PECB.ISO-IEC-27001-Lead-Implementer.v2026-06-29.q119

試験コード：	ISO-IEC-27001-Lead-Implementer
試験名称：	PECB Certified ISO/IEC 27001 Lead Implementer Exam
認証ベンダー：	PECB
無料問題の数：	119
バージョン：	v2026-06-29
ページの閲覧量：	107
問題集の閲覧量：	1246

https://www.jpnshiken.com/shiken/PECB.ISO-IEC-27001-Lead-Implementer.v2026-06-29.q119.html

質問: **1**
シナリオ2 :NyvMarketingは、さまざまな業界の顧客に多様なサービスを提供するマーケティング会社です。デジタルマーケティング、ブランディング、市場調査の専門知識を活かし、革新的でインパクトのあるマーケティングキャンペーンを提供することで確固たる評判を築いてきました。マーケティング業界におけるデータセキュリティと情報保護の重要性の高まりを受け、同社はISMS 27001に基づくISMSを導入することを決定しました。
NyvMarketingはISMSを導入する際に、リソース不足という重大な課題に直面しました。この課題はISMSの目標を効果的に達成する上でリスクとなり、機密情報の保護に向けた同社の取り組みを損なう可能性がありました。この脅威に対処するため、NyvMarketingはリソース制約に関連するリスクを管理する担当者としてマイケルを任命するという積極的なアプローチを採用しました。
マイケルは、NyvMarket*ngにおけるISMS導入において、リソース不足の特定と対処、リスク軽減戦略の策定、効果的なリソース配分において極めて重要な役割を果たし、リソース不足に対する同社の回復力を強化した。
さらに、NyvMarketingは情報セキュリティにおける業界標準とベストプラクティスを優先し、ISO/IEC 27002ガイドラインを徹底的に遵守しました。卓越性とISO/IEC 27001の要件に基づいたこの取り組みは、NyvMarketingが最高水準の情報セキュリティガバナンスを維持するという強い意志を明確に示しています。
ISMS導入作業中、NyvMarketingは能力に関する要求事項（ISO/IEC 27001、7.2項に規定）の1つを除外することを選択しました。同社は、既存の従業員がISMS関連業務を遂行するために必要な能力を備えていると考えていましたが、この除外に対する正当な理由を提示しませんでした。さらに、ISO/IEC 27001の附属書Aに記載されている特定の管理策が実施されなかった際も、NyvMarketingはこれらの除外に対する適切な理由を提示しませんでした。
ISMS導入の過程で、NFMarketingは情報セキュリティに影響を与える可能性のある脆弱性を徹底的に評価しました。これらの脆弱性には、ストレージメディアの不十分なメンテナンスと不適切なインストール、機器の不十分な定期交換計画、不十分なソフトウェアテス

ト、および保護されていない通信回線が含まれていました。これらの脆弱性がデータセキュリティにリスクをもたらす可能性があることを認識したNFMarketingは、必要な制御と対策を実施することで、これらの特定の弱点に対処するための措置を講じました。上記のシナリオに基づいて、次の質問に答えてください。
シナリオ2において、NyvMarketingはISMS導入中にリソース不足の脅威に直面しました。この脅威は次のどのカテゴリに該当しますか？
シナリオ2によると、NyvMarketingは附属書Aの管理策の実施に関して、ISO/IEC 27001に準拠した措置を講じましたか？
A. はい、NyvMarketingが附属書Aの管理策の実施中に取った措置はISOに準拠しています。/IEC 27001
B. いいえ、NyvMarketingの行為はISO/IEC 27001に準拠していません。なぜなら、同社は正当な理由を示すことなく附属書Aの管理策の1つを除外したからです。
C. いいえ、NyvMarketingの行為はISO/IEC 27001に準拠していませんでした。なぜなら、附属書Aのすべての管理策が含まれていなかったからです。
D. はい、ISO/IEC 27002では除外が認められているからです。
正解: **(**正解を表示します**)**
ISO/IEC 27001:2022では、組織が附属書Aの管理策を除外する場合、それぞれの除外について正当な理由を提示しなければならないと規定されています（6.1.3.d項）。文書化された正当な理由なしに管理策や要求事項（例えば、能力、7.2項）を単に省略することは、ISO/IEC 27001への不適合となります。すべての除外は、リスク評価およびリスク対応プロセスの結果に基づき、正当な理由をもって行われなければなりません。
「省略された管理策はすべて正当化されなければならず、その正当化は適用範囲に関する声明の一部として文書化されなければならない。」
- ISO/IEC 27001:2022、6.1.3項 d)
「組織は、管理策の包含および除外を正当化する適用性に関する声明書を作成しなければならない。」
- ISO/IEC 27001:2022、6.1.3項 d)

質問: **2**
情報セキュリティリスクに関する以下の記述のうち、正しくないものはどれですか？
A. 情報セキュリティリスクとは、情報資産の脆弱性が脅威によって悪用される可能性に関連するものです。
B. 情報セキュリティリスクは、対処せずに、またはリスク対処の過程で容認することはできません。
C. 情報セキュリティリスクは、不確実性が情報セキュリティ目標に及ぼす影響として表現できる。
正解: **B (**コメントを発表する**)**
ISO/IEC 27001:2022によると、情報セキュリティリスクは、リスクの回避、修正、共有に加えて、リスク処理の4つの選択肢の1つとして受け入れることができます12。リスクの受容

とは、組織がリスクを軽減するためのさらなる措置を講じることなく、リスクのレベルを容認することを決定することを意味します3。リスクの受容は、組織のリスク基準と残存リスクレベルに応じて、リスク処理プロセスの前、途中、または後に行うことができます4。

質問: **3**
残存リスクに関する以下の記述のうち、正しいものはどれですか？
A. それは未確認のリスクを含む可能性があります。
B. 保有リスクのみで構成されます。
C. 契約や保険を通じて移転されたリスクは除外されます。
正解: **(**正解を表示します**)**
ISO/IEC 27000:2018では、残留リスクはリスク処理後に残るリスクとして定義されています。
ISO/IEC 27005:2022によれば、残留リスクには、リスク評価プロセス中に特定されなかったリスクが含まれる可能性があります。つまり、未特定リスクは残留リスクの一部を構成するということです。これは、リスク評価は網羅的ではないため、評価範囲外に未知の脅威や新たな脅威が存在する可能性があるためです。オプションBは、残留リスクは保持リスクのみに限定されず、修正、共有、回避など、すべての対策オプションの後に残るリスクが含まれるため、誤りです。オプションCは、移転されたリスク（保険や契約によるもの）も、移転が部分的または不完全な場合があるため、残留リスクに寄与するため、誤りです。したがって、完全に正しい記述は、残留リスクは未特定リスクで構成される可能性があるというものであり、これはISO/IEC 27005と一致しています。
2022年リスク管理ガイダンス

質問: **4**
権力／利害マトリックスはどのような目的で使用されるのですか？
A. ビジネス要件を特定する
B. 情報セキュリティと物理的境界を定義する
C. 利害関係者を特定し、管理する
正解: **C (**コメントを発表する**)**

質問: **5**
シナリオ4 :TradeBは、市場に参入したばかりの商業銀行で、顧客から預金を受け入れ、基本的な金融サービスと投資ローンを提供しています。TradeBは、ISO/IEC 27001に基づく情報セキュリティマネジメントシステム（ISMS）を導入することを決定しました。マネジメントの経験がないTradeBは、
[^システム実装、TradeBの経営陣はISMS実装プロジェクトを指揮・管理するために2人の専門家と契約しました。
まず、プロジェクトチームはISO/IEC 27001附属書Aの93の管理策を分析し、会社とその目的に適用可能と判断されたセキュリティ管理策のみをリストアップしました。この分析に

基づいて、適用性に関する声明書を作成しました。その後、リスク評価を実施し、ハードウェア、ソフトウェア、ネットワークなどの資産、脅威、脆弱性を特定し、潜在的な結果と発生可能性を評価し、3つの非数値カテゴリ（低、中、高）に基づいてリスクレベルを決定しました。彼らはリスク評価基準に基づいてリスクを評価し、高リスクカテゴリのみを扱うことに決定しました。また、アクセス制御ポリシーの新しいバージョンを確立し、ユーザーアクセスを管理および制御するための制御を実装し、事業継続のためのICT準備のための制御を実装することにより、管理者権限の不正使用と複数のハードウェア障害によるシステムの中断に主に焦点を当てることも決定しました。最後に、彼らはリスク評価レポートを作成し、これらのセキュリティ制御の実装後にリスクレベルが許容レベルを下回る場合は、リスクを受け入れると記述しました。残存リスクに対処するために、TradeBは何をすべきでしょうか。シナリオ4を参照してください。

A. TradeBは、リスク処理後のリスク軽減の価値を評価、計算、文書化する必要があります。

B. TradeBは、すべての残存リスクに対処するため、直ちに新たな管理策を実施すべきである。

C. TradeBは、許容レベルを超える残存リスクのみを受け入れるべきである。

正解: **(**正解を表示します**)**

ISO/IEC 27001:2022の主たる実施者によると、残留リスクとは、リスク対策後に残るリスクのことです。残留リスクは、組織が許容できるリスクレベルである許容リスクレベルと比較する必要があります。残留リスクが許容リスクレベルを下回る場合は、リスクを受け入れることができます。残留リスクが許容リスクレベルを上回る場合は、追加のリスク対策を検討する必要があります。したがって、TradeBは、リスク対策後のリスク低減値（初期リスクと残留リスクの差）を評価、計算、文書化する必要があります。これにより、TradeBは、リスク対策が効果的であったかどうか、また残留リスクが許容範囲内であるかどうかを判断することができます。

質問: **6**

シナリオ 7: InfoSec は、マサチューセッツ州ボストンに本社を置く多国籍企業で、プロフェッショナル向け電子機器、ゲーム、エンターテイメント サービスを提供しています。InfoSec は、数々の情報セキュリティ インシデントに直面した後、将来起こりうるインシデントを防止するためのチームを設立し、対策を実施することを決定しました。Emma、Bob、Anna は、セキュリティ アーキテクチャ チーム、インシデント対応チーム (IRT)、フォレンジック チームで構成される InfoSec の情報セキュリティ チームの新しいメンバーとして採用されました。Emma の仕事は、InfoSec がインシデントに効果的に対応できるようにするための情報セキュリティ計画、ポリシー、プロトコル、トレーニングを作成することです。Emma と Bob は InfoSec の正社員ですが、Anna は外部コンサルタントとして契約しています。

ネットワークのエキスパートであるボブは、スクリーニングされたサブネットネットワークアーキテクチャを導入します。このアーキテクチャは、ホストされているパブリックサービスが接続されている非武装地帯（DMZ）と、情報セキュリティ部門の公開アクセス可

能なリソースを、プライベートネットワークから分離します。これにより、情報セキュリティ部門は、潜在的な攻撃者が社内ネットワーク内で望ましくない事象を引き起こすのを阻止できるようになります。ボブはまた、予期せぬ事象が発生した場合、その事象がどのように発生したか、そしてそれが何や誰に影響を与える可能性があるかといった詳細を含め、その事象の性質を徹底的に評価する責任も負っています。
アンナは、懲戒処分や法的措置のための証拠を保管し、将来のインシデントを防止するために、データ、レビュー、分析、レポートの記録を作成します。この作業を適切に行うためには、事前に会社の情報セキュリティインシデント管理ポリシーを理解しておく必要があります。このポリシーでは、作成する記録の種類、保管場所、特定の記録の種類ごとに必要な形式や内容などが規定されています。
シナリオ7によると、InfoSecのネットワーク内に非武装地帯（DMZ）が設置されています。この場合、InfoSecはどのような制御を実装しているのでしょうか？
A. 探偵
B. 予防
C. 修正
正解: **(**正解を表示します**)**
説明
非武装地帯（DMZ）とは、内部ネットワークとインターネットなどの外部ネットワークを分離するネットワークセグメントです。ウェブサーバー、メールサーバー、DNSサーバーなど、組織外部からアクセスする必要のあるパブリックサービスをホストするために使用されます。DMZは、パブリックサービスの露出を制限し、外部ネットワークからの不正アクセスを防止することで、内部ネットワークを保護するレイヤーを提供します。DMZは予防的制御の一例であり、予防的制御とは、情報セキュリティインシデントの発生を防止または抑止することを目的とした制御の一種です。予防的制御は、脅威が脆弱性を悪用して組織の情報資産に損害を与える可能性を低減します。その他の予防的制御の例としては、暗号化、認証、ファイアウォール、ウイルス対策ソフトウェア、セキュリティ意識向上トレーニングなどがあります。
参考文献：
ISO/IEC 27001 : 2022 リードインプリメンター学習ガイド、セクション 8.2.3.2.1、162 ページ ISO/IEC 27001 : 2022 リードインプリメンター情報キット、13 ページ ISO/IEC 27002 : 2022、セクション 13.1.3、66 ページ

質問: **7**
シナリオ 6: CB Consulting は、アイルランドのダブリンに拠点を置く評判の高い企業です。多様なクライアントに戦略的なビジネス ソリューションを提供しています。専門家からなる専任チームを擁する CB Consulting は、卓越性、誠実さ、顧客満足への取り組みを誇りとしています。CB Consulting は、情報セキュリティの実践を強化するという継続的な取り組みの一環として、ISO 1EC 27001 に準拠した ISMS の導入を開始しました。このプロ

セス全体を通して、効果的なコミュニケーションと確立されたセキュリティ プロトコルの遵守を確保することが不可欠です。
CB社の従業員であるサラは、機密性の高い顧客データの管理に焦点を当てた新しいプロジェクトの責任者に任命されました。さらに、彼女はインシデント管理の対応フェーズにおける活動の監督、インシデント管理チームのインシデントマネージャーへの定期的な報告、主要な関係者への情報提供なども担当します。一方、CBコンサルティングはトムを同社の法務コンサルタントに異動させました。
CBコンサルティングは、以前ITセキュリティアナリストだったクレアを情報セキュリティ責任者に再任し、ISMSの導入を監督し、ISO/IEC 27001への準拠を確保するよう指示しました。クレアの主な責任は、定期的なリスク評価を実施し、潜在的な脆弱性を特定し、リスクを効果的に軽減するための適切なセキュリティ対策を実施することです。クレアは、情報セキュリティリスク評価は重大な変更が発生した場合にのみ実施するという手順を確立しました。これは、会社のセキュリティ体制を強化し、潜在的な脅威から保護する上で重要な役割を果たします。
CBコンサルティングは、情報セキュリティ目標を達成できる有能な人材を確保するため、サラ、トム、クレアを含む全従業員が、学歴、研修、または経験に基づき必要な能力を備えていることを検証するプロセスを導入しました。不足が認められた場合は、追加の研修やメンター制度の提供など、具体的な対策を講じています。さらに、CBコンサルティングは、必要な能力と習得した能力の証拠として、文書化された情報を保管しています。
CBコンサルティングは、安全かつ効果的な情報交換を確保するために、業界標準に準拠した強固なコミュニケーション戦略を確立しました。関連する問題に関するコミュニケーションの要件を特定しました。まず、同社は特定の役割を指定しました。外部コミュニケーションのための広報担当者や、データ漏洩などの機密事項を管理する内部問題のためのセキュリティ担当者などです。次に、
コミュニケーションのきっかけ、内容、および受信者は慎重に定義され、必要に応じてメッセージは経営陣の事前承認を得ました。最後に、送信される情報の機密性と完全性を確保するために、専用のチャネルが導入されました。
上記のシナリオに基づいて、次の質問に答えてください。
CBコンサルティングは、信頼を醸成し、ステークホルダーの関与を高め、情報セキュリティにおける卓越性への取り組みを強化するために、透明性と実質的なコミュニケーションの実践を優先しています。このアプローチによって強調されている効果的なコミュニケーションの原則はどれですか？
透明性
CBコンサルティングは、必要な能力の習得に関するISO/IEC 27001の要求事項への準拠を確保するために適切な措置を講じましたか？シナリオ6を参照してください。
A. はい。CBコンサルティングは、必要な能力の取得に関して法令遵守措置を講じています。
B. いいえ、ISMS導入管理に直接関連する業務に既存の従業員を再配置することは認められません。

C. いいえ、既存の従業員を法律相談関連の業務に再配置することは認められていません。
正解: **(**正解を表示します**)**
ISO/IEC 27001:2022の7.2項では、組織は従業員が教育、訓練、または経験に基づいて能力を有していることを確認し、不足が認められた場合は適切な措置を講じることを求めています。CBコンサルティングは、能力の検証、必要に応じた追加訓練と指導の提供、証拠としての記録の保管など、規格に準拠した対応を行いました。
組織は、従業員が適切な教育、訓練、または経験に基づいて能力を有していることを保証しなければならない。該当する場合は、必要な能力を習得するための措置を講じ、能力の証拠として適切な文書情報を保持しなければならない。」
- ISO/IEC 27001:2022、7.2項

質問: **8**
従業員および契約社員に対し、情報セキュリティポリシーまたは手順の違反を報告するための匿名通報チャネル（内部告発」）を提供することは認められています。
A. 真
B. 偽
正解: **(**正解を表示します**)**

質問: **9**
コンピュータシステムにとって、人間以外の脅威としては洪水が挙げられる。洪水が常に脅威となるのはどのような状況か？
A. 組織が川の近くに位置している場合。
B. コンピュータシステムを地下の地下室に保管する場合。
C. リスク分析が実施されていない場合。
D. コンピュータシステムに保険がかけられていない場合。
正解: **B (**コメントを発表する**)**

質問: **10**
組織は、外部の第三者によって情報が転送または処理される際に、情報のセキュリティを確保するためにどのような措置を講じるべきでしょうか？
A. 外部の当事者との契約にセキュリティ条項を含める
B. リスクエクスポージャーを制限するために、ISMSの範囲から外部関係者を除外する。
C. 外部の関係者にセキュリティ対策の実施を委託する
正解: **(**正解を表示します**)**

質問: **11**
A社が従業員に対し、少なくとも60日に1回はメールのパスワードを変更することを義務付けている場合、どのようなリスク対策を実施していると言えるでしょうか？
A. リスク修正
B. リスク回避

C. リスク保持
正解: **(**正解を表示します**)**
リスク修正は、ISO/IEC 27001で定義されている4つのリスク対策オプションの1つであり、リスクの発生確率や影響を低減するための対策を講じるものです。A社は、従業員に少なくとも60日に1回メールのパスワードを変更することを義務付けることで、メールアカウントへの不正アクセスリスクを低減するリスク修正オプションを実施しています。パスワードを頻繁に変更することで、攻撃者がパスワードを推測したり解読したりすることが難しくなり、パスワードが漏洩した場合の被害を最小限に抑えることができます。
その他の3つのリスク治療オプションは以下のとおりです。
リスク回避 :この選択肢は、リスクの原因を取り除くか、リスクを引き起こす活動を中止することです。例えば、A社はメールを一切使用しないことでメール漏洩のリスクを回避できますが、これは同時にメールによるコミュニケーションのメリットを失うことにもなります。
リスク保持 :この選択肢は、リスクが低すぎて対策を講じる必要がない場合、または対策費用が潜在的な損失に比べて高すぎる場合など、リスクとその結果を受け入れることを意味します。例えば、A社はセキュリティ対策を一切講じないことでメール侵害のリスクを保持できますが、その場合、情報漏洩や評判の低下といった潜在的なリスクにさらされることになります。
リスク移転 :このオプションでは、保険会社、サプライヤー、パートナーなどの第三者とリスクを共有または移転します。例えば、A社はメールサービスをクラウドプロバイダーにアウトソーシングすることで、メールアカウントのセキュリティと可用性をクラウドプロバイダーに委託し、メール侵害のリスクを移転することができます。
参照：
ISO/IEC 27001:2013、6.1.3項：情報セキュリティリスクの取り扱い
ISO/IEC 27001 リードインプリメンターコース、モジュール 4: ISO/IEC 27001 に基づく ISMS の計画 ISO/IEC 27001 リードインプリメンターコース、モジュール 6: ISO/IEC 27001 に基づく ISMS の実装 ISO/IEC 27001 リードインプリメンターコース、モジュール 7: ISO/IEC 27001 に基づく ISMS のパフォーマンス評価、監視、測定 ISO/IEC 27001 リードインプリメンターコース、モジュール 8: ISO/IEC 27001 に基づく ISMS の継続的改善 ISO/IEC 27001 リードインプリメンターコース、モジュール 9: ISMS 認証監査の準備 ISO 27001 リスク評価とリスク処理: 完全ガイド - Advisera1 ISO 27001 要求事項 8.3 の情報セキュリティリスク処理 - ISMS.online2 ISO 27001 条項 6.1.3 情報セキュリティリスク処理 3 ISO 27001 リスク対策計画 - Scrut Automation4

質問**: 12**
ある組織が、ISO/IEC 27001附属書Aの管理策に加えて、他の情報源からの追加的な管理策を導入しました。これは許容範囲内でしょうか？
A. いいえ、組織は付属書Aに記載されている管理策のみを実施する必要があります。
B. はい、組織は他の情報源からの追加的な管理策を取り入れることができます。

C. はい、ただし、追加の管理措置が既存の附属書Aの管理措置に取って代わる場合に限ります。
正解: **(**正解を表示します**)**

質問: **13**
「ISMSは、XYZ社内で顧客データにアクセスするすべての部門を対象としています。ISMSの目的は、顧客データの機密性、完全性、可用性を確保し、情報セキュリティに関する適用可能な規制要件を遵守することです。」この記述は何を意味しているのでしょうか。
^"説明してください?
A. ISMSの適用範囲における情報システムの境界
B. ISMSの適用範囲の組織的境界
C. ISMSの適用範囲の物理的境界
正解: **(**正解を表示します**)**
この声明では、ISMSの適用範囲の組織的境界について説明しています。これは、組織のどの部分がISMSに含まれるか、または除外されるかを定義するものです。組織的境界は、部門、機能、プロセス、活動、場所などの基準に基づいて設定できます。この場合、声明では、ISMSはXYZ社内で顧客データにアクセスできるすべての部門を対象とし、アクセスできない部門は除外すると明記しています。また、この声明では、ISMSの目的についても説明しています。その目的は、顧客データの機密性、完全性、可用性を確保し、情報セキュリティに関する適用可能な規制要件を遵守することです。
この声明では、ISMSの適用範囲における情報システムの境界、つまりISMSに含まれる情報システムと除外される情報システムを定義する境界については説明されていません。情報システムの境界は、ハードウェア、ソフトウェア、ネットワーク、データベース、アプリケーションなどの基準に基づいて設定できます。また、この声明では、ISMSの対象となる特定の情報システムについても言及されていません。
また、この声明では、ISMSの適用範囲の物理的な境界、つまりISMSの対象となる物理的な場所と対象外となる場所について説明されていません。物理的な境界は、建物、部屋、キャビネット、機器などの基準に基づいて設定できます。声明では、ISMSの対象となる具体的な物理的な場所については一切言及されていません。
参考文献：
* ISO/IEC 27001:2013、4.3項：情報セキュリティマネジメントシステムの適用範囲の決定
* ISO/IEC 27001 リードインプリメンターコース、モジュール4：ISO/IEC 27001に基づくISMSの計画
* ISO/IEC 27001 リードインプリメンターコース、モジュール6：ISO/IEC 27001に基づくISMSの実装
* ISO/IEC 27001 リードインプリメンターコース、モジュール7：ISO/IEC 27001に基づくISMSのパフォーマンス評価、監視、測定
* ISO/IEC 27001 リードインプリメンターコース、モジュール8：ISO/IEC 27001に基づくISMSの継続的改善

