらく以下のことが可能になります。
A. 企業リスク許容レベルの引き下げ。
B. 企業リスクを低減する情報セキュリティ対策。
C. 情報セキュリティ予算の経営陣による承認。
D. セキュリティ運用の効率向上。
正解: **(**正解を表示します**)**
Integrating information security risk management processes into corporate risk management helps ensure that information security controls are aligned with overall enterprise risk management objectives. This integration results in the implementation of security controls that effectively reduce the organization's enterprise risk, making it a key part of the broader risk management strategy.

質問: **390**
組織の情報セキュリティプログラムが法的および規制上のコンプライアンス要件に準拠していることを最も確実にする手段は次のうちどれですか？
A. コンプライアンス要件を満たすために必要なセキュリティ対策の費用対効果分析を実施する
B. コンプライアンス要件を全体的なセキュリティ要件に統合する

C. 法律専門家を起用してコンプライアンス要件を評価し、アプローチを提案してもらう
D. コンプライアンス要件を遵守しないユーザーに対する懲戒手続きの策定
正解: (正解を表示します)
Integrating legal and regulatory compliance requirements directly into the overall security requirements ensures they are embedded into policies, standards, controls, and operational processes. This approach makes compliance part of the security program's design and execution, providing sustained and systematic adherence rather than isolated or reactive efforts.

質問: **391**
発見された脆弱性からセキュリティ制御の欠陥を特定する最も効果的な方法は、次のうちどれですか？
A. 自己評価(CSA)を実施する。
B. 現在の事業運営状況を見直す。
C. 過去の事件報告書を確認する。
D. ギャップ分析を実施する。
正解: (正解を表示します)
A gap analysis compares the current control environment against required standards, policies, baselines, or risk expectations. This is the best way to identify which security controls are missing, weak, or ineffective based on discovered vulnerabilities.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu ↑**193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **392**
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. 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
B. 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
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: (正解を表示します)
The metric that would provide an accurate measure of an information security program's performance is a combination of qualitative and quantitative trends that enable decision making.
This approach offers a comprehensive view by combining numerical data with qualitative insights, allowing for informed decision-making and a deeper understanding of the security program's effectiveness.
This combination allows organizations to capture the nuances of security performance and better assess the overall effectiveness of their information security efforts.

質問: **393**
情報セキュリティ手順の開発には、以下のどのグループが必ず関与しなければなりませんか？
A. 上級管理職
B. 内部監査
C. コンプライアンス部門
D. 事業部門
正解: **(**正解を表示します**)**
Information security procedures describe how security requirements are applied in day-to-day operations. Business units must be involved because they understand the actual processes, systems, workflows, and operational constraints.

質問: **394**
ゼロトラストセキュリティモデルにおいて、組織のリソースへの不正アクセスを防止するための最も効果的な戦略は次のうちどれですか？
A. 職務役割に基づいて管理権限を割り当てる
B. 継続的な認証と本人確認の実施
C. 複雑なパスワードを使用して機密データへのアクセスを制限する
D. 境界ファイアウォールと仮想プライベートネットワーク(VPN)トンネルに依存する
正解: **B (**コメントを発表する**)**
Zero Trust is based on "never trust, always verify." Continuous authentication and identity verification ensure access is repeatedly validated based on user identity, device status, context, and risk before allowing access to resources.

質問: **395**
情報セキュリティプログラムの効率性を測定するのに最適な指標は次のうちどれですか？
A. 特定されたリスクあたりの平均緩和コスト
B. 完了した学習活動の数
C. リスク評価と脆弱性スキャンの比率(経時変化)
D. 制御基準値が定義されているシステムの割合
正解: **(**正解を表示します**)**
The percentage of systems with defined control baselines is the best metric to measure the efficiency of an information security program, as it reflects how well security controls are implemented and standardized across the organization. This helps in maintaining a consistent security posture and reducing vulnerabilities.

質問: **396**
インシデントが解決された後、情報セキュリティマネージャーにとって最も重要な重点分野は次のうちどれですか？
A. インシデント管理プロセスの見直し
B. セキュリティポリシーの更新

C. 影響を受けるシステムを隔離する
D. 教訓共有セッションの開催
正解: **(**正解を表示します**)**
After remediation, the most important focus for the information security manager is to conduct a lessons learned session. This enables the organization to analyze the root cause, assess response effectiveness, and apply improvements to prevent recurrence. It's a critical step in strengthening the overall security posture and refining incident response procedures.

質問: **397**
あるオンライン取引会社が、ネットワーク攻撃によってファイアウォールが突破されたことを発見しました。情報セキュリティマネージャーは、まず何に対応すべきでしょうか？
A. ファイアウォールのログを調べて攻撃者を特定する。
B. 緩和策を実施する。
C. 事業への影響を評価する。
D. 規制当局に事故を通知する。
正解: **C (**コメントを発表する**)**

質問: **398**
買収のデューデリジェンス段階において、情報セキュリティマネージャーにとって最も重要な行動は以下のとおりです。
A. 情報セキュリティポリシーの見直し。
B. セキュリティ意識の現状を確認する。
C. ギャップ分析を実施する。
D. リスク評価を実施する。
正解: **D (**コメントを発表する**)**
During due diligence, conducting a risk assessment is key to uncovering the target's security exposures, quantifying their potential impact, and informing both go/no-go decisions and negotiation of remediation or pricing.

質問: **399**
情報セキュリティプログラムの指標を設定する際、最適なアプローチは、以下の指標を特定することです。
A. 企業のリスク文化を反映する。
B. 主要な情報セキュリティ対策を支援する。
C. セキュリティプログラムの有効性を実証する。
D. 情報セキュリティプログラムへの支出を削減する。
正解: **(**正解を表示します**)**

質問: **400**
組織内で望ましい情報セキュリティ文化を醸成するために、次のうちどれが最も役立ちますか？
A. 効果的な情報セキュリティポリシーと手順
B. 情報セキュリティの役割と責任の委任

C. 情報セキュリティ意識向上トレーニングおよびキャンペーン
D. 適切な情報セキュリティ関連行動に対するインセンティブ
正解: **(**正解を表示します**)**

質問: **401**
以下のバックアップのうち、フォレンジック調査に最適なものはどれですか？
A. ファイルシステムのダンプ
B. 仮想化イメージ
C. ファイル割り当てテーブルのダンプ
D. ビット単位のコピー
正解: **D (**コメントを発表する**)**
For forensic purposes, the bit-by-bit copy is the best choice because:
* Preserves all data: A bit-by-bit copy captures every bit of data on the storage device, including deleted files, unallocated space, and file system metadata. This level of detail is crucial for forensic investigations.
* Integrity and accuracy: Bit-by-bit copies ensure that the forensic image is an exact replica of the original storage medium, minimizing the risk of data loss or alteration during the backup process.
* Legal admissibility: In forensic investigations, maintaining the integrity of evidence is critical. Bit- by-bit copies can be hashed to verify that the image has not been tampered with, which supports legal admissibility.

質問: **402**
事業継続計画(BCP)の発動につながる事象が発生しました。事象発生時には全従業員に通知され、計画に従って対応しました。しかし、主要サプライヤー2社は、混乱を知らなかったため納期を守れませんでした。今後、同様の事態を防ぐための最善策は何でしょうか？
A. サプライヤーとのサービスレベル契約(SLA)が確実に履行されるようにする。
B. BCPコミュニケーションプランのテストを実施する。
C. 侵入テストを実施する。
D. サプライヤーにBCP文書へのアクセスを提供する。
正解: **(**正解を表示します**)**
The best way to prevent a similar situation in the future is to perform testing of the BCP communication plan. Regularly testing how the organization communicates with suppliers during a disruption ensures that everyone involved knows how to respond and that communication channels are effective, reducing the risk of missed deadlines.

質問: **403**
ある事業部門が、顧客向けサービスを提供するモバイルアプリを開発しました。ユーザーエクスペリエンスへの懸念から、事業部門が強力なパスワードポリシーの導入に抵抗する場合、情報セキュリティマネージャーが取るべき最善のアプローチは次のうちどれでしょうか？
A. 事業部門とセキュリティリスクについて検討する。
B. ユーザーエクスペリエンスを向上させることによるコストとメリットを評価する。
C. リスクとユーザーへの影響を上級管理職に提示する。

D. 事業部門にポリシーを遵守させる。
正解: **(**正解を表示します**)**
The best approach is to collaborate with the business unit by reviewing the security risks associated with weak passwords. This allows the security manager to communicate the potential threats in a way that aligns with business objectives. By discussing possible alternatives, such as multi-factor authentication (MFA) or biometric authentication, the security manager can help find a balance between security and user experience without imposing rigid policies.

質問: **404**
クラウド環境でホストされている一部のITサービスが侵害された、範囲が限定的なインシデントに対処する際に、最も効果的なインシデント封じ込め戦略は次のうちどれですか？
A. 今回の事態によるさらなる被害を防ぐため、直ちに全てのクラウドサービスを停止してください。
B. 不正アクセスを防ぐため、関連するユーザーアカウントを無効にします。
C. オンプレミスのバックアップから復元して、サービスを即座に再開します。
D. 他のサービスの可用性を維持しながら、影響を受けるクラウド リソースを隔離します。
正解: **D (**コメントを発表する**)**
For a limited-scope cloud incident, the best containment approach is targeted isolation. It prevents the incident from spreading while preserving business availability for unaffected services.

質問: **405**
情報セキュリティガバナンスを企業ガバナンスに統合する上で、最も大きな課題となるのは次のうちどれですか？
A. 利害関係者は情報セキュリティプログラムに投資していません。
B. 情報セキュリティのベストプラクティスは十分に理解されていない。
C. セキュリティ組織構造は明確に定義されていない。
D. 重要なセキュリティプロセスは外部委託されています。
正解: **(**正解を表示します**)**
Integrating information security governance into corporate governance requires active stakeholder engagement and ownership. If stakeholders are not invested, governance cannot be embedded into decision-making, prioritization, and accountability, making this the greatest challenge.

質問: **406**
情報セキュリティプログラムを企業統治に統合する上で、最も効果的な方法はどれでしょうか？
A. 最低限のセキュリティ基準
B. 残存リスクの文書化
C. 脅威状況の文書化
D. 最新のセキュリティ戦略
正解: **(**正解を表示します**)**
An up-to-date security strategy is crucial for integrating the information security program into corporate governance. It ensures alignment between business objectives and security goals, helping to communicate security priorities and actions to senior management and other stakeholders effectively.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu **193**問、３０%ディスカウント、特別な割引コード:**JPNshiken**」

質問: **407**
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する最善の方法は、次の点を確保することです。
A. 情報セキュリティ運営委員会は、セキュリティ ポリシーの遵守を監視します。
B. 経営チームは情報セキュリティをビジネスプロセスに組み込みます。
C. 意識向上プログラムには、情報セキュリティ ガバナンスに関する業界のベスト プラクティスが含まれます。
D. 情報セキュリティ プログラムは定期的な外部監査に含まれています。
正解: **(**正解を表示します**)**
The best way to integrate information security governance with corporate governance is for management teams to embed information security into business processes. The CISM Review Manual explains that aligning security objectives and activities with organizational goals and business processes ensures that security is a core part of business operations and strategy, not an isolated activity.

質問: **408**
情報セキュリティガバナンスフレームワークの承認責任者は誰ですか？
A. 上級管理職
B. 情報セキュリティ運営委員会
C. 情報セキュリティマネージャー
D. 企業リスク委員会
正解: **(**正解を表示します**)**
Senior management is accountable for approving the information security governance framework because governance requires executive authority to set direction, assign accountability, and ensure alignment with business objectives and risk appetite.

質問: **409**
効果的な情報セキュリティガバナンスの重要な利点は次のとおりです。
A. 情報セキュリティコンプライアンス要件との整合性。
B. 情報に基づいた情報セキュリティの意思決定。
C. 情報セキュリティプロジェクトの優先順位付け。
D. 情報セキュリティリスクの回避。
正解: **(**正解を表示します**)**

Effective information security governance enables informed decision making by establishing accountability, oversight, and clear direction so leaders can make risk-based security decisions aligned with business needs.

質問: **410**
セキュリティインシデントを分類する最も重要な理由は以下のとおりです。
A. インシデント解決の効率と効果を向上させる。
B. セキュリティイベントとインシデントのログ記録をより適切に管理する。
C. インシデント対応計画を企業方針に合わせる。
D. インシデントリーダーへのインシデント状況の報告を強化する。
正解: **(**正解を表示します**)**
Classifying security incidents enables proper prioritization, routing, and assignment of response actions. This ensures the right resources and procedures are applied quickly, improving both the speed and effectiveness of incident resolution.

質問: **411**
組織のリスク許容度がリスク対策プロセスの一部として考慮されるようにするための最善の方法は、次のうちどれですか？
A. リスク対策計画には運営委員会の承認が必要です。
B. 定量的リスク評価手法を用いる。
C. リスク登録簿を参照してください。
D. リスク対策に関する定期的な報告を上級管理職に提供する。
正解: **(**正解を表示します**)**
Requiring steering committee approval of risk treatment plans ensures that the organization's risk appetite is considered, as the steering committee typically includes senior management who are responsible for setting the organization's risk tolerance and aligning it with business objectives.
This step ensures that the risk treatment process is in line with the organization's strategic goals and risk appetite.

質問: **412**
情報セキュリティ管理者が組織のインシデント管理準備レベルを判断する上で、最も有効な方法はどれですか？
A. インシデント対応ポリシーの更新
B. 外部侵入テスト
C. 卓上運動
D. インシデント対応プレイブックの開発
正解: **C (**コメントを発表する**)**
Tabletop exercises are the best method for determining an organization's incident management readiness because they simulate real-world scenarios and test the effectiveness of the incident response plan. These exercises help identify gaps, improve coordination, and enhance preparedness. While updated policies, penetration testing, and playbooks are valuable, they do not actively test the organization's ability to respond to incidents in a controlled setting.

質問: **413**
新任の情報セキュリティマネージャーが、現在のインシデント通知およびエスカレーションプロセスを評価する際に、最初に行うべきことは次のうちどれですか？
A. 現在のインシデント関連の通信計画をテストする。
B. 主要なインシデント対応関係者へのインタビュー。
C. 業界のベストプラクティスがプロセスに組み込まれていることを確認する。
D. 最近のセキュリティインシデントに関する調査結果をレビューする。
正解: **(**正解を表示します**)**
Interviewing key stakeholders provides firsthand insight into how the current incident notification and escalation processes function in practice, helping the new manager identify strengths, weaknesses, and areas for improvement.

