ISACA.IT-Risk-Fundamentals.v2025-10-17.q49

試験コード:	IT-Risk-Fundamentals
試験名称:	IT Risk Fundamentals Certificate Exam
認定資格:	ISACA
無料問題数:	49
バージョン:	v2025-10-17
アクセス数:	128
ページビュー数:	490
https://www.jpnpdf.com/ISACA.IT-Risk-Fundamentals.v2025-10-17.q49-mondaishu.html	

最新問題: **1**
I&T リスク関連のリスクシナリオを開発するためのボトムアップアプローチ:
A. 組織内の誰でもリスク シナリオを開発できる汎用的な方法です。
B. 特定の I&T 機能を実行する人々が想定する仮想的な状況に基づいています。
C. I&T 関連イベントを評価するために他のアプローチと組み合わせて使用しないでください。
Answer: B (メーッセージを残す)
リスクシナリオ策定におけるボトムアップアプローチは、運用レベルから始まります。I&T機能に最も近い関係者、つまり実際に業務を遂行する人々が、それぞれの領域における潜在的なリスクと脆弱性に関する理解に基づいてシナリオを策定します。これらのシナリオは、より上位のレベルで集約・分析されます。
組織内の誰もがリスク特定（A）に貢献できますが、ボトムアップアプローチは、特定のI&T機能（B）を担う担当者の専門知識に特化します。包括的な視点を得るためには、トップダウンなどの他のアプローチ（C）と組み合わせて活用する必要があります。

最新問題: **2**
次のリスク分析方法のうち、インタビュー中に個人または小グループによって検証およびランク付けされるさまざまな種類の潜在的なリスクのアイデアを収集するものはどれですか。
A. ブレインストーミングモデル
B. デルファイ法
C. モンテカルロ解析
Answer: (解答を表示する)
デルファイ法は、インタビュー中に個人または小グループが検証し、ランク付けするさまざまな種類の潜在的なリスクのアイデアを収集するために使用されます。その理由は次のとおりです。

* ブレインストーミングモデル :グループでアイデアを生み出す手法で、通常は即時の検証や順位付けは行いません。構造化された分析よりも、アイデア創出に重点が置かれます。
* デルファイ法 :この手法は、構造化されたコミュニケーション（通常はアンケート）を用いて専門家からのアイデアを収集 -精緻化します。複数回のインタビューを実施し、フィードバックを集約 -共有することで、参加者はアイデアを検証し、優先順位を付けることができます。この反復的なプロセスは、潜在的なリスクに関する合意形成に役立ちます。
* モンテカルロ分析 :これは、様々な結果の確率をモデル化するシミュレーションを含むリスク分析に使用される定量的な手法です。インタビューを通じてアイデアを収集し、ランク付けするためには使用されません。
したがって、デルファイ法は、インタビュー中に潜在的なリスクのアイデアを収集、検証、ランク付けするのに適した方法です。

最新問題: **3**
高度な持続的脅威 (APT) 攻撃の最初のステップは次のどれですか?
A. 管理者を識別し、パスワードを解読して管理者アクセスを取得します。
B. ソーシャル エンジニアリングを使用して、従業員に感染した Web サイトにアクセスするよう促します。
C. 組織のインフラストラクチャに関する情報を収集して、どこを攻撃するかを把握します。
Answer: C (メーッセージを残す**)**
APT攻撃の最初のステップは通常、偵察です。攻撃者は、攻撃を効果的に計画 -実行するためには、標的組織のインフラストラクチャ、システム、そして人員を理解する必要があります。これには、組織のネットワーク、システム、アプリケーション、セキュリティ管理、そして従業員に関する情報の収集が含まれます。この偵察段階は、攻撃者が脆弱性と侵入ポイントを特定するために不可欠です。
ソーシャル エンジニアリング (B) とパスワード クラッキング (A) は APT でよく使用される戦術ですが、通常は最初のステップにはなりません。

最新問題: **4**
組織を有害な脅威にさらす可能性が最も高いのは次のどれですか?
A. 複雑なエンタープライズアーキテクチャ
B. 不適切に構成されたネットワークデバイス
C. サイバーセキュリティトレーニング記録が不完全です
Answer: B (メーッセージを残す**)**
組織を有害な脅威にさらす最も可能性の高い要因は、ネットワークデバイスの設定が不適切であることです。その理由は次のとおりです。
* 複雑なエンタープライズアーキテクチャ：複雑さは脆弱性を生み出し、セキュリティ管理の難易度を高める可能性がありますが、それ自体がセキュリティリスクの最大の原因とな

るわけではありません。適切に管理された複雑なアーキテクチャであっても、セキュリティは確保できます。
* 不適切に構成されたネットワーク デバイス: これが脅威にさらされる最も可能性の高い原因です。
ルーター、ファイアウォール、スイッチなどのネットワークデバイスは、セキュリティ境界の維持とアクセス制御に不可欠です。これらのデバイスが正しく設定されていない場合、重大な脆弱性が生じる可能性があります。例えば、デフォルトの設定や脆弱なパスワードは、攻撃者に簡単に悪用され、不正アクセスされ、データ侵害やネットワークの混乱につながる可能性があります。
* サイバーセキュリティ研修記録の不完全性：研修記録の不完全性は重要ですが、それだけでは組織が直接脅威にさらされるわけではありません。これは、認識と準備態勢に潜在的なギャップがあることを示唆するものの、悪用される可能性のある脆弱性に直接つながるものではありません。
ネットワーク デバイスは組織のセキュリティ インフラストラクチャで重要な役割を果たしているため、これらのデバイスの構成が不適切だと、悪意のある脅威にさらされるリスクが最大限に高まります。
参考文献:
* ISA 315 フェーズ 5 および 6: 組織の環境における IT リスクと制御、特に IT インフラストラクチャの構成と管理を理解します。
* SAP レポート: 構成例とネットワーク デバイスの誤った構成がセキュリティに与える影響。

最新問題: **5**
次のどれがガバナンスの主な目的ですか?
A. 組織全体にわたるコントロールの作成
B. 組織のあらゆるレベルでリスク認識を高める
C. 組織への投資を通じて価値を創造する
Answer: (解答を表示する**)**
ガバナンスは、組織が目標を達成し、効率的に運営され、ステークホルダーに価値を付加することを確実にすることに主眼を置いています。ガバナンスの主な目的は、組織への投資を通じて価値を創造することです。これには、組織の目標に沿った戦略的意思決定を行うこと、資源が効果的に活用されること、そして組織の活動が持続可能で長期的な利益をもたらすことが含まれます。統制の構築とリスク認識はガバナンスの重要な側面ですが、それらは戦略的投資を通じた価値創造というより広範な目標にも貢献します。この概念は、ISO/IEC 38500やCOBIT（情報および関連技術の管理目標）などのコーポレートガバナンスのフレームワークや標準に見られる原則と一致しています。

最新問題: **6**
組織のリスク範囲を定義する際に最も重要なのは次のどれですか?
A. リスク環境が組織に与える影響を理解する

B. リスク管理へのトップダウンアプローチの開発
C. 経営幹部へのリスク報告の要件策定
Answer: A (メーッセージを残す**)**
リスクの範囲を定義するということは、リスク管理プロセスに含めるリスクを決定することを意味します。最も重要なのは、リスク環境が組織に及ぼす潜在的な影響を理解することです。これには、組織の目標達成能力に影響を与える可能性のある内的要因と外的要因の両方を分析することが含まれます。これらの影響を理解することによってのみ、リスク管理活動の範囲を効果的に定義することができます。
ERMの導入においてはトップダウンアプローチ（B）が推奨されることが多いものの、スコープ定義において最も重要な要素ではありません。リスク報告要件（C）は重要ですが、スコープ定義の結果として生じるものであり、その逆ではありません。