* ISO/IEC 27001 リードインプリメンターコース、モジュール9 :ISMS認証監査の準備
* ISO/IEC 27001 適用範囲記述書 | ISMS の適用範囲を設定する方法 - Advisera1
* ISO 27001 スコープステートメントの書き方（3つの例） - Compleye2
* 情報フローマップを使用してISMSの適用範囲を決定する方法3
* ISMS適用範囲文書 - Resolver4
* 範囲と目的を定義する - ISMS Info5

質問: **14**
シナリオ1 :NobleFindは、高級カスタムデザイン家具を専門とするオンライン小売業者です。同社は、住宅および商業顧客のニーズに合わせてカスタマイズされた、幅広い手作りの家具を提供しています。
NobleFindは、専門的なデザインコンサルティングサービスも提供しています。NobleFindはオンラインショッププラットフォームのセキュリティ維持に努めてきましたが、最近のデータ漏洩など、度重なる問題に直面しました。こうした継続的な課題は、通常の業務を阻害し、セキュリティ対策の強化の必要性を浮き彫りにしました。専任のITチームは迅速に対応し、問題を解決しました。これらの問題に対処するため、NobleFindはセキュリティの向上、顧客データの保護、サービスの安定性確保を目的として、ISO/IEC 27001に基づく情報セキュリティマネジメントシステム（ISMS）を導入することを決定しました。
NobleFindは情報セキュリティへの取り組みに加え、製品データの正確性と完全性の維持にも注力しています。これは、バージョン管理を綿密に行い、情報を定期的にチェックし、厳格なアクセスポリシーを適用し、バックアップ手順を実施することで実現しています。さらに、製品の詳細情報や顧客のデザインデータは、多要素認証やデータアクセスポリシーなどのセキュリティ対策により、権限のある担当者のみがアクセスできるようになっています。
NobleFindは、情報セキュリティに対する包括的なアプローチの一環として、ISMS内にインシデント調査プロセスを導入しました。さらに、各製品に関するオンライン情報および顧客情報が、権限のある組織によっていつでも容易にアクセスおよび利用できる状態を維持できるよう、記録保持ポリシーを確立しました。NobleFindは、履歴データの保護に関する明確なガイドラインを提供する情報セキュリティポリシーを策定しました。また、従業員に機密保持契約への署名を義務付け、資格のある人材のみを採用することにも取り組んでいます。加えて、NobleFindは、システムで使用されるリソースの監視、ユーザーアクセス権限の見直し、監査ログの徹底的な分析を実施し、セキュリティ上の異常を迅速に特定して対処するための措置を講じています。
NobleFindは、情報セキュリティマネジメントシステム（ISMS）を導入することで、幅広いデータ、記録、仕様を含む文書化された情報を維持・保護しています。これらの文書化された情報は、顧客データ、履歴記録、財務情報のセキュリティと完全性を確保する上で、同社の事業運営に不可欠です。
上記のシナリオに基づいて、次の質問に答えてください。

NobleFindが経験したサービス中断中に影響を受けた情報セキュリティ原則はどれですか？
A. 機密保持
B. 誠実さ
C. 入手可能性
D. 否認禁止
正解: **(**正解を表示します**)**
NobleFindのサービス中断時に影響を受けた原則は、可用性です。
ISO/IEC 27001:2022によると、情報セキュリティはCIAトライアドとして知られる3つの基本原則に基づいて構築されています。
機密保持：情報へのアクセス権限を持つ者のみが情報にアクセスできるようにすること。
完全性：情報および処理方法の正確性と完全性を確保すること。
可用性：承認されたユーザーが、必要なときに情報および関連資産にアクセスできることを保証する。
サービスの中断は、情報とサービスの可用性に直接影響を与えます。これは、ISO/IEC 27001:2022の附属書A、管理策A.8.14「情報処理設備の冗長性」で明確に示されており、情報と資産が必要なときに確実に利用できるようにすることの重要性が強調されています。さらに、ISO/IEC 27001:2022の条項6.1.2(c)1では、ISMSの範囲内で機密性、完全性、可用性の喪失に関連するリスクを特定する必要性が強調されています。NobleFindが直面したサービス中断のような、通常の運用における障害は、可用性の原則違反に該当します。
参考抜粋：
「情報セキュリティマネジメントシステムの範囲内の情報の機密性、完全性、可用性の喪失に関連するリスクを特定するために、情報セキュリティリスク評価プロセスを適用する...」- ISO/IEC 27001:2022、条項 6.1.2 (c)1。
「可用性：権限のある主体が要求に応じてアクセスおよび使用できる性質」- ISO/IEC 27000:2018、3.7（ISO/IEC 27001:2022、第3項「用語と定義」で参照されている）。
「混乱とは、組織の目標に従って期待される製品やサービスの提供から、計画外のマイナスの逸脱を引き起こす事象である。」- ISO/IEC 27002:2022、3.1.9 混乱。
顧客のアクセスや企業の業務に影響を与えるサービスの中断は、可用性インシデントの典型的な例である。
参考文献：
ISO/IEC 27001:2022、6.1.2(c)1項
ISO/IEC 27001:2022、第3項 用語及び定義
ISO/IEC 27002:2022、3.1.9 中断
ISO/IEC 27000:2018（用語はISO/IEC 27001:2022で参照されている）

質問: **15**
シナリオ：

ある製造会社は、サプライチェーンの混乱の可能性により、生産遅延のリスクに直面していた。同社は潜在的な影響を評価した結果、混乱が業務に大きな影響を与える可能性は低いと判断した。そして、リスクを受け入れることを決定した。
質問：
このケースにおいて、会社はどのリスク対策を選択したのでしょうか？
A. リスク回避
B. リスク保持
C. リスク回避
正解: **B** (コメントを発表する)
ISO/IEC 27001:2022 6.1.3 (a) 項によれば、組織は適切なリスク処理オプションを決定しなければならない。ISO 27005:2022 (8.2.2 項) では、リスク保持を次のように定義している。『リスクを軽減するための対策を講じることなくリスクを受け入れるという決定。多くの場合、リスク軽減のコストが利益を上回るためである。』同社はリスクの発生可能性と影響を評価し、リスク軽減を行わないことを決定した。これはリスク保持（ISO 27001 6.1.3(f) 項ではリスク受容とも呼ばれる）に該当する。
参考文献：
ISO/IEC 27001:2022 条項 6.1.3 (f)
ISO/IEC 27005:2022 条項 8.2.2 - リスク処理オプション

質問: **16**
情報セキュリティポリシーにおいて、以下の選択肢のうちどれを取り上げるべきでしょうか？
A. 情報セキュリティインシデント発生後に実施すべき措置
B. 組織に課せられた法的および規制上の義務
C. 情報セキュリティプロセスの複雑性とそれらの相互作用
正解: (正解を表示します)
ISO/IEC 27001:2022規格によれば、情報セキュリティポリシーとは、組織内の情報セキュリティに関する管理手法と目標を定義する高レベルの文書です。これには、情報セキュリティに関連する法律、契約、協定、規格の遵守など、組織に課せられる法的および規制上の義務が含まれるべきです。また、情報セキュリティポリシーは、情報セキュリティマネジメントシステム（ISMS）の確立、導入、維持、および継続的な改善の基礎となるものでなければなりません。
参照：
ISO/IEC 27001:2022、第5.2項 方針
ISO/IEC 27002:2022、第5.1項 情報セキュリティに関する方針
PECB ISO/IEC 27001 リードインプリメンターコース、モジュール3：情報セキュリティマネジメントシステム（ISMS）

質問: **17**
質問：
セキュリティ監査中に、アナリストは、攻撃者がブラックボックス型の機械学習モデルに繰り返しクエリを実行し、特定のデータポイントがトレーニングセットに含まれているかどうかを推測していたことを発見しました。攻撃者は、トレーニング中に個人のデータが使用されたかどうかを判断できた可能性があります。この攻撃はどのような脅威に該当するでしょうか？
A. トレーニングセット内のバックドア
B. データポイズニング
C. メンバーシップ推論攻撃
正解: **(**正解を表示します**)**
ISO/IEC 23894:2023（人工知能リスク管理）およびNIST SP 800-207Aは、メンバーシップ推論攻撃（MIA）を次のように定義しています。
「攻撃者が、特定のデータが機械学習モデルのトレーニング段階で使用されたかどうかを判断しようとする。」これはプライバシーの脅威であり、特に個人情報（PII）に関しては、データ漏洩につながる可能性があります。
これは、トレーニングプロセスを操作するデータポイズニングや、意図的に動作を変更するバックドアとは異なります。
参考文献：
ISO/IEC 23894:2023 条項 8.2 - 機械学習の脅威
ISO/IEC 27001:2022 - 管理策 A.8.10 および A.8.12 (データ保護、漏洩防止)

質問: **18**
シナリオ 9: OpenTech は IT および通信サービスを提供しています。データ通信企業やネットワーク事業者がマルチサービスプロバイダーになるのを支援しています。内部監査中に、内部監査員の Tim は監視手順に関連する不適合を特定しました。彼はいくつかのシステム脆弱性を特定し、評価しました。
ティムは、機密情報を処理するシステムやサービスのユーザーIDが再利用されており、アクセス制御ポリシーが遵守されていないことを発見しました。この不適合の根本原因を分析した後、ISMSプロジェクトマネージャーは、不適合を解決するための可能なアクションのリストを作成しました。次に、ISMSプロジェクトマネージャーはそのリストを分析し、

根本原因の排除と将来同様の状況の防止を可能にする活動を選択しました。これらの活動はアクションプランに含まれました。経営陣によって承認されたアクションプランは、次のように記述されています。
アクセス制御ポリシーの新しいバージョンが策定され、情報通信技術（ICT）部門によるネットワークアクセスの効果的な管理と監視を確実にするための新しい制限が設けられます。承認された行動計画が実施され、計画に記載されているすべての行動が文書化されました。
このシナリオに基づいて、次の質問に答えてください。
OpenTech社は、アクセス制御ポリシーの新しいバージョンを策定することを決定しました。このような変更が発生した場合、同社はどのような対応を取るべきでしょうか？
A. 監視すべき変化要因を特定する
B. 情報セキュリティ目標を更新する
C. 変更内容をスコープに含める
正解: **(**正解を表示します**)**
ISO/IEC 27001:2022の6.2項によれば、組織は関連する機能およびレベルで情報セキュリティ目標を設定しなければならない。情報セキュリティ目標は、情報セキュリティポリシーと整合し、情報セキュリティリスクに関連するものでなければならない。組織は、変更が生じた場合、情報セキュリティ目標を更新しなければならない。したがって、OpenTechがアクセス制御ポリシーの新しいバージョンを設定することを決定した場合、変更を反映し、ポリシーとの整合性を確保するために、情報セキュリティ目標を適切に更新する必要がある。
ISO/IEC 27001:2022、6.2項 ;PECB ISO/IEC 27001 リードインプリメンターコース、モジュール10、スライド8。

質問: **19**
シナリオ10 :NetworkFuse社は、ネットワークハードウェアの開発、製造、販売を行っています。同社は、ISO/IEC 27001の要件に基づく運用情報セキュリティ管理システム（ISMS）と、ISO 9001に基づく品質管理システム（QMS）を約2年間運用してきました。最近、ISO/IEC 27001とISO 9001の両方の認証を取得するために、統合認証監査を申請しました。
認証機関を選定した後、NetworkFuse は監査に向けて従業員を準備しました。同社は、経営陣によれば必要ないということで、監査前に自己評価を実施しないことを決定しました。さらに、内部監査レポートや経営陣のレビュー、導入済みのテクノロジー、ISMS および QMS の一般的な運用など、文書化された情報が利用可能であることを確認しました。しかし、同社は認証機関に対し、文書を社外に持ち出せないように要求しました。しかし、NetworkFuse が割り当てられた監査チームリーダーを拒否し、その交代を要求したため、監査は予定された日数内には実施されませんでした。同社は、同じ監査チームリーダーが主要な競合他社に認証の推奨を発行しており、これは同社の経営陣にとって潜在的な利益相反であると主張しました。認証機関はこの要求を受け入れませんでした。シナリオ 10

に基づくと、NetworkFuse は監査前に ISMS の自己評価を実施しませんでした。これは ISO/IEC 27001 に準拠していますか?
A. はい、基準では監査前に自己評価を実施することは義務付けられていませんが、実施することは良い慣行です。
B. はい、規格では、被監査者は認証監査の準備にあたり、内部監査報告書と経営レビュー報告書のみに依拠しなければならないと規定されています。
C. いいえ、被監査者は認証監査を実施する前に、第4項から第10項までの要件を確認する必要があります。
正解: **(**正解を表示します**)**

質問: **20**
シナリオ5に基づき、OperazeはISMSの円滑な運用を確保するために、どの委員会を設置すべきでしょうか？
A. 運営委員会
B. 運営委員会
C. 情報セキュリティ委員会
正解: **(**正解を表示します**)**

質問: **21**
セキュリティインシデントの影響を推定する際に考慮すべき要素はどれですか？
A. 確率
B. 結果の深刻度
C. イベントの期間
正解: **(**正解を表示します**)**
セキュリティインシデントの影響を評価する際には、その影響の深刻度を考慮することが極めて重要です。これはISO/IEC 27005にも明記されており、影響とはリスクインシデントの影響または深刻度を指すとされています。
結果：目標に影響を与える出来事の結果。影響の深刻度を含む。」
- ISO/IEC 27005:2022、セクション8.3.2

質問: **22**
シナリオ 7: モナコに本社を置く保険会社 Yefund は、商業、産業、企業サービスにおいて信頼できる企業です。数十年にわたる豊かな歴史を持つ Yefund は、あらゆる規模の企業に合わせた保険ソリューションを一貫して提供し、資産を保護し、リスクを軽減してきました。先進的な企業として Yefund は、機密データを保護し、顧客からの信頼を維持する上で情報セキュリティが重要であることを認識しています。そのため、ISO/IEC 27001-iS に基づく ISMS の実装に向けた変革の旅に着手し、最先端の AI 技術を ISMS に導入して、情報資産の識別と管理を改善しています。AI を通じて、資産の識別を自動化し、時間の経過に伴う変化を追跡し、資産の機密性と露出に基づいて戦略的に制御を選択します。この積極的なアプローチにより、Yefund は、新たな脅威から重要な情報資産を保護する上で、俊敏性と適

応性を維持します。Yetundはセキュリティ体制の強化が喫緊の課題であることを認識していましたが、導入チームはISMSの各要素を段階的に統合するアプローチを採用しました。正式なローンチを待つのではなく、セキュリティ対策を慎重にテストおよび検証し、各要素が完成・承認されるにつれて徐々に運用モードに移行していきました。この体系的なプロセスにより、暗号化プロトコル、アクセス制御、監視システムなどの重要なセキュリティ対策が完全に機能し、個人情報、ポリシー、財務情報を含む顧客情報を効果的に保護することが保証されました。
最近、Vefundの情報セキュリティチームのメンバーであるKianが2つのセキュリティイベントを特定しました。評価の結果、報告された1つのインシデントは、インシデントとして分類される基準を満たしていませんでした。しかし、2つ目のインシデントは、重要なネットワークコンポーネントのダウンタイムに関係しており、機密データのセキュリティに対する潜在的なリスクについて懸念が生じたため、インシデントとして分類されました。最初のイベントは、それ以上の措置を講じることなくレポートとして記録されましたが、2つ目のインシデントは、調査、封じ込め、根絶、復旧、解決、クローズ、インシデント報告、およびインシデント後の活動を含む一連の措置を促しました。さらに、イベントの分類に従ってイベントに対処するために、IRTSが設立されました。
この事件の後、YetundはISMSフレームワークを改善するための唯一の必要性として、内部コミュニケーションプロトコルの開発を認識しました。Yetundは、何を、いつ、誰と、どのように効果的にコミュニケーションするかといったコミュニケーションの側面が重要であると判断しました。Yetundは、顧客や規制機関など、安全かつタイムリーなコミュニケーションを必要とする外部の利害関係者がいるにもかかわらず、内部コミュニケーションプロトコルの開発に注力することを決定しました。これは、内部調整が最優先事項であるという理由からです。
さらに、Yefund は包括的なトレーニング プログラムを通じて従業員の専門能力開発を優先しており、Yefund は Kirkpatrick の 4 段階のトレーニング評価モデルを使用してトレーニング イニシアチブの有効性と影響を評価しています。トレーニングへの参加と印象の測定 (レベル 1) から、学習成果 (レベル 2)、トレーニング後の行動 (レベル 3)、および具体的な結果 (レベル 4) の評価まで、Yefund はトレーニング プログラムが包括的で、影響力があり、組織目標と整合していることを保証します。
YefundがISMS（情報セキュリティマネジメントシステム）の導入に向けて歩んできた道のりは、セキュリティ、イノベーション、そして継続的な改善への強いコミットメントを反映しています。テクノロジーを活用し、積極的な警戒心を持つ文化を醸成し、コミュニケーションプロセスを強化し、従業員の能力開発に投資することで、Yefundは顧客とステークホルダーの利益を守る信頼できるパートナーとしての地位を確固たるものにすることを目指しています。
シナリオ7に基づくと、YefundによるISMS要素の統合は許容範囲内と言えるでしょうか？
A. いいえ、すべての要素が完成するまで運用モードを一時的に延期することをお勧めします。
B. はい、ISMSの要素は段階的に完成、承認され、運用モードに移行できます。

C. いいえ、ISMS要素を活性化してその有効性を評価し、運用モードでのパフォーマンスに基づいて完了および承認する必要があります。
正解: (正解を表示します)
ISO/IEC 27001:2022では、ISMSのすべての構成要素を一度に導入する必要はありません。各ISMS要素が検証、承認され、準備が整った時点で運用開始される段階的な導入は、有効性とリスク軽減を確保するための最良の方法とみなされ、完全に受け入れられています。
「ISMSの構成要素を段階的に実装および検証し、完了および承認された各構成要素を運用モードに移行させることは許容される。ただし、最終的にシステム全体が要件を満たすことが条件となる。」
- ISO/IEC 27003:2017、8.5項 ;ISO/IEC 27001:2022、4.4項

質問: **23**
シナリオ4 :TradeBは、市場に参入したばかりの商業銀行で、顧客から預金を受け入れ、基本的な金融サービスと投資ローンを提供しています。TradeBは、ISO/IEC 27001に基づく情報セキュリティマネジメントシステム（ISMS）を導入することを決定しました。マネジメントの経験がないTradeBは、
[^システム実装、TradeBの経営陣はISMS実装プロジェクトを指揮・管理するために2人の専門家と契約しました。
まず、プロジェクトチームはISO/IEC 27001附属書Aの93の管理策を分析し、会社とその目的に適用可能と判断されたセキュリティ管理策のみをリストアップしました。この分析に基づいて、適用性に関する声明書を作成しました。その後、リスク評価を実施し、ハードウェア、ソフトウェア、ネットワークなどの資産、脅威、脆弱性を特定し、潜在的な結果と発生可能性を評価し、3つの非数値カテゴリ（低、中、高）に基づいてリスクレベルを決定しました。彼らはリスク評価基準に基づいてリスクを評価し、高リスクカテゴリのみを扱うことに決定しました。また、アクセス制御ポリシーの新しいバージョンを確立し、ユーザーアクセスを管理および制御するための制御を実装し、事業継続のためのICT準備のための制御を実装することにより、管理者権限の不正使用と複数のハードウェア障害によるシステムの中断に主に焦点を当てることも決定しました。最後に、彼らはリスク評価レポートを作成し、これらのセキュリティ制御の実装後にリスクレベルが許容レベルを下回る場合は、リスクを受け入れると記述しました。残存リスクに対処するために、TradeBは何をすべきでしょうか。シナリオ4を参照してください。
A. TradeBは、リスク処理後のリスク軽減の価値を評価、計算、文書化する必要があります。
B. TradeBは、すべての残存リスクに対処するため、直ちに新たな管理策を実施すべきである。
C. TradeBは、許容レベルを超える残存リスクのみを受け入れるべきである。
正解: (正解を表示します)
ISO/IEC 27001:2022の主たる実施者によると、残留リスクとは、リスク処理後に残るリスクのことである。

残存リスクは、組織が許容できるリスクレベルである許容リスクレベルと比較する必要があります。残存リスクが許容リスクレベルを下回る場合は、リスクを受け入れることができます。残存リスクが許容リスクレベルを上回る場合は、追加のリスク対策を検討する必要があります。したがって、TradeBは、リスク対策後のリスク低減額（初期リスクと残存リスクの差）を評価、計算、文書化する必要があります。これにより、TradeBはリスク対策が効果的であったかどうか、また残存リスクが許容範囲内であるかどうかを判断することができます。
参考文献：
* ISO/IEC 27001 : 2022 リードインプリメンター学習ガイドおよび文書、セクション 8.3.2 リスク処理
* ISO/IEC 27001 : 2022 リードインプリメンター情報キット、14ページ、リスク管理プロセス