質問: **414**
フィッシングメールが悪質かどうかを判断するのに最も役立つのは次のどれですか?
A. セキュリティ意識向上トレーニング
B. リバースエンジニアリング
C. 脅威情報
D. サンドボックス
正解: **(**正解を表示します**)**
The option that is most helpful in determining whether a phishing email is malicious is threat intelligence. Threat intelligence provides context and information about known phishing tactics, techniques, and indicators of compromise. It can help identify whether the email is part of a larger campaign or associated with known malicious actors.

質問: **415**
組織のセキュリティ基準は、以下の点に基づいて策定されるべきである。
A. 政策。
B. ガイドライン。
C. 規格。
D. 手順。
正解: **(**正解を表示します**)**
Security baselines are derived from standards because standards define the mandatory minimum requirements that baselines translate into specific secure configuration starting points.

質問: **416**
セキュリティ会社が、外部向けウェブページの暗号化プロトコルに重大なセキュリティ上の欠陥があることを公表しました。情報セキュリティマネージャーは、まず次のうちどれを行うべきでしょうか？
A. 脆弱性を修正してください。
B. 暗号化キーを回転させます。
C. リスク評価を実施する。

D. インシデント対応チームをアクティブ化する。
正解: **(**正解を表示します**)**
The first action the information security manager should take is to perform a risk assessment.
This allows the organization to assess the potential impact of the vulnerability, determine the exposure, and prioritize the response based on the level of risk to the organization.

質問: **417**
既存システムに新たなリスクが存在するかどうかを判断するための最適な方法は、次のうちどれですか？
A. 頻繁なセキュリティアーキテクチャレビュー
B. 定期的なセキュリティ監査
C. リスク登録簿の頻繁な更新
D. 定期的なリスク評価
正解: **(**正解を表示します**)**
Regularly scheduled risk assessments are the best method for determining whether new risks exist in legacy systems. These assessments allow for an ongoing review of the systems to identify emerging risks, vulnerabilities, or changes in the threat landscape that may not have been previously addressed, ensuring that any new risks are detected and mitigated in a timely manner.

質問: **418**
脆弱性分析の結果、重要なソフトウェアプラットフォームのアップグレードが必要であることが判明した。
アップグレードのための投資を調達する最良の方法はどれですか？
A. 脅威評価を実施する。
B. ギャップ分析レポートを提示する。
C. セキュリティリスクシナリオを作成する。
D. ビジネスケースを作成する。
正解: **(**正解を表示します**)**
The best way to obtain investment for a critical software platform upgrade is to prepare a business case. A business case outlines the justification for the upgrade, including costs, benefits, risk mitigation, and how it aligns with organizational goals. It helps senior management understand the need for the upgrade in terms of business value, financial impact, and potential risk reduction. While threat assessments, gap analysis reports, and security risk scenarios provide valuable technical insights, a business case communicates the strategic and financial necessity to secure investment.

質問: **419**
ある組織が、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った場合、情報セキュリティマネージャーが取るべき最も重要な行動は次のうちどれでしょうか？
A. 第三者との契約を解除することをお勧めします。
B. 契約した第三者の外部監査を実施する。
C. 第三者の外部プロバイダーに対する独立した監査を実施する。
D. 第三者と外部プロバイダーとの間の契約を評価する。

正解: **D** (コメントを発表する)

質問: **420**
データ分類は主に以下の者の責任です:
A. 上級管理職。
B. データ管理者。
C. データの所有者。
D. セキュリティ マネージャー。
正解: **C** (コメントを発表する)
Data classification is primarily the responsibility of the data owner. The data owner is responsible for determining the sensitivity and value of the data and deciding how it should be classified, based on the organization's policies and regulatory requirements.

質問: **421**
情報セキュリティマネージャーが事業計画書を検討した結果、残存リスクが組織のリスク許容度を超えることが判明しました。この場合、事業計画書に以下のうちどれを追加すべきでしょうか？
A. 調整されたリスク許容度
B. 緩和策
C. 代替事業計画
D. 費用便益分析
正解: **B** (コメントを発表する)
When residual risk exceeds the organization's risk tolerance, mitigating actions must be added to the business case to reduce the risk to an acceptable level and ensure alignment with organizational risk management policies.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu 「**193**問、３０%ディスカウント、特別な割引コード:**JPNshiken**」

質問: **422**
ゼロトラストが正常に実装されたことを最も確実に保証するのは、次のうちどれですか？
A. 関係者へのアンケート調査
B. 内部監査の実施
C. 独立した評価を実施する
D. 脆弱性テストの実施
正解: **C** (コメントを発表する)

An independent assessment provides the greatest assurance because it offers an objective, unbiased evaluation of whether Zero Trust principles (continuous verification, least privilege, segmentation, monitoring) are truly implemented and operating effectively across the organization.

質問: **423**
脆弱性評価の結果、エンドポイントに承認されていないポートが開いていることが判明しました。情報セキュリティ管理者は、まず最初に次のうちどれを行うべきでしょうか？
A. 脆弱なデバイスをすべてシャットダウンしてください。
B. 脆弱性の根本原因を特定する。
C. 脆弱性について上級管理職に報告する。
D. 脆弱性の影響を判断する。
正解: **(**正解を表示します**)**
Before taking action, the information security manager should first assess the impact of the vulnerability to prioritize response efforts appropriately and avoid unnecessary disruption.

質問: **424**
次のうち、インシデント封じ込め手順の目的はどれですか？
A. 将来の事件を防ぐ
B. 攻撃を無力化しようとする
C. さらなる影響を最小限に抑える
D. 事件の深刻度を判断する
正解: **C (**コメントを発表する**)**
The primary objective of incident containment procedures is to minimize further impact by stopping the spread or escalation of the incident, allowing for effective recovery and mitigation.

質問: **425**
情報セキュリティプログラムにおいて、最も重要な目標は次のうちどれですか？
A. リソースの最適化
B. ビジネス意思決定の強化
C. 管理コントロール
D. 危険因子の低減
正解: **(**正解を表示します**)**

質問: **426**
ソフトウェア会社が、Webアプリケーションで第三者によって開発されたコードを使用する際に伴うリスクを最小限に抑えるための最も効果的な方法は、次のうちどれですか？
A. リリース前に静的および動的コードスキャンを実施してください。
B. ウェブに公開されているインフラストラクチャの脆弱性スキャンを実行します。
C. 第三者に対し、組織の開発基準を遵守するよう求める。
D. ソフトウェア構成分析を開発標準に組み込むことを保証する。

正解: **(**正解を表示します**)**
Software composition analysis (SCA) specifically identifies vulnerabilities, outdated components, and licensing risks in third-party libraries and dependencies. Integrating SCA into development standards ensures continuous monitoring and management of third-party code risks throughout the software development lifecycle, making it the most effective control for this scenario.

質問: **427**
組織のインシデント対応能力の有効性を最もよく示しているのは、次のうちどれですか？
A. 処理したインシデントの数
B. 事件解決までの時間
C. 年間損失期待値(ALE)の低減
D. インシデント対応トレーニングを受けた従業員の数
正解: **(**正解を表示します**)**
Time to closure of incidents directly measures how quickly and effectively the organization can detect, contain, and resolve security events, reflecting the strength of its incident response capabilities.

質問: **428**
新しく導入したファイアウォールの有効性を検証する最良の方法は何ですか？
A. 構成レビュー
B. 脆弱性スキャン
C. 侵入テスト
D. 自動アクセス制御リストのレビュー
正解: **(**正解を表示します**)**
Penetration testing is the best way to verify the effectiveness of a newly implemented firewall because it actively tests the firewall's ability to block unauthorized access and identifies any exploitable weaknesses in a real-world scenario.

質問: **429**
生産システムのセキュリティメカニズムが管理目標を満たしていることを検証する最適なタイミングはいつですか？
A. 監視活動と自動化ツールを通じて継続的に実施
B. 侵入テストで推奨された対策が完了した後
C. 品質検査および受入検査中
D. 年次内部監査およびコンプライアンス監査の実施中
正解: **A (**コメントを発表する**)**
Continuous monitoring provides real-time assurance that a system's security mechanisms are functioning as intended and meeting control objectives, allowing for prompt detection and response to deviations.

質問: **430**

組織のデバイスに不適切なコンテンツをダウンロードしたという容疑を否定した従業員が解雇されました。懲戒処分を裏付けるために、法的証拠の収集が必要です。情報セキュリティマネージャーにとって、次のうちどれが最も適切な推奨事項でしょうか？
A. 従業員のエンドポイントセキュリティログから証拠を収集する。
B. ファイアウォールのログから証拠を収集する。
C. 従業員のデバイスにログインし、フォレンジックコピーをUSBドライブに作成します。
D. 元のファイルシステムのフォレンジックイメージを作成します。
正解: **(**正解を表示します**)**
The best recommendation for collecting legal evidence is to create a forensic image of the original file system, as it preserves the integrity of the data and ensures that the evidence remains admissible in legal proceedings. A forensic image is an exact copy of the system, including metadata and deleted files, and allows for a detailed analysis without altering the original data. While logs provide useful information, they do not offer the same level of comprehensive, legally defensible evidence as a forensic image.

質問: **431**
ある組織がコールセンターアプリケーションにIT障害を発見しました。以下のうち、このリスクを負うべき者は誰でしょうか？
A. コールセンター責任者
B. 最高経営責任者(CEO)
C. 情報セキュリティマネージャー
D. IT部門責任者
正解: **(**正解を表示します**)**
The head of the call center should own the risk related to IT failures in the call center application.
While the IT department may be responsible for maintaining the infrastructure, the call center manager has the primary responsibility for ensuring the smooth operation of the call center's processes and handling any disruptions, including IT-related issues. This ensures accountability and prompt response to address the impact on operations.

質問: **432**
情報セキュリティプログラムに関して、経営陣の賛同を得るべき最も重要な理由は次のうちどれですか？
A. スタッフ向けの情報セキュリティ研修を実施する
B. ガバナンス、リスク、コンプライアンス(GRC)機能の実装
C. 重要なシステム復旧活動のための資金を割り当てる
D. 情報セキュリティポリシーおよび標準の実施を支援する
正解: **(**正解を表示します**)**
Senior management buy-in gives the information security program authority, visibility, and organizational support. This is essential for enforcing policies and standards across business units.

質問: **433**
情報セキュリティ戦略委員会への報告のための指標を設定する際に、最も重要な考慮事項は何ですか？
A. 指標の基準値について合意する

B. 指標を伝えるためのダッシュボードの開発
C. 指標の期待値を業界標準と比較する
D. 指標を組織文化に合わせる
正解: **(**正解を表示します**)**

質問: **434**
インシデント発生後の調査により、インシデントがデータ管理者へタイムリーに報告されていないことが判明しました。組織がこの問題に対処するための最善の方法は次のうちどれですか？
A. インシデントギャップ分析を実施する。
B. 事業影響分析(BIA)を実施する。
C. 事業継続計画(BCP)を実施する。
D. インシデント対応計画を更新する。
正解: **D (**コメントを発表する**)**
The issue identified is a deficiency in the incident reporting and escalation process. Updating the incident response plan ensures clear roles, responsibilities, and notification timelines are formally defined and enforced. Strengthening the documented response procedures directly addresses delayed reporting and improves future incident handling effectiveness.

質問: **435**
セキュリティポリシーにおいて、最も重要なのは次のうちどれですか？
A. 取締役会の懸念
B. 組織目標
C. 例外処理
D. 必要な業務管理
正解: **B (**コメントを発表する**)**
Security policies must be aligned with and support the organization's objectives to ensure relevance, executive support, and effective implementation. Without alignment to organizational objectives, security policies may fail to address the most critical business risks and priorities.

質問: **436**
悪意のある活動をブロックする侵入防止機能を備えた新しいファイアウォールを設置してから数か月後、設置直後にファイアウォールを突破した侵害が発見されました。この侵害は、ファイアウォールを以下のように実装することで、より早期に検出できた可能性があります。
A. パケットフィルタリング
B. アプリケーション認識
C. ウェブ閲覧コントロール
D. ログ監視
正解: **(**正解を表示します**)**

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu ↾**193**問、３０%ディスカウント、特別な割引コード:**JPNshiken**」

質問: **437**
オンライン専業企業における可用性に関する懸念に対処するために、以下のリスク評価結果のうちどれを最優先すべきでしょうか？
A. プロバイダーへの支払いを処理するバックオフィスシステムが遅くなっています。
B. オンラインストアのウェブサーバーが分散型サービス拒否(DDoS)攻撃に対して脆弱であることが判明しました。
C. シングルサインオン(SSO)サービスへのコネクタを介したメール認証は、過去に失敗歴があります。
D. 訪問者用WiFiネットワークのアクセスポイントには、パッチが適用されていない脆弱性が複数存在します。
正解: **B** (コメントを発表する)
https://hyperproof.io/resource/the-ultimate-guide-to-risk-prioritization/

質問: **438**
ホットサイトを利用する主な理由として、次のうちどれが挙げられますか？
A. リスク受容
B. 回復ポイント
C. 回復時間
D. サービス提供
正解: (正解を表示します)
The primary reason to use a hot site is to ensure minimal recovery time in the event of a disaster or system failure. A hot site is a fully equipped and operational backup facility that allows for immediate resumption of business operations with little to no downtime. This addresses the Recovery Time Objective (RTO) by providing rapid failover capabilities. While recovery point, service delivery, and risk acceptance are important, recovery time is the key factor driving the use of a hot site.

質問: **439**
セキュリティメカニズムのコストは、以下の点に合致するべきである。
A. 年間損失期待値(ALE)。
B. セキュリティインシデントの予測コスト。
C. 保護対象となるアプリケーションの費用。
D. 期待される利益。
正解: **A** (コメントを発表する)

Annual loss expectancy (ALE) quantifies the expected financial loss from a risk over a one-year period by considering likelihood and impact. The cost of a security mechanism should be justified by and aligned with the potential annualized loss it is intended to reduce, ensuring economically sound risk management decisions.