最新問題**: 7**
リスク監視は、次の場合に最も効果的です。
A. ビジネス環境の変化に応じて。
B. リスク対応計画の完了前と完了後。
C. リスク対応計画プロセス全体を通じて。
Answer: C (メーッセージを残す**)**
リスク監視の有効性:
* リスク対応計画プロセス全体を通じて継続的にリスクを監視することで、リスク環境の変化を早期に検出し、迅速に対処することができます。
* リスク対応計画をリアルタイムで調整および改善できます。
リスク監視のフェーズ:
* 治療前: 初期モニタリングは、ベースラインのリスク レベルを理解し、注意が必要な重要な領域を特定するのに役立ちます。
* 治療中:継続的な監視により、リスク治療対策が効果的であり、逸脱があれば適時に修正されることが保証されます。
* 治療後:治療後のモニタリングでは、リスク対応の長期的な有効性を検証し、残留リスクを特定します。
参考文献:
* ISA 315（2019 年改訂）、基準 5 では、変化に適応し、リスク処理の有効性を確保するために、リスク管理における継続的な監視の重要性について説明しています。

最新問題**: 8**
効果的な資産評価の最大の利点は次のどれですか?
A. 企業が資産の純資産額を超える保護費を支払うことから保護します。
B. 資産評価が企業全体のすべての資産に一貫して適用されることを保証します。
C. 資産がプロセスにリンクされ、ビジネス価値に基づいて分類されることを保証します。
Answer: C (メーッセージを残す**)**

効果的な資産評価はいくつかの理由から重要ですが、最大のメリットは、資産をプロセスにリンクさせ、ビジネス価値に基づいて分類できることです。以下に詳しく説明します。
* 資産とプロセスのリンク:
* 資産活用の理解：資産を効果的に評価することで、組織は各資産が様々なプロセスでどのように使用されているかをより深く理解できます。この連携により、資産の活用を最適化し、事業運営への効果的な貢献を実現できます。
* プロセス効率の向上: 資産が正しく評価され、プロセスにリンクされると、組織は業務を合理化し、無駄を減らし、全体的な効率を向上させることができます。
* ビジネス価値に基づく分類:
* リソースの優先順位付け：効果的な資産評価により、組織は最もビジネス価値の高い資産にリソースを優先的に配分できます。つまり、主要なビジネスプロセスを支える重要な資産に、必要な注意と投資が向けられるということです。
* 情報に基づいた意思決定: 正確な評価により、経営陣は資産の保守、交換、強化について情報に基づいた意思決定を行うために必要な情報を得ることができ、資産がビジネスに価値を提供し続けることが保証されます。
* リスク管理:
* 財務リスクの軽減：資産の正確な価値を把握することで、組織は保護対策への過剰投資や不足投資を回避できます。このバランスは、資産管理に関連する財務リスクの軽減に役立ちます。
* コンプライアンスと報告: 適切な資産評価により、財務報告基準および規制への準拠が確保され、法律上または規制上の問題のリスクが軽減されます。
参考文献:
* 資産をビジネス プロセスにリンクすることと、ビジネス価値に基づいてそれらを分類することの重要性は、COBIT や ITIL などのさまざまな監査および IT 管理フレームワークで強調されています。
* ISA 315 では、資産の評価と管理を含む、企業の情報システムと関連する管理を理解することの重要性が強調されています。

最新問題**: 9**
企業のリスク許容度を確立するために、組織は次のことを行う必要があります。
A. 組織全体でリスク分類を標準化します。
B. すべての事業分野のリスクステートメントを集約します。
C. 各事業部門のリスク許容度を確立します。
Answer: C (メーッセージを残す**)**
企業全体のリスク選好を確立するには、各事業部門のリスク許容度を確立することが不可欠です。リスク許容度とは、各事業部門がそれぞれの目標達成のために受け入れるリスクの具体的なレベルを定義するものです。このアプローチにより、リスク管理を組織内の各部門固有の状況や業務上の実態に合わせて調整することができ、より正確で効果的なリスク管理戦略が可能になります。リスク分類の標準化とリスクステートメントの集約は、よ

り広範なリスク管理プロセスにおける重要なステップですが、リスク許容度の確立は、事業部門レベルでのリスク選好を定義する上で不可欠です。この概念は、ISO 31000などの規格や、COSO ERM（Enterprise Risk Management）などのフレームワークによってサポートされています。

最新問題: **10**
制御の有効性を示すためにリスク レポートに含めるのに最も役立つ情報はどれですか。
A. リスクを許容レベルまで低減するための管理が適切に機能しているかどうか
B. 統制パフォーマンスを監視するための指標がリスク管理基準と一致しているかどうか
C. 外部監査が内部監査で報告されたのと同じ管理上の欠陥を確認しているかどうか
Answer: A (メーッセージを残す**)**
リスク報告書に統制の有効性に関する記載すべき最も有用な情報は、統制が意図したとおりに機能してリスクを許容レベルまで低減しているかどうかです。これは、統制の本質的な目的に直接関係しています。
標準規格への適合（B）は重要ですが、有効性を保証するものではありません。外部監査（C）による欠陥の確認は重要ですが、主な焦点は管理が機能しているかどうかにあります。

最新問題: **11**
リスク影響基準は主に以下の目的で使用されます。
A. 企業のリスク許容度を確立するのに役立ちます。
B. 特定の IT 資産に関連する損失を特定します。
C. 企業のリスク対応の優先順位を決定します。
Answer: (解答を表示する**)**
リスク影響基準は、リスク事象が発生した場合の潜在的な影響を定義します。これらの基準は主に、リスク対応の優先順位付けに使用されます。様々なリスクの潜在的な影響を理解することで、組織は最も重要なリスクから軽減することに注力することができます。
影響度基準はリスク選好度（A）の判断材料となりますが、主な用途は優先順位付けです。特定のIT資産に関連する損失の特定（B）は影響度評価の一部ですが、基準自体は優先順位付けに使用されます。

最新問題: **12**
ある企業は現在、許容できない8%という処理エラー率に直面しており、エラー率が5%を超えないようにするポリシーを策定することでリスクを管理したいと考えています。さらに、経営陣はエラー率が4%以上になった場合にアラートを通知したいと考えています。企業は、以下のどのレベルで主要業績評価指標（KPI）を設定するべきでしょうか？
A. 5%
B. 4%
C. 8%
Answer: (解答を表示する**)**
KPI の設定:

* 主要業績評価指標 (KPI) は、望ましいパフォーマンス レベルからの逸脱を早期に検出して対応できるレベルに設定する必要があります。
* この場合、許容限度は 5% ですが、エラー率が 4% 以上になると管理者は警告を受けることを望んでいます。
アラートしきい値:
* KPI を 4% に設定すると、許容できないエラー率 5% に達する前に、経営陣がタイムリーに警告を受け取ることができます。
* このアプローチにより、プロセスを積極的に管理および修正することができ、エラー率を許容範囲内に維持することができます。
参考文献:
* ISA 315（2019 年改訂）、基準 5 では、リスクを効果的に管理および軽減するために、パフォーマンス指標とリスク指標を監視し、適切なしきい値を設定することの重要性について説明しています。