質問: **24**
シナリオ6 :グリーンウェーブ
持続可能でエネルギー効率の高い家庭用電化製品の製造業者である GreenWave は、太陽光発電機器、EV 充電器、スマートサーモスタットを専門としています。顧客データと社内業務をデジタル脅威から保護するために、同社は ISO/IEC 27001 に基づく情報セキュリティ管理システム (ISMS) を導入しました。GreenWave はまた、建物のエネルギー効率をさらに向上させるための革新的な IoT ソリューションも検討しています。GreenWave は、業務内で高い水準の情報セキュリティを維持することに尽力しています。継続的改善アプローチの一環として、同社は ISMS を管理するために必要な能力レベルを決定するプロセスを進めています。GreenWave は、これらの能力要件を定義する際に、技術の進歩、規制要件、会社の使命、戦略目標、利用可能なリソース、顧客のニーズと期待など、さまざまな要素を考慮しました。さらに、同社は ISO/IEC 27001 のコミュニケーション要件を遵守することに引き続き尽力しています。ISMS に関連する社内外のコミュニケーションについて明確なガイドラインを確立し、共有する情報、共有するタイミング、共有相手、およびチャネルを定義しました。しかし、すべてのコミュニケーションが正式に文書化されたわけではなく、同社はニーズに基づいてコミュニケーションを分類・管理し、ISMSの有効性に必要な範囲でのみ文書が維持されるようにした。
GreenWaveは、顧客の嗜好を理解し、電子製品に関するパーソナライズされた推奨を提供するために、AIソリューションの導入を検討してきました。その目的は、AI技術を活用して問題解決能力を高め、顧客に提案を行うことでした。この戦略的取り組みは、データに基づいた洞察を通じて顧客体験を向上させるというGreenWaveのコミットメントに合致するものでした。
さらに、GreenWave は、特定のサービスを内部の安全なインフラストラクチャでホストし、他のサービスを外部の拡張可能なプラットフォームでホストしてどこからでもアクセスできるようにする柔軟なクラウド インフラストラクチャを探していました。この構成により、さまざまな展開オプションが可能になり、GreenWave の電子製品開発に不可欠な情

報セキュリティが強化されます。GreenWave によると、ISMS 実装計画に追加の制御を導入することは成功裏に実行され、同社は運用モードに移行する準備ができていました。GreenWave は、社内でこの変更の重要性を判断する責任を Colin に割り当てました。
質問：
GreenWaveは、自社のISMSを支えるために必要な能力レベルを適切に判断したか？
A. はい、GreenWaveは自社の事業運営にとって最も重要な内部要因のみを考慮したからです。
B. いいえ。GreenWaveはISMSに関連する外部要因を考慮していないためです。
C. はい。GreenWaveは外部の問題、内部要因、そして関係する利害関係者のニーズと期待を考慮したからです。
正解: **C (**コメントを発表する**)**
ISO/IEC 27001:2022 条項 7.2 - 能力国家:
「組織は、内部および外部の問題、ならびにISMSに関連する利害関係者のニーズと期待を考慮して、必要な人材の能力を決定しなければならない。」GreenWaveはこの条項に従い、規制要件や顧客要件を含む内部および外部の影響の両方を考慮に入れました。この包括的な視点により、担当者がISMS機能を適切に管理するための十分な能力を備えていることが保証されます。

質問: **25**
シナリオ3 :Socket Inc.は、高品質で安全な通信ソリューションの提供に尽力する、ワイヤレス製品とサービスを専門とするダイナミックな通信会社です。Socket Inc.は、高い可用性、拡張性、柔軟性で知られるMongoDBデータベースをはじめとする革新的なテクノロジーを活用し、信頼性が高く、アクセスしやすく、効率的で、整理されたサービスを顧客に提供しています。最近、同社はセキュリティ侵害に直面しました。設定の不備が適切に対処されていなかったため、外部のハッカーがMongoDBデータベースのデフォルト設定を悪用したのです。
幸いにも、入念なデータバックアップとサーバーを介した集中ログ記録のおかげで、情報の損失は発生しませんでした。この事件を受けて、Socket Inc.はセキュリティ対策の徹底的な評価を実施しました。同社は情報セキュリティの改善が喫緊の課題であると認識し、ISO/IEC 27001に基づいた情報セキュリティマネジメントシステム（ISMS）を導入することを決定しました。
データセキュリティの向上とリソースの保護のため、Socket Inc. は入退室管理と安全なアクセスポイントを導入しました。これらの対策は、機密データや重要な資産を保管する重要エリアへの不正アクセスを防止するために設計されています。関連法規、規制、倫理基準を遵守し、Socket Inc. はこれらの対策を実施しました。
事業ニーズ、情報分類、および関連リスクに合わせて調整された、採用前の身元調査を実施した。また、方針違反に対処するための正式な懲戒手続きも確立した。
さらに、組織の敷地外でアクセス、処理、または保存される情報を保護するために、リモートワークを行う従業員向けにセキュリティ対策が実施されました。

ソケット社は、停電やその他の障害から情報処理施設を保護した。
外部ソースからの重要な記録への不正アクセスにより、部門間および外部ネットワーク間の不正アクセスを防止するためのデータフロー制御サービスが導入されました。さらに、Socket Inc.
組織のアクセス制御に関するトピックレベルの一般方針およびその他の関連するトピックレベルの一般方針と業務要件に基づき、適用法令を考慮したデータマスキングを実施しました。また、情報処理施設のすべての運用手順を更新および文書化し、それらが経営幹部のみにアクセス可能であることを保証しました。
同社はまた、データベースを不正アクセスから保護するため、暗号鍵管理を含む暗号化技術の効果的な利用に関する規則を定義・実施する管理体制を構築した。この導入は、関連するすべての協定、法令、規制、および情報分類体系に基づいている。セキュリティの向上と管理業務の軽減のため、VPNを用いたネットワーク分離が提案された。
Socket Inc.は、セキュリティ対策の設計と説明に関して、それらをグループ分けし、すべての対策を単一の文書に統合しました。さらに、情報セキュリティ上の脅威に関する情報を維持、収集、分析し、情報セキュリティをプロジェクト管理に統合するための新しいシステムを導入しました。
上記のシナリオに基づいて、次の質問に答えてください。
Socket Inc. は、採用前の身元調査を実施することで、以下のどの管理策を実施しましたか？シナリオ 3 を参照してください。
A. 付録A 6.1 スクリーニング
B. 付録A 6.7 リモートワーク
C. 付属書A 6.4 懲戒手続き
正解: **A** (コメントを発表する)

質問: **26**
ある組織は、全従業員を対象に情報セキュリティに関する意識向上と研修を毎月実施することを決定しました。これらの研修に参加した従業員のうち、試験に合格できたのはわずか45%でした。この割合は何を意味するのでしょうか？
A. 測定対象
B. パフォーマンス指標
C. 属性
正解: (正解を表示します)

質問: **27**
シナリオ 3: スウェーデンで設立され、スウェーデンに本社を置くスウェーデンの自動車メーカーである Auto Tsaab は、自動車業界における革新性でよく知られています。この高い評判にもかかわらず、同社は文書化された情報の管理においてかなりの課題に直面しています。

過去にはこの情報の取り扱いに手動の方法でも十分だったかもしれませんが、現在では効率性、正確性、拡張性において大きな課題が生じています。さらに、文書化された情報の管理責任を1人の個人に委ねると、組織の情報管理システム内に潜在的な単一障害点が生じるという重大な脆弱性が生じます。これらの課題に対処し、情報資産の保護に対する取り組みを強化するために、Auto TsaabはISO/IEC 27001に準拠した情報セキュリティ管理システム（ISMS）を導入しました。この措置は、特に手動から自動化された情報管理方法への移行に伴い、会社の情報のセキュリティ、機密性、完全性を確保する上で非常に重要でした。当初、Auto Tsaabはデータの破損を検出し修正する自動チェックシステムを構築しました。これらの自動チェックを導入することで、Auto Tsaabはデータの正確性と一貫性を維持する能力を向上させただけでなく、検出されないエラーのリスクも大幅に低減しました。
Auto ISMS の中心は文書化されたプロセスです。ISMS の範囲、情報セキュリティ ポリシー、運用計画と管理、情報セキュリティ リスク評価、内部監査、および管理レビューなどの重要な側面とプロセスを文書化することにより、Auto Tsaab はこれらの文書がすぐに利用可能で適切に保護されていることを保証しました。さらに、Auto Tsaab は、製品、サービス、ハードウェア、およびソフトウェアにわたる 36 の異なるカテゴリを組み込んだ包括的なフレームワークを使用しています。このフレームワークは、6 行と 6 列の 2 次元マトリックスに整理されており、小型自動車のコンポーネントとアセンブリの技術的な詳細の仕様を容易にします。業界標準を維持するために、同社の革新と品質への取り組みを強調し、Auto Tsaab は人材の選定において厳格なプロトコルに従っています。
チームメンバー全員が適格であるだけでなく、組織内でのそれぞれの役割に十分適していることを保証する。さらに、同社はポリシー違反に対処するための正式な手順を確立し、文書化とセキュリティ対策を継続的に強化するために社内コンサルタントを任命した。
Auto Tsaab社のポリシー違反への対処および懲戒手続きの実施方法は、ISO/IEC 27001に準拠していますか？シナリオ3を参照してください。
A. はい、管理はISO/IEC 27001に従って定義されています。
B. いいえ、この管理は社内のリモートワーク体制に関する責任を明確にするためだけに実施されるべきです。
C. いいえ、制御は通信プロトコルを確立するために実施されるべきです
正解: **(**正解を表示します**)**
Auto Tsaabは「ポリシー違反に対処するための正式な手順を確立した」。これは、セキュリティポリシー違反に対する懲戒処分を規定する付属書A 6.4「懲戒手続き」に合致する。
「情報セキュリティ侵害を犯した従業員に対して措置を講じるための、正式かつ周知徹底された懲戒手続きを設けるべきだ。」
- ISO/IEC 27001:2022、附属書A、管理6.4 懲戒プロセス

質問: **28**
シナリオ6 :Skyver社は、ゲーム機、薄型テレビ、コンピューター、プリンターなどの電子製品を世界中に配送しています。情報セキュリティを確保するため、同社はISO/IEC 27001の

要件に基づいた情報セキュリティマネジメントシステム（ISMS）を導入することを決定しました。
社内で最も優秀な情報セキュリティ専門家であるコリンは、情報セキュリティ上の課題やその他の情報セキュリティ関連の対策について、社員を対象とした研修会を開催することを決定した。研修会では、Skyverの情報セキュリティへの取り組み方や、フィッシングやマルウェア対策の手法などが取り上げられた。
セッションの参加者の 1 人は、人事部に勤務する Lisa です。Colin は Skyver の既存の情報セキュリティ ポリシーと手順を正直かつ公平に説明していますが、彼女は議論されている問題の一部が技術的すぎると感じ、セッションを完全に理解していません。そのため、多くの場合、彼女はトレーナーや同僚に追加の支援を求めます。シナリオ 6 に基づくと、Lisa はトレーニングと意識向上セッションで議論されている問題の一部が技術的すぎると感じ、セッションを完全に理解していません。これは何を示していますか?
A. リサは必要な能力を習得するための行動をとらなかった
B. 研修および啓発セッションの効果は評価されなかった。
C. Skyverは、チームが行う活動や意図する結果に応じて、異なるチームのニーズを判断しませんでした。
正解: **(**正解を表示します**)**
ISO/IEC 27001:2022 リードインプリメンタートレーニングコースガイド1によると、ISO/IEC 27001の要求事項の1つは、組織の管理下で業務を行うすべての人が、情報セキュリティポリシー、ISMSの有効性への貢献、ISMSの要求事項に適合しない場合の影響、および情報セキュリティパフォーマンスの向上によるメリットを認識していることを保証することです。これを実現するために、組織は、情報セキュリティパフォーマンスに影響を与える管理下で業務を行う人の必要な能力を決定し、必要な能力を習得するためのトレーニングを提供するか、その他の措置を講じ、講じた措置の有効性を評価し、能力の証拠として適切な文書化された情報を保持する必要があります。また、組織は、チームが行う活動と意図する結果に応じて、チームのニーズの違いを決定し、それらのニーズを満たすための適切なトレーニングおよび啓発プログラムを提供する必要があります。
したがって、このシナリオは、Skyverが各チームの活動内容や期待される成果に応じて、チームごとのニーズを把握していなかったことを示しています。人事部に勤務するリサは、研修・啓発セッションで議論された内容の一部が専門的すぎると感じ、セッションの内容を十分に理解できなかったからです。これは、セッションが人事担当者の具体的なニーズや役割に合わせて調整されておらず、情報セキュリティ専門家が、彼らが効果的かつ安全に業務を遂行するために必要な技術的な知識やスキルレベルを考慮していなかったことを示唆しています。
参照：
ISO/IEC 27001:2022 リードインプリメンタートレーニングコースガイド1
ISO/IEC 27001:2022 リードインプリメンター情報キット2

質問: **29**

質問：
ISO/IEC 27002:2022 条項 8.28 の目的は何ですか？
A. 情報セキュリティの脆弱性を低減するために、ソフトウェアが安全に記述されていることを確認する。
B. アプリケーション開発中にすべてのセキュリティ要件が満たされるようにするため
C. 安全なシステム設計原則が遵守されていることを確認する
正解: **(**正解を表示します**)**

質問: **30**
シナリオ 3: スウェーデンで設立され、スウェーデンに本社を置くスウェーデンの自動車メーカーである Auto Tsaab は、自動車業界における革新性でよく知られています。この高い評判にもかかわらず、同社は文書化された情報の管理においてかなりの課題に直面しています。
過去にはこの情報の取り扱いに手動の方法でも十分だったかもしれませんが、現在では効率性、正確性、拡張性において大きな課題が生じています。さらに、文書化された情報の管理責任を1人の個人に委ねると、組織の情報管理システム内に潜在的な単一障害点が生じるという重大な脆弱性が生じます。これらの課題に対処し、情報資産の保護に対する取り組みを強化するために、Auto TsaabはISO/IEC 27001に準拠した情報セキュリティ管理システム（ISMS）を導入しました。この措置は、特に手動から自動化された情報管理方法への移行に伴い、会社の情報のセキュリティ、機密性、完全性を確保する上で非常に重要でした。
当初、Auto Tsaabはデータの破損を検出し修正する自動チェックシステムを構築しました。これらの自動チェックを導入することで、Auto Tsaabはデータの正確性と一貫性を維持する能力を向上させただけでなく、検出されないエラーのリスクも大幅に低減しました。
Auto ISMS の中心は文書化されたプロセスです。ISMS の範囲、情報セキュリティ ポリシー、運用計画と管理、情報セキュリティ リスク評価、内部監査、および管理レビューなどの重要な側面とプロセスを文書化することにより、Auto Tsaab はこれらの文書がすぐに利用可能で適切に保護されていることを保証しました。さらに、Auto Tsaab は、製品、サービス、ハードウェア、およびソフトウェアにわたる 36 の異なるカテゴリを組み込んだ包括的なフレームワークを使用しています。このフレームワークは、6 行と 6 列の 2 次元マトリックスに整理されており、小型自動車のコンポーネントとアセンブリの技術的な詳細の仕様を容易にします。業界標準を維持するために、同社の革新と品質への取り組みを強調し、Auto Tsaab は人材の選定において厳格なプロトコルに従っています。
チームメンバー全員が適格であるだけでなく、組織内でのそれぞれの役割に十分適していることを保証する。さらに、同社はポリシー違反に対処するための正式な手順を確立し、文書化とセキュリティ対策を継続的に強化するために社内コンサルタントを任命した。
ISO/IEC 27001への準拠を約束した後、Auto Tsaabの情報セキュリティ管理システムに文書化された情報は、同規格に準拠して管理されていましたか？
A. はい、その会社は文書化された情報の管理に手作業のみに頼っていました。

B. はい、会社は文書化された情報が必要に応じて利用可能で保護されていることを確認しました。
C. はい、会社は文書化された情報の管理責任を1人の担当者に委任しました。
正解: (正解を表示します)
このシナリオでは、 Auto Tsaab社は、これらの文書が容易に入手可能であり、適切に保護されていることを保証した」と述べられています。これは、文書化された情報が利用可能であり、使用に適しており、適切に保護されていることを要求しているISO/IEC 27001:2022の7.5項と完全に一致しています。
「ISMSおよび本国際規格で要求される文書化された情報は、必要な場所および必要な時に利用可能かつ適切に使用できるように管理され、かつ適切に保護されなければならない。」 - ISO/IEC 27001:2022、7.5項

質問: **31**
シナリオ10によると、NetworkFuseは認証機関に対し、すべての文書を現地でのみ審査するよう要請しました。これは許容範囲内でしょうか？
A. はい、監査チームが正式に機密保持契約に署名した場合に限ります。
B. いいえ、認証機関が文書審査をオンサイトで行うかオフサイトで行うかを決定します。
C. はい、被監査者は文書レビューを現地で行うよう要求することができます。
正解: (正解を表示します)

質問: **32**
シナリオ8 :SunDeeは、米国カリフォルニア州に本社を置くアメリカのバイオ医薬品会社です。心血管疾患、腫瘍学、骨の健康、炎症に焦点を当てた新規ヒト治療薬の開発を専門としています。同社は過去2年間、ISO/IEC 27001に基づく情報セキュリティマネジメントシステム（ISMS）を導入してきました。しかし、ISMSのパフォーマンスと有効性を監視または測定しておらず、定期的な経営陣によるレビューも実施していませんでした。再認証監査の直前に、同社は内部監査を実施することを決定しました。また、ほとんどの従業員に、過去2年間の各部門の個人報告書をまとめるよう依頼しました。これにより、生産部門は部門の労働力が最適よりも少なくなり、会社の在庫が減少しました。

テッサはサンディーの内部監査員でした。50人の異なる従業員によって複数のレポートが作成されたため、内部監査プロセスは計画よりもはるかに時間がかかり、非常に一貫性がなく、定性的な尺度がまったくありませんでした。テッサは、サンディーがISMSのパフォーマンスを適切に評価する必要があると結論付けました。彼女は、サンディーのISMSパフォーマンス評価の怠慢を重大な不適合と定義し、不適合の説明、監査結果、および推奨事項を含む不適合レポートを作成しました。さらに、テッサはサンディーがこれらの問題を解決できるようにする新しい計画を作成し、それを経営陣に提示しました。シナリオ8に基づいて、不適合レポートには必要なすべての側面が含まれていましたか?
A. はい、報告書には必要な事項がすべて含まれていました。
B. いいえ、報告書には不適合の根本原因も明記する必要があります。
C. いいえ、報告書には監査基準も明記する必要があります。
正解**: B (**コメントを発表する**)**
ISO/IEC 27001:2022によると、不適合報告書とは、監査中に特定された監査基準からの逸脱の詳細を記録した文書である2。監査基準とは、監査証拠と比較するための参照として使用される一連の方針、手順、要求事項、または仕様のことである3。したがって、不適合報告書には以下の側面を含める必要がある。
不適合の説明には、逸脱の内容、発生場所、検出された日時を明確に記載する必要があります。監査結果には、不適合の特定を裏付ける客観的な証拠を提供する必要があります。監査基準には、不適合が逸脱している参照文書または規格を指定する必要があります。推奨事項には、不適合に対処するために講じることができる是正措置または改善策を提案する必要があります。シナリオ 8 では、テッサの不適合報告書には、不適合の説明、監査結果、推奨事項が含まれていましたが、監査基準が指定されていませんでした。そのため、報告書には必要なすべての側面が含まれておらず、不完全でした。
1 :ISO/IEC 27001:2022、9.2.3項
2 :ISO/IEC 27001:2022、条項3.23
3 :ISO/IEC 27001:2022、3.5項
ISO/IEC 27001:2022、附属書A.9.2.3

質問**: 33**
シナリオ 1: HealthGenic は、ウェブベースの医療ソフトウェアを使用して乳幼児から成人初期までの個人の健康と成長をモニタリングする小児科クリニックです。このソフトウェアは、予約のスケジュール設定、カスタマイズされた医療レポートの作成、患者のデータと病歴の保存、およびすべての関係者とのコミュニケーションにも使用されます。
[^両親、他の医師、医療検査技師を含む関係者。
先月、HealthGenicはソフトウェアにアクセスするユーザー数の増加により、何度かサービスの中断に見舞われた。同社がソフトウェアを使用する際に直面したもう一つの問題は、複雑なユーザーインターフェースであり、訓練を受けていない従業員にとっては使いこなすのが難しいと感じられた。

HealthGenicの経営陣は、この問題について直ちにソフトウェア開発会社に報告した。ソフトウェア会社は問題を修正したが、その過程でHealthGenicの患者に関する機密情報を含む一部のファイルを改変してしまった。その結果、医療報告書が不完全かつ不正確になり、さらに重要なことに、患者のプライバシーが侵害された。
シナリオ1で説明されている状況のうち、HealthGenicにとって脅威となるのはどれですか？
A. HealthGenicは従業員にソフトウェアの使用方法に関するトレーニングを実施していませんでした。
B. ソフトウェア会社がHealthGenicの患者に関する情報を改ざんした
C. HealthGenicは、患者の機密情報を保管するためにウェブベースの医療ソフトウェアを使用していた。
正解: **(**正解を表示します**)**
説明
ISO/IEC 27001:2022によると、脅威とは、資産の機密性、完全性、または可用性に悪影響を及ぼす可能性のあるあらゆる事象を指します。このシナリオでは、資産とは、ウェブベースの医療ソフトウェアによって保存および処理されるHealthGenicの患者に関する情報です。ソフトウェア会社がHealthGenicの患者に関する機密情報を含む一部のファイルを改変したことは、不完全かつ不正確な医療レポートの作成や患者のプライバシー侵害につながり、資産の機密性と完全性に悪影響を及ぼす可能性のある事象です。したがって、この状況はHealthGenicにとって脅威となります。
参考文献：
ISO/IEC 27001:2022 - 情報セキュリティ、サイバーセキュリティおよびプライバシー保護 - 情報セキュリティマネジメントシステム - 要求事項 ISO 27001 主要用語 - PJR