質問: **440**
ある組織が情報セキュリティプログラムを開発しています。この取り組みの初期段階で最も役立つのは次のうちどれでしょうか？
A. 組織の情報資産の目録作成
B. 事業影響分析(BIA)の実施
C. 脅威監視サービスへの加入
D. 情報セキュリティ意識向上トレーニングの実施
正解: **A (**コメントを発表する**)**
Identifying and inventorying information assets is essential in the early stages to understand what needs protection and to prioritize subsequent security efforts.

質問: **441**
新しいサイバーセキュリティ規制が導入された後、情報セキュリティ管理者はまず次のうちどれを行うべきでしょうか？
A. ギャップ分析を実施します。
B. リスク登録簿を更新する。
C. 上級管理職に報告する。
D. 費用対効果分析を実施する。
正解: **(**正解を表示します**)**
A new regulation introduces business, legal, and strategic implications. Senior management must be informed first to set direction, determine urgency, and allocate resources.

質問: **442**
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."

質問: **443**

組織が、災害発生時にウォームサイトのサーバーバックアップが適切に維持され、使用可能であることを保証するための最善の方法は次のうちどれですか？
A. 暖かい場所に予備の機器を用意しておく。
B. 施設を点検し、バックアップ機器の在庫を四半期ごとに確認する。
C. ウォームサイトのバックアップメディア保管設備を確認する。
D. ウォームサイト施設の機器を使用してバックアップを読み取ります。
正解: **(**正解を表示します**)**
The best assurance that backups are properly maintained and usable is to actually validate readability using the warm-site equipment (i.e., perform restore/read tests). Inspections and reviews don't confirm the backups can be successfully accessed and restored during a disaster.

質問: **444**
組織の情報セキュリティ文化を向上させるために、経営陣にとって最も重要なことは以下のとおりです。
A. セキュリティ予算とリソースの見直し。
B. 優れたセキュリティ対策を実践する。
C. セキュリティ研修に参加する。
D. セキュリティポリシーを承認する。
正解: **B (**コメントを発表する**)**

質問: **445**
組織の買掛金部門では、各請求書を従業員がアプリケーションに入力し、上司が確認する必要があります。次のうち、実装するのに最適なアクセス制御の種類はどれですか？
A. 役割ベースアクセス制御(RBAC)
B. 物理的なアクセス制御
C. 強制アクセス制御
D. 多要素認証(MFA)
正解: **(**正解を表示します**)**
In the CISM framework, RBAC is the standard for managing access based on organizational functions rather than individual identity. The scenario describes a classic "maker-checker" requirement: one person inputs, another verifies. RBAC allows the Information Security Manager to define two distinct roles -- "Clerk" and "Supervisor" -- and ensure that the permissions assigned to the "Clerk" role do not overlap with the "Supervisor" role. This prevents a single user from both entering and approving an invoice.

質問: **446**
ある組織は最近、ベンダーとのデータ交換を強化するために、追加のアプリケーションプログラミングインターフェース(API)を導入しました。次回のAPI管理プロセス監査において、API関連のリスクを確実に網羅するために最も重要なことは次のうちどれですか？
A. APIエンドポイントを保護するために導入されている認証メカニズムのテスト
B. APIドキュメントとバージョン管理のプロセスを見直し、正確性と一貫性を確保する。
C. 重要なAPIに対する災害復旧計画および事業継続計画の妥当性を検証する

D. APIが組織の標準およびベストプラクティスに準拠しているかどうかを評価する
正解: **(**正解を表示します**)**
The most important action to ensure API-related risk coverage is testing the authorization mechanisms securing API endpoints. APIs can expose sensitive data or functionality, so strong authentication and authorization controls are critical to prevent unauthorized access and data breaches.

質問: **447**
サイバーインシデント対応の根絶フェーズにおいて、以下の活動のうちどれが最も適切でしょうか？
A. 影響を受けたシステムを隔離し、さらなる損傷を防いでください。
B. 影響を受けたシステムを正常な動作状態に戻す。
C. 事故によって生じた損害額を推定する。
D. 悪用された脆弱性を軽減し、将来のインシデントを阻止する。
正解: **D (**コメントを発表する**)**
During the eradication phase, the primary focus is on eliminating the root cause of the incident, including mitigating any vulnerabilities that were exploited. This ensures that the same type of attack cannot occur again in the future.

質問: **448**
クラウドベースのアプリケーションを利用する組織内で、クレデンシャルスタッフィング攻撃を軽減するための最も効果的な方法はどれですか？
A. クラウドアクセスセキュリティブローカー(CASB)を使用して、セキュリティポリシーをクラウドアプリケーションに拡張します。
B. パスワードの使い回しの危険性と認証情報の衛生管理の重要性についてユーザーに教育する。
C. 複雑なパスワードポリシーと定期的なパスワード変更を義務付ける。
D. すべてのユーザーアカウントに多要素認証(MFA)を実装する。
正解: **(**正解を表示します**)**
Credential stuffing uses valid stolen username/password pairs, so the most effective mitigation is enforcing MFA, which blocks account access even when passwords are compromised.

質問: **449**
高または重大と分類される脆弱性について、修復措置の優先順位を決定する際に最も重要な考慮事項は次のうちどれですか？
A. 影響を受けるデバイスの数
B. 初回検出からの経過時間
C. 緩和に必要な努力
D. 悪用可能性
正解: **D (**コメントを発表する**)**
Exploitability directly measures how easily an attacker can leverage the vulnerability; high or critical flaws that are readily exploitable pose the greatest immediate risk and should be remediated first.

質問: **450**

アプリケーションシステムの監査により、以前の監査で指摘されたのと同じセキュリティ上の脆弱性が発見され、リスク受容期限が近づいています。リスク管理の観点から、情報セキュリティマネージャーにとって最適な行動は次のうちどれでしょうか？
A. リスク登録簿の既存の所見を更新し、リスク受容期間を延長する。
B. リスク登録簿に新しいエントリを作成し、以前のリスク発見をクローズします。
C. リスクを保険契約に移転し、リスク発見を終了させる。
D. 事業リスク責任者に観察結果を伝え、リスク対策の選択肢について話し合う。
正解: **(**正解を表示します**)**
The best course of action is to raise the observation to the business risk owner to discuss risk treatment options. Since the risk acceptance period is about to expire and the same weakness has been identified again, it is essential to engage the business risk owner in a discussion about how to address the risk-whether through remediation, mitigation, transfer, or re-evaluation of the risk acceptance. This ensures that the risk is effectively managed, and the business is informed of any potential impact. Simply extending or closing the risk acceptance without addressing the underlying issue may leave the organization exposed.

質問: **451**
クラウドサービスプロバイダーを利用する際に、データが混ざったり漏洩したりしないようにするための最善の方法は次のうちどれですか？
A. 独立監査報告書を入手する。
B. 契約書にセキュリティ侵害に対する高額な罰則条項を含める。
C. プロバイダーの情報セキュリティポリシーを確認してください。
D. プロバイダーに厳格なデータ分類手順に従うことを義務付ける。
正解: **D (**コメントを発表する**)**

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu 📢**193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **452**
情報セキュリティの現状に関する最新情報を提供する際に、情報セキュリティ管理者が最も重視すべき事項は次のうちどれですか？
A. 事業補償統制
B. ビジネスへの影響
C. 固有のリスクレベル
D. 業界ベンチマーク
正解: **(**正解を表示します**)**

Updates on information security status should be meaningful to management and business stakeholders. Focusing on business impact shows how current risks, incidents, control gaps, and security activities affect operations, revenue, compliance, reputation, and strategic objectives.

質問: **453**
情報セキュリティ管理者が統制上の不備分析を行った際に、データ漏洩が発生したことが判明しました。最初に行うべきことは次のうちどれでしょうか？
A. 補償制御を展開する。
B. 関係者に情報漏洩を通知する。
C. 根本原因分析を実施する。
D. インシデントのトリアージを実施する。
正解: **(**正解を表示します**)**
Upon discovering a data breach, the first step is to perform incident triage to confirm the incident, assess its scope, and determine severity. Triage establishes the facts necessary to initiate appropriate containment, escalation, and response actions in a structured and controlled manner.

質問: **454**
組織のフィッシングシミュレーションプログラムの有効性を評価する際に、情報セキュリティマネージャーが最も懸念すべき事項は次のうちどれでしょうか？
A. 報告されたフィッシング攻撃件数の増加
B. フィッシングシミュレーションソフトウェアのライセンス費用の増加
C. 上級管理職による監視の強化
D. 時間の経過に伴うクリック率の上昇
正解: **(**正解を表示します**)**
Increasing click rates over time indicate users are becoming more susceptible (or the program is not improving behavior), meaning the phishing simulation and awareness efforts are not effectively reducing risk.

質問: **455**
組織の情報セキュリティプログラムの有効性を測定するための最適なデータソースは次のうちどれですか？
A. インシデント対応テスト結果
B. 主要業績評価指標(KPI)
C. 主要リスク指標(KRI)
D. リスク評価
正解: **(**正解を表示します**)**
Key performance indicators (KPIs) are specifically designed to measure how effectively an information security program is performing against its objectives, making them the best source of data for evaluating overall program effectiveness.

質問: **456**
情報セキュリティ違反を上級管理職に報告するための最適な方法は、次のうちどれですか？

A. 不遵守の根本原因を説明してください。
B. 法令違反に対する是正措置の費用について説明してください。
C. 競合組織における法令違反のシナリオを説明する。
D. 法令遵守違反の潜在的な影響について説明してください。
正解: **(**正解を表示します**)**
Senior management is primarily concerned with business impact. Explaining the potential impact of noncompliance translates security issues into business risk, enabling informed decision- making, whereas root causes or remediation costs are secondary at the executive level.

質問: **457**
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."

質問: **458**
データ所有者の主な責任は次のうちどれですか？
A. 分類情報
B. データ保持スケジュールの決定
C. ユーザーアクセス管理
D. 情報の保護
正解: **A (**コメントを発表する**)**
The primary responsibility of a data owner is to classify information. This involves determining the sensitivity and criticality of data, which guides the implementation of appropriate security controls and access permissions. Accurate classification ensures that data is protected according to its value and risk level.
While data owners may also be involved in determining data retention schedules, securing information, and administering user access, these tasks are typically shared with other roles such as data stewards, IT security teams, and system administrators. However, the foundational step of classifying information falls primarily to the data owner, as it informs all subsequent data management and protection efforts.

質問: **459**
情報セキュリティ管理者は、組織がランサムウェア攻撃を受けた疑いがあると述べている。
まず最初に何をすべきでしょうか？

A. 感染を確認する。
B. 上級管理職に報告する。
C. 災害復旧計画(DRP)を発動します。
D. 最新のバックアップから復元します。
正解: **(**正解を表示します**)**
If ransomware is only suspected, the first step is to validate whether an incident has actually occurred. Confirmation determines the scope, affected systems, severity, and whether containment, escalation, or DRP activation is required.

質問: **460**
情報セキュリティインシデントが発生した場合、一貫性のある正確な情報を一般に伝えるために最も役立つのは次のうちどれですか？
A. 広報室にはコミュニケーション用のテンプレートが用意されています。
B. インシデント対応チームがプレスリリースを配布します。
C. 広報室は、インシデント対応計画に関与しています。
D. 包括的な技術データが通信室に提供されます。
正解: **(**正解を表示します**)**
The most helpful way to ensure consistent and accurate information is communicated to the public during an incident is by involving the communications office in incident response planning.
This allows the communications team to be familiar with the process, understand key messages, and prepare templates for timely and coordinated public communication.

質問: **461**
セキュリティ運用においてAIツールを使用する最大のメリットは次のうちどれですか？
A. 定義されたリスク許容度
B. 優先度の高い脆弱性
C. 脅威の迅速な検知と対応
D. システムのパッチ適用に必要な時間と労力を削減
正解: **(**正解を表示します**)**
AI tools in security operations provide the greatest benefit by enabling rapid detection and response to threats through automated analysis, pattern recognition, and real-time decision- making, significantly improving incident handling efficiency.

質問: **462**
顧客データを含む新しいアプリケーションは、展開前にテストする必要があります。必要なテストレベルを主に決定する要因は次のうちどれですか？
A. データの分類
B. 費用便益分析の結果
C. アプリケーションがホストされている場所
D. 開発者が使用するプログラミング言語

正解: (正解を表示します)
The classification of the data determines its sensitivity and criticality, which directly drives the level of security controls and testing rigor required. Applications handling highly sensitive customer data require more extensive testing to ensure confidentiality, integrity, and compliance obligations are adequately addressed.

質問: **463**
事業継続管理において、最も重要な考慮事項は次のうちどれでしょうか？
A. 重要なビジネスプロセスの特定
B. 機密情報資産の保護
C. バックアップデータの定期テスト
D. 人々の安全を確保する
正解: **D** (コメントを発表する)
The most important consideration of business continuity management is ensuring human safety.
In any disaster or crisis situation, protecting the safety and well-being of personnel is the top priority. Once human safety is ensured, the focus can shift to restoring critical business functions and securing assets.

質問: **464**
ある組織は、リアルタイムの視覚データを処理するサーバーが、ランサムウェア攻撃における横方向移動段階に対して脆弱である可能性があることを発見しました。この脆弱性を最も効果的に軽減できる対策は次のうちどれですか？
A. 転送中のデータの暗号化
B. 侵入検知システム(IDS)
C. データ損失防止(DLP)
D. ネットワークセグメンテーション
正解: (正解を表示します)
Network segmentation limits the ability of attackers to move laterally between systems, effectively reducing the risk of ransomware spreading from one compromised server to others.

質問: **465**
情報セキュリティ管理者が効果的な情報セキュリティポリシーを策定する際に考慮すべき最も重要な側面は、次のうちどれですか？
A. 経営陣は方針に同意すべきである
B. 新しい技術が導入された際には、政策を更新する必要がある。
C. 従業員はセキュリティポリシーに関する研修を受けるべきである
D. 方針は事業と整合しているべきである
正解: **D** (コメントを発表する)
Aligning information security policies with the organization's business objectives ensures that security measures support and enhance the company's goals rather than hinder them. This alignment facilitates seamless integration of security practices into daily operations, promoting compliance and fostering a culture where security is viewed as a business enabler.