最新問題: **13**
リスク識別プロセスの情報を提供するために、I&T 資産インベントリに含めるべき項目は次のどれですか?
A. 資産の損失シナリオ情報
B. 資産のセキュリティ分類
C. 資産の規制要件
Answer: B (メーッセージを残す**)**
IT資産インベントリは、組織の技術資産、その分類、および関連するリスクを体系的に記録することで、リスク特定プロセスにおいて重要な役割を果たします。提供されるオプションの中で、資産のセキュリティ分類は、各資産の機密性、整合性、および可用性（CIA）要件の決定に役立つため、リスク特定において最も重要な要素です。
セキュリティ分類がリスク識別に重要な理由
リスクの優先順位付け:
セキュリティ分類が高い資産 (機密データや制限付きデータなど) には、公開資産や重要度の低い資産に比べて、より厳格なセキュリティ制御が必要です。
組織は分類に基づいてリスク対応の優先順位を決定できます。
脅威と脆弱性の評価:
どの資産に機密情報が含まれているかを把握することで、リスク管理者はサイバー攻撃、データ侵害、内部脅威などの潜在的な脅威を特定できます。
セキュリティ分類は、侵害された場合にどの資産が規制上の罰則を受けやすいかを判断するのに役立ちます。
規制とコンプライアンスに関する考慮事項:
多くの規制フレームワーク (GDPR、HIPAA、ISO 27001 など) では、必要なセキュリティ制御を適用するためにデータと資産の分類が必要です。
セキュリティ分類により、リスク管理戦略を法的要件および業界要件に適合させることでコンプライアンスが確保されます。

他の選択肢はなぜダメなのか？
オプションA（資産の損失シナリオ情報）：
損失シナリオはリスク影響分析には役立ちますが、通常は IT 資産インベントリの一部ではありません。
これらは通常、資産分類ではなく、ビジネス影響分析 (BIA) とリスク評価で考慮されます。
オプションC（資産の規制要件）：
コンプライアンスは重要ですが、高リスク資産が法的義務を満たしていることを確認するために、セキュリティ分類後に規制要件が適用されます。
これらはポリシーと制御の定義に役立ちますが、リスク識別の主な要素ではありません。
結論：
セキュリティ分類は、組織が資産の優先順位付け、脅威の評価、適切なセキュリティ対策の適用を行う上で不可欠であり、効果的なリスク特定に不可欠です。明確な分類に基づき、適切に構造化されたIT資産インベントリを維持することで、企業はリスク管理を強化し、コンプライアンスを向上させ、脅威を効率的に軽減することができます。
参考資料: インシデント対応と災害復旧の原則 - モジュール1: リスク管理の概要

最新問題: **14**
頻度分析の結果を検証する際に確認することが重要なのは次のうちどれですか?
A. 分析中に使用された推定値は、信頼できる履歴データに基づいています。
B. 分析は独立した第三者によって実施されました。
C. 分析方法は完全に文書化され、説明されています。
Answer: A (メーッセージを残す**)**
頻度分析の結果を検証する際には、分析中に使用された推定値が信頼できる過去のデータに基づいていることを確認することが重要です。その理由は次のとおりです。
* 分析に使用された推定値は、信頼性の高い過去のデータに基づいています。これにより、分析が現実に根ざし、実際の過去の傾向やパターンを反映していることが保証されます。信頼性の高いデータは分析の精度と信頼性を高め、結果の信頼性と実用性を高めます。
* 分析は独立した第三者によって実施されました :これは公平性の要素となる可能性がありますが、使用されるデータの正確性と信頼性ほど重要ではありません。データの質と関連性に重点を置くべきです。
* 分析方法は完全に文書化され、説明されています：文書化は透明性と再現性にとって重要ですが、頻度推定の精度に直接影響を与えるものではありません。データの信頼性が最も重要です。
したがって、推定値が信頼できる履歴データに基づいていることを確認することは、頻度分析を検証する上で最も重要な要素です。

最新問題: **15**
リスク分析により、次の点に関して影響を伝えやすくなります。
A. I&T 資産の重要性。
B. 生産性が低下しました。

C. 評判の失墜。
Answer: A (メーッセージを残す**)**
リスク分析は、リスクの潜在的な影響を定量化し、明確に表現するのに役立ちます。リスク分析は、資産の重要性、生産性の低下、そして風評被害という3つの領域すべてに対応できますが、最も直接的かつ定量化可能な影響は、通常、I&T資産の重要性です。リスク分析は、資産の利用不能やセキュリティ侵害の影響を評価できるため、事業運営におけるこれらの資産の重要性をより容易に伝えることができます。
生産性の損失や評判の失墜も評価できますが、より定性的または間接的な尺度が必要となる場合があり、正確に伝えるのがやや難しくなります。

最新問題**: 16**
組織が L&T 関連のリスクを定期的に監視およびレビューする主な理由は次のうちどれですか。
A. 外部および内部のリスク要因の変化に対処する
B. リスクが許容範囲内で管理されるようにする
C. レガシーIT資産のタイムリーな特定と交換を容易にする
Answer: A (メーッセージを残す**)**
IT関連リスクの監視とレビュー:
* 組織がリスク レベルに影響を及ぼす可能性のある内部および外部の変化に適応できるようにするには、IT 関連のリスクを定期的に監視およびレビューすることが不可欠です。
主な理由:
* この継続的なプロセスの主な理由は、外部 (規制の変更、市場の状況など) および内部 (組織の変更、新しい IT の導入など) のリスク要因の変化に対処することです。
* リスクは動的であり、様々な要因によって変化する可能性があります。そのため、継続的な監視は、新たなリスクや既存のリスクの変化を特定し、適切な管理を確実にするのに役立ちます。
オプションの比較:
* リスクが許容範囲内で管理されていることを確認することは、監視の重要な成果ですが、定期的なレビューの主な動機ではありません。
* レガシー IT 資産の識別と置き換えを促進することは運用上の懸念事項ですが、リスク管理のより広範な範囲を網羅するものではありません。
* リスク要因の変化に対処することは、組織が潜在的な問題を先取りし、効果的なリスク管理体制を維持できるようにする積極的なアプローチです。
結論：
* したがって、組織が IT 関連のリスクを定期的に監視およびレビューする主な理由は、外部および内部のリスク要因の変化に対処するためです。

最新問題**: 17**
企業は、ビジネス目標を達成するためにどの程度のリスクを負う意思があるかをどのように決定するのでしょうか?
A. 類似のビジネスに基づいて許容可能なリスクの業界標準を調査することにより
B. 事業のリスク状況と、これらのリスクが現実化した場合の損失の影響を特定することにより
C. 事業計画を調査し、どのようなリスクが事業を停止させるのかを判断することで
Answer: (解答を表示する**)**
企業は、事業のリスク状況を特定し、潜在的な損失の影響を評価することで、どの程度のリスクを許容するか（リスク選好度）を決定します。このアプローチにより、組織のリスクテイクが戦略目標、財務能力、そして事業回復力と整合したものになります。
* ビジネス影響分析（BIA）：
* リスク条件を評価すると、どのような脅威が存在するか、その可能性、および潜在的な影響を理解するのに役立ちます。
* 損失影響評価により、企業はどのリスクが許容可能か、容認できるか、または軽減する必要があるかを判断できます。
* カスタマイズされたリスク許容レベル:
* すべてのビジネスには、業界規制、財務の安定性、競争環境など、固有のリスク要因があります。
* リスクを認識した文化により、組織固有のリスク プロファイルに基づいて意思決定が行われます。
* リスクと報酬のバランス:
* 成長と革新を達成するには、ある程度のリスクは必要です。
* 構造化されたリスク評価プロセスは、潜在的な利益と起こりうる損失を比較検討するのに役立ちます。
* オプションA（許容可能なリスクに関する業界標準の調査）：
* 業界ベンチマークはガイドラインを提供しますが、各企業の財務状況、規制環境、運用モデルに応じてリスク許容度は異なります。
* 業界の標準に盲目的に従うと、過度のリスクを負ったり、過度に保守的な決定を下したりする可能性があります。
* オプション C (事業活動を停止させるリスクを特定するための事業イニシアチブの調査):