質問: **34**
シナリオ 9: OpenTech は IT および通信サービスを提供しています。データ通信企業やネットワーク事業者がマルチサービスプロバイダーになるのを支援しています。内部監査中に、内部監査員の Tim は監視手順に関連する不適合を特定しました。彼はいくつかのシステム脆弱性を特定し、評価しました。
ティムは、機密情報を処理するシステムやサービスのユーザーIDが再利用されており、アクセス制御ポリシーが遵守されていないことを発見しました。この不適合の根本原因を分析した後、ISMSプロジェクトマネージャーは、不適合を解決するための可能なアクションのリストを作成しました。次に、ISMSプロジェクトマネージャーはそのリストを分析し、根本原因の排除と将来同様の状況の防止を可能にする活動を選択しました。これらの活動はアクションプランに含まれました。経営陣によって承認されたアクションプランは、次のように記述されています。
アクセス制御ポリシーの新しいバージョンが策定され、情報通信技術（ICT）部門によるネットワークアクセスの効果的な管理と監視を確実にするための新しい制限が設けられま

す。承認された行動計画が実施され、計画に記載されているすべての行動が文書化されました。
シナリオ9に基づくと、特定された不適合に対する是正措置計画は、検出された不適合を解消するのに十分でしょうか？
A. いいえ、行動計画には実施期限が含まれていないためです。
B. はい、特定された不適合に対して別途アクションプランが作成されているためです。
C. いいえ、なぜなら、その行動計画は特定された不適合の根本原因に対処していないからです。
正解: **(**正解を表示します**)**

質問: **35**
ある金融機関のIT部門は、潜在的なセキュリティ侵害を回避するために予防的な対策を実施することを決定しました。そのため、開発、テスト、運用機器を分離し、オフィスを安全に管理し、暗号鍵を使用しました。しかし、セキュリティを強化し、セキュリティ侵害のリスクを最小限に抑えるためのさらなる対策を模索しています。以下のどの対策が、IT部門がこの目的を達成するのに役立つでしょうか？
A. 熱、煙、火災、水に関連する危険を検知する警報装置
B. すべてのシステムのパスワードをすべて変更する
C. 機密ファイルへのアクセスを制限するアクセス制御ソフトウェア
正解: **(**正解を表示します**)**
説明
アクセス制御ソフトウェアは、ユーザーの身元、役割、または権限レベルに基づいて機密ファイルや情報へのアクセスを制限するように設計された予防的制御の一種です。アクセス制御ソフトウェアは、権限のないユーザーによる情報の閲覧、変更、削除を防止することで、情報の機密性、完全性、可用性を保護します。また、アクセス制御ソフトウェアは、誰がいつどの情報にアクセスしたかを記録する監査証跡を作成するのにも役立ち、これは説明責任やコンプライアンスの目的で有用です。
ある金融機関のIT部門は、潜在的なセキュリティ侵害を回避するために予防的な対策を実施することを決定しました。そのため、開発、テスト、運用機器を分離し、オフィスを厳重に管理し、暗号鍵を使用しました。しかし、セキュリティをさらに強化し、セキュリティ侵害のリスクを最小限に抑えるための追加措置を模索しています。アクセス制御ソフトウェアを導入することで、機密ファイルや情報に保護層を追加し、権限のある担当者のみがアクセスできるようにすることで、IT部門はこの目標を達成できるでしょう。
参考文献：
ISO/IEC 27001:2022 リードインプリメンターコースガイド1
ISO/IEC 27001:2022 リードインプリメンター情報キット2
ISO/IEC 27001:2022 情報セキュリティマネジメントシステム - 要求事項3 ISO/IEC 27002:2022 情報セキュリティ管理策の実施規範4 情報セキュリティ管理策とは？ - SecurityScorecard4 情報セキュリティ管理策の種類とは？ - RiskOptics2 完全性とは、情報と処理方法の正確性と完全性を保護する特性です。情報が不正または意図しない方法で変

更または破壊された場合、完全性の侵害が発生します。このケースでは、ダイアナが誤って顧客の許可なく注文の詳細を変更したため、顧客は間違った製品を受け取りました。これは、顧客の注文に関する情報が正確または完全ではなかったことを意味し、したがって、完全性の原則が侵害されました。可用性と機密性は、他の2つの情報セキュリティ原則ですが、このケースでは侵害されていません。可用性とは、権限のあるエンティティが要求に応じてアクセスおよび使用できる特性であり、機密性とは、権限のない個人またはシステムへの情報の開示を防止する特性です。
参照: ISO/IEC 27001:2022 リードインプリメンターコースコンテンツ、モジュール 5: ISO/IEC 27001:2022 に基づく情報セキュリティ管理の概要 1; ISO/IEC 27001:2022 情報セキュリティ、サイバーセキュリティおよびプライバシー保護、条項 3.7: 完全性 2

質問: **36**
シナリオ2によると、Beautyはすべてのユーザーアクセス権限を確認しました。これはどのような種類の制御ですか？
A. 法律および技術
B. 是正および管理
C. 探偵および事務
正解: **C** (コメントを発表する)

質問: **37**
質問：
組織は、それぞれの分野における情報セキュリティリスクに関する情報を得るために、誰にインタビューを行うべきでしょうか？
A. 情報セキュリティに直接責任を負う専門家のみ
B. 情報セキュリティ活動および業務に携わる従業員のみ
C. 専門家であるか否かを問わず、すべての関係者
正解: **C** (コメントを発表する)
ISO/IEC 27001:2022 条項 4.2 - 利害関係者のニーズと期待の理解 には次のように記載されています。
組織は以下を決定するものとする。
a) ISMSに関連する利害関係者
b) これらの利害関係者の関連する要件。
リスク特定には、専門家を含む ただしこれに限定されない）すべての関係者からの意見を取り入れる必要がある。
実際、ISO/IEC 27005:2022は、リスクの状況をより深く理解し、包括的な意見を取り入れるために、リスク評価における利害関係者の関与を重視しています。

質問: **38**

シナリオ3 :Socket Incは、主に無線製品とサービスを提供する通信会社です。同社は、高可用性、拡張性、柔軟性を備えたドキュメントモデルデータベースであるMongoDBを使用しています。
先月、Socket Inc.は情報セキュリティインシデントを報告した。データベース管理者がデフォルト設定を変更していなかったため、パスワードが設定されておらず、誰でもアクセスできる状態になっており、ハッカー集団が同社のMongoDBデータベースに侵入した。
幸いなことに、Socket Inc.はMongoDBデータベースで定期的な情報バックアップを実施していたため、今回のインシデントで情報が失われることはありませんでした。さらに、syslogサーバーによってすべてのログを1つのサーバーに一元管理することができました。同社は、ユーザーのエラーや例外を記録したイベントログを精査した結果、永続的なバックドアが仕掛けられておらず、攻撃は社内の従業員によって開始されたものではないことを突き止めました。
今後同様の事態を防ぐため、Socket Inc.は、権限のある担当者のみにアクセスを許可するアクセス制御システムを採用することを決定しました。また、データベースを不正アクセスから保護するため、暗号鍵管理を含む暗号化技術の効果的な使用に関するルールを定義・実装する制御システムも導入しました。この導入は、関連するすべての協定、法令、規制、および情報分類体系に基づいて行われました。セキュリティの向上と管理業務の軽減のため、VPNを使用したネットワーク分離が提案されました。
最後に、Socket Inc.は、情報セキュリティ上の脅威に関連する情報を維持、収集、分析し、情報セキュリティをプロジェクト管理に統合するための新しいシステムを導入しました。
Socket Inc.は、暗号化と暗号鍵管理を効果的に利用するための管理策を導入しました。これはISO/IEC 27001に準拠していますか？シナリオ3を参照してください。
A. いいえ、この制御は暗号鍵管理のルールを定義するためだけに実装されるべきです。
B. はい、暗号化を効果的に利用するための制御には、暗号鍵管理が含まれます。
C. いいえ、標準規格では暗号鍵管理のための別の制御が規定されているからです。
正解: **B** (コメントを発表する)
ISO/IEC 27001:2022 附属書 A.8.24 によれば、暗号化の有効利用のための管理策は、情報の機密性、真正性、および／または完全性を保護するために、暗号化を適切かつ効果的に利用することを保証することを目的としています。この管理策には、暗号鍵管理が含まれます。
暗号鍵管理とは、暗号鍵を安全な方法で生成、配布、保管、使用、および破棄するプロセスです。暗号鍵管理は、暗号化、デジタル署名、認証などの暗号ソリューションのセキュリティと機能性を確保するために不可欠です。
この規格では、この管理策を実施するための以下のガイダンスを提供しています。
暗号化制御の使用に関する方針を策定し、実施する必要がある。
この方針では、情報分類体系、関連する協定、法令、規制、および評価されたリスクに基づいて、さまざまな種類の暗号化制御を使用すべき状況と条件を明確に定めるべきである。
また、このポリシーでは、アルゴリズム、鍵長、鍵フォーマット、鍵のライフサイクルなど、各タイプの暗号化制御に使用される標準と技術を定義する必要がある。

技術、ビジネス環境、および法的要件の変化を反映させるため、ポリシーは定期的に見直し、更新する必要がある。
暗号鍵は、生成から破棄までの全ライフサイクルを通して、必要最小限のアクセス権限と職務分掌の原則に従い、安全かつ管理された方法で管理されるべきである。
暗号鍵は、暗号化、アクセス制御、バックアップ、監査などの適切な物理的および論理的なセキュリティ対策を用いて、不正アクセス、開示、改ざん、紛失、盗難から保護されなければならない。
暗号鍵は、暗号化サービスの継続性と情報の可用性を確保するための定められた手順に従って、定期的に、または侵害の疑いがある場合に、変更または交換する必要があります。
暗号鍵は、不要になった場合、または使用期限が切れた場合は、復元や再構築が不可能な方法を用いて安全に破棄する必要がある。
参照：
ISO/IEC 27001:2022 リードインプリメンターコースガイド1
ISO/IEC 27001:2022 リードインプリメンター情報キット2
ISO/IEC 27001:2022 情報セキュリティマネジメントシステム - 要求事項3 ISO/IEC 27002:2022 情報セキュリティ管理策の実施規範4 情報セキュリティにおける暗号化管理策の理解5

質問: **39**
以下の規格のうち、プライバシー情報管理システム（PIMS）を構築するための要件とガイドラインを規定しているのはどれですか？
A. ISO/IEC 27009
B. ISO/IEC 27011
C. ISO/IEC 27701
正解: **(**正解を表示します**)**

質問: **40**
優れた物理的セキュリティ対策の例を挙げてください。
A. 故障したプリンターや交換されたプリンターは、直ちに撤去され、リサイクル用のゴミとして処分されます。
B. すべての従業員と訪問者はアクセスパスを携帯しています。
C. 災害発生時に保守担当者がサーバーエリアに迅速かつ支障なくアクセスできるようにします。
正解: **(**正解を表示します**)**

質問: **41**
ISO/27002の「9. アクセス制御」領域に対応する制御項目を選択してください（3つ選択）。
A. 資産の返還
B. アクセス権の撤回または変更
C. 情報へのアクセス制限

D. 特別な権限を持つアクセス権限の管理
正解: **A,B,C** (コメントを発表する)

質問: **42**
質問：
ある組織が、実際の業績を事前に設定された業績目標と比較しました。この行動の主な目的は何でしょうか？
A. すべてのセキュリティインシデントが解決されたことを確認する
B. 組織のセキュリティ目標が達成されているかどうかを評価する
C. 手動による追跡と報告の必要性を排除するため
正解: (正解を表示します)
ISO/IEC 27001:2022 9.1項 - 監視、測定、分析、評価:
組織は、情報セキュリティ管理システムのパフォーマンスと有効性を評価しなければならない。評価には、パフォーマンス指標およびセキュリティ目標との比較が含まれる。」その目的は、セキュリティ目標（第6.2項）が達成されていることを確認することである。パフォーマンスを測定することで、組織は、管理策とプロセスが効果的であり、戦略目標と整合しているかどうかを判断できる。
オプションAは範囲が狭すぎ、オプションCは場合によっては手動追跡が必要になる可能性があるため不適切です。
参考文献：
ISO/IEC 27001:2022 条項6.2および9.1
ISO/IEC 27004:2016 - 条項 7.2 (客観的評価のための指標の使用)

質問: **43**
シナリオ 8: SunDee は、米国カリフォルニア州に本社を置くアメリカのバイオ医薬品会社です。同社は、心血管疾患、腫瘍、骨の健康、炎症に重点を置いた新しいヒト治療薬の開発を専門としています。同社は、過去 2 年間、SO/IEC 27001 に基づく情報セキュリティ管理システム (ISMS) を導入してきました。しかし、ISMS のパフォーマンスと有効性を監視または測定しておらず、定期的な管理レビューも実施していませんでした。再認証監査の直前に、同社は内部監査を実施することにしました。また、ほとんどの従業員に、過去 2 年間の各部門の書面による個人レポートをまとめるよう依頼しました。これにより、生産部門の人員が最適人数を下回り、会社の在庫が減少しました。
テッサはサンディーの内部監査員でした。50人の異なる従業員によって複数のレポートが作成されたため、内部監査プロセスは計画よりもはるかに時間がかかり、非常に一貫性がなく、定性的な尺度は全くありませんでした。テッサは、サンディーがISMSのパフォーマンスを適切に評価する必要があると結論付けました。彼女は、サンディーのISMSパフォーマンス評価の怠慢を重大な不適合と定義し、不適合の説明、監査結果、および推奨事項を含む不適合レポートを作成しました。さらに、テッサはサンディーがこれらの問題を解決で

きるようにする新しい計画を作成し、それを経営陣に提示しました。サンディーの怠慢はISMS認証にどのように影響しますか？シナリオ8を参照してください。
A. 内部監査が予定より長引いたため、SunDeeはISMS認証を更新できない可能性がある。
B. SunDeeはISMSの有効性を評価するための内部監査を実施したため、ISMS認証を更新します。
C. SunDeeは計画された間隔で経営レビューを実施していないため、ISMS認証を更新できない可能性があります。
正解: **(**正解を表示します**)**

質問: **44**
NeuroTrustMedは、韓国ソウルに本社を置く大手医療技術企業です。同社は、神経疾患の早期診断と治療計画に使用されるAI支援型神経画像ソリューションの開発を専門としています。機密性の高い患者の健康記録や医療研究データを扱うデータ集約型企業として、NeuroTrustMedはサイバーセキュリティと規制遵守を非常に重視しています。同社は過去3年間、ISO/IEC 27001認証を取得したISMSを維持しています。新たな脅威への対応、医療診断におけるイノベーションの支援、ステークホルダーの信頼維持のため、ISMSを継続的に見直し、改善しています。継続的改善への取り組みの一環として、NeuroTrustMedは潜在的な不適合を積極的に追跡し、根本原因分析を実施し、是正措置と予防措置を実施し、すべての変更が文書化され、同社の戦略目標と整合していることを確認しています。地域をまたいだデータ処理に影響を与える新たなデータ保護規制が施行された際、情報セキュリティチームは現行のポリシーと新規制とのギャップ評価を実施しました。その後、コンプライアンスを満たすために関連文書とプロセスを更新しました。これらの改訂を受けて、NeuroTrustMedはISMS文書を更新し、改善登録簿に新しいエントリを追加しました。構造化されたスプレッドシート形式で管理されている登録簿には、固有の変更番号、更新の説明、法的コンプライアンスによる優先度の高い分類、開始日と完了日、および情報セキュリティマネージャーによる承認が含まれていました。ほぼ同時期に、定期的な管理レビュー中に、情報セキュリティチームはオンボーディングエラーのパターンも特定しました。これらのエラーはデータ漏洩には至っていませんでしたが、不正アクセスのリスクがありました。これに対応して、オンボーディング手順が改訂され、アクセスを許可する前に正確性を確保するための自動検証ステップが追加されました。根本原因を理解するために、チームはプロビジョニングプロセスに関するデータを収集しました。プロセスログを分析し、オンボーディングスタッフにインタビューを行い、アクセスエラーをHRからITへの引き継ぎワークフローにおける設定ミスのあるステップまで追跡しました。チームは変更を実装する前に、テストケースを通じてこの発見を検証しました。確認後、情報セキュリティチームはISMSログに不適合を記録しました。文書には、問題の説明、影響を受けたシステム、影響を受けたユーザー、およびアクセス管理に関連する潜在的な影響に関する簡単なリスク評価が含まれていました。上記のシナリオに基づいて、次の質問に答えてください。シナリオ10を参照して、認証決定委員会の構成は適切でしょうか？
A. はい、認証の決定を下す人と監査を実施した人は異なるからです。

B. いいえ、委員会は監査チームのメンバーのみで構成され、監査に関わっていない他の専門家は含めるべきではありませんでした。
C. いいえ、委員会には監査チームのメンバー1名と、認証機関に勤務するその他の個人を含める必要があります。
正解: **(**正解を表示します**)**
ISO/IEC 27001の認証制度においては、認証決定は監査自体に参加していない者によって行われることが基本要件となっている。この分離によって、認証決定の客観性、独立性、および信頼性が確保される。
ISO/IEC 27001はISMSの要求事項を定義しているが、認証決定のガバナンスについてはISO/IEC 17021-1で規定されており、以下のことが求められている。
監査チームは認証の決定を行いません。
* 監査とは独立した有能な担当者によって決定が下される シナリオ 10 は、認証決定委員会が監査チームとは別の個人で構成されていたことを示しており、この要件を満たしています。
* 選択肢Bは誤りです。意思決定委員会は監査チームのメンバーだけで構成されるべきではありません。
* 選択肢Cは、監査チームのメンバーを意思決定機関に含めると独立性が損なわれるため、誤りです。
この構造は、ISMS（情報セキュリティマネジメントシステム）の監査を行う認証機関を規定し、公平な認証決定の必要性を強調するISO/IEC 27006にも合致している。

質問: **45**
シナリオ 8: SunDee は、米国カリフォルニア州に本社を置くアメリカのバイオ医薬品会社です。同社は、心血管疾患、腫瘍、骨の健康、炎症に重点を置いた新しいヒト治療薬の開発を専門としています。同社は、過去 2 年間、SO/IEC 27001 に基づく情報セキュリティ管理システム (ISMS) を導入してきました。しかし、ISMS のパフォーマンスと有効性を監視または測定しておらず、定期的な管理レビューも実施していませんでした。再認証監査の直前に、同社は内部監査を実施することにしました。また、ほとんどの従業員に、過去 2 年間の各部門の書面による個人レポートをまとめるよう依頼しました。これにより、生産部門の人員が最適人数を下回り、会社の在庫が減少しました。
テッサはサンディーの内部監査員でした。50人の異なる従業員によって複数のレポートが作成されたため、内部監査プロセスは計画よりもはるかに時間がかかり、非常に一貫性がなく、定性的な尺度がまったくありませんでした。テッサは、サンディーがISMSのパフォーマンスを適切に評価する必要があると結論付けました。彼女は、サンディーのISMSパフォーマンス評価の怠慢を重大な不適合と定義し、不適合の説明、監査結果、および推奨事項を含む不適合レポートを作成しました。さらに、テッサはサンディーがこれらの問題を解決できるようにする新しい計画を作成し、それを経営陣に提示しました。シナリオ8に基づいて、不適合レポートには必要なすべての側面が含まれていましたか?
A. はい、報告書には必要な事項がすべて含まれていました。

B. いいえ、報告書には不適合の根本原因も明記する必要があります。
C. いいえ、報告書には監査基準も明記する必要があります。
正解**: (**正解を表示します**)**
ISO/IEC 27001:2022によると、不適合報告書とは、監査中に特定された監査基準からの逸脱の詳細を記録した文書である2。監査基準とは、監査証拠と比較するための参照として使用される一連の方針、手順、要求事項、または仕様のことである3。したがって、不適合報告書には以下の側面を含める必要がある。
不適合の説明には、逸脱の内容、発生場所、および検出された日時を明確に記載する必要があります。
監査結果は、不適合の特定を裏付ける客観的な証拠を提供するものである。
* 監査基準には、不適合が逸脱している参照文書または規格を明記する必要があります。
* 推奨事項とは、不適合に対処するために講じることができる是正措置または改善策を提案するものです。シナリオ 8 では、テッサの不適合報告書には不適合の説明、監査結果、推奨事項が含まれていましたが、監査基準が明記されていませんでした。そのため、報告書には必要なすべての側面が含まれておらず、不完全でした。
参考文献：
* 1: ISO/IEC 27001:2022、9.2.3項
* 2: ISO/IEC 27001:2022、条項3.23
* 3: ISO/IEC 27001:2022、3.5項
* : ISO/IEC 27001:2022、附属書A.9.2.3

質問**: 46**
シナリオ2 :NyvMarketingは、さまざまな業界の顧客に多様なサービスを提供するマーケティング会社です。デジタルマーケティング、ブランディング、市場調査の専門知識を活かし、革新的でインパクトのあるマーケティングキャンペーンを提供することで確固たる評判を築いてきました。マーケティング業界におけるデータセキュリティと情報保護の重要性の高まりを受け、同社はISMS 27001に基づくISMSを導入することを決定しました。
NyvMarketingはISMSを導入する際に、リソース不足という重大な課題に直面しました。この課題はISMSの目標を効果的に達成する上でリスクとなり、機密情報の保護に向けた同社の取り組みを損なう可能性がありました。この脅威に対処するため、NyvMarketingはリソース制約に関連するリスクを管理する担当者としてマイケルを任命するという積極的なアプローチを採用しました。
マイケルは、NyvMarket*ngにおけるISMS導入において、リソース不足の特定と対処、リスク軽減戦略の策定、効果的なリソース配分において極めて重要な役割を果たし、リソース不足に対する同社の回復力を強化した。
さらに、NyvMarketingは情報セキュリティにおける業界標準とベストプラクティスを優先し、ISO/IEC 27002ガイドラインを徹底的に遵守しました。卓越性とISO/IEC 27001の要件に基づいたこの取り組みは、NyvMarketingが最高水準の情報セキュリティガバナンスを維持するという強い意志を明確に示しています。