質問: **466**
次のうち、新たなIT関連の脅威が組織に影響を与えていることを最もよく示しているのはどれですか？
A. サーバーアクティビティの低下
B. システム上で異常な活動が増加
C. 利用可能な収納スペースの減少
D. パッチ未適用サーバー数の増加
正解: **(**正解を表示します**)**
An increase in unusual activity on a system is a strong indicator that an emerging IT-related threat may have impacted the organization, as it reflects potential unauthorized or anomalous behavior requiring investigation.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu 📌**193**問、３０%ディスカウント、特別な割引コード:**JPNshiken**」

質問: **467**
組織の情報セキュリティポリシーを策定する際に、最も重要な考慮事項は次のうちどれでしょうか？
A. これらのポリシーは業界のベストプラクティスに準拠しています。
B. ポリシーは事件発生後に更新されます。
C. 署名済みのユーザーによるポリシーへの同意が必要です。
D. 経営陣はこれらの方針を支持しています。
正解: **(**正解を表示します**)**
Senior management support is critical to ensure policies are enforced, resourced, and integrated into organizational governance. Without leadership backing, policies lack authority, accountability, and organizational commitment, making effective implementation unlikely regardless of their content.

質問: **468**
情報セキュリティ管理者が侵入テストを実施するために外部業者と契約する主な理由は次のうちどれですか？
A. 脆弱性に関する独立した見解を得るため
B. 検査費用を削減するため
C. 既存の警備スタッフを訓練する
D. システム脆弱性の全リストを取得する
正解: **(**正解を表示します**)**
Contracting with an external provider for penetration testing primarily aims to obtain an independent view of vulnerabilities within an organization's systems. External testers bring a fresh perspective, free from internal biases, and can identify security weaknesses that internal teams might overlook. This independent assessment is crucial

for uncovering vulnerabilities that could be exploited by malicious actors, thereby enhancing the organization's security posture.
While other factors like cost reduction, staff training, and comprehensive vulnerability identification are important, the key benefit of engaging an external provider is the objective evaluation they offer. This objectivity ensures that the organization receives an accurate and unbiased assessment of its security vulnerabilities.

質問: **469**
組織の情報セキュリティポリシーと現地の規制との間に矛盾が生じた場合、情報セキュリティマネージャーはまず次のうちどれを行うべきでしょうか？
A. 地域の規制を施行する。
B. 規制に関する独立した評価を取得する。
C. 法律相談を受ける。
D. 組織の情報セキュリティポリシーを徹底する。
正解: **(**正解を表示します**)**
When policy conflicts with local regulation, the first step is to obtain legal guidance to accurately interpret legal obligations and determine required changes or exceptions, ensuring the organization remains compliant.

質問: **470**
情報セキュリティ運営委員会の機能として適切なものはどれですか？
A. セキュリティ戦略をビジネス目標と整合させる。
B. 規制要件を監視する。
C. セキュリティフレームワークをセキュリティ標準に準拠させる。
D. インシデント対応中に外部とのコミュニケーションを行う。
正解: **(**正解を表示します**)**
A key function of the information security steering committee is to align security strategy with business objectives. The committee ensures that the organization's security efforts support its overall goals and priorities, facilitating the integration of security into business processes.
While monitoring regulatory requirements and aligning frameworks with standards are important, they are typically the responsibility of the security team or compliance officers. External communication during incident response is also usually handled by a designated incident response or communication team.

質問: **471**
新しいセキュリティ対策への資金提供について、上級管理職の承認を得る上で最も役立つのは次のうちどれですか？
A. ギャップ分析
B. 事業影響分析(BIA)
C. ビジネスケース
D. 脆弱性評価
正解: **(**正解を表示します**)**

A business case is the most useful for obtaining senior management approval for funding a new security initiative. It outlines the benefits, costs, risks, and strategic value of the initiative, helping senior management make an informed decision about its funding and alignment with organizational objectives.

質問: **472**
災害復旧計画(DRP)とインシデント対応計画の整合性を確保するために、情報セキュリティマネージャーが確認すべき最も重要な事項は次のうちどれですか？
A. 事業影響分析(BIA)が最近更新されました。
B. これらの計画は、エスカレーションに関して同様の要件を持っています。
C. 関連するテストは、同じ組織部門が担当します。
D. 計画書には、さまざまなチーム間の引き継ぎが記載されています。
正解: **(**正解を表示します**)**
To ensure alignment between the disaster recovery plan (DRP) and the incident response plan, it is most important to verify that the plans document the handoff between various teams. This ensures smooth coordination and transition of responsibilities between teams when responding to an incident, minimizing delays and confusion during critical recovery efforts.

質問: **473**
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べき最も重要な項目は次のうちどれですか？
A. 回復手順
B. 封じ込め手順
C. セキュリティプログラムの主要目標
D. 通知基準
正解: **D (**コメントを発表する**)**
https://blog.jirivanek.eu/en/escalation-policy-in-cybersecurity-a-critical-component-of-incident-response/

質問: **474**
情報セキュリティソリューションが組織にもたらすメリットを最もよく示しているのは、次のうちどれですか？
A. セキュリティ上の脅威とリスクへの対応
B. ソリューションによって生み出されるリソース効率
C. 時間経過に伴うコストとリスクの削減額
D. セキュリティ研修要件の軽減
正解: **(**正解を表示します**)**
The clearest organizational benefit is demonstrating costs and measurable risk reduction over time, because it ties the security solution directly to business value and risk management outcomes.

質問: **475**
情報セキュリティプログラムの主な役割は何ですか？
A. 事業に関連する情報セキュリティ要件を承認する
B. 組織のセキュリティリスク管理に関するガイダンスを提供する

C. 情報セキュリティ要件に関して関係者を教育する。
D. 定期的なリスク評価および事業影響分析(BIA)を実施する
正解: **(**正解を表示します**)**
The primary role of the information security program is to guide the organization in identifying, assessing, and managing security risks in alignment with business objectives and risk appetite.

質問: **476**
法的手続きにおいて証拠として頻繁に必要とされるアクセスログは、以下のように保存する必要があります。
A. 機密性を維持する方法で。
B. ハードコピー形式。
C. 取り外し不可能なメディアに記録します。
D. 誠実さを維持する方法で。
正解: **(**正解を表示します**)**
Access logs frequently required as evidence in legal proceedings must be stored in a manner that maintains their integrity. This ensures that the logs are not tampered with, preserving their authenticity and reliability as evidence in legal contexts.

質問: **477**
高価値資産の保護、または信頼性に関する懸念のある環境への対応において、最も優れた多層防御の実装方法は次のうちどれですか？
A. 区画化
B. 重複冗長性
C. 多要素認証(MFA)
D. 継続的なモニタリング
正解: **A (**コメントを発表する**)**
Compartmentalization separates high-value assets into isolated zones or segments with stricter access controls. This limits lateral movement and reduces the blast radius if one area is compromised, which is especially important in environments with trust concerns.

質問: **478**
侵入試行アラートを特定し、関連付けるのに最適なツールは次のうちどれですか？
A. 脅威分析ソフトウェア
B. SIEM
C. ホスト侵入検知システム
D. ネットワーク侵入検知システム
正解: **(**正解を表示します**)**
A SIEM aggregates logs and alerts from multiple sources, applies correlation rules to identify patterns of intrusion attempts, and provides centralized analysis - making it the optimal tool for correlating and identifying security events.

質問: **479**
情報セキュリティガバナンスフレームワークを導入した後、情報セキュリティプロジェクト計画を策定する上で、次のうちどれが最適な情報となるでしょうか？
A. リスク対策計画
B. 最近の監査結果
C. リスクヒートマップ
D. ギャップ分析
正解: **(**正解を表示します**)**
After implementing an information security governance framework, the gap analysis would provide the best information to develop an information security project plan. A gap analysis identifies the discrepancies between the current state of security and the desired state, which helps prioritize the necessary security initiatives and projects to close those gaps.

質問: **480**
次のうち、新たなリスクの監視を最も効果的に行う方法はどれですか？
A. 主要業績評価指標(KPI)
B. 主要リスク指標(KRI)
C. 定期的なリスク評価
D. 脆弱性スキャン
正解: **(**正解を表示します**)**
KRIs are designed to provide early warning signals that risk exposure is increasing or changing.
They help monitor emerging risks before they become incidents or exceed the organization's risk tolerance.

質問: **481**
重要な業務システムにおいて潜在的な業務侵害が発見された場合、情報セキュリティマネージャーが最初にとるべき行動は次のうちどれでしょうか？
A. 上級管理職に情報漏洩を報告する。
B. 直ちに緩和策を実施する。
C. 違反を検証する。
D. インシデント対応計画を発動する。
正解: **(**正解を表示します**)**
Before taking further action, the information security manager must first validate the breach to confirm its authenticity and scope. This ensures that appropriate and proportionate response measures are taken.

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

ス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu 1193問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **482**
従業員のセキュリティポリシー遵守を最も効果的に促進するのは、次のうちどれでしょうか？
A. 職務記述書にセキュリティポリシーを組み込む。
B. セキュリティ意識向上プログラムを実施する。
C. 従業員にポリシーへの署名による同意を求める。
D. 定期的に従業員のセキュリティクイズを実施する。
正解: **(**正解を表示します**)**
A security awareness program most effectively improves compliance by building understanding and reinforcing desired behaviors, making employees more likely to follow policies consistently than acknowledgements or quizzes alone.

質問: **483**
インシデント管理プログラムを継続的に支援してもらうために、上級管理職に提供すべき最も重要な情報は何ですか？
A. 主要業績評価指標(KPI)
B. 復旧時間目標(RTO)
C. 主要リスク指標(KRI)
D. リカバリポイント目標(RPO)
正解: **A (**コメントを発表する**)**
Senior management continued support depends on demonstrating program effectiveness and value. KPIs show how well the incident management program is performing (e.g., time to detect/respond, closure rates, trends), enabling informed decisions on resourcing and improvements.

質問: **484**
組織は、新しいシステム開発のどの段階で、最初に発生するリスクに対処すべきでしょうか？
A. テスト
B. 計画
C. 実装
D. デザイン
正解: **(**正解を表示します**)**
Emerging risks should first be identified and considered during the planning phase, when objectives, scope, requirements, and constraints are defined. Addressing risk at this early stage enables risk mitigation to be built into system requirements and architecture before design and implementation decisions are finalized.

質問: **485**
以下のうち、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どれですか？
A. 情報セキュリティプログラムは事業主によって承認されています。

B. 情報セキュリティ機能は事業全体に統合されています。
C. 情報セキュリティはアプリケーション開発プロセスの一部です。
D. 経営陣は情報セキュリティプログラムを支持している。
正解: **(**正解を表示します**)**
The best indication of a mature information security program is that information security functions are integrated throughout the business. This integration indicates that security is not just a standalone function but is embedded in all aspects of the organization, including operations, processes, and culture.
While approval from business owners, support from senior management, and inclusion in the application development process are important factors, the comprehensive integration of security across the organization reflects a higher level of maturity and commitment to protecting information assets.

質問: **486**
ゼロデイ脆弱性を悪用した標的型攻撃を検出するのに最も役立つ対策はどれですか？
A. 脆弱性スキャン
B. エンドポイント検出 ･対応(EDR)
C. 拡張型検出 ･対応(XDR)
D. 侵入防止システム(IPS)
正解: **(**正解を表示します**)**

質問: **487**
情報セキュリティ管理者が、新興技術による脅威状況の変化を特定するのに最も役立つのは、次のうちどれですか？
A. 年次セキュリティ評価
B. 外部専門家からの意見
C. 定期的なリスク評価
D. 業界他社とのベンチマーク
正解: **C (**コメントを発表する**)**

質問: **488**
組織の強力なサイバーセキュリティ文化を構築するために、以下のうちどれが最も重要ですか？
A. 従業員はゼロトラストアーキテクチャの基盤に適応します。
B. 従業員は情報セキュリティに関する意識向上研修に参加する。
C. 従業員はセキュリティポリシーとプロセスを理解している。
D. リスクシナリオの策定に従業員が参加します。
正解: **(**正解を表示します**)**
The most important factor for building a strong cybersecurity culture is ensuring employees participate in information security awareness and training. This helps them understand security risks, adopt secure practices, and foster a collective sense of responsibility for protecting the organization's assets.

質問: **489**

インシデント対応チームのトレーニングを強化するための最良の方法は、次のうちどれですか？
A. 事後検証を実施する。
B. インシデントの主要業績評価指標(KPI)を設定する。
C. 組織単位へのインタビューを実施する。
D. 緊急対応活動に参加する。
正解: **A (**コメントを発表する**)**

質問: **490**
情報セキュリティマネージャーが事業部門に伝えるべき最も重要な内容は次のうちどれですか？
A. 脆弱性評価
B. 脅威インテリジェンスレポート
C. リスクの所有権
D. 事業影響分析(BIA)
正解: **(**正解を表示します**)**
The most relevant information for an information security manager to communicate to business units is risk ownership. Clearly defining risk ownership ensures that business units understand their responsibilities regarding information security risks, which is crucial for effective risk management and accountability within the organization. While vulnerability assessments, threat intelligence reports, and business impact analyses are important, communicating risk ownership directly involves business units in the security process, helping to foster a culture of accountability and proactive risk management.

質問: **491**
個人データの収集および処理において、最も大きなプライバシー上の懸念事項は次のうちどれですか？
A. プライバシーポリシーが古くなっています
B. 収集したデータを保存するために、より多くのストレージ容量が必要
C. 同意なしに収集されたデータ
D. 必要な時間とリソースの増加
正解: **(**正解を表示します**)**
Collecting and processing personal data without consent undermines lawful basis and individual rights, creating the greatest privacy risk and potential regulatory exposure compared to operational or documentation issues.

質問: **492**
組織が情報セキュリティガバナンスフレームワークを導入する際に、経営陣が最も重視すべき事項は次のうちどれでしょうか？
A. 最適化された情報セキュリティリソース
B. セキュリティ管理の影響力増大
C. 組織全体のセキュリティ意識向上トレーニングの改善
D. 情報セキュリティ戦略の一貫した実行
正解: **(**正解を表示します**)**

The primary expectation of management when introducing an information security governance framework is the consistent execution of the organization's information security strategy. This ensures that security efforts align with business objectives and are effectively managed across all levels of the organization.