* これは、事前対応型ではなく事後対応型のアプローチです。
* 企業は、業務を停止させる可能性のあるリスクが特定されるまで待つのではなく、予防的なリスク管理に重点を置く必要があります。
リスク条件と損失の影響を特定することが最善のアプローチである理由と、他のオプションではない理由
結論：企業がリスク許容度を決定する最良の方法は、リスク状況を特定し、損失の潜在的な影響を評価することです。これにより、事業目標と整合しつつレジリエンスを維持し、バランスの取れたリスクテイクが可能になります。
? 参考資料: インシデント対応と災害復旧の原則 - モジュール2: ビジネス影響分析

最新問題: **18**
脆弱性評価の主な目的は次のどれですか?
A. 脅威と潜在的な影響に基づいて最善の行動方針を決定する
B. ITシステム内の不十分な制御条件に関する知識を向上させる
C. 新しい脆弱性を特定してカタログ化する作業量を削減する
Answer: B (メーッセージを残す**)**
脆弱性評価の主な目的は、ITシステムおよびアプリケーションの弱点を特定し、文書化することです。悪用される可能性のある脆弱性を明らかにすることで、不十分な管理状況の理解を深めることを目指します。
脆弱性評価は最善の行動方針（A）を示しますが、それは評価の結果であり、それ自体が主な目的ではありません。新たな脆弱性を特定するための労力の削減（C）は、優れたプロセスの望ましい成果ですが、主な目標ではありません。

最新問題: **19**
急速に変化する市場環境の中で上級管理職を導くためのリスクシナリオの使用は、重要なリスク管理と考えられている。
A. 利益。
B. インセンティブ。
C. 機能。
Answer: A (メーッセージを残す**)**
急速に変化する市場環境において、経営陣を導くためにリスクシナリオを活用することは、リスク管理における重要なメリットと考えられています。その理由は以下のとおりです。
* メリット :リスクシナリオを活用することで、経営陣は将来起こり得る事象とその影響を把握し、戦略的優位性を獲得できます。これにより、不確実な状況下においても、より的確な意思決定と備えが可能になります。
* インセンティブ: リスク シナリオはリスク管理プラクティスを改善する動機となる可能性がありますが、最も重要なのは戦略計画とリスク軽減にもたらされるメリットです。
* 能力 :これは組織のリスク管理能力を指します。リスクシナリオを活用することでリスク管理能力が向上しますが、主にリスクを理解し、備えることに役立ちます。

したがって、リスク シナリオを使用すると、変化する環境に対応する上級管理職の能力が向上するため、重要なメリットとなります。

最新問題: **20**
脆弱性評価に関する主な懸念事項は次のどれですか?
A. 脅威の軽減
B. レポートサイズ
C. 誤検知
Answer: C (メーッセージを残す**)**
脆弱性評価における最大の懸念は、誤検知の存在です。その理由は次のとおりです。
* 脅威の軽減：脆弱性評価は、軽減が必要な潜在的な脆弱性を特定するのに役立ちますが、これは懸念事項ではなく、評価の目的です。より適切な脅威軽減のための情報を提供することが目的です。
* レポート サイズ: 脆弱性評価から生成されるレポートのサイズは、主な懸念事項ではありません。
焦点はレポートの量ではなく、調査結果の正確性と関連性にあります。
* 誤検知：脆弱性評価において、実際には存在しないセキュリティ問題を誤って特定した場合に発生します。誤検知は、存在しない問題の調査と対処に時間と労力が費やされるため、リソースの無駄につながる可能性があります。また、真の脆弱性への対処が滞る原因にもなり、重大な懸念事項となります。
したがって、主な懸念事項は、脆弱性評価が正確かつ効果的であることを保証するため、誤検知を管理および削減することです。

最新問題: **21**
企業に悪影響を及ぼす可能性のある技術環境または運用環境の変化を評価する評価の種類はどれですか?
A. 脆弱性評価
B. 脅威評価
C. 自己評価の管理
Answer: (解答を表示する**)**
脅威評価は、企業に悪影響を及ぼす可能性のある技術環境または運用環境の変化を評価するものです。このプロセスでは、システムの脆弱性を悪用し、組織の業務、財務状況、または評判に重大な影響を与える可能性のある潜在的な脅威を特定します。評価には、以下の種類があります。
* 脆弱性評価：脅威によって悪用される可能性のあるシステムの弱点を特定することに重点を置いています。環境の変化を具体的に評価するのではなく、システム内の既存の脆弱性を評価します。
* 脅威評価：新たな脅威をもたらしたり、既存の脅威の影響を変化させたりする可能性のある技術環境または運用環境の変化を評価します。外部および内部の変化が組織に潜在的な

リスクをもたらす可能性を検討します。この評価は、変化する環境が脅威の状況にどのような影響を与えるかを理解するために不可欠です。
* 統制自己評価（CSA）：内部統制を担当する従業員が評価するプロセス。統制上のギャップを特定するのに役立ちますが、環境の変化やその影響に特に焦点を当てるものではありません。
これらの定義を考慮すると、企業に悪影響を及ぼす可能性のある技術環境または運用環境の変化を評価する正しいタイプの評価は、脅威評価です。

最新問題: **22**
次のうち、リスクの継続的な監視の責任者として最も適しているのは誰でしょうか?
A. 最高リスク管理責任者（CRO）
B. リスクアナリスト
C. リスクオーナー
Answer: C (メーッセージを残す**)**
リスクオーナーとは、特定のリスクの管理を直接担当する個人またはチームです。関連する活動や統制について最も深い知識と理解を有しているため、リスクを継続的に監視するのに最適な立場にあります。
CRO（A）はリスク管理全般の責任を負いますが、通常、すべてのリスクを直接監視するわけではありません。リスクアナリスト（B）はプロセスをサポートしますが、主な責任はオーナーにあります。

最新問題: **23**
リスク マップは、次のどれを特定するために共通のプロファイルを作成するのに役立ちますか?
A. 明確に特定され、所有権が割り当てられたリスク
B. 十分な予算があるリスク改善活動
C. より効率的に実施できるリスク対応活動
Answer: C (メーッセージを残す**)**
リスクマップは、発生可能性や影響度など、リスクを様々な側面から視覚的に表現するツールとしてよく利用され、リスク対応活動を特定し、最適化することで効率性を高めるのに役立ちます。以下に詳細を説明します。
* リスクマップの理解 :リスクマップは、組織内の様々なリスクを視覚的に表現します。通常、これらのマップはリスクをマトリックス上にプロットし、軸は発生確率と組織への潜在的な影響を表します。
* リスクマップの目的 :リスクマップを使用する主な目的は、組織がリスク管理活動の優先順位付けを支援することです。リスクを視覚化することで、組織はどのリスクに早急な対応が必要で、どのリスクを長期的に監視すればよいかをより適切に把握できるようになります。
* 効率的なリスク対応活動の特定 :リスクマップは、より効率的なリスク対応活動を特定するのに役立ちます。これは、複数のリスクが重複している領域、または既存のリスク対応活

動が重複または重複している可能性のある領域をハイライトすることで実現されます。これらの重複を分析することで、組織はリスク対応活動を合理化し、効率性を向上させ、コストを削減できます。
* 専門家ガイドラインへの参照: ISA 315 によれば、リスク評価プロセスを含む企業の環境を理解することは、重大な虚偽表示のリスクを特定するのに役立ちます。
同様に、組織がこれらのリスクにどのように対応するかを理解することは、監査人やリスク管理者がリスク対応活動を計画し、最適化するのに役立ちます。