ISMS導入作業中、NyvMarketingは能力に関する要求事項（ISO/IEC 27001、7.2項に規定）の1つを除外することを選択しました。同社は、既存の従業員がISMS関連業務を遂行するために必要な能力を備えていると考えていましたが、この除外に対する正当な理由を提示しませんでした。さらに、ISO/IEC 27001の附属書Aに記載されている特定の管理策が実施されなかった際も、NyvMarketingはこれらの除外に対する適切な理由を提示しませんでした。
ISMS導入の過程で、NFMarketingは情報セキュリティに影響を与える可能性のある脆弱性を徹底的に評価しました。これらの脆弱性には、ストレージメディアの不十分なメンテナンスと不適切なインストール、機器の不十分な定期交換計画、不十分なソフトウェアテスト、および保護されていない通信回線が含まれていました。これらの脆弱性がデータセキュリティにリスクをもたらす可能性があることを認識したNFMarketingは、必要な制御と対策を実施することで、これらの特定の弱点に対処するための措置を講じました。上記のシナリオに基づいて、次の質問に答えてください。
シナリオ2において、NyvMarketingはISMS導入中にリソース不足の脅威に直面しました。この脅威は次のどのカテゴリに該当しますか？
NyvMarketingは、ISMS導入時に以下のどの脆弱性カテゴリに対処しましたか？シナリオ2を参照してください。
A. ネットワーク、人員、およびサイトの脆弱性
B. 組織および施設の脆弱性
C. ハードウェア、ソフトウェア、およびネットワークの脆弱性
D. 物理的および管理上の脆弱性
正解: **C** (コメントを発表する)
シナリオ 2 では、NyvMarketing は「ストレージ メディアの不十分なメンテナンスと不適切なインストール、機器の不十分な定期交換計画、不十分なソフトウェア テスト、保護されていない通信回線」などの脆弱性を特定しました。ストレージ メディアと機器: ハードウェアの脆弱性 不十分なソフトウェア テスト: ソフトウェアの脆弱性 保護されていない通信回線: ネットワークの脆弱性 ISO/IEC 27001:2022 (およびリスク管理に関する ISO/IEC 27005:2022) によると、組織は ISMS の有効性を確保するために、ハードウェア、ソフトウェア、ネットワークの弱点を含む技術的な脆弱性を特定して評価する必要があります。
「ハードウェア、ソフトウェア、人材、組織プロセスには脆弱性が存在する可能性がある。情報資産に関連する脆弱性の特定が必要である。」
- ISO/IEC 27005:2022、8.2.2

質問: **47**
ISMSの継続的な改善を支えるものは何ですか？
A. 文書情報の更新
B. 行動計画の更新
C. 永久監査報告書の更新
正解: **(**正解を表示します**)**
ISO/IEC 27001:2022規格によれば、組織は情報セキュリティマネジメントシステム（ISMS）に影響を与える変更を管理し、ISMSの適合性、妥当性、有効性を継続的に改善するためのプロセスを確立、実施、維持する必要がある（8.1.3項および10.2項）。また、同規格では、組織は変更および改善プロセスの結果を反映させるため、必要に応じてISMSの文書化された情報を更新する必要があると規定されている（8.1.3.2項および10.2.2項）。したがって、文書化された情報の更新は、ISMSが組織および利害関係者の現在および将来のニーズと期待に合致することを保証することにより、ISMSの継続的な改善を支えるものである。
参照：
ISO/IEC 27001:2022、情報セキュリティ、サイバーセキュリティおよびプライバシー保護 - 情報セキュリティマネジメントシステム - 要求事項1 ISO/IEC 27001 リードインプリメンター情報キット ISO 27001 要求事項 10.22 の継続的改善

質問: **48**
シナリオ10：NetworkFuse社は、ネットワークハードウェアの開発、製造、販売を行っています。同社は、ISO/IEC 27001の要件に基づく運用情報セキュリティ管理システム（ISMS）と、ISO 9001に基づく品質管理システム（QMS）を約2年間運用してきました。最近、ISO/IEC 27001とISO 9001の両方の認証を取得するために、統合認証監査を申請しました。
認証機関を選定した後、NetworkFuseは従業員を監査に向けて準備させた。経営陣の判断により、監査前に自己評価を実施する必要はないと判断されたため、同社は自己評価を行わないことを決定した。さらに、内部監査報告書や経営陣によるレビュー、導入済みの技術、ISMSおよびQMSの一般的な運用状況など、文書化された情報が利用可能であることを確認した。
しかし、同社は認証機関に対し、文書を社外に持ち出すことはできないと要請した。しかし、NetworkFuseが割り当てられた監査チームリーダーを拒否し、その交代を要請したため、監査は予定された日数内には実施されなかった。同社は、同じ監査チームリーダーが主要な競合他社に認証の勧告を出しており、これは同社の経営陣にとって潜在的な利益相反であると主張した。認証機関はこの要請を受け入れなかった。シナリオ10に基づく

と、NetworkFuseは監査前にISMSの自己評価を実施しなかった。これはISO/IEC 27001に準拠しているか？
A. いいえ、被監査者は認証監査を実施する前に、第4項から第10項までの要件を確認する必要があります。
B. はい、基準では、被監査者は認証監査の準備にあたり、内部監査報告書と経営レビュー報告書のみに依拠しなければならないと規定されています。
C. はい、基準では監査前に自己評価を実施することは義務付けられていませんが、実施することは良い慣行です。
正解: **C** (コメントを発表する)
ISO/IEC 27001:2022規格によれば、組織は、規格の要求事項に従って情報セキュリティマネジメントシステム（ISMS）を確立、実施、維持、継続的に改善する責任を負います（第4.1項）。この規格では、認証監査の前に組織がISMSの自己評価を実施することを明示的に要求していません。認証監査とは、独立した認証機関がISMSの規格への適合性を検証し、認証を付与するために実施する外部監査です（第9.3.2項）。しかし、この規格では、組織がISMSの有効性、適切性、妥当性を確保し、改善の機会と是正措置を特定するために、計画された間隔でISMSの内部監査（第9.2項）とマネジメントレビュー（第9.3項）を実施することを要求しています。
したがって、認証監査の前にISMSの自己評価を実施することは、組織が監査に備え、ギャップや不適合を特定し、認証取得への取り組みと準備状況を示すのに役立つため、従うべき良い慣行である。
ISO/IEC 27001:2022、情報セキュリティ、サイバーセキュリティおよびプライバシー保護 - 情報セキュリティマネジメントシステム - 要求事項1 ISO/IEC 27001 リードインプリメンター情報キット 自己評価チェックリスト ISO/IEC 27001:20222

質問: **49**
シナリオ 1: HealthGenic は、ウェブベースの医療ソフトウェアを使用して乳幼児から成人初期までの個人の健康と成長をモニタリングする小児科クリニックです。このソフトウェアは、予約のスケジュール設定、カスタマイズされた医療レポートの作成、患者のデータと病歴の保存、およびすべての関係者とのコミュニケーションにも使用されます。
[^両親、他の医師、医療検査技師を含む関係者。
先月、HealthGenicはソフトウェアにアクセスするユーザー数の増加により、何度かサービスの中断に見舞われた。同社がソフトウェアを使用する際に直面したもう一つの問題は、複雑なユーザーインターフェースであり、訓練を受けていない従業員にとっては使いこなすのが難しいと感じられた。
HealthGenicの経営陣は、この問題について直ちにソフトウェア開発会社に報告した。ソフトウェア会社は問題を修正したが、その過程でHealthGenicの患者に関する機密情報を含む一部のファイルを改変してしまった。その結果、医療報告書が不完全かつ不正確になり、さらに重要なことに、患者のプライバシーが侵害された。

シナリオ1で説明されている状況のうち、HealthGenicにとって脅威となるのはどれですか？
A. HealthGenicは従業員にソフトウェアの使用方法に関するトレーニングを実施していませんでした。
B. ソフトウェア会社がHealthGenicの患者に関する情報を改ざんした
C. HealthGenicは、患者の機密情報を保管するためにウェブベースの医療ソフトウェアを使用していた。
正解: **(**正解を表示します**)**
ISO/IEC 27001:2022によると、脅威とは、資産の機密性、完全性、または可用性に悪影響を及ぼす可能性のあるあらゆる事象を指します。このシナリオでは、資産とは、ウェブベースの医療ソフトウェアによって保存および処理されるHealthGenicの患者に関する情報です。ソフトウェア会社がHealthGenicの患者に関する機密情報を含む一部のファイルを改変したことは、不完全かつ不正確な医療レポートの作成や患者のプライバシー侵害につながり、資産の機密性と完全性に悪影響を及ぼす可能性のある事象です。したがって、この状況はHealthGenicにとって脅威となります。
ISO/IEC 27001:2022 - 情報セキュリティ、サイバーセキュリティおよびプライバシー保護 - 情報セキュリティマネジメントシステム - 要求事項 ISO 27001 主要用語 - PJR

質問: **50**
シナリオ8 :サンディー社は、米国カリフォルニア州に本社を置くバイオ医薬品企業です。ヒト治療薬分野における先駆的な業績で知られるサンディー社は、特に心血管疾患、腫瘍学、骨の健康、炎症といった分野における重要な医療課題への取り組みに重点を置いています。
SunDeeは、過去2年間、ISO/IEC 27001に基づいた効果的な情報セキュリティ管理システム（ISMS）を維持することで、データセキュリティとデータ完全性に対する取り組みを示してきました。
再認証監査の準備として、SunDee社は内部監査を実施しました。同社の経営陣は、過去6か月間コンプライアンス部門の日常業務を積極的に管理してきたアレックスを内部監査員に任命しました。この二重の役割を担うアレックスは、コンプライアンスを確保する監査を実施するとともに、業務効率を向上させるための有益な提言を行う任務を負っています。
内部監査において、いくつかの不適合事項が特定された。これらに包括的に対処するため、当社は監査チームリーダーと緊密に連携しながら、各不適合事項に対する改善計画を作成した。
サンディーの経営陣は、ISMSの適切性、十分性、効率性を評価するため、ISMSの包括的な見直しを実施しました。これは、定期的な経営会議に組み込まれました。監査報告書、アクションプラン、見直し結果などの重要な文書は、会議前に全メンバーに配布されました。議題には、前回の見直しの進捗状況、ISMSに影響を与える変更点、フィードバック、ステークホルダーからの意見、改善の機会などが含まれました。ISMSの改善を目的とした決定と行

動が下され、ISMSコーディネーターと内部監査チームがフォローアップアクションプランの作成において重要な役割を果たし、その後、経営陣によって承認されました。
レビュー結果を受けて、SunDeeは速やかに是正措置を実施し、情報セキュリティ対策を強化しました。さらに、組織の情報セキュリティ管理を監視するために不可欠な主要業績評価指標（KPI）の概要を一目で把握できるダッシュボードツールを導入しました。これらの指標には、セキュリティインシデント、そのコスト、システム脆弱性テスト、不適合検出、解決時間に関する指標が含まれており、監視活動の効果的な記録、報告、追跡を容易にしました。また、SunDeeは進行中のプロジェクトの進捗状況と成果を評価するための包括的な測定プロセスに着手し、すべてのプロセスにわたって広範な測定を実施しました。経営陣は、測定に寄与するデータの所有者である情報責任者が、これらの測定活動の実行責任者にも指定されることを決定しました。
上記のシナリオに基づいて、次の質問に答えてください。
アレックスは社内の内部監査役の職務に適しているでしょうか？
A. はい、アレックスのコンプライアンス部門の日常業務における最近の経験は、内部監査員の役割に役立つでしょう。
B. いいえ、内部監査は業務経験のない者のみが実施できます。
C. いいえ、アレックスは内部監査役の職に就く前に、適切な期間を待つべきです。
正解: **(**正解を表示します**)**

質問: **51**
シナリオ10 :NetworkFuse社は、ネットワークハードウェアの開発、製造、販売を行っています。同社は、ISO/IEC 27001の要件に基づく運用情報セキュリティ管理システム（ISMS）と、ISO 9001に基づく品質管理システム（QMS）を約2年間運用してきました。最近、ISO/IEC 27001とISO 9001の両方の認証を取得するために、統合認証監査を申請しました。
認証機関を選定した後、NetworkFuse は監査に向けて従業員を準備しました。同社は、経営陣によれば必要ないということで、監査前に自己評価を実施しないことを決定しました。さらに、内部監査レポートや経営陣のレビュー、導入済みのテクノロジー、ISMS および QMS の一般的な運用など、文書化された情報が利用可能であることを確認しました。しかし、同社は認証機関に対し、文書を社外に持ち出せないように要求しました。しかし、NetworkFuse が割り当てられた監査チームリーダーを拒否し、その交代を要求したため、監査は予定された日数内には実施されませんでした。同社は、同じ監査チームリーダーが主要な競合他社に認証の推奨を発行しており、これは同社の経営陣にとって潜在的な利益相反であると主張しました。認証機関はこの要求を受け入れませんでした。シナリオ 10 に基づくと、NetworkFuse は監査前に ISMS の自己評価を実施しませんでした。これは ISO/IEC 27001 に準拠していますか?
A. いいえ、被監査者は認証監査を実施する前に、第4項から第10項までの要件を確認する必要があります。

B. はい、基準では、被監査者は認証監査の準備にあたり、内部監査報告書と経営レビュー報告書のみに依拠しなければならないと規定されています。
C. はい、基準では監査前に自己評価を実施することは義務付けられていませんが、実施することは良い慣行です。
正解: **C** (コメントを発表する)
ISO/IEC 27001:2022規格によれば、組織は、規格の要求事項に従って情報セキュリティマネジメントシステム（ISMS）を確立、実施、維持、および継続的に改善する責任を負います（第4.1項）。この規格では、認証監査（ISMSが規格に適合していることを検証し、認証を付与するために独立した認証機関によって実施される外部監査）の前に、組織がISMSの自己評価を実施することを明示的に要求していません（第9.3.2項）。しかし、この規格では、組織がISMSの有効性、適切性、妥当性を確保し、改善の機会と是正措置を特定するために、計画された間隔でISMSの内部監査（第9.2項）とマネジメントレビュー（第9.3項）を実施することを要求しています。したがって、認証監査の前にISMSの自己評価を実施することは、組織が監査に備え、ギャップや不適合を特定し、認証に対する組織のコミットメントと準備状況を示すのに役立つため、従うべき良い慣行です。
参照：
ISO/IEC 27001:2022、情報セキュリティ、サイバーセキュリティおよびプライバシー保護 - 情報セキュリティマネジメントシステム - 要求事項1 ISO/IEC 27001 リードインプリメンター情報キット 自己評価チェックリスト ISO/IEC 27001:20222

質問: **52**
シナリオ3 :Socket Incは、主に無線製品とサービスを提供する通信会社です。同社は、高可用性、拡張性、柔軟性を備えたドキュメントモデルデータベースであるMongoDBを使用しています。
先月、Socket Inc.は情報セキュリティインシデントを報告した。データベース管理者がデフォルト設定を変更していなかったため、パスワードが設定されておらず、誰でもアクセスできる状態になっており、ハッカー集団が同社のMongoDBデータベースに侵入した。幸いなことに、Socket Inc.はMongoDBデータベースで定期的な情報バックアップを実施していたため、今回のインシデントで情報が失われることはありませんでした。さらに、syslogサーバーによってすべてのログを1つのサーバーに一元管理することができました。同社は、ユーザーのエラーや例外を記録したイベントログを精査した結果、永続的なバックドアが仕掛けられておらず、攻撃は社内の従業員によって開始されたものではないことを突き止めました。
今後同様の事態を防ぐため、Socket Inc.は、権限のある担当者のみにアクセスを許可するアクセス制御システムを採用することを決定しました。また、データベースを不正アクセスから保護するため、暗号鍵管理を含む暗号化技術の効果的な使用に関するルールを定義・実装する制御システムも導入しました。この導入は、関連するすべての協定、法令、規制、および情報分類体系に基づいて行われました。セキュリティの向上と管理業務の軽減のため、VPNを使用したネットワーク分離が提案されました。

最後に、Socket Inc.は、情報セキュリティ上の脅威に関連する情報を維持、収集、分析し、情報セキュリティをプロジェクト管理に統合するための新しいシステムを導入しました。Socket Inc.は、ユーザーのエラーや例外を記録したイベントログを分析することで、永続的なバックドアが仕掛けられておらず、攻撃が社内の従業員によって開始されたことを突き止めることができるでしょうか？シナリオ3を参照してください。
A. はい。Socket Inc.は、ユーザーのエラーログと例外ログを確認するだけで、永続的なバックドアが仕掛けられていないことを検出できます。
B. いいえ、Socket Inc.はユーザーアクティビティを記録するイベントログも確認すべきです。
C. いいえ、Socket Inc.はsyslogサーバー上のすべてのログを確認すべきでした。
正解: **(**正解を表示します**)**
イベントログは、システムやネットワークで発生するイベント（ユーザー操作、障害、例外、エラー、警告、セキュリティインシデントなど）の記録です。監視、監査、トラブルシューティングに役立つ貴重な情報を提供します。イベントログは、イベントの発生源と性質に応じて、さまざまな種類に分類できます。たとえば、ユーザーアクティビティログには、ログイン、ログアウト、ファイルアクセス、コマンド実行など、ユーザーが行った操作が記録されます。ユーザー障害および例外ログには、無効なデータ入力、不正アクセス試行、システムクラッシュなど、ユーザーの入力や動作によって発生するエラーや異常が記録されます。シナリオ3では、Socket Inc.はsyslogサーバーを使用してすべてのログを1つのサーバーに集約しており、これはログ管理の優れた方法です。しかし、永続的なバックドアが仕掛けられておらず、攻撃が社内の従業員から開始されたものではないことを知るには、Socket Inc.はユーザー障害および例外ログだけでなく、ユーザーアクティビティログも確認する必要がありました。ユーザーアクティビティログからは、ハッカーや従業員によるファイルの作成、変更、削除、コマンドの実行、ソフトウェアのインストールなど、疑わしい、あるいは悪意のある行為が明らかになる可能性があります。Socket Inc.は、これら2種類のログを精査することで、インシデントとその根本原因をより包括的に把握できるでしょう。ただし、一部のログは無関係であったり、分析するには量が多すぎたりする可能性があるため、syslogサーバー上のすべてのログを精査する必要はない、あるいは現実的ではないかもしれません。

質問: **53**
シナリオ 6: CB Consulting は、アイルランドのダブリンに拠点を置く評判の高い企業です。多様なクライアントに戦略的なビジネス ソリューションを提供しています。専門家からなる専任チームを擁する CB Consulting は、卓越性、誠実さ、顧客満足への取り組みを誇りとしています。CB Consulting は、情報セキュリティの実践を強化するという継続的な取り組みの一環として、ISO 1EC 27001 に準拠した ISMS の導入を開始しました。このプロセス全体を通して、効果的なコミュニケーションと確立されたセキュリティ プロトコルの遵守を確保することが不可欠です。

CB社の従業員であるサラは、機密性の高い顧客データの管理に焦点を当てた新しいプロジェクトの責任者に任命されました。さらに、彼女はインシデント管理の対応フェーズにおける活動の監督、インシデント管理チームのインシデントマネージャーへの定期的な報告、主要な関係者への情報提供なども担当します。一方、CBコンサルティングはトムを同社の法務コンサルタントに異動させました。
CBコンサルティングは、以前ITセキュリティアナリストだったクレアを情報セキュリティ責任者に再任し、ISMSの導入を監督し、ISO/IEC 27001への準拠を確保するよう指示しました。クレアの主な責任は、定期的なリスク評価を実施し、潜在的な脆弱性を特定し、リスクを効果的に軽減するための適切なセキュリティ対策を実施することです。クレアは、情報セキュリティリスク評価は重大な変更が発生した場合にのみ実施するという手順を確立しました。これは、会社のセキュリティ体制を強化し、潜在的な脅威から保護する上で重要な役割を果たします。
CBコンサルティングは、情報セキュリティ目標を達成できる有能な人材を確保するため、サラ、トム、クレアを含む全従業員が、学歴、研修、または経験に基づき必要な能力を備えていることを検証するプロセスを導入しました。不足が認められた場合は、追加の研修やメンター制度の提供など、具体的な対策を講じています。さらに、CBコンサルティングは、必要な能力と習得した能力の証拠として、文書化された情報を保管しています。
CBコンサルティングは、安全かつ効果的な情報交換を確保するために、業界標準に準拠した強固なコミュニケーション戦略を確立しました。関連する問題に関するコミュニケーションの要件を特定しました。まず、同社は特定の役割を指定しました。外部コミュニケーションのための広報担当者や、データ漏洩などの機密事項を管理する内部問題のためのセキュリティ担当者などです。次に、
コミュニケーションのきっかけ、内容、および受信者は慎重に定義され、必要に応じてメッセージは経営陣の事前承認を得ました。最後に、送信される情報の機密性と完全性を確保するために、専用のチャネルが導入されました。
上記のシナリオに基づいて、次の質問に答えてください。
CBコンサルティングは、信頼を醸成し、ステークホルダーの関与を高め、情報セキュリティにおける卓越性への取り組みを強化するために、透明性と実質的なコミュニケーションの実践を優先しています。このアプローチによって強調されている効果的なコミュニケーションの原則はどれですか？
透明性
CBコンサルティングは、ベストプラクティスに従って、関連する課題に関するコミュニケーション要件をどの程度特定したか。シナリオ6の最後の段落を参照してください。
A. 当社は、ベストプラクティスに沿って、すべてのコミュニケーション要件を完全に特定しました。
B. 同社は、通信の意図された相手を特定できなかった。
C. 同社は、メッセージが適切に送信され、受信されることを保証するプロセスを確立していませんでした。
正解: **(**正解を表示します**)**

CBコンサルティングは、メッセージの役割、トリガー、コンテンツ、受信者、事前承認プロセス、および専用チャネルを定義し、ベストプラクティスに基づいたコミュニケーション要件の完全な特定を示しました。
組織は、情報セキュリティマネジメントシステム（ISMS）に関連する内部および外部コミュニケーションの必要性を、何を、いつ、誰と、誰がコミュニケーションを行うかを含めて決定しなければならない。」
- ISO/IEC 27001:2022、7.4項

質問: **54**
リスク保持の例となる記述はどれですか？
A. ある組織がデータ損失防止ソフトウェアを導入しました
B. 激しい嵐のため、建設現場での作業が中断された。
C. 組織は、軽微なバグがまだ修正されていないにもかかわらず、ソフトウェアをリリースすることを決定しました。
正解: **(**正解を表示します**)**

質問: **55**
ある組織は、セキュリティ関連のイベントやその他の記録されたデータの相関分析を可能にし、情報セキュリティインシデントの調査を支援したいと考えています。どのような制御策を導入すべきでしょうか？
A. クロック同期
B. オペレーティングシステムへのソフトウェアのインストール
C. 特権ユーティリティプログラムの使用
正解: **(**正解を表示します**)**