質問: **493**
情報の完全性に対処するために最も適切な管理策は次のうちどれですか？
A. メールの暗号化
B. インターネットセキュリティアプリケーションの実装
C. 冗長サーバーシステムの導入
D. 適切なアクセス権限の割り当て
正解: **(**正解を表示します**)**

質問: **494**
ある事業部門が、リスク軽減のために導入された管理策を遵守していない。なぜなら、遵守しないと事業目標の達成に支障をきたすからである。この不遵守を上級管理職に報告する際、情報セキュリティマネージャーが取るべき最善の勧告は何だろうか？
A. 例外処理プロセスを修正します。
B. 補償制御を実施する。
C. ギャップ分析を実施する。
D. ルールを守らないユーザーを教育する。
正解: **B (**コメントを発表する**)**
If a business unit cannot comply with a control due to its impact on business goals, recommending compensating controls is the best course of action. These provide alternative ways to mitigate the risk while allowing the business to achieve its objectives.

質問: **495**
金融機関のセキュリティチームが、クラウドに保存されている顧客の財務記録に適切な暗号化キー管理およびローテーションポリシーが欠けていることを発見しました。特定されたギャップに対処するための最適なアプローチは次のうちどれですか？
A. クラウド環境へのアクセスを制限する。
B. リスクに基づいた是正計画を策定する。
C. 財務データをオンプレミスストレージに転送します。
D. 追加の暗号化制御を実装する。
正解: **B (**コメントを発表する**)**
The issue is not simply "no encryption"; it is a governance/control gap around key management and rotation for sensitive cloud data. The best CISM-style response is to create a risk-based remediation plan that prioritizes actions based on data sensitivity, regulatory impact, likelihood, and business criticality.

質問: **496**

ある組織が、認証機関によって大幅に改訂されたセキュリティ標準を使用しています。認証を維持したい組織は、旧バージョンの標準を使用できなくなります。最初に取るべき行動は次のうちどれでしょうか？
A. 新しい基準が事業に適用可能かどうかを検討する。
B. 新しい基準を上級幹部に伝える。
C. 認証維持にかかる費用を評価する。
D. 新たな要件が確実に満たされるよう、ポリシーを修正する。
正解: **A** (コメントを発表する)

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu を**193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **497**
サイバーセキュリティインシデント発生後の復旧において、以下のうちどれを最優先すべきでしょうか？
A. 復旧したシステムをオンラインにする
B. 上級管理職向け報告書の作成
C. 悪用された脆弱性の特定
D. 法医学的証拠の保存
正解: (正解を表示します)
The highest priority during recovery after a cybersecurity incident should be bringing restored systems online. Ensuring that critical business systems and services are operational is essential to minimize downtime and restore normal business functions.

質問: **498**
ランサムウェア攻撃後に組織がデータを復旧するのに最も適したバックアップの種類はどれですか？
A. オフ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. オンラインバックアップ
正解: **A** (コメントを発表する)
An offline backup is the best option for recovering data after a ransomware attack. It is stored in a manner that is not accessible from the network, making it less vulnerable to encryption or deletion by ransomware. Since offline backups are not directly connected to the systems, they provide a secure recovery option without the risk of the ransomware affecting the backup data.

質問: **499**

ベンダーとの関係において効果的な情報セキュリティ管理を実施する上で、最も重要な考慮事項は次のうちどれですか？
A. セキュリティ契約上の要件
B. サイバーセキュリティ保険の補償範囲
C. ベンダー向けの災害復旧計画(DRP)
D. 監査権の義務化
正解: **(**正解を表示します**)**
The most important consideration for implementing effective information security management in vendor relationships is security contractual requirements. These requirements ensure that the vendor understands and adheres to the necessary security standards and practices, protecting the organization's data and interests throughout the partnership.
While factors like a disaster recovery plan and right-to-audit mandates are important, clear and enforceable security contractual requirements provide the foundation for managing and enforcing security obligations with vendors.

質問: **500**
情報セキュリティマネージャーは、複数の事業部門で発生した複数のセキュリティインシデントについて警告を受けました。これらのインシデントには、機密データへの不正アクセスや、重要システムからのデータ漏洩の可能性が含まれています。これらのインシデントを適切に分類し、優先順位付けするための最善の対応策は次のうちどれですか？
A. インシデント対応チームを編成し、インシデントを評価する。
B. データ分類基準に基づいてインシデントの優先順位を付ける。
C. 危機コミュニケーション計画を開始し、関係者に事件を通知する。
D. 外部のインシデント対応コンサルタントを起用し、独立した調査を実施する。
正解: **B (**コメントを発表する**)**
Using data classification standards allows the organization to assess the sensitivity and criticality of the data involved, ensuring incidents are classified and prioritized according to their potential business impact.

質問: **501**
疑わしいインシデント発生時のネットワーク活動に関する詳細情報が必要な場合、次のうちどれが最も役立ちますか？
A. パケットスニファ
B. アクセスログのレビュー
C. ネットワークタイムプロトコル
D. 法医学的調査
正解: **(**正解を表示します**)**
A packet sniffer captures and analyzes network packets, providing the most detailed visibility into actual network activity (communications, protocols, payload patterns) during a suspected incident.

質問: **502**
システムがマルウェアに感染した場合、最初に行うべきことは次のうちどれですか？

A. 影響を受けているシステムをネットワークから隔離します。
B. ファイアウォールのログを確認して、不審なイベントがないか調べます。
C. 感染をベンダーに報告し、さらなる調査を依頼してください。
D. 影響を受けたシステムにおけるデータ損失を特定します。
正解: **A** (コメントを発表する)
The first step when a system is infected with malware is to isolate the affected system from the network. This helps to prevent the malware from spreading to other systems and causing further damage. Once the system is isolated, other investigative and response actions can be taken.

質問: **503**
サイバー攻撃が確認された場合、最初に行うべきことは次のうちどれですか？
A. 影響を受けたシステムを隔離します。
B. 重症度基準
C. 根本原因分析
D. リスク許容度
正解: **A** (コメントを発表する)
The first action after confirming a cybersecurity attack is to isolate the affected system. This helps prevent the spread of the attack to other systems, containing the incident and minimizing further damage. Once the system is isolated, other actions such as severity assessment, root cause analysis, and addressing risk appetite can follow.

質問: **504**
ある組織は、事業を展開する地域市場の一つにおいて、厳格なサイバーセキュリティ法規制の要件を遵守してきましたが、最近、その法規制に変更がありました。組織はまず、次のうちどれを行うべきでしょうか？
A. 既存の管理策の有効性を判断する。
B. 事業に対する要件の適用可能性を再評価する。
C. 要件の変更点を上級管理職に伝達する。
D. コンプライアンス上のギャップに対処するための実施計画を策定する。
正解: **B** (コメントを発表する)
When legislation changes, the first step is to reassess how the updated requirements apply to the organization's business. This determines scope and impact, and only after applicability is understood can control effectiveness be evaluated, gaps identified, management informed, or implementation plans developed.

質問: **505**
情報セキュリティフレームワークの実装を最も容易にするのは、次のうちどれですか？
A. 包括的なコミュニケーション計画
B. 十分な情報セキュリティ予算
C. すべての関係者に対するセキュリティ意識向上トレーニングの義務化
D. 組織全体の関係者からの賛同
正解: (正解を表示します)

The best way to enable the implementation of an information security framework is to secure buy- in from stakeholders throughout the organization. This ensures that everyone is aligned with the framework's goals, that resources are committed, and that all departments support and follow security initiatives, leading to a more effective and comprehensive security posture.

質問: **506**
サイバーセキュリティインシデントの結果として失われたデータの復旧を最も容易にするのは、次のうちどれですか？
A. 災害復旧計画(DRP)
B. 取り外し可能なストレージメディア
C. オフサイトデータバックアップ
D. 暗号化されたデータドライブ
正解: **(**正解を表示します**)**

質問: **507**
侵入検知システム(IDS)が外部ネットワークベースの攻撃を報告した場合、ファイアウォールのログを確認する主な理由は次のうちどれですか？
A. ペイロード署名を検証する
B. インシデント対応戦略を策定する
C. ネットワーク構成を確認する
D. 事件を検証する
正解: **(**正解を表示します**)**
The primary reason to review the firewall logs when an external network-based attack is reported by the IDS is to validate the incident. Firewall logs provide detailed information on the traffic passing through the network, helping to confirm whether the IDS alert corresponds to a legitimate security event or a false positive.

質問: **508**
情報セキュリティ戦略を提示する際に、上級幹部の支持を得るために最も重要なことは、次のうちどれですか？
A. この戦略は、経営陣が許容できるリスクレベルに合致しています。
B. この戦略は業界のベンチマークと基準に合致しています。
C. この戦略は、効果のない情報セキュリティ管理に対処するものです。
D. この戦略は、組織の成熟度と脅威環境に対処するものです。
正解: **(**正解を表示します**)**
Aligning the information security strategy with management's acceptable level of risk is most important to gain senior leadership support. This ensures the strategy is relevant to the organization's goals, risk appetite, and priorities, making it more likely to receive buy-in and necessary resources.

質問: **509**
組織のポリシーを評価するIS監査担当者にとって、以下のうちどれが最も大きな懸念事項となるべきでしょうか？
A. 従業員は、これらのポリシーを正式に承認したり署名したりしていません。

B. ポリシーは毎年更新されるものではありません。
C. ポリシーは最高情報責任者(CIO)によってレビューされません。
D. ポリシーでは、組織を保護するための適切な管理策やプロセスが規定されていません。
正解: **(**正解を表示します**)**
Policies that do not identify adequate controls or processes to protect the organization represent the greatest concern, as this undermines the very purpose of having policies - to enforce security, compliance, and risk management. Without adequate controls, the organization is left vulnerable to threats and regulatory non-compliance.

質問: **510**
インシデント後の調査で、既知の脆弱性が悪用されてシステムへのアクセス権が取得されたことが判明しました。問題のシステムに対する修復作業の一環として、脆弱性は修正されました。次に実行すべきことは次のうちどれですか？
A. 脆弱性管理プロセスをレビューする。
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. 他のシステムにも脆弱性が存在するかどうかをスキャンして確認します。
D. 脆弱性の根本原因を上級管理職に報告する
正解: **(**正解を表示します**)**
After patching the offending system, the next step should be to scan other systems to determine whether the same vulnerability exists elsewhere in the environment. This helps prevent further exploitation of the same vulnerability and ensures the security of the entire system.

質問: **511**
フィッシング攻撃の成功件数が増加している組織が、情報セキュリティマネージャーに対し、問題解決のための対策を講じるよう要請しました。以下のうち、最も効果的な戦略はどれでしょうか？
A. 悪意のあるメールを送信する問題のあるドメインを隔離します。
B. メールのスパムフィルタリングを定期的に見直す。
C. セキュリティポリシーを更新し、違反した場合の罰則を明記する。
D. スタッフの現在の情報セキュリティ意識を評価する。
正解: **D (**コメントを発表する**)**
Assessing the current awareness of staff helps identify knowledge gaps that contribute to successful phishing attacks, allowing for targeted training and awareness programs to effectively reduce user susceptibility.

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

ス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu 1193問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **512**
ある重大なセキュリティインシデントへの対応中に、情報セキュリティマネージャーは、現在のインシデント対応計画にいくつかの不備があることに気づきました。計画を更新する最適なタイミングはいつでしょうか？
A. 事件を封じ込めながら
B. 回復期前
C. 事後検証中
D. リスク再評価後
正解: **(**正解を表示します**)**
The incident response plan should be updated during the post-incident review, when the incident is stabilized and the organization can capture lessons learned and incorporate needed changes without distracting from containment, eradication, and recovery.

質問: **513**
情報セキュリティ戦略に対する組織全体の支持を維持するための最良の方法は、次のうちどれでしょうか？
A. 情報セキュリティポリシーに容易にアクセスできるようにしてください。
B. ユーザーの活動を監視し、情報セキュリティポリシー違反を特定および追跡します。
C. 情報セキュリティに関する啓発資料を人目につく場所に設置する。
D. 主要な関係者が情報セキュリティの目標を理解していることを確認する。
正解: **D (**コメントを発表する**)**
Organization-wide support is best maintained when key stakeholders understand the information security objectives, because understanding drives buy-in, prioritization, and sustained commitment across business units.

質問: **514**
インシデント管理チームの準備状況を判断する最良の方法は次のうちどれですか？
A. 過去のインシデント対応統計の評価
B. 定期的な自己評価調査の実施
C. 過去の独立監査における問題点の評価
D. 定められた間隔で模擬試験を実施する
正解: **(**正解を表示します**)**
Simulated testing (e.g., tabletop exercises and drills) is the best way to determine readiness because it validates roles, procedures, coordination, and decision-making under realistic conditions, revealing practical gaps that metrics, surveys, or past audit findings may miss.

質問: **515**
ある組織が新しい会社を買収する過程にある。統合前に新たに取得したデータ資産を保護する方法を決定するための最初のステップは次のうちどれか？
A. データアーキテクチャをレビューする。

B. 契約書にセキュリティ要件を含める。
C. セキュリティ対策を評価する。
D. 在庫情報資産。
正解: **(**正解を表示します**)**
Before determining protection measures, the organization must first identify and inventory the newly acquired data assets. An accurate inventory establishes visibility into what data exists, its location, ownership, and sensitivity, forming the foundation for assessing controls and defining appropriate protection strategies.

質問: **516**
組織の情報セキュリティに関するビジョンと戦略を支援する上で、最も優れた情報源は次のうちどれですか？
A. ガバナンスポリシー
B. 指標ダッシュボード
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. 能力成熟度モデル
正解: **(**正解を表示します**)**
The best source of information to support an organization's information security vision and strategy is the enterprise information security architecture. This architecture provides a comprehensive framework that aligns security initiatives with the organization's goals, ensuring that the security strategy is integrated with overall business operations and IT infrastructure.

質問: **517**
効果的に設計された主要リスク指標(KRI)の最も優れた証拠は、次のうちどれですか？
A. KRIは定量的な指標です。
B. KRIは業界ベンチマークに準拠しています。
C. KRIは残存リスクを測定します。
D. KRIはリスク許容度を考慮します。
正解: **(**正解を表示します**)**
The best evidence of an effectively designed key risk indicator (KRI) is that it is quantitative. A quantitative KRI provides measurable data that allows the organization to track, assess, and respond to risk in a clear, objective manner. This makes it easier to identify trends and trigger appropriate actions.