最新問題: **24**
組織のサイバーセキュリティ プロファイルに関する次の記述のうち、経営陣へのプレゼンテーションに最も適しているのはどれですか。
A. サイバー攻撃の発生確率は、「低い」から「非常に高い」まで変化します。
B. リスク管理では、サイバー攻撃の可能性は差し迫っていないと考えています。
C. サイバー攻撃のリスクを最小限に抑えるためのセキュリティ対策が設定されています。
Answer: C (メーッセージを残す)
サイバーセキュリティプロファイルの伝達:
* 組織のサイバーセキュリティ プロファイルを経営陣に提示する際には、実施されているセキュリティ対策の有効性とリスクを最小限に抑える能力に焦点を当てることが重要です。
明確さと関連性:
* ステートメントA（「サイバー攻撃の確率は、低いから非常に高いまで変化する」）は曖昧すぎる
* 実用的な情報は提供されません。
* ステートメント B (「リスク管理では、サイバー攻撃の可能性は差し迫っていないと考えている」) は具体性が欠けており、講じられた対策の詳細が示されていません。
セキュリティ対策の有効性:
* ステートメントCは、リスクを最小限に抑えるためのセキュリティ対策を積極的に講じていることを強調しています。このアプローチにより、経営陣は現在のサイバーセキュリティ体制に信頼を抱く可能性が高まります。
* NIST や ISO 27001 などのさまざまなフレームワークで概説されている IT リスク管理のベスト プラクティスによれば、セキュリティ制御の有効性と構成に重点を置くことが、サイバーセキュリティ リスクを管理する鍵となります。
結論：
* したがって、経営陣に提示するのに最適なステートメントは次のようになります。セキュリティ対策は、サイバー攻撃のリスクを最小限に抑えるように構成されています。

最新問題: **25**
次のリスク対応戦略のうち、新しい制御の実装を必要とするものはどれですか?
A. 軽減

B. 回避
C. 承認
Answer: A (メーッセージを残す**)**
定義とコンテキスト:
* 軽減とは、多くの場合、新たな管理策や安全策の導入などによって、何かの重大性、深刻さ、または苦痛を軽減するための措置を講じることを指します。これには、リスクを軽減するために設計されたプロセス、手順、または物理的な対策が含まれます。
* 回避とは、リスクを生み出す活動を行わないことでリスクを完全に回避することを意味します。
* 受容とは、リスクを認識し、リスクが受容可能とみなされるか、リスクを軽減または回避する実行可能な方法がないために、行動しないことを選択することを意味します。
ITリスク管理への応用:
* IT リスク管理における軽減には、多くの場合、セキュリティ パッチ、ファイアウォール、暗号化、ユーザー認証プロトコル、定期的な監査などの新しい制御を実装してリスク レベルを軽減することが含まれます。
* これは、ISAなどのさまざまなIT管理フレームワークと標準で概説されている原則と一致しています。
315 では、IT 関連のリスクを管理する上でのコントロールの重要性が強調されています。
結論：
* したがって、新しい管理策の実装を含むリスク対応戦略を検討する場合、 軽減」はリスクを軽減するための対策を実施するアクションに具体的に対処するため、正しい答えです。

最新問題**: 26**
ビジネス影響分析 (BIA) は、次の場合に最大の利益を生み出します。
A. 影響基準とコスト データを可能な限り一般的なものに保ちます。
B. 既存の影響基準を財務面のみで測定します。
C. 標準化された頻度と影響のメトリックを使用します。
Answer: C (メーッセージを残す**)**
ビジネスインパクト分析（BIA）は、標準化された頻度と影響度の指標を用いることで、最大の効果を発揮します。その理由は次のとおりです。
* 影響基準とコスト データを可能な限り一般的なものに保つ: このアプローチでは、組織への固有の影響を理解するために必要な特異性と正確性が得られません。
一般的なデータには、効果的な意思決定に必要な精度が欠けています。
* 既存の影響基準を財務指標のみで測定すること：財務指標は重要ですが、分析を財務指標のみに限定すると、風評への影響、業務の中断、コンプライアンス問題といった他の重要な要素が考慮されなくなります。包括的なBIAには、様々な影響基準を含める必要があります。

* 標準化された頻度と影響度の指標の使用：標準化により、収集されたデータの一貫性、比較可能性、信頼性が確保されます。これにより、様々なシナリオにおけるリスクと影響を体系的に評価できるようになり、より適切な意思決定と優先順位付けが可能になります。
したがって、BIA から最大の利益を得るには、標準化された頻度と影響のメトリックを使用することが不可欠です。

最新問題: **27**
組織のサイバーセキュリティ プロファイルに関する次の記述のうち、経営陣へのプレゼンテーションに最も適しているのはどれですか。
A. サイバー攻撃の発生確率は、「低い」から「非常に高い」まで変化します。
B. リスク管理では、サイバー攻撃の可能性は差し迫っていないと考えています。
C. サイバー攻撃のリスクを最小限に抑えるためのセキュリティ対策が設定されています。
Answer: C (メーッセージを残す**)**
サイバーセキュリティプロファイルの伝達:
* 組織のサイバーセキュリティ プロファイルを経営陣に提示する際には、実施されているセキュリティ対策の有効性とリスクを最小限に抑える能力に焦点を当てることが重要です。
明確さと関連性:
* ステートメント A (「サイバー攻撃の可能性は、低いから非常に高いまで変化する」) は漠然としすぎていて、実用的な情報を提供していません。
* ステートメント B (「リスク管理では、サイバー攻撃の可能性は差し迫っていないと考えている」) は具体性が欠けており、講じられた対策の詳細が示されていません。
セキュリティ対策の有効性:
* ステートメントCは、リスクを最小限に抑えるためのセキュリティ対策を積極的に講じていることを強調しています。このアプローチにより、経営陣は現在のサイバーセキュリティ体制に信頼を抱く可能性が高まります。
* NIST や ISO 27001 などのさまざまなフレームワークで概説されている IT リスク管理のベスト プラクティスによれば、セキュリティ制御の有効性と構成に重点を置くことが、サイバーセキュリティ リスクを管理する鍵となります。
結論：
* したがって、経営陣に提示するのに最適な記述は次のようになります。「セキュリティ対策は、サイバー攻撃のリスクを最小限に抑えるように構成されています。」

最新問題: **28**
事業継続性と災害復旧に関連する計画の正確性と適切性に最も影響を与えるのは次のどれでしょうか?
A. インシデント対応計画の重要な更新
B. データのバックアップがクラウドに移動されています
C. ビジネス影響評価（BIA）の変更

Answer: C (メーッセージを残す)
定義とコンテキスト:
* ビジネス影響評価（BIA）は、組織が重要なビジネス機能を特定し、ビジネス中断がそれらに及ぼす可能性のある影響を把握するのに役立つプロセスです。これは、事業継続計画と災害復旧計画の策定において不可欠です。
事業継続性と災害復旧への影響:
* インシデント対応計画の重要な更新はビジネスの継続性に影響を与える可能性がありますが、通常はビジネスへの影響を理解するための戦略的な転換ではなく、インシデントに対する戦術的な対応です。
* データのバックアップをクラウドに移行すると、回復力と復旧時間が向上しますが、この変更の戦略的重要性は、データの重要度とクラウド プロバイダーの信頼性によって左右されます。
* BIAの変更は、事業継続および災害復旧に関連する計画の正確性と適切性に直接影響を及ぼします。BIAは、何が重要か、許容可能なダウンタイム、そして復旧の優先順位を定義します。したがって、BIAの変更は、事業継続および復旧戦略に大きな変化をもたらす可能性があります。
結論：
* ビジネス継続計画における BIA の戦略的役割を考慮すると、BIA への変更は、ビジネス継続および災害復旧計画の正確性と適切性に最も大きな影響を及ぼします。