質問: **56**
ISO/IEC 27001で規定されている、組織が不適合を検出した際に取るべき手順に含まれていないものはどれですか？
A. 不適合に対して反応し、それを制御 -是正するための措置を講じ、その結果に対処する。
B. 不適合の原因を排除し、再発または他所での発生を防ぐための対策の必要性を評価する。
C. 不適合の詳細を組織の全従業員に伝え、不適合の原因となった従業員を停職処分にする。
正解: **(**正解を表示します**)**
ISO/IEC 27001:2022 リードインプリメンターコースによると、組織が不適合を検出した場合に取るべきISO/IEC 27001で要求される手順は次のとおりです1:
不適合に対応し、それを制御および修正するための措置を講じ、その結果に対処する 不適合が再発したり、他の場所で発生したりしないように、不適合の原因を排除するための措置の必要性を評価する 必要な措置を実施する 是正措置の有効性をレビューする 必要に応

じて情報セキュリティ管理システム（ISMS）を変更する したがって、不適合の詳細を組織のすべての従業員に伝え、不適合を引き起こした従業員を停職させることは、ISO/IEC 27001 で要求される手順の一部ではありません。このオプションは不要であるだけでなく、情報の機密性、完全性、可用性の原則、および関係する従業員の人権と尊厳を侵害する可能性があるため、潜在的に有害です 2。代わりに、組織は不適合の報告、記録、分析に関する確立された手順に従い、是正措置が適切、比例的、かつ公正であることを保証する必要があります 3。

質問: **57**
IoT（モノのインターネット）デバイスが相互に（あるいは「外部世界」と）通信する方法の一つに、いわゆる短距離無線プロトコル（SRRP）があります。では、スマートフォンをクレジットカードとして利用することを可能にするのは、どのような種類の短距離無線プロトコルなのでしょうか？
A. Bluetooth
B. 無線周波数識別（RFID）
C. 4Gプロトコル
D. 近距離無線通信（NFC）
正解: **D** (コメントを発表する)

質問: **58**
シナリオ8によると、テッサはISMSの監視と測定に関する計画を作成し、それを経営陣に提示しました。これは受け入れられますか？
A. いいえ、テッサは発見した問題点を経営陣にのみ報告すべきです。
B. いいえ、テッサは監査中に発見された問題に対する必要な改善策をすべて実施しなければなりません。
C. はい、テッサは経営陣に対し、会社の機能改善について助言することができます。
正解: **C** (コメントを発表する)

質問: **59**
シナリオ6：Skyver社は、ゲーム機、薄型テレビ、コンピューター、プリンターなどの電子製品を世界中に配送しています。情報セキュリティを確保するため、同社はISO/IEC 27001の要件に基づいた情報セキュリティマネジメントシステム（ISMS）を導入することを決定しました。
社内で最も優秀な情報セキュリティ専門家であるコリンは、情報セキュリティ上の課題やその他の情報セキュリティ関連の対策について、社員を対象とした研修と啓発セッションを開催することを決定した。セッションでは、Skyverの情報セキュリティへの取り組み方や、フィッシングやマルウェア対策の手法などが取り上げられた。
セッションの参加者の1人は、人事部に勤務するリサです。コリンはスカイバーの既存の情報セキュリティポリシーと手順を正直かつ公平に説明しますが、リサは議論されている問題の一部が専門的すぎると感じ、セッションを完全に理解できません。そのため、多くの場

合、彼女はトレーナーや同僚に追加のサポートを求めます。シナリオ6に基づくと、コリンはいつ次のトレーニングと意識向上セッションを実施すべきでしょうか？
A. 対象となる従業員グループが組織のニーズを満たしたことを確認した後
B. 能力ニーズ分析を実施し、能力関連の問題を記録した後
C. 従業員の勤務可能時間とモチベーションを確認した後
正解: **(**正解を表示します**)**
ISO/IEC 27001:2022の7.2.3項によれば、組織は、ISMSのパフォーマンスと有効性に影響を与える業務を自らの管理下で遂行する者の必要な能力を判断するために、能力ニーズ分析を実施しなければならない。また、組織は、必要な能力を獲得するために講じた措置の有効性を評価し、能力の証拠として適切な文書化された情報を保持しなければならない。
したがって、コリンは能力ニーズ分析を実施し、理解度、知識のギャップ、参加者からのフィードバックなど、能力に関連する問題点を記録した上で、次回の研修および啓発セッションを実施すべきである。

質問: **60**
シナリオ2 :Beautyは、最近従来の小売販売からeコマースモデルに移行した化粧品会社です。経営陣は、自社で独自のプラットフォームを構築し、オンライン送金に対応したオンライン決済システムを運営する外部プロバイダーに決済処理を委託することを決定しました。
このビジネスモデルの変革に伴い、重要な資産に関連する特定された脅威と脆弱性に基づいて、多数のセキュリティ対策が実施されました。これは、顧客の情報を保護するためです。
ビューティー社の従業員は機密保持契約書に署名しなければならなかった。さらに、同社はすべてのユーザーアクセス権限を見直し、許可された担当者のみが機密ファイルにアクセスできるようにし、新たな職務分掌図を作成した。
しかし、この移行はITチームにとって困難なものでした。eコマースモデルへの移行後まもなく、セキュリティインシデントが発生したのです。インシデントを調査した結果、チームは、マルウェア対策ソフトウェアが旧式であったために、攻撃者がファイルへのアクセス権を不正に取得し、顧客の名前や住所などの顧客情報を漏洩させたという結論に至りました。
ITチームは、旧型のマルウェア対策ソフトウェアの使用を中止し、同様の事態が発生した場合に悪意のあるコードを自動的に削除する新しいソフトウェアを導入することを決定しました。新しいソフトウェアは、社内のすべてのワークステーションにインストールされました。インストール後、チームは最新のマルウェア定義でソフトウェアを更新し、常に最新の状態を保つために自動更新機能を有効にしました。さらに、機密情報へのアクセス時にユーザーIDとパスワードを要求する認証プロセスを確立しました。
さらに、ビューティー社は、システムおよびネットワークセキュリティの重要性に対する意識を高めるため、ITチームや機密情報にアクセスするその他の従業員を対象に、情報セキュリティに関する啓発セッションを複数回実施した。

シナリオ2に基づくと、ITチームは機密情報へのアクセス時にユーザーIDとパスワードを要求するユーザー認証プロセスを確立することで、どの情報セキュリティ原則を確保しようとしているのでしょうか？
A. 誠実さ
B. 機密保持
C. 入手可能性
正解: **(**正解を表示します**)**
説明
機密性は、完全性、可用性とともに、CIAトライアドを構成する3つの情報セキュリティ原則の1つです。機密性とは、情報への不正アクセスや漏洩を防ぎ、閲覧または使用を許可された者のみがアクセスまたは使用できるようにすることです。機密性は、顧客、従業員、ビジネスパートナーなどの情報所有者のプライバシーと信頼を維持するために不可欠です。Beauty社のITチームは、機密情報へのアクセス時にユーザーIDとパスワードを要求するユーザー認証プロセスを確立することで、機密性の確保を目指しています。ユーザー認証とは、システムやネットワークへのアクセスを試みるユーザーの身元と資格情報を検証し、権限レベルに基づいてアクセスを許可または拒否するセキュリティ制御です。ユーザー認証は、ハッカー、競合他社、悪意のある内部関係者など、権限のないユーザーが、閲覧または使用すべきでない機密情報にアクセスするのを防ぐのに役立ちます。また、ユーザー認証は、誰がいつどの情報にアクセスしたかを記録する監査証跡を作成するのにも役立ち、説明責任とコンプライアンスの目的で有用です。
参考文献：
ISO/IEC 27001:2022 リードインプリメンターコースガイド1
ISO/IEC 27001:2022 リードインプリメンター情報キット2
ISO/IEC 27001:2022 情報セキュリティマネジメントシステム - 要求事項3 ISO/IEC 27002:2022 情報セキュリティ管理策の実施規範 情報セキュリティとは何か | ポリシー、原則、脅威 | Imperva1 情報セキュリティとは何か？定義、原則、および職務2 情報セキュリティとは何か？原則、種類 - KnowledgeHut3

質問: **61**
情報セキュリティ委員会は、次のうちどれを担当しますか？
A. ISMSの円滑な運用を確保する
B. 不適合の処理
C. 年間目標とISMS戦略を設定する
正解: **(**正解を表示します**)**

質問: **62**
シナリオ 4: L.JXfUI デザイン、QA およびソフトウェア テスト、モバイル アプリケーション開発を専門とする UX Software 社は、情報セキュリティ対策を改善する必要性を認識し、ISO/IEC 27001 に基づく ISMS を導入しました。この戦略的な取り組みは、業界標準およびベスト プラクティスに準拠し、社内外で共有される情報の機密性、可用性、および完全性を強化することを目的としていました。
ISMSをUX Softwareの既存プロセスに統合し、これらのプロセスがISMSのフレームワークに準拠するように調整されたことは、組織の情報セキュリティへの取り組みを強調する重要な節目となりました。UX Softwareは、ISMSフレームワークに沿うようこれらの手順を綿密に調整し、状況や文化に即した適切なものとなるよう配慮するとともに、不整合を回避しました。この積極的な姿勢は、従業員に安心感を与え、顧客からの信頼を高め、業務全体を通して機密データの保護を確実なものにしました。
UX Softwareの経営陣は、この取り組みを推進するため、ISMSの適用範囲をISO 1EC 27003に準拠させるべく行動を起こしました。UX Softwareの経営陣の主要メンバーであるSvenは、プロジェクトスポンサーの役割を担いました。これは、適切なリソースでISMSの実装を確実に実行するという重要な役割です。Svenのリーダーシップは、プロジェクトをISO 1EC 27003への準拠へと導く上で極めて重要な役割を果たしました。
UX Softwareは、情報セキュリティへの取り組みと並行して、セキュリティ管理策の技術仕様を適用性声明の正当化セクションに組み込みました。このアプローチは、ISO/IEC 27001の要求事項を満たすという同社のコミットメントを示し、セキュリティ管理策の徹底的な文書化と正当化を保証し、組織全体のセキュリティフレームワークを強化しました。さらに、UX Softwareは、是正措置の有効性を確保し、ISMS文書化情報を管理し、不適合に対処しながらISMSを継続的に改善する責任を負う委員会を設立しました。
ISO/IEC 27001に基づくISMSを導入することで、UX Softwareは情報セキュリティを向上させ、信頼できるパートナーとしての地位を強化しました。この情報セキュリティへの取り組みは、UX Softwareが社内関係者と大切な顧客の利益を守りながら、高品質なソフトウェアソリューションを提供することへの強い決意の証です。
シナリオ4によると、UX Software社はISO/IEC 27003のガイドラインに基づいてISMSの適用範囲を定義することに決定しました。定義された適用範囲はこれらのガイドラインに準拠していますか？
A. はい、彼らはISO/IEC 27003に従って範囲を定義しました。
B. いいえ、彼らはまず最終的な範囲を決定すべきでした
C. いいえ、経営陣代表者と改善を含む多段階アプローチに従うべきでした
正解: **(**正解を表示します**)**

質問: **63**
利害関係者を特定、分析、管理するために使用されるツールはどれですか？
A. 確率／影響マトリックス
B. 権力／利害マトリックス
C. 可能性／重症度マトリックス
正解: **(**正解を表示します**)**
パワー／インタレストマトリックスは、ISO/IEC 27001:2022 に準拠して利害関係者を特定、分析、管理するために使用できるツールです。パワー／インタレストマトリックスは、組織の情報セキュリティ目標との関連において、各利害関係者のパワーとインタレストのレベルをプロットした2次元図です。パワー／インタレストマトリックスは、組織が利害関係者の優先順位付け、彼らの期待とニーズの理解、適切なコミュニケーションおよびエンゲージメント戦略の策定に役立ちます。また、組織が利害関係者に関連する潜在的なリスクと機会を特定するのにも役立ちます。

質問: **64**
シナリオ：
エバーグリーン社は、自社の内部構造とニーズに合わせて、情報セキュリティポリシーの形式と命名規則をカスタマイズした。
これは許容範囲でしょうか？
A. いいえ - ポリシーの形式と命名規則は、実施前に外部監査人による承認を受ける必要があります。
B. いいえ - ポリシーは ISO/IEC 27001 で定義されたテンプレートに準拠する必要があります
C. はい、組織は組織のニーズを満たすこれらのポリシー文書の形式と名称を決定できます。
正解: **(**正解を表示します**)**

質問: **65**
あなたは別の会社に求人応募し、採用されました。契約書とともに、行動規範への署名を求められました。行動規範とは何でしょうか？
A. 行動規範は企業によって異なり、とりわけ情報システムの使用に関する行動規則を規定しています。
B. 行動規範は、従業員がどのように行動すべきかを規定するものであり、すべての企業で共通です。
C. 行動規範は労働契約の標準的な一部です。
正解: **(**正解を表示します**)**

質問: **66**

シナリオ7 :マサチューセッツ州ボストンに拠点を置くInfoSec社は、業務用電子機器、ゲーム、エンターテイメント製品を提供する多国籍企業です。複数の情報セキュリティインシデントが発生したことを受け、InfoSec社は専門家チームを編成し、将来起こりうるインシデントを防止するための対策を実施することを決定しました。
エマ、ボブ、アンナは、InfoSecの情報セキュリティチームの新しいメンバーとして採用されました。このチームは、セキュリティアーキテクチャチーム、インシデント対応チーム（IRT）、およびフォレンジックチームで構成されています。エマの仕事は、InfoSecがインシデントに効果的に対応できるよう、情報セキュリティ計画、ポリシー、プロトコル、およびトレーニングを作成することです。エマとボブはInfoSecの正社員ですが、アンナは外部コンサルタントとして契約しました。
ネットワークのエキスパートであるボブは、スクリーニングされたサブネットネットワークアーキテクチャを実装します。このアーキテクチャにより、ホストされているパブリックサービスが接続されている非武装地帯（DMZ）と、情報セキュリティ部門の公開アクセス可能なリソースが、プライベートネットワークから分離されます。これにより、情報セキュリティ部門は、潜在的な攻撃者が社内ネットワーク内で望ましくない事象を引き起こすのを阻止できるようになります。ボブはまた、予期せぬ事象が発生した状況、その事象が何に、あるいは誰に影響を与える可能性があるかなど、事象の性質を徹底的に評価する責任も負っています。
一方、アンナは、懲戒処分や法的措置の証拠として、また将来のインシデント防止のために、データ、レビュー、分析、レポートなどの記録を作成します。この作業を適切に行うためには、事前に会社の情報セキュリティインシデント管理ポリシーを理解しておく必要があります。このポリシーには、作成すべき記録の種類、保管場所、特定の記録の種類ごとに必要な形式や内容などが規定されています。
InfoSecが情報セキュリティ対策を強化する取り組みの一環として、アンナは重大な変更が提案された場合にのみ情報セキュリティリスク評価を実施し、その結果を文書化します。リスク評価プロセスが完了したら、アンナは情報セキュリティリスクに対処するための計画を策定・実施し、その対策結果を文書化する責任を負います。
さらに、情報セキュリティに関するコミュニケーション計画を実施するにあたり、InfoSecの経営陣は新製品開発のためのロードマップ作成にも責任を負いました。このアプローチにより、同社はセキュリティ対策を製品開発の取り組みと整合させることができ、事業運営のあらゆる側面にセキュリティを統合するという強い意志を示すことができました。
InfoSecは、Webまたはアプリケーションプログラミングインターフェース（API）を介してアクセスされるクラウドベースのアプリケーションを含むクラウドサービスモデルを採用しています。すべてのクラウドサービスはクラウドサービスプロバイダーによって提供され、データはInfoSecによって管理されます。これにより、特有のセキュリティ上の考慮事項が生じ、この環境においてデータとシステムが保護されるよう、情報セキュリティチームが最優先事項として取り組むことになります。
このシナリオに基づいて、次の質問に答えてください。

InfoSecは、情報セキュリティリスク対策計画に関して、ISO/IEC 27001の要件に準拠していますか？
A. はい、リスク対策計画を実施し、リスク対策の結果を文書化することで、ISO/IEC 27001の要求事項に準拠しています。
B. いいえ、リスク評価結果に関する文書化された情報のみを保持する必要があります。
C. いいえ、情報セキュリティリスク対策計画はトップマネジメントのみが策定すべきです。
正解: **A (**コメントを発表する**)**

質問: **67**
シナリオ10 :ProEBank
ProEBankは、包括的な銀行サービスで知られるオーストリアの金融機関です。
ウィーンに本社を置くProEBankは、同市の高度な技術と金融のエコシステムを拠点としています。セキュリティ体制を強化するため、ProEBankはISO/IEC 27001に基づく情報セキュリティマネジメントシステム（ISMS）を導入しました。ISMS導入から1年後、同社はISO/IEC 27001の認証を取得するために認証監査を申請することを決定しました。
監査に備えるため、同社はまず従業員に監査の実施を通知し、準備のための研修会を開催した。また、外部監査人が文書の確認を求めてきた際にすぐに提出できるよう、事前に文書化された情報も準備した。さらに、外部監査人が業務プロセスを理解し評価する上で役立つ知識を持つ従業員を特定した。
監査の計画段階で、ProEBank は認証機関から提供された割り当てられた監査員のリストを確認しました。リストを確認したところ、ProEBank は監査員の 1 名が以前銀行業界で ProEBank の競合企業で働いていたことから、潜在的な利益相反があることに気づきました。監査プロセスの完全性を確保するため、ProEBank は全く新しい監査チームが割り当てられるまで監査を受けることを拒否しました。これに対し、認証機関は利益相反を認め、監査チームの公平性を確保するために必要な調整を行いました。この問題が解決した後、監査チームは ISMS が規格の要件と会社の目標の両方を満たしているかどうかを評価しました。このプロセスでは、監査チームは文書化された情報のレビューに重点を置きました。
3 週間後、チームは被監査者の所在地を訪問し、ISMS が ISO/IEC 27001 の要求事項に適合しているかどうかを評価することを目的とした。ISMS は効果的に実装され、被監査者が情報セキュリティの目標を達成できるようにした。現地訪問後、チームは監査結論を作成し、軽微な不適合がいくつか検出されたことを被監査者に通知した。その後、監査チームリーダーは認証の勧告を発行した。
監査チームリーダーからの推薦を受け、認証機関は認証の可否を決定するための委員会を設置した。委員会は、監査チームのメンバー1名と、認証機関に所属する他の専門家2名で構成されていた。
ProEBankは、ISO/IEC 27001認証監査に備えるため、従業員への研修、文書の準備、監査をサポートする主要担当者の選定を行った。しかし、監査前に自己評価は実施しなかった。
質問：

ProEBankは、認証監査の準備において、すべてのベストプラクティスに従ったのでしょうか？
A. はい、当社は認証監査の準備において、あらゆるベストプラクティスに従いました。
B. いいえ、会社は監査に備えて自己評価も実施すべきでした。
C. いいえ、会社は従業員に今後の監査について通知すべきではありませんでした
正解: **(**正解を表示します**)**
ISO/IEC 27001:2022では正式な自己評価は義務付けられていませんが、ISO/IEC 27003やISMS導入ツールキットなどの導入ガイドに記載されている、広く認知されたベストプラクティスです。自己評価または内部監査シミュレーション：
組織がギャップを特定し、準備状況をテストし、正式な監査段階に入る前に監査担当者の信頼を築くのに役立ちます。」ProEBankはいくつかの優れた取り組みを行いましたが、自己評価を省略したことで準備状況に潜在的なギャップが生じ、予期せぬ問題が発生した場合に認証が遅れる可能性があります。
参考文献：
ISO/IEC 27003:2017 条項 11.1 - ISMSの準備状況とギャップ分析
ISMSツールキット - ステップ28：自己評価または模擬監査を実施する

質問: **68**
シナリオ2 :Beautyは、最近従来の小売販売からeコマースモデルに移行した化粧品会社です。経営陣は、自社で独自のプラットフォームを構築し、オンライン送金に対応したオンライン決済システムを運営する外部プロバイダーに決済処理を委託することを決定しました。
このビジネスモデルの変革に伴い、重要な資産に関連する特定された脅威と脆弱性に基づいて、多数のセキュリティ対策が実施されました。これは、顧客の情報を保護するためです。
ビューティー社の従業員は機密保持契約書に署名しなければならなかった。さらに、同社はすべてのユーザーアクセス権限を見直し、許可された担当者のみが機密ファイルにアクセスできるようにし、新たな職務分掌図を作成した。
しかし、この移行はITチームにとって困難なものでした。eコマースモデルへの移行後まもなく、セキュリティインシデントが発生したのです。インシデントを調査した結果、チームは、マルウェア対策ソフトウェアが旧式であったために、攻撃者がファイルへのアクセス権を不正に取得し、顧客の名前や住所などの顧客情報を漏洩させたという結論に至りました。
ITチームは、旧型のマルウェア対策ソフトウェアの使用を中止し、同様の事態が発生した場合に悪意のあるコードを自動的に削除する新しいソフトウェアを導入することを決定しました。新しいソフトウェアは、社内のすべてのワークステーションにインストールされました。インストール後、チームは最新のマルウェア定義でソフトウェアを更新し、常に最新の状態を保つために自動更新機能を有効にしました。さらに、機密情報へのアクセス時にユーザーIDとパスワードを要求する認証プロセスを確立しました。

さらに、ビューティー社は、システムおよびネットワークセキュリティの重要性に対する意識を高めるため、ITチームや機密情報にアクセスするその他の従業員を対象に、情報セキュリティに関する啓発セッションを複数回実施した。
上記のシナリオに基づいて、次の質問に答えてください。
事件の調査後、Beauty社は新しいマルウェア対策ソフトウェアをインストールすることにしました。この場合、どのようなセキュリティ対策が実施されたのでしょうか？
A. 予防
B. 探偵
C. 修正
正解: **(**正解を表示します**)**
上記のシナリオにおいて、セキュリティインシデント発生後にBeauty社が新たなマルウェア対策ソフトウェアを導入するという決定は、予防的制御に該当します。この種の制御は、悪意のあるコードを削除し、マルウェア感染から保護することで、将来のセキュリティインシデントを防止することを目的としています。新たなマルウェア対策ソフトウェアの目的は、潜在的な脅威から会社のシステムとデータを積極的に保護することであり、したがって予防措置の範疇に含まれます。