質問: **518**
情報セキュリティ管理者が組織に対する新たなリスクを特定するための最良の方法は、次のうちどれですか？
A. 外部の脅威情報源を購読する。
B. 管理目標を満たしていることを確認するために、管理策の定期的なテストを実施する。
C. 責任者を定めた最新のリスク登録簿を維持する。
D. 上級関係者との定期的なリスク会議を開催する。
正解: **A (**コメントを発表する**)**

Subscribing to external threat intelligence sources is the best way for an information security manager to identify emerging risks. These sources provide timely and relevant information about new threats, vulnerabilities, and attack techniques that may affect the organization, allowing for proactive risk management and response.

質問: **519**
セキュリティインシデントを適切な関係者にエスカレーションするために、以下のうち最も重要なものはどれですか？
A. リスク受容基準
B. 重症度基準
C. 根本原因分析
D. リスク許容度
正解: **B** (コメントを発表する)
Severity criteria are the most important factor in ensuring that security incidents are escalated to the appropriate stakeholders. These criteria define the impact, urgency, and required response level for incidents, helping ensure that critical threats receive immediate attention. While risk acceptance, root cause analysis, and risk appetite play roles in risk management, they do not directly enable timely and appropriate incident escalation like severity criteria do.

質問: **520**
情報セキュリティプログラムを開発する際に、最初に実施すべき項目は次のうちどれですか？
A. 情報セキュリティ手順
B. 情報セキュリティフレームワーク
C. 情報セキュリティポリシー
D. 情報セキュリティの基準
正解: **C** (コメントを発表する)
An information security program should start with a formal information security policy because it defines management's direction, expectations, scope, and authority for security across the organization.

質問: **521**
以下のうち、インシデント撲滅段階における主要な目的はどれですか？
A. システムをクリーンな状態に復元する
B. 攻撃方法の決定
C. インシデント対応の有効性の評価
D. さらなる汚染を防ぐ
正解: (正解を表示します)
The eradication phase focuses on removing the root cause and malicious artifacts, such as malware, unauthorized accounts, backdoors, or vulnerable components, so the system can be returned to a clean and trusted state.

質問: **522**
治安対策費の増額を正当化する上で、最も重要な要素は次のうちどれですか？

A. セキュリティのベストプラクティスとの整合性
B. 残存リスクを許容レベルまで低減
C. 新たな業界脅威インテリジェンスの紹介
D. 最新のセキュリティ対策の導入率
正解: **(**正解を表示します**)**
The strongest justification for increased security funding is demonstrating it will reduce residual risk to within the organization's acceptable risk level, tying spend directly to business risk reduction.

質問: **523**
新たに任命された情報セキュリティマネージャーは、5年以上変更されていないセキュリティ関連のポリシーと手順をすべて更新するよう求められました。まず最初に何をすべきでしょうか？
A. 現在のセキュリティポリシーを一覧し、見直します。
B. 法的および規制上の要件を確認する。
C. 最良のビジネス慣行に従って更新します。
D. 現在のIT環境のリスク評価を実施する。
正解: **A (**コメントを発表する**)**
The first step is to inventory and review the existing security policies and procedures to understand what currently exists, identify outdated or missing items, and establish the baseline needed before assessing regulatory changes, aligning to best practices, or performing deeper risk-based updates.

質問: **524**
情報セキュリティプログラムへの継続的な資金確保を支援するために、以下のうちどれを整備しておくことが最も重要ですか？
A. 証券投資収益率レポート
B. 情報セキュリティリスク登録簿
C. 情報セキュリティ戦略
D. 脅威評価レポート
正解: **C (**コメントを発表する**)**
The most important factor to have in place to secure ongoing funding for the information security program is an information security strategy. A well-defined strategy aligns security efforts with the organization's business objectives, demonstrating the value and necessity of ongoing security investments to senior management.

質問: **525**
アプリケーションのテストに、サニタイズ済みのデータのみを使用する場合、どのようなリスクが生じますか？
A. データ移行中にデータ漏洩が発生する可能性があります。
B. 法令遵守義務違反が発生する。
C. 生産過程で予期せぬ結果が生じる可能性があります。
D. テスト段階でデータ損失が発生する可能性があります。
正解: **C (**コメントを発表する**)**

Using only sanitized (non-production-like) data can fail to represent real data patterns, edge cases, and quality issues, so defects may not appear during testing and can lead to unexpected outcomes once the application is in production.

質問: **526**
ゼロトラストアーキテクチャ(ZTA)において、不正アクセス試行をリアルタイムで識別し、軽減するために最も効果的な方法はどれですか？
A. ユーザーに対して厳格なパスワードの再利用と複雑性に関するポリシーを適用する
B. ゲートウェイにネットワーク侵入検知システム(IDS)を導入する
C. 悪用可能な脆弱性を減らすために、定期的な脆弱性スキャンを実施する
D. 行動分析に基づく継続的認証の実装
正解: **(**正解を表示します**)**
Zero Trust relies on continuous verification, not one-time login trust. Behavioral analytics can detect abnormal user activity in real time and trigger mitigation, such as step-up authentication, session restriction, or access termination.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu 📌**193**問、３０%ディスカウント、特別な割引コード**:** **JPNshiken**」

質問: **527**
情報セキュリティ管理者にとって、ビジネス目標に影響を与える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提供するものは、次のうちどれですか？
A. 外部監査報告書
B. 内部脆弱性評価報告書
C. 内部脅威分析レポート
D. 業界脅威インテリジェンスレポート
正解: **(**正解を表示します**)**
An industry threat intelligence report offers the most useful insights on new threats and emerging risks by providing up-to-date, external perspectives that help anticipate and mitigate threats impacting business objectives.

質問: **528**
リスク評価を実施した結果、情報セキュリティマネージャーは、財務部門が利用しているサードパーティベンダーにIT上の問題があることを特定しました。以下のうち、リスク対策計画を策定するのに最も適任なのは誰でしょうか？
A. IT部門責任者
B. 財務部長

C. ベンダー管理責任者
D. 情報セキュリティ責任者
正解: **(**正解を表示します**)**
The finance department is the business owner of the vendor relationship and the associated business risk. Therefore, the head of finance is best positioned to define the risk treatment plan (e.g., accept, mitigate via contractual/compensating controls, replace the vendor), with input from IT and information security.

質問: **529**
重要なビジネスアプリケーションの可用性を損なう可能性のある脆弱性の発生を防ぐ上で、最も効果的な対策は次のうちどれですか？
A. 変更管理統制
B. 論理アクセス制御
C. パッチ管理プロセス
D. バージョン管理
正解: **(**正解を表示します**)**

質問: **530**
組織の災害復旧計画(DRP)を策定する際、情報セキュリティ管理者はまず次のうちどれを行うべきでしょうか？
A. リスク評価を実施する
B. ビジネス要件を特定する
C. 災害復旧手順書を作成する
D. 事業影響分析(BIA)を実施する
正解: **D (**コメントを発表する**)**
The first step in developing a disaster recovery plan is performing a business impact analysis (BIA) to identify critical business functions, recovery priorities, and the potential impact of disruptions, which informs the DRP's scope and design.

質問: **531**
ある金融機関が海外に事業を拡大しており、顧客情報の保護に留意しています。以下のうち、最も懸念すべき事項はどれでしょうか？
A. 複数の管轄区域におけるセキュリティ管理の監視および実施能力
B. 組織が事業を展開する各国で利用可能な情報セキュリティリソース
C. グローバル決済カード業界の規制
D. 組織が事業を展開する各国のプライバシー関連法規
正解: **(**正解を表示します**)**

質問: **532**
アクセス権限の見直しにより、一部の元従業員のアクセス権限が依然として有効であることが判明しました。アクセス権限を取り消した後、再発防止のために最も効果的な対策は次のうちどれでしょうか？
A. アクセス制御ポリシーの見直しを開始する。

B. データ損失防止(DLP)システムを導入する。
C. 人事部の退職手続きプロセスを検証する。
D. 根本原因分析を実施する。
正解: **(**正解を表示します**)**
The best course of action to prevent the recurrence of former employees retaining access is to validate and improve the HR offboarding processes. Ensuring that these processes are comprehensive and consistently followed helps ensure that access rights are revoked in a timely manner when employees leave the organization, reducing the risk of unauthorized access.

質問: **533**
先日発生したマルウェア感染事件を受け、ある組織のIT運営委員会は、情報セキュリティマネージャーに対し、情報セキュリティプログラムの現状に関するプレゼンテーションを依頼した。
プレゼンテーションで最も重要な内容は次のうちどれですか？
A. 情報セキュリティアーキテクチャの最近の変更
B. パッチ管理の修復スケジュール
C. 災害復旧および事業継続計画
D. データ漏洩のリスクを防止するために講じられた措置
正解: **(**正解を表示します**)**
The steering committee needs a business-focused view of the information security program, especially after a malware incident. The most important point is how the program is reducing organizational risk, including controls and actions taken to prevent data compromise.

質問: **534**
バックアップ頻度を決定する際に、最も重要な考慮事項は次のうちどれですか？
A. リカバリポイント目標(RPO)
B. 最大許容停電時間(MTO)
C. 許容される中断時間
D. 復旧時間目標(RTO)
正解: **A (**コメントを発表する**)**
The most important factor to consider when determining backup frequency is the Recovery Point Objective (RPO). RPO defines the maximum acceptable amount of data loss measured in time, indicating how frequently backups need to occur to minimize the loss of critical data in the event of an incident.

質問: **535**
組織がパブリックAIツールを使用する際に、最も大きな潜在的リスクとなるのは次のうちどれですか？
A. 機密情報の漏洩
B. 方針の不遵守
C. 従業員研修の必要性の高まり
D. IT部門の関与なしにツールを使用すること
正解: **A (**コメントを発表する**)**

The greatest risk of using public AI tools is the potential exposure of sensitive information, as data input into these tools may be stored, processed, or shared externally. This could lead to data breaches, regulatory violations, or intellectual property leaks. While compliance issues, training needs, and unauthorized tool usage are concerns, they do not pose as severe a risk as unintended data exposure in public AI systems.

質問: **536**
離職率の高い組織でインシデント通知およびエスカレーション プロセスを実装する上で、最も大きな障害となるのは次のどれでしょうか。
A. 知識のある人材の不足
B. コミュニケーションプロセスの欠如
C. プロセスのドキュメント不足
D. 組織目標との整合性の欠如
正解: **(**正解を表示します**)**
The greatest obstacle to implementing incident notification and escalation processes in an organization with high turnover is the lack of knowledgeable personnel. High turnover can lead to a continuous loss of experienced staff who are familiar with incident response processes, making it difficult to establish and maintain effective incident notification and escalation protocols.
While communication processes, documentation, and alignment with organizational goals are important, the absence of knowledgeable personnel directly impacts the ability to effectively implement and execute incident response processes.

質問: **537**
重要なITアプリケーションのリスク対応戦略の優先順位付けを行う際に、最も重要な入力項目は次のうちどれですか？
A. 事業影響分析(BIA)の結果
B. 独立監査結果
C. ITリスク軽減予算
D. 貫通試験結果
正解: **A (**コメントを発表する**)**
BIA results identify the criticality of applications, business impact of disruption, recovery priorities, RTOs, and RPOs. This is the best input for prioritizing risk response strategies for critical IT applications.

質問: **538**
組織のセキュリティ文化が成熟していることを最もよく示すのは、次のうちどれですか？
A. 上級管理職向けのセキュリティポリシーはカスタマイズされています。
B. すべてのユーザーは定期的なセキュリティ意識向上トレーニングに参加する必要があります。
C. 情報セキュリティマネージャーは、すべてのセキュリティリソース割り当て決定を承認します。
D. 経営陣がセキュリティプログラムへの支持を表明する。
正解: **(**正解を表示します**)**

A mature security culture is best indicated by visible and consistent support from senior management, as their commitment drives organization-wide prioritization of security and fosters accountability at all levels.

質問: **539**
侵入テストの結果、ファイアウォールの設定ミスによるセキュリティ上の脆弱性が明らかになった場合、情報セキュリティ管理者が取るべき最善の行動は次のうちどれですか？
A. マイルストーンを含む計画が策定されていることを確認してください。
B. 分散型サービス拒否(DDoS)攻撃対策を実施する。
C. 新しい主要業績評価指標(KPI)を定義する。
D. インシデント対応チームに連絡してください。
正解: **(**正解を表示します**)**
A penetration test finding is typically handled through remediation, not incident response. The best action is to ensure a corrective plan with milestones is developed so the misconfiguration is fixed, tracked, and validated.

質問: **540**
外部の業者に侵入テストの実施を依頼する場合、最も重要なことは以下のとおりです。
A. ネットワークドキュメントを提供する。
B. 従業員に検査について通知する。
C. 最新の資産目録を提供する。
D. プロジェクトの範囲を定義する。
正解: **(**正解を表示します**)**

質問: **541**
新規事業買収後に組織の事業継続計画(BCP)を更新する際に、最初に考慮すべき事項は次のうちどれですか？
A. ビジネス戦略
B. 新規事業に伴うリスク
C. IT予算の更新
D. 新たなビジネスインフラ要件
正解: **(**正解を表示します**)**
After an acquisition, the first consideration for updating the BCP is assessing the risk associated with the new business (critical processes, dependencies, threats, and impacts). This determines continuity priorities and requirements before budgets or infrastructure plans are addressed.

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

ス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu 1193問、３０%ディスカウント、特別な割引コード: JPNshiken」

質問: **542**
組織における情報セキュリティガバナンスの実装を最適化するために、情報セキュリティマネージャーは以下のことを行うべきである。
A. 変更管理プロセスが整備されていることを確認する。
B. 国際基準に準拠したプロセスを実施する。
C. 可能な限り既存の統治構造を活用する。
D. 従業員の抵抗を最小限に抑えるために、ガバナンスを段階的に変更する。
正解: (正解を表示します)
Leveraging existing governance structures (e.g., risk committees, steering committees, established reporting lines) is the most effective way to optimize implementation because it embeds security into how the organization already makes decisions and ensures quicker adoption and sustainability.

質問: **543**
ある組織が最近、新たな事業体を買収しました。買収した事業体の文化を考慮せずにセキュリティ戦略を統合した場合、次のうちどの問題が最も発生しやすいでしょうか？
A. 実施に対する抵抗
B. 技術的な専門知識とスキルが不足している
C. コンプライアンス期限の遅延
D. 利用可能な資源の不足
正解: (正解を表示します)
If the acquired entity's culture is not considered, employees are more likely to resist new security expectations and processes, which undermines adoption and the success of the integrated security strategy.