最新問題: **29**
プロジェクト計画を策定する際に、主要リスク指標 (KRI) は次のどの目的で使用されますか?
A. リソース割り当ての決定
B. リスクオーナーの割り当て
C. ギャップ分析の実行
Answer: C (メーッセージを残す)
重要リスク指標（KRI）は、組織が潜在的なリスクを特定し、重大な問題に発展する前に監視するのに役立つ早期警告指標です。プロジェクト計画を策定する際には、KRIはギャップ分析を行う際に最も効果的に活用されます。これは、現在のリスク状況と望ましいリスク管理目標を比較するのに役立つためです。
ギャップ分析に KRI が使用される理由
* リスク管理における弱点の特定:
* KRI は、既存のリスク管理が不十分な領域や新たな脅威が発生する可能性のある領域を強調表示します。
* リスク軽減戦略が効果的に機能しているかどうかを測定するための定量的および定性的なデータを提供します。
* リスク対応計画の改善：
* KRI は、予想されるリスクしきい値からの逸脱を評価するのに役立ち、組織がそれに応じてリスク対応を調整できるようにします。

* 現在の状況をベンチマークと比較することで、組織はセキュリティ、コンプライアンス、および回復力の対策におけるギャップを特定できます。
* プロジェクト計画における意思決定の強化：
* KRI を使用して適切に実行されたギャップ分析により、プロジェクト計画に最初から適切なリスク管理戦略が確実に組み込まれます。
* これにより、プロジェクト実行中の予期しない中断、コスト超過、コンプライアンスの問題が最小限に抑えられます。
他の選択肢はなぜダメなのか？
* オプションA（リソース割り当ての決定）：
* KRIはリスクに関する洞察を提供しますが、リソースを直接割り当てるわけではありません。リソースの割り当ては、KRIだけでなく、プロジェクトの予算と優先順位に基づいて行われます。
* オプションB（リスクオーナーの割り当て）：
* KRI はリスクの特定に役立ちますが、リスクを管理する責任は通常、KRI だけでなく、組織のリスク管理フレームワークとガバナンス ポリシーに基づいて割り当てられます。
結論：
KRI は、実際のリスク露出を定義されたリスク管理目標と比較するのに役立ち、組織が脆弱性を特定してリスク軽減戦略を改善できるため、ギャップ分析に最適です。
参考資料: インシデント対応と災害復旧の原則 - モジュール1: リスク管理フレームワーク

最新問題**: 30**
現在のコントロールの状態を評価する際に、企業のプロセス、インシデント、ログ、脅威環境の最も包括的な分析を提供するのは次のどれですか?
A. エンタープライズアーキテクチャ（EA）評価
B. IT運用と管理の評価
C. 第三者保証レビュー
Answer: (解答を表示する**)**
IT運用管理評価は、上記の領域の中で最も包括的な分析を提供します。通常、企業プロセス、インシデント対応手順、システムログ、脅威環境のレビューを行い、既存の管理策の有効性を評価します。
EA評価（A）はITアーキテクチャに焦点を当てており、必ずしも運用面に焦点を当てているわけではありません。第三者による保証レビュー（C）は有益ですが、その範囲は限定的になる可能性があります。

最新問題**: 31**
主要リスク指標 (KRI) を開発して監視する最も重要な理由は、次の点が提供されるためです。
A. 許容可能なリスク レベルを測定可能なメトリック。
B. 制御コンプライアンスに関する情報。

C. リスクが顕在化する可能性があるという早期警告。
Answer: (解答を表示する**)**
すべての参考文献を含むステップバイステップの包括的詳細説明：
* KRIの目的:
* KRI は、潜在的なリスク イベントに関する早期警告を提供するように設計されています。
* リスクが重大な問題になる前に組織が予防措置を講じるのに役立ちます。
* 早期警報システム:
* KRI はプロアクティブなリスク管理に不可欠であり、組織がリスク レベルの変化に迅速に対応できるようにします。
* 早期検出に重点を置くことで、他のリスク管理ツールを補完します。
* 参考文献:
* ISA 315 (2019 年改訂)、基準 5 では、リスクを効果的に管理および軽減するためのタイムリーで正確な情報の重要性について説明しています。

最新問題**: 32**
企業の存続にとって最も大きなリスクとなるのは次のどれですか?
A. リスク選好度とリスク許容度が毎年見直される時期
B. 実際のリスクが最終的に組織のリスク許容度を超えた場合
C. リスク選好度と実際のリスクがリスク許容度を超えた場合
Answer: (解答を表示する**)**
リスク選好度とは、組織が目標達成のために受け入れるリスクの量です。リスク許容度とは、このリスク選好度からの許容可能な変動幅です。一方、リスクキャパシティとは、組織が重大な破綻に直面する前に吸収できるリスクの最大量を表します。実際のリスク、さらにはリスク選好度がリスクキャパシティを超えると、組織の存続そのものが脅かされます。このシナリオは、潜在的な損失が組織が利用できるリソースを超え、倒産や崩壊につながる可能性があることを示唆しています。
リスク許容度 (B) を超えることは望ましくなく、対策が必要ですが、必ずしも組織の存続が差し迫った危機に瀕しているわけではありません。年次レビュー (A) は良い実践です。

最新問題**: 33**

次のどれがサイバーリスクと考えられますか?
A. ユーザーのニーズを満たさないシステム
B. セキュリティ技術の変化
C. 情報の不正使用
Answer: C (メーッセージを残す)
サイバーリスクとは、情報への不正アクセスや不正利用によって生じるITシステムの脅威や脆弱性を指します。これには情報の不正利用も含まれます。
* 定義と例:
* サイバーリスク: サイバー攻撃、データ損失、情報盗難に関連するリスク。
* 情報の不正使用: 権限のない人物が機密データにアクセスするサイバーリスクの例。
* 保護対策:
* アクセス制御: 不正アクセスを防ぐための認証と承認。
* セキュリティ監視: 侵入検知システム (IDS) と定期的なセキュリティ監査。
参考文献:
* ISA 315: 情報への不正アクセスや不正使用を防止するための IT 制御の重要性。
* ISO 27001: 不正アクセスを含む情報セキュリティリスクを管理するためのフレームワーク。

最新問題**: 34**
機密データにアクセスするために 2 要素認証ログイン方法を使用する企業は、どのようなタイプの制御を実装していますか?
A. 予防的
B. 修正
C. 探偵
Answer: A (メーッセージを残す)
機密データへのアクセスに二要素認証ログイン方式を採用している企業は、予防措置を導入しています。その理由は次のとおりです。
* 予防制御: このタイプの制御は、セキュリティ インシデントが発生する前に防止するように設計されています。
二要素認証（2FA）は、機密データへのアクセスに2種類の認証方法（例:パスワードとモバイルコード）を要求することでセキュリティを強化します。これにより、たとえ1つの認証要素（パスワードなど）が漏洩したとしても、2つ目の要素が侵入の障壁として機能し、不正アクセスを防止します。
* 是正管理: これらの管理は、インシデントが発生した後に実行され、是正または
* 影響を軽減する。例としては、バックアップからデータを復元したり、脆弱性が悪用された後にパッチを適用したりすることが挙げられます。2FAはインシデントを修正するのではなく、インシデントの発生を予防します。
* 検出制御: これらの制御は、インシデントが発生したときにそれを検出して警告するように設計されています。