質問: **69**
シナリオ2 :Beautyは、最近従来の小売販売からeコマースモデルに移行した化粧品会社です。経営陣は、自社で独自のプラットフォームを構築し、オンライン送金に対応したオンライン決済システムを運営する外部プロバイダーに決済処理を委託することを決定しました。
このビジネスモデルの変革に伴い、重要な資産に関連する特定された脅威と脆弱性に基づいて、多数のセキュリティ対策が実施されました。これは、顧客の情報を保護するためです。
ビューティー社の従業員は機密保持契約書に署名しなければならなかった。さらに、同社はすべてのユーザーアクセス権限を見直し、許可された担当者のみが機密ファイルにアクセスできるようにし、新たな職務分掌図を作成した。
しかし、この移行はITチームにとって困難なものでした。eコマースモデルへの移行後まもなく、セキュリティインシデントが発生したのです。インシデントを調査した結果、チームは、マルウェア対策ソフトウェアが旧式であったために、攻撃者がファイルへのアクセス権を不正に取得し、顧客の名前や住所などの顧客情報を漏洩させたという結論に至りました。
ITチームは、旧型のマルウェア対策ソフトウェアの使用を中止し、同様の事態が発生した場合に悪意のあるコードを自動的に削除する新しいソフトウェアを導入することを決定しました。新しいソフトウェアは、社内のすべてのワークステーションにインストールされました。インストール後、チームは最新のマルウェア定義でソフトウェアを更新し、常に最新の状態を保つために自動更新機能を有効にしました。さらに、機密情報へのアクセス時にユーザーIDとパスワードを要求する認証プロセスを確立しました。

さらに、ビューティー社は、システムおよびネットワークセキュリティの重要性に対する意識を高めるため、ITチームや機密情報にアクセスするその他の従業員を対象に、情報セキュリティに関する啓発セッションを複数回実施した。
以下の記述のうち、Beauty社がインシデントの発生を回避するのに役立つ管理統制を実施していることを示唆しているのはどれですか？シナリオ2を参照してください。
A. ビューティー社の従業員は機密保持契約書に署名しました
B. ビューティーは、ITチームや機密情報にアクセスできる他の従業員向けに、情報セキュリティに関する意識向上セッションを複数回実施した。
C. ビューティーが職務分担表を更新しました
正解: **(**正解を表示します**)**
説明
管理統制とは、人間の行動に影響を与えることでセキュリティインシデントの発生を防止または軽減することを目的とした管理上の措置です。これには、ポリシー、手順、ガイドライン、基準、トレーニング、および啓発プログラムが含まれます。シナリオ2では、Beauty社はITチームおよび機密情報にアクセスできるその他の従業員向けに情報セキュリティ啓発セッションを実施することで、管理統制を実施しています。これらのセッションは、システムおよびネットワークセキュリティの重要性、潜在的な脅威と脆弱性、およびインシデントの発生を回避するために従うべきベストプラクティスについて従業員を教育することを目的としています。従業員の意識と知識レベルを高めることで、Beauty社は情報資産のセキュリティを損なう可能性のある人的ミスや過失を減らすことができます。
参照文献 :ISO/IEC 27001:2022 リードインプリメンターコース内容、モジュール7：ISO/IEC 27001:2022に基づくISMSの実装1 ;ISO/IEC 27001:2022 情報セキュリティ、サイバーセキュリティおよびプライバシー保護、条項7.2：能力2 ;ISO/IEC 27002:2022 情報セキュリティ管理策の実施規範、条項7.2.2：情報セキュリティ意識向上、教育および訓練3

質問: **70**
情報セキュリティ対策を効果的に実施するために必要な手順は次のうちどれですか？
A. リスク評価を実施する前にセキュリティ対策を実施する
B. 各管理策の実施スケジュールを作成する
C. サイバーセキュリティの専門知識を持つ外部業者を雇う
正解: **B (**コメントを発表する**)**
ISO/IEC 27001:2022では、情報セキュリティ管理策を選択したら、組織はその実施計画を策定しなければならないと規定されています。明確なスケジュールを策定することで、各管理策が効果的に実施され、責任とスケジュールが適切に管理されることが保証されます。
組織は、責任の割り当てや実施スケジュールの策定を含め、情報セキュリティ対策の実施計画を策定しなければならない。」
- ISO/IEC 27001:2022、6.2項、8.1項、および8.3項

質問: **71**
どのフィードバックが、経営陣によるレビューにおける情報セキュリティのパフォーマンスに特に関連していますか？
A. 不適合および是正措置
B. 継続的な改善の機会
C. リスク評価結果
正解: **(**正解を表示します**)**

質問: **72**
シナリオ7 :テキサスH&H社におけるインシデント対応
攻撃者がシステムにアクセスできないことを確認した後、セキュリティ管理者はフォレンジック分析を進めることにした。その結果、アクセスセキュリティシステムは脅威検出、特に将来起こりうる攻撃の原因となる可能性のある悪意のあるファイルの検出を想定して設計されていなかったことが判明した。
これらの調査結果に基づき、Texas H$H inc.は、将来のインシデントを回避するためにアクセスセキュリティシステムを修正し、同様のインシデントへの対応方法に関する従業員への指針となるインシデント管理ポリシーを情報セキュリティポリシーに組み込むことを決定しました。
上記のシナリオに基づいて、次の質問に答えてください。
シナリオ7に基づくと、テキサスH&H社は事件対応において他にどのような措置を講じるべきでしょうか？
A. 今後の是正措置の参考資料として、インシデントを記録 ·文書化する。
B. 更新された情報セキュリティポリシーは、会社の経営陣のみに伝達する。
C. 今後同様の事態が発生するリスクを排除するため、クラウドサービスの利用を停止することを決定した。
正解: **A (**コメントを発表する**)**

質問: **73**
シナリオ2 :
ビューティーは、美容業界で確固たる地位を築いている化粧品会社です。数十年前、自然な美しさを引き出す高品質なスキンケア、メイクアップ、パーソナルケア製品の開発に情熱を注ぎ、設立されました。長年にわたり、革新的な製品開発、顧客満足へのこだわり、そして倫理的で持続可能なビジネス慣行への献身によって、高い評価を得ています。
消費者の購買習慣が急速に変化する状況に対応するため、ビューティー社は従来の小売業からeコマースモデルへと移行しました。この戦略を実行するにあたり、ビューティー社は包括的な情報セキュリティリスク評価を実施し、事業戦略および目標に沿って、新たなeコマース事業に関連する潜在的な脅威と脆弱性を分析しました。
特定されたリスクに関して、当社は複数の情報セキュリティ対策を実施しました。機密性の高い顧客データの保護の重要性を強調するため、全従業員に機密保持契約への署名を義務付けました。また、ユーザーのアクセス権限を徹底的に見直し、権限のある担当者のみが

機密情報にアクセスできるようにしました。さらに、倉庫には貴重な製品や独自の製法が保管されているため、あらゆる破壊行為を未然に防ぐため、警報システムとリアルタイムアラート機能を備えた監視カメラを設置しました。
しばらくして、情報セキュリティチームは監査ログを分析し、新たに導入されたセキュリティ対策全体にわたる活動を監視・追跡しました。監査ログを調査・分析した結果、マルウェア対策ソフトウェアが古いために攻撃者がシステムにアクセスし、顧客の氏名や住所などの機密情報が漏洩していたことが判明しました。これを受け、ITチームはマルウェア対策ソフトウェアを、同様のインシデントが発生した場合に悪意のあるコードを自動的に削除できる新しいソフトウェアに置き換えました。新しいソフトウェアはすべてのワークステーションにインストールされ、最新のマルウェア定義で定期的に更新され、自動更新機能が有効になっています。また、機密情報へのアクセスには、ユーザーIDとパスワードを必要とする認証プロセスも導入されました。
調査の結果、ビューティー社の情報セキュリティマネージャーであるマヤは、職務記述書における情報セキュリティに関する責任が明確に定義されていないことを発見し、同社は直ちに対応策を講じた。eコマース事業がグローバル展開されることを認識し、ビューティー社は業界の法的、法令、規制、契約上の要件を綿密に調査し、遵守した。データプライバシー法、消費者保護法、国際貿易協定など、国内外の規制を考慮した。
これらの要件を満たすため、Beauty社は法律顧問とコンプライアンス専門家を雇用し、事業を展開するすべての市場において、同社が法的基準を遵守していることを継続的に監視・確保しました。さらに、Beauty社はITチームおよび機密情報にアクセスするその他の従業員向けに、情報セキュリティに関する意識向上セッションを複数回実施し、システムおよびネットワークセキュリティの重要性を強調しました。
シナリオ2に基づくと、Beauty社が評価しなかった情報セキュリティ要件はどれですか？
A. 法的、規制的、契約上の義務の遵守
B. リスク評価と組織戦略との整合性
C. 情報ライフサイクルの原則と目的
正解: **(**正解を表示します**)**

質問: **74**
リスク評価の結果に基づき、ソケット社は以下の決定を下しました。
* 大文字と小文字、記号、数字を含む12文字以上のパスワードの使用を義務付ける
* パスワードは少なくとも60日ごとに変更することを義務付ける
* IT部門が提供するネットワークドライブにファイルのバックアップコピーを保存する
顧客の個人データが保存されているクラウドストレージファイルにアクセスするユーザーには、別のネットワークを割り当てる。
クラウドストレージの利用に関連して、Socket Inc.にとって最も重要な資産は何ですか？
シナリオ5を参照してください。
A. クラウドストレージファイルにアクセスできる従業員
B. 顧客の個人データ

C. IT部門が提供するネットワークドライブ
正解: **(**正解を表示します**)**

質問: **75**
シナリオ6 :Skyver社は、ゲーム機、薄型テレビ、コンピューター、プリンターなどの電子製品を製造しています。情報セキュリティを確保するため、同社はISO/IEC 27001に基づいた情報セキュリティマネジメントシステム（ISMS）を導入することを決定しました。
同社の情報セキュリティマネージャーであるコリンは、情報セキュリティリスクとその軽減策について、社員向けに研修と啓発セッションを実施することを決定した。セッションでは、Skyverの情報セキュリティへの取り組み、フィッシングやマルウェア対策、クラウドインフラストラクチャとサービスのセキュリティ確保に関するセッションなど、さまざまなトピックが取り上げられた。特にクラウドにおける責任共有モデルや、ID管理、アクセス管理といった概念が詳しく解説された。コリンは、魅力的なプレゼンテーション、インタラクティブなディスカッション、実践的なデモンストレーションを通して研修と啓発セッションを構成し、社員がセキュリティの原則と実践について十分に理解できるよう努めた。
セッションの参加者の一人に、人事部に勤務するリサがいました。コリンはスカイバーの情報セキュリティポリシーと手順を誠実かつ公平に説明しましたが、リサは議論された内容の一部が専門的すぎると感じ、セッションを完全に理解できませんでした。そのため、彼女はしばしばトレーナーや同僚に追加のサポートを求めました。コリンはリサを励ますように、もう一度セッションに参加することを提案しました。
Skyverは、顧客の嗜好を理解し、電子製品に関するパーソナライズされた推奨を提供するために、AIソリューションの導入を検討してきました。その目的は、AI技術を活用して問題解決能力を高め、顧客に提案を行うことでした。この戦略的な取り組みは、データに基づいた洞察を通じて顧客体験を向上させるというSkyverのコミットメントに合致するものでした。
さらに、Skyverは、特定のサービスを社内の安全なインフラストラクチャでホストし、その他のサービスを外部の拡張性の高いプラットフォームでホストし、どこからでもアクセスできる柔軟なクラウドインフラストラクチャを求めていました。この構成により、多様な展開オプションが可能になり、Skyverの電子製品開発にとって不可欠な情報セキュリティが強化されます。
Skyverによると、ISMS導入計画における追加的な管理策の実施は成功裏に完了し、同社は運用モードへの移行準備が整ったとのことだ。Skyverは、この変更が社内においてどの程度重要であるかを判断する責任をコリンに委任した。
上記のシナリオに基づいて、次の質問に答えてください。
Skyver社は、ISMSの運用モードへの移行の重要性を判断するために適切な担当者を任命しましたか？
A. いいえ、この決定はISMS導入チームが責任を負うべきです。

B. はい、この変更の重要性については情報セキュリティマネージャーが判断する必要があります。
C. いいえ、この決定は経営陣が責任を負うべきです
正解: **B** (コメントを発表する)

質問: **76**
情報セキュリティリスクに関する以下の記述のうち、正しくないものはどれですか？
A. 情報セキュリティリスクとは、情報資産の脆弱性が脅威によって悪用される可能性に関連するものです。
B. 情報セキュリティリスクは、対処せずに、またはリスク対処の過程で容認することはできません。
C. 情報セキュリティリスクは、不確実性が情報セキュリティ目標に及ぼす影響として表現できる。
正解: **B** (コメントを発表する)
ISO/IEC 27001:2022によると、情報セキュリティリスクは、リスクの回避、修正、共有に加えて、リスク処理の4つの選択肢の1つとして受け入れることができます12。リスクの受容とは、組織がリスクを軽減するためのさらなる措置を講じることなく、リスクのレベルを容認することを決定することを意味します3。リスクの受容は、組織のリスク基準と残存リスクレベルに応じて、リスク処理プロセスの前、途中、または後に行うことができます4。
1: ISO 27001 リスクアセスメント | IT Governance UK 2: ISO 27001 リスクアセスメント: 7 ステップガイド - IT Governance UK ブログ 3: ISO 27001 条項 6.1.2 情報セキュリティリスクアセスメントプロセス 4: ISO 27001 リスクアセスメントとリスク対策: 完全ガイド - Advisera

質問: **77**
シナリオ 7: InfoSec は、マサチューセッツ州ボストンに本社を置く多国籍企業で、プロフェッショナル向け電子機器、ゲーム、エンターテイメント サービスを提供しています。InfoSec は、数々の情報セキュリティ インシデントに直面した後、将来起こりうるインシデントを防止するためのチームを設立し、対策を実施することを決定しました。Emma、Bob、Anna は、セキュリティ アーキテクチャ チーム、インシデント対応チーム

(IRT)、フォレンジック チームで構成される InfoSec の情報セキュリティ チームの新しいメンバーとして採用されました。Emma の仕事は、InfoSec がインシデントに効果的に対応できるようにするための情報セキュリティ計画、ポリシー、プロトコル、トレーニングを作成することです。Emma と Bob は InfoSec の正社員ですが、Anna は外部コンサルタントとして契約しています。
ネットワークのエキスパートであるボブは、スクリーニングされたサブネットネットワークアーキテクチャを導入します。このアーキテクチャは、ホストされているパブリックサービスが接続されている非武装地帯（DMZ）と、情報セキュリティ部門の公開アクセス可能なリソースを、プライベートネットワークから分離します。これにより、情報セキュリティ部門は、潜在的な攻撃者が社内ネットワーク内で望ましくない事象を引き起こすのを阻止できるようになります。ボブはまた、予期せぬ事象が発生した場合、その事象がどのように発生したか、そしてそれが何や誰に影響を与える可能性があるかといった詳細を含め、その事象の性質を徹底的に評価する責任も負っています。
アンナは、懲戒処分や法的措置のための証拠を保管し、将来のインシデントを防止するために、データ、レビュー、分析、レポートの記録を作成します。この作業を適切に行うためには、事前に会社の情報セキュリティインシデント管理ポリシーを理解しておく必要があります。このポリシーでは、作成する記録の種類、保管場所、特定の記録の種類ごとに必要な形式や内容などが規定されています。
このシナリオに基づいて、次の質問に答えてください。
ボブは担当業務に基づいて、どのチームに所属していると考えられますか？
A. 鑑識チーム
B. インシデント対応チーム
C. セキュリティアーキテクチャチーム
正解: **(**正解を表示します**)**

質問: **78**
情報セキュリティリスクに関する以下の記述のうち、正しくないものはどれですか？
A. 情報セキュリティリスクは、対処せずに、またはリスク対処の過程で容認することはできません。
B. 情報セキュリティリスクとは、情報資産の脆弱性が脅威によって悪用される可能性に関連するものです。
C. 情報セキュリティリスクは、不確実性が情報セキュリティ目標に及ぼす影響として表現できる。
正解: **(**正解を表示します**)**

質問: **79**
情報は様々な方法で入手・提供できます。情報の価値は、その信頼性によって決まります。情報の信頼性にはどのような側面があるのでしょうか？
A. 適時性、正確性、完全性

B. 可用性、完全性、機密性
C. 可用性、完全性、網羅性
D. 可用性、情報価値、機密性
正解: **(**正解を表示します**)**

質問: **80**
シナリオ2：
ビューティーは、美容業界で確固たる地位を築いている化粧品会社です。数十年前、自然な美しさを引き出す高品質なスキンケア、メイクアップ、パーソナルケア製品の開発に情熱を注ぎ、設立されました。長年にわたり、革新的な製品開発、顧客満足へのこだわり、そして倫理的で持続可能なビジネス慣行への献身によって、高い評価を得ています。
消費者の購買習慣が急速に変化する状況に対応するため、ビューティー社は従来の小売業からeコマースモデルへと移行しました。この戦略を実行するにあたり、ビューティー社は包括的な情報セキュリティリスク評価を実施し、事業戦略および目標に沿って、新たなeコマース事業に関連する潜在的な脅威と脆弱性を分析しました。
特定されたリスクに関して、当社は複数の情報セキュリティ対策を実施しました。機密性の高い顧客データの保護の重要性を強調するため、全従業員に機密保持契約への署名を義務付けました。また、ユーザーのアクセス権限を徹底的に見直し、権限のある担当者のみが機密情報にアクセスできるようにしました。さらに、倉庫には貴重な製品や独自の製法が保管されているため、あらゆる破壊行為を未然に防ぐため、警報システムとリアルタイムアラート機能を備えた監視カメラを設置しました。
しばらくして、情報セキュリティチームは監査ログを分析し、新たに導入されたセキュリティ対策全体にわたる活動を監視・追跡しました。監査ログを調査・分析した結果、マルウェア対策ソフトウェアが古いために攻撃者がシステムにアクセスし、顧客の氏名や住所などの機密情報が漏洩していたことが判明しました。これを受け、ITチームはマルウェア対策ソフトウェアを、同様のインシデントが発生した場合に悪意のあるコードを自動的に削除できる新しいソフトウェアに置き換えました。新しいソフトウェアはすべてのワークステーションにインストールされ、最新のマルウェア定義で定期的に更新され、自動更新機能が有効になっています。また、機密情報へのアクセスには、ユーザーIDとパスワードを必要とする認証プロセスも導入されました。
調査の結果、ビューティー社の情報セキュリティマネージャーであるマヤは、職務記述書における情報セキュリティに関する責任が明確に定義されていないことを発見し、同社は直ちに対応措置を講じた。
Beauty社は、自社のeコマース事業が世界規模に及ぶことを認識し、業界の法的、法令、規制、契約上の要件を綿密に調査し、遵守した。データプライバシー法、消費者保護法、国際貿易協定など、国内外の規制を考慮に入れた。
これらの要件を満たすため、ビューティー社は法律顧問やコンプライアンス専門家に投資し、事業を展開するすべての市場において、同社が法的基準を遵守していることを継続的に監視・確保した。

さらに、ビューティー社はITチームや機密情報にアクセスできる他の従業員向けに、情報セキュリティに関する意識向上セッションを複数回実施し、システムおよびネットワークセキュリティの重要性を強調した。
シナリオ2に基づくと、ビューティー社はインシデント調査中にどのような種類の制御措置を講じましたか？
A. 是正措置
B. 予防的管理
C. 探偵の操作
正解: **(**正解を表示します**)**

質問: **81**
シナリオ：
Reyae Ltdの従業員が、メールの自動入力候補の誤りにより、重要なビジネス戦略を含むメールを誤って競合他社に送信してしまった。このメールには、企業秘密や機密性の高い顧客データが含まれていた。メールを受け取った競合他社は、その情報を改ざんし、顧客を欺いて他社サービスに乗り換えさせようとした。
質問：
次の記述のうち、この状況で影響を受けるセキュリティ原則を正しく説明しているのはどれですか？
A. Reyae Ltdの機密情報が最初に漏洩し、競合他社の行為が誠実性の侵害につながった。
B. Reyae Ltdの信頼性が最初に損なわれ、競合他社の行動が可用性違反につながった。
C. Reyae Ltdの可用性が最初に損なわれたが、競合他社の行動により誠実性の侵害が発生した。
正解: **(**正解を表示します**)**
ISO/IEC 27002:2022によると、情報セキュリティは機密性、完全性、可用性（CIA）の原則に基づいています。機密性とは不正な情報漏洩を防止することであり、完全性とは情報の正確性と信頼性を確保することであり、可用性とは必要なときに情報にアクセスできることを保証することです。
この場合：
機密性の高いメールが誤って競合他社に送信されたため、機密性が損なわれた。
競合他社が顧客を誤解させるために専有データを改ざんしたことにより、完全性が侵害された。
これは、ISO/IEC 27002:2022、条項3.1.7（機密情報の定義と直接一致しており、
3.1.13（情報セキュリティ侵害）

質問: **82**
セキュリティインシデントの影響を推定する際に考慮すべき要素はどれですか？
A. イベントの期間
B. 結果の重大性
C. 確率

正解: (正解を表示します)