質問: **544**
ある組織は、カスタムソフトウェアの開発を第三者のサービスプロバイダーに委託することを計画している。
以下のうち、ソフトウェアのセキュリティを最も確実に保証するのに役立つのはどれですか？
A. サービスプロバイダーのソフトウェア開発スタッフ向けセキュリティ研修
B. サービスプロバイダーのソフトウェア開発ポリシーのレビュー
C. 個々の開発者が保有する資格の検証
D. 関連基準に対する独立した評価
正解: (正解を表示します)
An independent assessment against a relevant standard provides the greatest assurance of software security by objectively verifying that secure development practices are being followed and controls are effectively implemented.

質問: **545**
規制の厳しい環境下で情報セキュリティ対策のビジネスケースを作成する際に、最初に行うべきことは次のうちどれですか？

A. 競合他社とのベンチマーク。
B. リスク評価を実施する。
C. 実現可能性調査を実施する。
D. 法律顧問に相談してください。
正解: **(**正解を表示します**)**
A business case for a security initiative should first be based on the risk it addresses, especially in a highly regulated environment. A risk assessment identifies the likelihood, impact, compliance exposure, and business consequences, which justify the initiative.

質問: **546**
大規模組織において、災害復旧計画および事業継続計画において最も重要なことは以下のとおりです。
A. 統合されたプランです。
B. 別々にテストされます。
C. 使用されているすべてのバックアップシステムを指定します。
D. すべての業務機能を統合する。
正解: **(**正解を表示します**)**
In a large organization, it is most important that disaster recovery and business continuity plans are integrated into one cohesive plan. This ensures that all aspects of recovery and continuity are aligned, avoiding gaps in the response and ensuring a coordinated effort to maintain critical operations during and after an incident.

質問: **547**
組織のインシデント検出能力と対応能力を向上させるための最良の方法は次のうちどれですか?
A. ビジネス影響分析 (BIA) を実施します。
B. 定期的な意識啓発トレーニングを実施します。
C. セキュリティギャップ分析を実行します。
D. ネットワーク侵入テストを実行します。
正解: **B (**コメントを発表する**)**
https://www.logsign.com/blog/10-tips-for-improving-your-incident-response-strategy/

質問: **548**
企業の情報セキュリティポリシーに含めるべき最も重要な項目は次のうちどれですか？
A. 許容される使用
B. セキュリティ目標
C. セキュリティ指標
D. 監査証跡レビュー要件
正解: **(**正解を表示します**)**
https://blog.rsisecurity.com/key-elements-of-an-enterprise-information-security-policy/

質問: **549**

ある組織がゼロトラストアーキテクチャへの移行を進めています。情報セキュリティマネージャーが取締役会に対し、この移行の影響を伝え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. トレーニング計画とエンドユーザーからのフィードバックを社内ポータルにまとめ、そのリンクを役員会に送信する。
B. アーキテクチャの変更を視覚化するために、ゼロトラストの中核となる論理コンポーネントの図を提示します。
C. ステータスダッシュボードとタイムラインを含む、ゼロトラスト実装に関するレポートを作成する。
D. リスク軽減とユーザーエクスペリエンスの変化という観点から、ビジネスへの影響の概要を説明します。
正解: **(**正解を表示します**)**
Board-level communication should focus on strategic outcomes. Highlighting how Zero Trust impacts business - particularly in terms of reducing risk and affecting user experience - aligns with the board's priorities and facilitates informed decision-making.

質問: **550**
コンピュータフォレンジック調査を実施する際、セキュリティインシデント対応チームのリーダーが最も注意すべき点は次のとおりである。
A. 保管管理記録。
B. チームメンバーの効率性。
C. 法務部に通知する。
D. 証拠分析。
正解: **(**正解を表示します**)**
During a computer forensics investigation, maintaining the chain of custody is crucial. It ensures that all evidence is handled, stored, and documented properly to preserve its integrity, authenticity, and admissibility in court. The chain of custody establishes a record of who collected, handled, transferred, or analyzed the evidence, which is essential for it to be credible in a legal process.

質問: **551**
情報セキュリティ戦略の策定において、以下のうち最も重要なものはどれですか？
A. 適切な情報セキュリティ予算の確保
B. 制御環境の評価
C. インシデント対応チームの構築
D. 情報セキュリティ要件の評価
正解: **(**正解を表示します**)**
Understanding and evaluating information security requirements is most important, as it ensures the strategy aligns with business needs, regulatory obligations, and risk posture from the outset.

質問: **552**
情報セキュリティマネージャーは、2人の上級管理職が社内会計システムにおいて自身の権限を昇格できる権限を持っているという通知を受けました。これはポリシー違反です。この問題に対処するための最初のステップは何でしょうか？
A. 幹部のアクセス権限を即時停止します。

B. セキュリティ ポリシー違反を CISO に通知します。
C. 過去 90 日間のすべてのシステム トランザクションを完全にレビューします。
D. システム アクセス レビューを実行します。
正解: **D (**コメントを発表する**)**
The first step is to perform a system access review to verify who holds elevated privileges and understand the scope of the violation before taking any disruptive action or escalating.

質問: **553**
事業継続計画および災害復旧計画に関する文書を定期的に更新する主な理由は次
のうちどれですか？
A. 事業資産の在庫管理
B. 事業運営の可用性を確保するため
C. セキュリティポリシー要件を遵守する
D. 監査およびコンプライアンス要件を満たすため
正解: **B (**コメントを発表する**)**

質問: **554**
情報セキュリティプログラムへの支持を構築する際に、以下の要素のうちどれが最も重要ですか？
A. 既存の脆弱性の特定
B. 情報リスク評価
C. 事業影響分析(BIA)
D. 脅威分析
正解: **(**正解を表示します**)**

質問: **555**
次のうち、電子取引の否認防止を保証するものはどれですか？
A. 対称アルゴリズム
B. 第三者機関の証明書
C. 定期的な再認定
D. 多要素認証(MFA)
正解: **(**正解を表示します**)**
Third-party certificates, such as those issued by a trusted Certificate Authority (CA), provide nonrepudiation by ensuring that the identity of the sender is verified and cannot be denied. They are used in digital signatures to confirm authenticity and integrity of electronic transactions.

質問: **556**
セキュリティインシデントの深刻度階層を定義する主な目的は次のうちどれですか？
A. インシデントの根本原因分析を容易にするため
B. 組織のIT資産の分類を容易にするため
C. 利用可能なインシデント対応リソースの優先順位付け

D. リスク分析プロセスを効率化するため
正解: **(**正解を表示します**)**
A severity hierarchy classifies incidents by impact and urgency so the organization can allocate incident response resources appropriately. Higher-severity incidents receive faster escalation, more attention, and stronger response actions.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu ⇑**193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **557**
ある組織が、大量の機密情報を拡張性の高いクラウドデータベースに移行した。
組織は、データの機密性を保護するためにクラウドプロバイダーの暗号化を使用することに同意しました。情報セキュリティマネージャーにとって最も重要な考慮事項は次のうちどれですか？
A. 復旧時間目標(RTO)の定義
B. 主要なライフサイクル管理プロセス
C. 記録の誤分類の可能性
D. 独立セキュリティ監査結果
正解: **B (**コメントを発表する**)**
If the organization relies on the cloud provider's encryption, the most important concern is how encryption keys are generated, stored, rotated, accessed, backed up, revoked, and destroyed.
Weak key lifecycle management can undermine confidentiality even if encryption is enabled.

質問: **558**
特定の脆弱性に対処するための制御策を分析する際に、最も重要な目標は次のうちどれですか？
A. 情報漏洩の影響を最小限に抑えるため
B. 緩和策にかかる時間とコストを最小限に抑える
C. リスクおよびコントロールの責任者からの支持を得るため
D. リスクを許容できるレベルまで低減する
正解: **D (**コメントを発表する**)**
The primary goal when analyzing controls for a specific vulnerability is to reduce the associated risk to an acceptable level based on the organization's risk appetite. Security measures should be implemented in a way that effectively mitigates the risk while aligning with business objectives.
While minimizing breach impact, cost, and gaining stakeholder support are important, they are secondary to ensuring that the risk is adequately addressed.

質問: **559**
組織の情報セキュリティ戦略を策定する際、どこに注力すべきかを理解するために最も役立つのは次のうちどれですか？
A. 脆弱性評価
B. プロジェクト計画
C. 事業影響分析(BIA)
D. ギャップ分析
正解: **(**正解を表示します**)**
A gap analysis shows the difference between the current security posture and the desired/required state (based on objectives and requirements), which most directly highlights where efforts should be focused when developing the strategy.

質問: **560**
サイバー攻撃に関する情報を提示し、経営陣から対策強化への支持を得るために、最も重要な強調事項は次のうちどれですか？
A. 多層防御アーキテクチャにおける制御ギャップ
B. 残存リスクへの曝露
C. 内部システムに対する脅威
D. 同業種における最近のデータ漏洩
正解: **(**正解を表示します**)**
Emphasizing residual risk exposure highlights the potential impact of unaddressed risks despite existing controls, making it most effective in securing senior management support for additional security investments.

質問: **561**
情報セキュリティ部門は、ウェアラブルテクノロジーも含まれるようになった最近更新されたBYOD(Bring Your Own Device)ポリシーに対応するため、新しいツールへの投資が必要です。戦略委員会に提出して検討してもらう際に、リスク管理への投資対効果(ROI)を最も効果的に示すのは、次のうちどれでしょうか？
A. 事業影響分析(BIA)
B. リスク評価
C. ビジネスケース
D. リスク監査報告書
正解: **(**正解を表示します**)**
A business case formally presents the expected benefits, costs, risk reduction, and strategic alignment of the investment. To demonstrate return on investment (ROI) in risk management, the proposal must clearly quantify how the new tools reduce risk exposure relative to cost -- which is the purpose of a business case.

質問: **562**
ある組織でフィッシング攻撃が増加しています。この状況に対処するために最も効果的なリスク管理策は次のうちどれですか？

A. フィッシング関連のデータ漏洩による潜在的な金銭的損失を補償するために、サイバー保険に加入してください。
B. フィッシングのリスクをリスクレジスターに記録し、潜在的な影響を受け入れる。
C. 明確な責任契約を結んだ第三者サービスプロバイダーにメール管理をアウトソーシングする。
D. メールフィルタリングシステムを導入し、従業員向けの必須研修プログラムを実施する。
正解: **(**正解を表示します**)**
Phishing risk is best reduced through a combination of technical controls and human-focused controls. Email filtering helps block malicious messages before they reach users, while mandatory training helps employees recognize and report phishing attempts.

質問: **563**
情報リスク管理プログラムの有効性を判断するための最適な方法は、次のうちどれですか？
A. 独立したリスク評価の実施
B. 主要リスク指標(KRI)の設定
C. 主要業績評価指標(KPI)の評価
D. 情報セキュリティ管理の基準値の設定
正解: **(**正解を表示します**)**
Key risk indicators (KRIs) are the best method because they measure changes in risk exposure over time and show whether risk is being kept within defined thresholds, directly reflecting the effectiveness of the information risk management program.

質問: **564**
経営陣は、組織のシステムで使用されるアプリケーションへのAIの統合が進んでいることを懸念しています。AI統合アプリケーションを安全かつ効果的に使用できるようにするには、次のうちどれが最適なアプローチでしょうか？
A. ベンダーと協力して、AI統合アプリケーションの根本的な脆弱性を修復する。
B. AI統合アプリケーションの使用に関するユーザー意識向上トレーニングを更新する。
C. AI統合アプリケーションの使用に伴うリスクを特定し、評価する。
D. AI統合アプリケーションが適切に構成されているかどうかを判断します。
正解: **(**正解を表示します**)**
The best approach to ensuring AI-integrated applications can be used securely and effectively is to identify and assess the risks associated with their use. This includes evaluating data privacy concerns, bias in AI models, security vulnerabilities, compliance requirements, and potential misuse. Once risks are understood, appropriate controls and policies can be implemented. While working with vendors, updating training, and checking configurations are important, they should be based on a comprehensive risk assessment.

質問: **565**
ユーザー認証情報の漏洩に起因する一連のセキュリティインシデントを受け、ある組織はゼロトラストアーキテクチャ(ZTA)を導入することを決定しました。ゼロトラストの原則を実装するための最適なアプローチは次のうちどれですか？

A. 不正アクセスを制限するために、内部ネットワークと外部ネットワークを分離する堅牢なファイアウォールを導入します。
B. リモートアクセスを保護するために仮想プライベートネットワーク(VPN)への依存度を高め、内部ユーザーは信頼できるものとみなす。
C. セッションごとに多要素認証(MFA)を実装し、最小権限アクセスを強制します。
D. 重要な資産の周囲にセキュリティ境界を確立しつつ、内部の移動は制限なく行う。
正解: **(**正解を表示します**)**
Zero Trust is based on continuous verification, strong identity assurance, and least privilege. MFA helps address compromised credentials, while per-session least privilege ensures users receive only the access needed for that specific context.

質問: **566**
大規模なシステム障害発生後、組織が通常の業務運営に戻るために最も効果的な方法はどれですか？
A. 事業影響分析(BIA)
B. 運用上のレジリエンス戦略
C. リスク評価
D. 災害復旧計画(DRP)
正解: **(**正解を表示します**)**
A DRP provides the specific procedures to recover critical IT systems, data, infrastructure, and services after a major outage. Restoring these capabilities is what enables the organization to resume normal business operations.

質問: **567**
新しいクラウドベンダーへの移行を試みた際、組織は独自のクラウドアクセスセキュリティブローカー(CASB)構成が新しいプラットフォームと互換性がないという重大な課題に直面しました。このリスクを管理する一環として、以下のうちどれが適切なリスクオーナーシップを確保するのに最も適していますか？
A. 移行リスクの責任をクラウドベンダーに委任し、運用効率に注力する
B. 移行責任をITチームに割り当て、ベンダー関連の決定はクラウドプロバイダーに委ねる。
C. 移行リスクと管理の明確な責任分担を含むガバナンスフレームワークを確立する
D. 将来的な互換性の問題を回避するため、CASBの使用を現在のクラウドベンダーに限定する
正解: **(**正解を表示します**)**
The issue is a migration and third-party technology risk. A governance framework clearly defines who owns the risk, who manages the controls, who approves decisions, and how vendor/platform dependencies are handled.