例としては、侵入検知システム (IDS) や監査ログなどが挙げられます。2FA は検出ではなく予防が目的です。
したがって、二要素認証は予防的な制御です。

最新問題**: 35**
次のどれがエクスプロイト イベントとみなされますか?
A. 攻撃者が脆弱性を悪用する
B. セキュリティ違反として検証されたイベント
C. 有害事象の実際の発生
Answer: (解答を表示する**)**
エクスプロイトとは、攻撃者が脆弱性を悪用して不正アクセスやシステムへの侵入を行うことを指します。これはITセキュリティにおける基本的な概念です。攻撃者がソフトウェア、ハードウェア、またはネットワークプロトコルの既知または未知の脆弱性を発見し、それを悪用することをエクスプロイトと呼びます。
* 定義と意味:
* エクスプロイトとは、システムの脆弱性を悪用するために使用される方法または技術です。
* 脆弱性には、ソフトウェア エラー、誤った構成、セキュリティ ホールなどがあります。
* エクスプロイトイベントの有効期限:
* 脆弱性の特定: 攻撃者はシステムの脆弱性を発見します。
* エクスプロイトの開発: 攻撃者は脆弱性を悪用するためにツールを開発するか、既存のツールを使用します。
* 攻撃の実行: 不正アクセスを取得したり、損害を与えたりするためにエクスプロイトが実行されます。
参考文献:
* ISA 315: 一般的な IT 管理と、IT の使用から生じるリスクを特定して管理する必要性。
* IDW PS 951: 年次財務諸表監査の文脈における IT リスクと管理。脆弱性を特定して評価するための管理の必要性を強調しています。

最新問題**: 36**
ある企業は、洪水の危険性が高く、サービスに重大な支障をきたした地域から、洪水の危険性のない地域へデータセンターを移転しました。この組織はどのようなリスク対応戦略を選択しましたか？
A. リスク軽減
B. リスク移転
C. リスク回避
Answer: (解答を表示する**)**
組織は、データセンターを洪水が発生しやすい地域から洪水地域ではない地域に移転することで、リスク回避戦略を選択しました。
* リスク対応戦略の概要:

* リスク受容: 何も行動を起こさずにリスクを受け入れることを選択すること。
* リスク回避:リスクを完全に回避するための措置を講じます。
* リスク軽減: リスクの発生可能性または影響を軽減するための対策を実施します。
* リスク移転: リスクを別の当事者に移すこと (例: 保険を通じて)。
* リスク回避の説明:
* リスク回避には、リスクを完全に回避するための計画の変更が含まれます。
* この場合、データセンターを洪水が発生しにくい地域に移転すると、洪水による混乱のリスクがなくなります。
* 参考文献:
* ISA 315 (2019 年改訂)、基準 6 では、さまざまなリスク対応戦略について説明し、実行可能な場合はリスクを回避するための措置を講じることの重要性を強調しています。

最新問題**: 37**
リスク対応プロセスで最も早く発生するのは次のどれですか?
A. リスク対応計画の策定
B. リスク対応の優先順位付け
C. リスク対応オプションの分析
Answer: C (メーッセージを残す**)**
リスク対応プロセスの手順:
* リスク対応プロセスには通常、リスク対応オプションの分析、リスク対応の優先順位付け、リスク対応計画の策定といういくつかの重要なステップが含まれます。
* リスク対応オプションの分析は、特定されたリスクに対処するためのさまざまな方法を評価することが含まれるため、最も早い段階で行われます。
ステップバイステップのプロセス:
* リスク対応オプションの分析 :これは、特定されたリスクに対する様々な潜在的な対応策を検討する最初のステップです。選択肢には、リスクの受容、回避、軽減、移転などが含まれます。
* リスク対応の優先順位付け: オプションを分析した後、次のステップは、影響、可能性、実装コストなどの要素に基づいて優先順位を付けることです。
* リスク対応計画の策定: 最後に、優先順位が付けられたリスク対応について、具体的な対応策、必要なリソース、タイムラインを概説した詳細な計画が作成されます。
参考文献:
* ISA 315 (2019 年改訂)、基準 5 は、適切なリスク対応の評価と選択を含む、リスク管理のコンポーネントを理解するためのフレームワークを提供します。

最新問題**: 38**
オンラインスキミング攻撃の増加への懸念に対処するため、ある企業はソフトウェア開発チームに対し、安全なソフトウェア開発手法に関するトレーニングを実施しています。これは、以下のリスク対応戦略のどれに該当しますか？
A. リスク受容

B. リスク回避
C. リスク軽減
Answer: C (メーッセージを残す**)**
企業は、オンラインスキミング攻撃の増加に対する懸念に対処するため、ソフトウェア開発チームに安全なソフトウェア開発手法に関するトレーニングを実施しています。これは、リスクの発生可能性や影響を軽減するための措置を講じるものであり、リスク軽減の一例です。
* リスク対応戦略の概要:
* リスク受容: 何も行動を起こさずにリスクを受け入れることを選択すること。
* リスク回避:リスクを完全に回避するための措置を講じます。
* リスク軽減: リスクの発生可能性または影響を軽減するための対策を実施します。
* リスク移転: リスクを別の当事者に移すこと (例: 保険を通じて)。
* リスク軽減の説明:
* リスク軽減には、リスクの発生可能性や影響を軽減する制御と対策を実施することが含まれます。
* 安全なソフトウェア開発手法についてソフトウェア開発チームをトレーニングすることで、オンラインスキミング攻撃で悪用される可能性のある潜在的な脆弱性に直接対処し、リスクを軽減します。
* 参考文献:
* ISA 315 (2019 年改訂)、基準 6 では、IT システムに関連するリスクを軽減するために IT 制御を理解して実装することの重要性について説明しています。

最新問題**: 39**
I&T 資産の重要性を判断する際には、次の点を特定することが最も重要です。
A. 資産評価の責任を負う資産所有者。
B. 目標を達成するために資産が使用されるビジネス プロセス。
C. 資産が処理および保存されるインフラストラクチャ。
Answer: B (メーッセージを残す**)**
I&T資産の重要度は、それがサポートするビジネスプロセスにおける重要性によって決まります。資産が重要なビジネスプロセスに不可欠な場合、その資産は「極めて重要」とみなされます。資産が利用できない場合、ビジネスプロセスに与える影響が重要な要素となります。
資産所有者 (A)は説明責任を果たす上で重要ですが、重要性を決定づけるのはビジネスプロセスです。インフラストラクチャ (C)はセキュリティ上の考慮事項に関連しますが、重要性を決定づけるのはビジネスプロセスです。

最新問題**: 40**
最近のセキュリティ評価で特定された制御欠陥のリストが IT リスク レジスタから除外される理由として最も可能性が高いのは次のどれですか。

A. 欠陥はビジネスとは関連性がありません。
B. 欠陥は実際の構成ミスです。
C. 欠陥はすでに解決されています。
Answer: C (メーッセージを残す**)**
ITリスク登録簿から統制上の不備を除外する最も可能性の高い理由は、それらが既に解決済みである場合です。リスク登録簿は、注意または対策が必要な現在のリスクに焦点を当てるべきです。
ビジネスとの関連性がない欠陥 (A)は優先度が低いかもしれませんが、リスクレジスターには関連する可能性があります。実際の設定ミス (B)は間違いなく関連するため、リスクレジスターに含める必要があります。

最新問題**: 41**
統計分析手法を I&T リスク シナリオに適用するのは、次のような場合に最も適しています。
A. 詳細なレビューのために定量化可能な履歴データが利用可能です。
B. リスク管理の専門家は定性的な手法に精通していません。
C. 上級管理職のメンバーは高度な数学の知識を持っています。
Answer: A (メーッセージを残す**)**
統計分析が意味を持つためには、定量化可能な過去のデータが必要です。これらの手法は、過去のデータに基づいて将来の確率と潜在的な影響を予測します。したがって、そのようなデータが利用可能な場合、統計分析は最も適切です。
定性的な手法への精通度 (B)は、統計分析が適切かどうかとは無関係です。また、上級管理職の数学的知識 (C)も決定要因ではありません。