質問: **568**
効果的なランサムウェア対策戦略を策定する際に、以下のうち最も重要なものはどれですか？
A. すべてのソフトウェアを定期的に最新バージョンにアップデートする
B. 適切なバックアッププロセスを維持する
C. 次世代ファイアウォールのインストール
D. サイバーセキュリティ意識に関する従業員向け研修を定期的に実施する。
正解: **B (**コメントを発表する**)**

An effective ransomware response strategy depends most critically on having reliable, regularly tested backups. This ensures data can be restored without paying a ransom, minimizing downtime and data loss.

質問: **569**
インシデント対応計画において、インシデントをエスカレーションする前に必ず実施しなければならない事項は次のうちどれですか？
A. 当該事象に関連するリスクを定量化する。
B. 事件の深刻度を判断する。
C. インシデントの根本原因を特定する。
D. 事件の経済的影響を定量化する。
正解: **(**正解を表示します**)**
Before an incident is escalated within an incident response plan, it is essential to determine the severity of the incident. Assessing the severity helps in deciding whether the incident warrants escalation and which resources and personnel need to be involved in the response.
While quantifying risk, determining root causes, and assessing financial impact are important steps in incident management, determining severity is the immediate action that guides the escalation process.

質問: **570**
情報セキュリティガバナンス委員会の主な責任は次のうちどれですか？
A. 情報セキュリティリスク登録簿の見直し
B. 今後の情報セキュリティプロジェクトについて話し合う
C. 情報セキュリティ戦略の変更を承認する
D. 月次の情報セキュリティ指標のレビュー
正解: **C (**コメントを発表する**)**

質問: **571**
ある組織が新たにBYOD(Bring Your Own Device：私物端末の業務利用)プログラムを導入しました。セキュリティマネージャーは、少数の従業員がモバイル端末を通じて無料のクラウドストレージサービスを利用して会社のデータを保存していることを確認しました。以下のうち、最も効果的な対策はどれでしょうか？
A. 従業員による会社のメールとデータへのリモートアクセスを無効にします。
B. デバイスのリモートワイプを開始します。
C. 安全なソリューションを提供するビジネス上の必要性を評価する。
D. 監視目的で一時的に練習を継続することを許可する。
正解: **(**正解を表示します**)**
The most effective action is to assess the business need and provide an approved secure alternative (e.g., managed corporate storage/containerization/CASB controls). This addresses the root cause and enables compliant behavior rather than reacting punitively without solving the underlying requirement.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu ↾**193**問、３０%ディスカウント、特別な割引コード:**JPNshiken**」

質問: **572**
情報セキュリティプログラムの初期開発において、最も適切な参考資料となるのは次のうちどれでしょうか？
A. インシデント対応計画
B. 業界で認められたセキュリティフレームワーク
C. 災害復旧計画(DRP)
D. 最近のセキュリティ監査結果
正解: **(**正解を表示します**)**
An industry-recognized security framework provides the best baseline reference for initially developing an information security program because it offers a comprehensive, structured set of control domains and governance practices that can be tailored to the organization.

質問: **573**
インシデント管理の復旧フェーズにおける主要な目的は次のうちどれですか？
A. ITサービスをオンラインに戻す
B. 教訓レビューを実施する
C. ITシステムの復旧のために講じた措置を記録する。
D. 事業運営支援の回復
正解: **D (**コメントを発表する**)**
The primary objective of the incident management recovery phase is to recover business operation support. The main focus of this phase is to ensure that critical business functions can continue or resume after an incident, restoring normal operations.

質問: **574**
組織の情報セキュリティ基準をサードパーティのバックアップサイトが引き続き満たすことを確実にするために、次のうちどれが最も役立ちますか？
A. 災害復旧計画(DRP)
B. サービスレベル契約(SLA)
C. 事業継続計画(BCP)
D. 覚書
正解: **(**正解を表示します**)**
An SLA defines and enforces the security expectations and performance requirements of the third-party backup site, helping ensure ongoing compliance with the organization's information security standards.

質問: **575**
組織に新技術が導入された場合、以下のうちどれが最も影響を受ける可能性が高いでしょうか？
A. 事業影響分析(BIA)
B. 制御効果
C. リスクプロファイル
D. セキュリティ手順
正解: **C (コメントを発表する)**
The introduction of emerging technologies is most likely to impact the organization's risk profile.
New technologies can introduce new vulnerabilities, threats, and compliance challenges, altering the overall risk landscape. It is essential to assess how these technologies affect the organization's exposure to risks.

質問: **576**
クラウドコンピューティングサービスを利用している組織にとって、ベンダーのインシデント管理計画に関して最も重要な考慮事項は次のうちどれですか？
A. セキュリティインシデントの分類に関する決定
B. インシデント対応を提供するベンダー担当者の専門知識
C. インシデント監視のための高度なSIEMの実装
D. ベンダーによる関連セキュリティインシデントの報告の適時性
正解: **(正解を表示します)**
In cloud services, the customer depends on the vendor to promptly notify them of incidents that may affect their data, systems, or compliance obligations. Timely reporting enables the organization to assess impact, meet regulatory notification deadlines, and coordinate response actions.

質問: **577**
ある組織は、従業員数名が最近、従業員のファイルを暗号化する悪意のあるメールリンクをクリックしたことを知りました。関連するリスクを軽減するための最適な予防策は次のうちどれですか？
A. エンドユーザー向けセキュリティトレーニング
B. ファイル流出監視
C. 多要素認証(MFA)
D. ネットワークセグメンテーション
正解: **(正解を表示します)**
The best preventive control to mitigate the risk of employees clicking on malicious links is end- user security training. Educating employees about recognizing phishing attempts and the dangers of clicking on suspicious links helps prevent such incidents from occurring in the first place.

質問: **578**
情報セキュリティ管理者がゼロデイ脆弱性を知るための最良の方法は次のうちどれですか？
A. シグネチャベースのマルウェア検出ツール
B. 最新の脆弱性スキャンツール
C. 侵入テストの結果

D. サイバーセキュリティ脅威インテリジェンスグループ
正解: **(**正解を表示します**)**
Zero-day vulnerabilities are newly discovered or actively exploited before normal patches or signatures may exist. Cybersecurity threat intelligence groups provide the earliest and most relevant information about emerging vulnerabilities, exploitation activity, indicators of compromise, and recommended mitigations.

質問: **579**
組織が新興技術を導入する過程において、情報セキュリティマネージャーの最も重要な役割は次のうちどれですか？
A. ベンダー契約およびサービスレベル契約(SLA)の見直し
B. 既存資源への影響を理解する
C. 同じ技術を使用している同業他社がどのような影響を受けているかを評価する
D. エンドユーザーが新しい技術に慣れるためのトレーニングを開発する
正解: **(**正解を表示します**)**
The most important role of the information security manager when the organization is adopting emerging technologies is understanding the impact on existing resources. This includes evaluating how the new technology affects the current security infrastructure, processes, and personnel, ensuring that any risks introduced by the new technology are adequately addressed.

質問: **580**
情報セキュリティチームは、攻撃者がアプリケーション内の新たに発表された重大な脆弱性を悪用していることを確認しました。最初に行うべきことは次のうちどれですか？
A. 追加のアプリケーション制御をインストールします。
B. 上級管理職に報告する。
C. アプリケーションへのアクセスを防止します。
D. インシデント対応計画を発動する。
正解: **D (**コメントを発表する**)**

質問: **581**
サイバーセキュリティインシデント対応において使用される事前決定済みの封じ込め方法は、主に以下の点に基づいているべきである。
A. 確認された事件の種類。
B. 影響を受けたユーザー数。
C. 予測される事象の継続時間。
D. インシデントハンドラーの能力。
正解: **A (**コメントを発表する**)**

質問: **582**
ある組織が、既知の重大なリスクに適用される新たな主要リスク指標(KRI)を特定した。
次のうち、最も重要な行動方針はどれですか？

A. リスクを上級管理職に報告する。
B. 現在の管理措置を監査する。
C. 保険に加入してリスクを移転する。
D. その事象が発生する可能性を再評価する。
正解: **(**正解を表示します**)**
A new KRI provides additional information about the risk environment. The most important action is to reassess the risk, especially the likelihood of the event occurring, to determine whether the current risk rating and treatment plan remain appropriate.

質問: **583**
組織の各事業部門に対して一連のセキュリティ対策が正常に導入されたら、情報セキュリティマネージャーにとって最も重要なことは以下のとおりです。
A. 管理策が継続的に有効であることを確認するために、定期的にテストを実施する。
B. 関連する事業主へ管理権限を引き渡す。
C. 将来のシステムアップグレードに備えて制御を適応させる準備をする。
D. 制御性能を業界水準と比較するためのテストを実施する。
正解: **(**正解を表示します**)**
Once a suite of security controls has been successfully implemented, it is most important for the information security manager to ensure the controls are regularly tested for ongoing effectiveness. Continuous testing and monitoring ensure that the controls remain effective over time, particularly as threats evolve and the organization's environment changes.

質問: **584**
BYOD(Bring Your Own Device)プログラムの導入準備において、情報セキュリティマネージャーが最も重視すべき事項は次のうちどれでしょうか？
A. モバイルデバイス管理(MDM)ソリューションの選択
B. リスク評価の実施
C. 業界内におけるBYODインシデントのベンチマーク
D. BYODポリシーと手順の文書化
正解: **(**正解を表示します**)**
Performing a risk assessment identifies the specific threats, vulnerabilities, and impact associated with BYOD, establishing the foundation for appropriate policies, controls, and technology choices to mitigate those risks.

質問: **585**
インシデント対応チームがその役割を果たすために必要な権限を確実に取得するために、以下のうちどれが最も重要ですか？
A. 承認された職務記述書
B. 取締役会承認済みのセキュリティ戦略
C. セキュリティ運営委員会が承認した憲章
D. チームにおける上級管理職の代表者

正解: **C** (コメントを発表する)
The most important factor in ensuring an incident response team has the necessary authorization to perform its role is a charter endorsed by the security steering committee. A charter formally defines the team's responsibilities, authority, and scope of actions, providing the necessary backing to act effectively during incidents.

質問: **586**
大企業の取締役会によるガバナンス構築を支援する際、情報セキュリティマネージャーの主な役割は次のうちどれですか？
A. 助言と指導を提供する。
B. 指標ダッシュボードの開発。
C. セキュリティ予算の準備。
D. 現在の脅威とリスクに関する報告。
正解: **A** (コメントを発表する)
The primary function of an information security manager in governance development is to advise and guide the board on security risks, best practices, and regulatory compliance. The board relies on this expertise to align security strategy with business objectives, ensuring effective risk management and decision-making. While reporting threats and preparing budgets are important, they are secondary to providing strategic advice on governance.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu **1193**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **587**
以下のうち、時間の経過とともに脆弱性が確実に解消される可能性が最も高いのはどれですか？
A. 脆弱性管理システムの導入
B. 侵入テストの結果に対するタイムリーな是正措置
C. 経営行動計画の定期報告
D. 監査結果に対するタイムリーな是正措置
正解: (正解を表示します)
A vulnerability management system provides a structured, continuous process for identifying, prioritizing, tracking, and remediating vulnerabilities over time, ensuring long-term resolution and risk reduction.

質問: **588**
インシデント対応計画を成功裏に実施するために、以下のうち最も重要なものはどれですか？
A. 対応スタッフの機能に関するRACIチャートを作成する

B. 対応要員が適切な訓練を受けていることを確認する
C. インシデント対応報告のための指標の開発
D. ヘルプデスクのエスカレーションプロセスを確立する
正解: **B (**コメントを発表する**)**
The most important factor for the successful implementation of an incident response plan is ensuring that response staff are properly trained. Even the best-designed plan will fail if the personnel responsible for executing it do not understand their roles, responsibilities, and procedures. Training ensures that staff can respond efficiently, follow escalation protocols, and minimize damage during an incident. While RACI charts, metrics, and escalation processes are valuable, they are secondary to ensuring the team is well-prepared and capable of executing the plan effectively.

質問: **589**
組織の事業継続計画(BCP)の一環として、既存のレガシーアプリケーションが稼働しているサーバーに新しいビジネスアプリケーションを導入した後、サーバーの高可用性戦略が強化されました。この変更の最も可能性の高い理由は次のうちどれですか？
A. より短い復旧時間目標(RTO)
B. より長い回復時間目標(RTO)
C. より長いリカバリポイント目標(RPO)
D. より短いリカバリポイント目標(RPO)
正解: **(**正解を表示します**)**
High availability is mainly used to reduce downtime. If a new business application is added to the server, the server may now support more critical business functions, requiring a shorter RTO.

質問: **590**
セキュリティ対策の有効性を評価するのに最適な時期は次のとおりです。
A. ソフトウェアパッチがリリースされた後。
B. 大規模なシステム変更後。
C. 主要リスク指標(KRI)の測定前。
D. システムが強化される前。
正解: **B (**コメントを発表する**)**
A "major modification" (such as a system upgrade, new integration, or architectural change) can inadvertently disable or bypass previously effective security controls. Evaluating immediately afterward ensures that the security posture remains intact.
When a system is modified, the threat landscape for that specific asset often changes. You must evaluate to confirm that the controls are still appropriate for the new configuration.
In a mature organization, security testing and evaluation are mandatory final steps in the Change Management process before a system is considered "fully operational."

質問: **591**

SIEM監視によってネットワーク攻撃が進行中であることが示された場合、次のうちどれが最善の対応策でしょうか？

A. 影響を受けた部分を隔離します。

B. イベントログを検証します。

C. 影響を受けているデバイスを再起動してください。

D. 影響を受けるデバイスの電源を切ってください。

正解: **A (**コメントを発表する**)**

Isolating the affected network segments is the best immediate response to contain the attack while minimizing impact on other parts of the network. It allows for investigation and remediation without disrupting the entire environment.

有効的な**CISM-JPN**問題集はJPNTest.com提供され、**CISM-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CISM-JPN**試験問題集を提供します。JPNTest.com CISM-JPN試験問題集はもう更新されました。ここで**CISM-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CISM-JPN-mondaishu　**193**問、３０%ディスカウント、特別な割引コード:**JPNshiken**」