最新問題**: 42**
リスクの計算に関連するリスク管理コンテキストを確立する際に、定義された基準と一致していなければならないのは次のどれですか。
A. リスク選好度と許容レベル
B. 影響と可能性を組み合わせるための公式と方法
C. 主要リスク指標 (KRI)と主要業績評価指標 (KPI)
Answer: B (メーッセージを残す**)**
リスク計算のためのリスク管理の枠組みを確立する際には、影響度と発生可能性を組み合わせるための計算式と手法が、定義された基準と整合している必要があります。これにより、リスク計算の正確性と意義が確保されます。計算式と手法が整合していない場合、結果として得られるリスクスコアは、リスクの真のレベルを正確に反映しない可能性があります。
リスク選好度とリスク許容度 (A)は全体的なリスク管理において重要ですが、計算式を直接決定するものではありません。KRIとKPI (C)は、計算ではなくモニタリングに使用されます。

最新問題: **43**
詳細なリスク管理レポートは、次の基準に基づいて特定の対象者を対象にする必要があります。
A. 知っておく必要があります。
B. 業界ベンチマーク。
C. 企業内の役職レベル。
Answer: A (メーッセージを残す**)**
詳細なリスク管理レポートは、 知る必要がある」という原則に基づいて作成する必要があります。これは、役割と責任を果たすために必要な人にのみ情報を提供することを意味します。これにより、情報の関連性と実用性を確保できます。
業界ベンチマーク (B)はレポート作成の参考になりますが、読者のニーズが最も重要です。
役職レベル (C)も重要な要素となりますが、情報に対する具体的なニーズの方が重要です。

最新問題: **44**
定性的なリスク分析を実行する理由として最も可能性が高いのは次のどれですか?
A. ビジネスユニット間の依存関係と相互作用を低コストで理解する
B. 企業のリスクを包括的に把握するために、リスクを意味のある方法で集約する
C. リスク対応のコストと直接比較できる利益の価値をマッピングする
Answer: A (メーッセージを残す**)**
定性的なリスク分析は、事業部門間の依存関係や相互作用を低コストで理解するために実施されることが多いです。その理由は次のとおりです。
* 事業部門間の依存関係と相互作用を低コストで理解する：定性リスク分析は、インタビュー、アンケート、専門家の判断といった主観的な尺度を用いて、リスクの特性と影響度に基づいてリスクを評価することに重点を置いています。定量分析に比べてリソース消費が少なく、事業部門間の依存関係と相互作用を幅広く理解することができます。
* 企業リスクの包括的な視点を得るためにリスクを意味のある方法で集約する: 定性分析はこれに貢献できますが、主な目的は集約ではなく、個々のリスクとその影響を理解することです。
* リスク対応のコストと直接比較できる利益の価値をマッピングする: これは通常、リスクとその影響を数値的に推定し、コストと利益を直接比較する定量的リスク分析の目標です。
したがって、定性的なリスク分析を実行する主な理由は、ビジネス ユニットの依存関係と相互作用を低コストで理解することです。

最新問題: **45**
次のどれがサイバーリスクと考えられますか?
A. ユーザーのニーズを満たさないシステム
B. セキュリティ技術の変化
C. 情報の不正使用

Answer: C (メーッセージを残す)
サイバーリスクとは、情報への不正アクセスや不正利用によって生じるITシステムの脅威や脆弱性を指します。これには情報の不正利用も含まれます。
* 定義と例:
* サイバーリスク: サイバー攻撃、データ損失、情報盗難に関連するリスク。
* 情報の不正使用: 権限のない人物が機密データにアクセスするサイバーリスクの例。
* 保護対策:
* アクセス制御: 不正アクセスを防ぐための認証と承認。
* セキュリティ監視: 侵入検知システム (IDS) と定期的なセキュリティ監査。
参考文献:
* ISA 315: 情報への不正アクセスや不正使用を防止するための IT 制御の重要性。
* ISO 27001: 不正アクセスを含む情報セキュリティリスクを管理するためのフレームワーク。

最新問題**: 46**
主要リスク指標 (KRI) は主に次のどの目的で使用されますか?
A. リスク管理の最適化
B. リスクイベントの予測
C. ダッシュボードレポートの容易化
Answer: B (メーッセージを残す)
* KRIの主な用途:
* KRI は主に、潜在的な問題を示す測定可能なデータを提供して、リスク イベントを予測するために使用されます。
* この予測機能は、組織がリスクが拡大する前にリスクを軽減するのに役立ちます。
* リスク予測:
* 効果的な KRI により、組織は潜在的なリスクを予測し、それらに積極的に対処するための対策を実施できます。
* これにより、リスク イベントの発生確率と影響が軽減され、全体的なリスク管理プロセスが改善されます。
* 参考文献:
* ISA 315 (2019 年改訂)、基準 6 では、組織の IT および運用環境内のリスクを監視および予測するための指標とメトリックの使用が強調されています。

最新問題: **47**
次のうち、リスクガバナンスの責任を負うステークホルダーグループはどれですか?
A. 取締役会
B. エンタープライズリスクマネジメント（ERM）
C. ビジネスユニット
Answer: A (メーッセージを残す)
リスクガバナンスの最終責任は取締役会にあります。ERM、事業部門、IT管理はいずれもリスク管理において重要な役割を果たしますが、リスクガバナンス（全体的なリスク選好の設定、役割と責任の明確化、リスク管理の有効性のモニタリング）は取締役会が担います。取締役会は、リスク管理が組織の戦略目標と統合されるように、監督と指示を行います。取締役会の責任は、組織とそのステークホルダーに対する受託者責任に由来します。取締役会は、リスクの効果的な管理を含む、企業全体の成功と持続可能性に責任を負います。

最新問題: **48**
プロジェクトのクリティカルパスを決定するために最も重要な情報はどれですか?
A. 規制要件
B. 費用便益分析
C. 指定された終了日
Answer: C (メーッセージを残す)
プロジェクト管理コンテキスト:
* プロジェクト管理におけるクリティカル パスとは、操作に必要な最小時間を決定する一連の段階のことです。
クリティカルパスに影響を与える要因:
* 規制要件は不可欠ですが、通常はタスクの順序を定義しません。
* 費用便益分析は意思決定に役立ちますが、タスクの依存関係やタイミングを直接決定するものではありません。
* 指定された終了日は、タスクのスケジュールと依存関係に直接影響し、プロジェクトが予定通りに完了することを保証するクリティカル パスを定義します。
結論：
* 指定された終了日は、すべてのタスクを完了する必要があるフレームワークを確立し、プロジェクトがスケジュールに準拠することを保証するため、クリティカル パスを決定するための最も重要な情報です。

最新問題: **49**
企業がサードパーティプロバイダーのスキルと専門知識を活用するために災害復旧活動をアウトソーシングする場合、どのリスク対応オプションが採用されていますか?
A. リスク軽減

B. リスク回避
C. リスク移転
Answer: C (メーッセージを残す**)**
災害復旧業務のアウトソーシングは、リスク移転の一例です。組織は災害リスク管理の責任をサードパーティのプロバイダーに移転します。組織は依然としてリスクに直面しますが、そのリスクを軽減する責任はプロバイダーに移ります。
リスク軽減 (A) には、災害の発生可能性または影響を軽減するための対策を実施することが含まれます。
リスク回避 (B) は、リスクを生み出す活動を停止することを意味します。