質問: **83**
シナリオ2 :NyvMarketingは、さまざまな業界の顧客に多様なサービスを提供するマーケティング会社です。デジタルマーケティング、ブランディング、市場調査の専門知識を活かし、革新的でインパクトのあるマーケティングキャンペーンを提供することで確固たる評判を築いてきました。マーケティング業界におけるデータセキュリティと情報保護の重要性の高まりを受け、同社はISMS 27001に基づくISMSを導入することを決定しました。
NyvMarketingはISMSを導入する際に、リソース不足という重大な課題に直面しました。この課題はISMSの目標を効果的に達成する上でリスクとなり、機密情報の保護に向けた同社の取り組みを損なう可能性がありました。この脅威に対処するため、NyvMarketingはリソース制約に関連するリスクを管理する担当者としてマイケルを任命するという積極的なアプローチを採用しました。
マイケルは、NyvMarket*ngにおけるISMS導入において、リソース不足の特定と対処、リスク軽減戦略の策定、効果的なリソース配分において極めて重要な役割を果たし、リソース不足に対する同社の回復力を強化した。
さらに、NyvMarketingは情報セキュリティにおける業界標準とベストプラクティスを優先し、ISO/IEC 27002ガイドラインを徹底的に遵守しました。卓越性とISO/IEC 27001の要件に基づいたこの取り組みは、NyvMarketingが最高水準の情報セキュリティガバナンスを維持するという強い意志を明確に示しています。
ISMS導入作業中、NyvMarketingは能力に関する要求事項（ISO/IEC 27001、7.2項に規定）の1つを除外することを選択しました。同社は、既存の従業員がISMS関連業務を遂行するために必要な能力を備えていると考えていましたが、この除外に対する正当な理由を提示しませんでした。さらに、ISO/IEC 27001の附属書Aに記載されている特定の管理策が実施されなかった際も、NyvMarketingはこれらの除外に対する適切な理由を提示しませんでした。
ISMS導入の過程で、NFMarketingは情報セキュリティに影響を与える可能性のある脆弱性を徹底的に評価しました。これらの脆弱性には、ストレージメディアの不十分なメンテナンスと不適切なインストール、機器の不十分な定期交換計画、不十分なソフトウェアテスト、および保護されていない通信回線が含まれていました。これらの脆弱性がデータセキュリティにリスクをもたらす可能性があることを認識したNFMarketingは、必要な制御と対策を実施することで、これらの特定の弱点に対処するための措置を講じました。上記のシナリオに基づいて、次の質問に答えてください。
シナリオ2において、NyvMarketingはISMS導入中にリソース不足の脅威に直面しました。この脅威は次のどのカテゴリに該当しますか？
シナリオ2によると、NyvMarketingにおけるマイケルの役割は何ですか？
A. インシデントマネージャー
B. ISMS監査員
C. リスク所有者

D. 危機管理担当者
正解: **C** (コメントを発表する)

質問: **84**
組織のインシデント管理プロセスは、情報セキュリティインシデントへの備えと対応を可能にするものです。さらに、組織は情報セキュリティ事象を評価するための手順を整備しています。ISO/IEC 27001によると、インシデント管理プロセスには他に何を含める必要があるでしょうか？
A. 情報セキュリティインシデントから得られた知識を活用するためのプロセス
B. 情報セキュリティインシデント対応チームを2つ設置する
C. サプライヤーとの契約で定められた、サプライヤーの情報セキュリティインシデントへの対応プロセス
正解: **(**正解を表示します**)**
ISO/IEC 27001によると、インシデント管理プロセスには、情報セキュリティインシデントから得られた知識を活用して将来のインシデントの発生確率や影響を軽減し、情報セキュリティの全体的なレベルを向上させるためのプロセスを含める必要があります。これは、組織がインシデントの根本原因分析を実施し、教訓を特定し、再発防止または影響軽減のための是正措置を実施する必要があることを意味します。また、組織はインシデント管理プロセスの結果を文書化して関係者に伝達し、リスク評価と対応計画をそれに応じて更新する必要があります。（ISO/IEC 27001 : 2022 リードインプリメンターのリソースから引用する必要があります）ISO/IEC 27001 : 2022 リードインプリメンター学習ガイドおよびドキュメント、具体的には：
ISO/IEC 27001:2022、10.2項 不適合および是正措置
ISO/IEC 27001:2022、附属書A.16 情報セキュリティインシデント管理、ISO/IEC TS 27022:2021、条項7.5.3.16 情報セキュリティインシデント管理プロセス、PECB ISO/IEC 27001 リードインプリメンターコース、モジュール9 :インシデント管理

質問: **85**
経営陣による評価に関する記述のうち、正しいものはどれですか？
A. 経営レビューは毎月実施しなければならない
B. 経営レビューは組織内のさまざまなレベルで実施されます
C. 経営陣は、経営評価プロセスの最終的な責任を組織で働く個人に委任することができる。
正解: **B** (コメントを発表する)

質問: **86**
シナリオ5 :Operazeは、世界中の様々な企業向けにアプリケーションを開発する小規模なソフトウェア開発会社です。最近、同社はデジタル環境での事業運営から生じる可能性のある情報セキュリティリスクを評価するため、リスクアセスメントを実施しました。侵入テスト、レスティングテスト、コードレビューなど、様々なテスト手法を用いて、同社はICT

システムにおけるいくつかの問題点を特定しました。これには、不適切なユーザー権限、セキュリティ設定の誤り、安全でないネットワーク構成などが含まれます。これらの問題を解決し、情報セキュリティを強化するため、OperazeはISO/IEC 27001に基づいた情報セキュリティマネジメントシステム（ISMS）を導入することを決定しました。
Operazeは小規模企業であるため、ITチーム全体がISMS導入プロジェクトに関与しました。まず、同社は業務要件と内部および外部環境を分析し、主要なプロセスと活動を特定し、関係者を特定して分析しました。さらに、Operazeの経営陣は、ISMSの範囲に会社のほとんどの部門を含めることを決定しました。定義された範囲には、組織的および物理的な境界が含まれます。ITチームは情報セキュリティポリシーを作成し、すべての関係者に伝達しました。さらに、セキュリティ問題の詳細を定めるための他の具体的なポリシーが開発され、すべての関係者に役割と責任が割り当てられました。
その後、人事部長はISMSによって作成される書類はISMSの価値に見合わないため、ISMSの導入を中止すべきだと主張した。しかし、経営陣はこの主張は妥当ではないと判断し、ISMSの利点を関係者全員に説明するための啓発セッションを開催した。
Operaze は、自社の物理サーバーをサードパーティのインフラストラクチャ上の仮想サーバーに移行することを決定しました。新しいクラウド コンピューティング ソリューションは、会社にさらなる変化をもたらしました。一方、Operaze の経営陣は、効果的な ISMS を導入するだけでなく、ISMS 運用のスムーズな実行も確保することを目指しました。この状況で、Operaze の経営陣は、情報セキュリティ戦略を実行するために外部の専門家のサービスが必要であると結論付けました。一方、IT チームは、ISMS の範囲の変更を開始し、会社のプロセスに必要な変更を実施することを決定しました。
シナリオ5に基づき、OperazeはISMSの円滑な運用を確保するために、どの委員会を設置すべきでしょうか？
A. 情報セキュリティ委員会
B. 運営委員会
C. 運営委員会
正解: **(**正解を表示します**)**
ISO/IEC 27001:2022の5.1項によれば、組織の最高経営陣はISMSのリーダーシップとコミットメントを確保する責任を負います。ただし、最高経営陣は、ISMSを監督し、その導入と運用に関するガイダンスとサポートを提供する情報セキュリティ委員会に、その責任の一部を委任することができます。情報セキュリティ委員会には、組織のさまざまな部門、機能、または階層の代表者、および外部の専門家やコンサルタントが含まれる場合があります。情報セキュリティ委員会は、次のようなさまざまな役割と責任を担う可能性があります。
情報セキュリティポリシーと目標の設定
リスク評価およびリスク処理の方法論と基準の承認 リスク評価およびリスク処理の結果と計画のレビューと承認 ISMS のパフォーマンスと有効性の監視と評価 内部および外部監査計画とレポートのレビューと承認 是正措置と予防措置の開始と承認 すべての関係者への ISMS の伝達と促進 ISMS が組織の戦略的方向性と目標に合致していることの確保

ISMS に必要なリソースと能力の確保 ISMS の継続的な改善の確保 したがって、シナリオ 5 では、Operaze は ISMS の円滑な運用を確保するために情報セキュリティ委員会を作成する必要があります。この委員会は、ISMS の実装と運用に必要なリーダーシップ、ガイダンス、およびサポートを提供します。

質問: **87**
ISMSモニタリングの文脈において、「情報ニーズ」は通常どのように定義されるのでしょうか？
A. 詳細な技術仕様として
B. 監視対象となる制御項目の事前定義リスト
C. 高度なセキュリティに関する質問または声明として
正解: **C** (コメントを発表する)
ISMS（情報セキュリティマネジメントシステム）のモニタリングにおいて、「情報ニーズ」とは、通常、経営陣が意思決定を支援するために回答を求める、高レベルのセキュリティに関する質問または声明として定義されます。これは、どのような情報が必要で、なぜ必要なのかを明確にするものであり、情報の技術的な測定方法を具体的に示すものではありません。
ISO/IEC 27001:2022 9.1項 - モニタリング、測定、分析および評価では、組織は以下を決定する必要がある。
* 監視および測定する必要があるもの、
* 監視および測定方法、
* 監視および測定を実施する場合、
* そして、結果を分析・評価する時期。
情報ニーズは、指標や測定基準に先行する。例としては以下のようなものがある。
「アクセス制御は不正アクセスを防止していますか？」
* 「インシデント対応はタイムリーかつ効果的ですか？」
これらは高度な質問であり、技術仕様（オプションA）でも、事前定義された管理リスト（オプションB）でもありません。指標、ダッシュボード、KPIは、情報ニーズが定義された後に導き出されます。
このアプローチにより、モニタリングがビジネスに関連性があり、リスクに焦点を当てたものとなり、測定が目標および経営陣のレビュー要件と整合することが保証されます。

質問: **88**
これらの信頼性の側面のうち、「完全性」はどれに該当しますか？
A. 機密保持
B. 誠実さ
C. 入手可能性
D. 独占権
正解: (正解を表示します)

質問: **89**
NyvMarketingは、ISO/IEC 27001認証を取得するために、ISO/IEC 27002のガイドラインに従う必要がありますか？
A. いいえ、ISO/IEC 27001認証にはISO/IEC 27002ガイドラインへの準拠は必須ではありません。
B. はい、ISO/IEC 27001の要件です。
C. はい、ISO/IEC 27001の附属書Aに規定されている管理策はISO/IEC 27002の管理策と一致しているためです。
D. はい、ISO/IEC 27002は監査可能な規格です。
正解: **(**正解を表示します**)**
ISO/IEC 27001:2022は、情報セキュリティマネジメントシステム（ISMS）の認証規格です。ISO/IEC 27002は、組織がISO/IEC 27001の附属書Aに記載されている管理策を実施するためのガイドラインとベストプラクティスを提供しますが、ISO/IEC 27001認証を取得するためにISO/IEC 27002に従うことは必須ではありません。組織は、リスク評価に基づいて、附属書Aから適切な管理策、または必要に応じてその他の管理策を選択して実施する必要があります。ISO/IEC 27002はガイダンスとして機能しますが、それ自体は監査または認証の要件ではありません。
附属書Aに記載されている管理策は網羅的なものではなく、追加の管理策が必要となる場合があります。ISO/IEC 27002は実施に関するガイダンスを提供するものであり、ISO/IEC 27001の認証取得に必須ではありません。」
- ISO/IEC 27001:2022、序文および6.1.3項 ;ISO/IEC 27002:2022、前書き

質問: **90**
情報セキュリティポリシー策定ライフサイクルにおける最初の段階は何ですか？
A. 政策構築
B. 政策立案／ニーズ評価
C. 政策実施
D. リスク評価
正解: **B (**コメントを発表する**)**

質問: **91**
ISO/IEC 27001に基づいたISMSを導入するために、組織はどの手法を用いるべきでしょうか？
A. 組織の規模に適したアプローチ
B. 12ヶ月以内にISMSの導入を可能にするあらゆるアプローチ
C. 標準で提供されるアプローチのみ
正解: **(**正解を表示します**)**
説明

ISO/IEC 27001:2022は、ISMSを導入するための特定のアプローチを規定するものではなく、組織の状況、範囲、および目的に合わせて調整できる一連の要求事項とガイドラインを提供するものです。
したがって、組織は、規格の要件を満たし、ISMSの意図する成果を達成できる限り、その範囲に適したあらゆるアプローチを採用することができます。また、そのアプローチは、利害関係者のニーズと期待、情報セキュリティに関連するリスクと機会、および組織の法的義務と規制上の義務も考慮する必要があります。
参照資料：ISO/IEC 27001:2022、4.1項；PECB ISO/IEC 27001 リードインプリメンターコース、モジュール4、スライド9。

質問: **92**
シナリオ8：サンディー社は、米国カリフォルニア州に本社を置くバイオ医薬品企業です。ヒト治療薬分野における先駆的な業績で知られるサンディー社は、特に心血管疾患、腫瘍学、骨の健康、炎症といった分野における重要な医療課題への取り組みに重点を置いています。
SunDeeは、過去2年間、ISO/IEC 27001に基づいた効果的な情報セキュリティ管理システム（ISMS）を維持することで、データセキュリティとデータ完全性に対する取り組みを示してきました。
再認証監査の準備として、SunDee社は内部監査を実施しました。同社の経営陣は、過去6か月間コンプライアンス部門の日常業務を積極的に管理してきたアレックスを内部監査員に任命しました。この二重の役割を担うアレックスには、コンプライアンスを確保する監査を実施するとともに、業務効率を向上させるための有益な提言を行う任務が与えられています。
内部監査において、いくつかの不適合事項が特定された。これらに包括的に対処するため、当社は監査チームリーダーと緊密に連携しながら、各不適合事項に対する改善計画を作成した。
サンディー社の経営陣は、ISMS（情報セキュリティマネジメントシステム）の適切性、十分性、効率性を評価するため、包括的な見直しを実施しました。この見直しは、定期的な経営会議に組み込まれました。

監査報告書、行動計画、レビュー結果などの重要な文書は、会議前に全メンバーに配布されました。議題は、過去のレビュー活動の状況、ISMSに影響を与える変更点、フィードバック、ステークホルダーからの意見、改善の機会などを網羅していました。ISMSの改善を目的とした決定と行動が下され、ISMSコーディネーターと内部監査チームがフォローアップ行動計画の作成において重要な役割を果たし、その後、経営陣によって承認されました。
レビュー結果を受けて、SunDeeは速やかに是正措置を実施し、情報セキュリティ対策を強化しました。さらに、組織の情報セキュリティ管理を監視するために不可欠な主要業績評価指標（KPI）の概要を高レベルで把握できるダッシュボードツールを導入しました。これらの指標には、セキュリティインシデント、そのコスト、システム脆弱性テスト、不適合検出、解決時間に関する指標が含まれており、監視活動の効果的な記録、報告、追跡を容易にしました。また、SunDeeは進行中のプロジェクトの進捗状況と成果を評価するための包括的な測定プロセスに着手し、すべてのプロセスにわたって広範な測定を実施しました。経営陣は、測定に寄与するデータの所有者であることに加えて、情報に責任を負う担当者が、これらの測定活動の実行責任者にも指定されることを決定しました。
上記のシナリオに基づいて、次の質問に答えてください。
SunDeeのアプローチは、ISMSの有効性を評価および維持するためのベストプラクティスに合致しているでしょうか？
A. はい、ISMSの目標を達成するには包括的なカバレッジが不可欠だからです。
B. いいえ、対策が多すぎるとSunDeeの焦点がずれ、本当に重要なことが見えにくくなるからです。
C. はい、多様な対策を講じることで、潜在的なセキュリティリスクを見落とす可能性を最小限に抑えることができるからです。
正解: **C** (コメントを発表する)

質問: **93**
シナリオ2 :Beautyは、最近従来の小売販売からeコマースモデルに移行した化粧品会社です。経営陣は、自社で独自のプラットフォームを構築し、オンライン送金に対応したオンライン決済システムを運営する外部プロバイダーに決済処理を委託することを決定しました。
このビジネスモデルの変革に伴い、重要な資産に関連する特定された脅威と脆弱性に基づいて、多数のセキュリティ対策が実施されました。これは、顧客の情報を保護するためです。
ビューティー社の従業員は機密保持契約書に署名しなければならなかった。さらに、同社はすべてのユーザーアクセス権限を見直し、許可された担当者のみが機密ファイルにアクセスできるようにし、新たな職務分掌図を作成した。
しかし、この移行はITチームにとって困難なものでした。eコマースモデルへの移行後まもなく、セキュリティインシデントが発生したのです。インシデントを調査した結果、チームは、マルウェア対策ソフトウェアが旧式であったために、攻撃者がファイルへのアクセス

権を不正に取得し、顧客の名前や住所などの顧客情報を漏洩させたという結論に至りました。
ITチームは、旧型のマルウェア対策ソフトウェアの使用を中止し、同様の事態が発生した場合に悪意のあるコードを自動的に削除する新しいソフトウェアを導入することを決定しました。新しいソフトウェアは、社内のすべてのワークステーションにインストールされました。インストール後、チームは最新のマルウェア定義でソフトウェアを更新し、常に最新の状態を保つために自動更新機能を有効にしました。さらに、機密情報へのアクセス時にユーザーIDとパスワードを要求する認証プロセスを確立しました。
さらに、ビューティー社は、システムおよびネットワークセキュリティの重要性に対する意識を高めるため、ITチームや機密情報にアクセスするその他の従業員を対象に、情報セキュリティに関する啓発セッションを複数回実施した。
シナリオ2によると、Beautyはすべてのユーザーアクセス権限を確認しました。これはどのような種類の制御ですか？
A. 探偵および事務
B. 是正および管理
C. 法律および技術
正解: **B** (コメントを発表する)
* 予防的制御 :これらは、セキュリティインシデントの発生を防止または抑止したり、発生確率を低減することを目的とした制御です。予防的制御の例としては、暗号化、ファイアウォール、ロック、ポリシーなどがあります。
* 検出制御 :これらは、セキュリティインシデントの発生またはその兆候を検出または発見することを目的とした制御です。検出制御の例としては、ログ、アラーム、監査などがあります。
* 是正措置 :これらは、セキュリティインシデント発生後に資産またはプロセスの正常な状態を修正または復元したり、その影響を軽減したりすることを目的とした措置です。是正措置の例としては、バックアップ、復旧計画、インシデント対応チームなどがあります。
* 管理上のコントロール :これらは、ポリシー、手順、役割、責任、意識向上、トレーニングなど、情報セキュリティの管理とガバナンスに関わるコントロールです。
* 技術的制御: これらは、暗号化、ファイアウォール、マルウェア対策、認証など、情報セキュリティを実装するためにテクノロジーやソフトウェアを使用する制御です。
* 物理的制御: これらは、物理的な資産や場所を保護するための制御です。
* ロック、フェンス、カメラ、警備員などに対する不正アクセス、損傷、盗難。
* 法的管理: これらは、プライバシー法、データ保護法、機密保持契約など、情報セキュリティに関連する法律、規制、契約、または合意の遵守を含む管理です。
参考文献 :
* ISO/IEC 27001:2022 - 情報セキュリティ、サイバーセキュリティおよびプライバシー保護 - 情報セキュリティマネジメントシステム - 要求事項

質問: **94**

シナリオ 1: HealthGenic は、ウェブベースの医療ソフトウェアを使用して乳幼児から成人初期までの個人の健康と成長をモニタリングする小児科クリニックです。このソフトウェアは、予約のスケジュール設定、カスタマイズされた医療レポートの作成、患者のデータと病歴の保存、およびすべての関係者とのコミュニケーションにも使用されます。
[^両親、他の医師、医療検査技師を含む関係者。
先月、HealthGenicはソフトウェアにアクセスするユーザー数の増加により、何度かサービスの中断に見舞われた。同社がソフトウェアを使用する際に直面したもう一つの問題は、複雑なユーザーインターフェースであり、訓練を受けていない従業員にとっては使いこなすのが難しいと感じられた。
HealthGenicの経営陣は、この問題について直ちにソフトウェア開発会社に報告した。ソフトウェア会社は問題を修正したが、その過程でHealthGenicの患者に関する機密情報を含む一部のファイルを改変してしまった。その結果、医療報告書が不完全かつ不正確になり、さらに重要なことに、患者のプライバシーが侵害された。
上記のシナリオに基づいて、次の質問に答えてください。
シナリオ 1 によると、(1)_____ を検出するために、アンティークスは (2) を実施すべきだった。
A. （1パッチ。（2アクセス制御ソフトウェア
B. （1ネットワークへの侵入。（？）侵入検知ステム
C. 1）技術的な脆弱性。2）ネットワーク侵入
正解: **(**正解を表示します**)**

質問: **95**
シナリオ 7: InfoSec は、マサチューセッツ州ボストンに本社を置く多国籍企業で、プロフェッショナル向け電子機器、ゲーム、エンターテイメント サービスを提供しています。InfoSec は、数々の情報セキュリティ インシデントに直面した後、将来起こりうるインシデントを防止するためのチームを設立し、対策を実施することを決定しました。Emma、Bob、Anna は、セキュリティ アーキテクチャ チーム、インシデント対応チーム (IRT)、フォレンジック チームで構成される InfoSec の情報セキュリティ チームの新しいメンバーとして採用されました。Emma の仕事は、InfoSec がインシデントに効果的に対応できるようにするための情報セキュリティ計画、ポリシー、プロトコル、トレーニングを作成することです。Emma と Bob は InfoSec の正社員ですが、Anna は外部コンサルタントとして契約しています。
ネットワークのエキスパートであるボブは、スクリーニングされたサブネットネットワークアーキテクチャを導入します。このアーキテクチャは、ホストされているパブリック サービスが接続されている非武装地帯 (DMZ) と、情報セキュリティ部門の公開アクセス可能なリソースを、プライベートネットワークから分離します。これにより、情報セキュリティ部門は、潜在的な攻撃者が社内ネットワーク内で望ましくない事象を引き起こすのを阻止できるようになります。ボブはまた、予期せぬ事象が発生した場合、その事象がどのよ

うに発生したか、そしてそれが何や誰に影響を与える可能性があるかといった詳細を含め、その事象の性質を徹底的に評価する責任も負っています。
アンナは、懲戒処分や法的措置のための証拠を保管し、将来のインシデントを防止するために、データ、レビュー、分析、レポートの記録を作成します。この作業を適切に行うためには、事前に会社の情報セキュリティインシデント管理ポリシーを理解しておく必要があります。このポリシーでは、作成する記録の種類、保管場所、特定の記録の種類ごとに必要な形式や内容などが規定されています。
シナリオ7に基づくと、InfoSecは外部コンサルタントとしてAnnaと契約しました。彼女の業務内容に基づくと、この行為はISO/IEC 27001°に準拠していますか？
A. いいえ、事件対応や鑑識分析のスキルは社内で育成する必要があります。
B. はい、法医学的調査は内部で行うことも、外部のコンサルタントを利用して行うことも可能です。
C. はい、組織は基準で定められているとおり、フォレンジック調査に外部コンサルタントを利用しなければなりません。
正解: **(**正解を表示します**)**
説明
ISO/IEC 27001:2022の8.2.3項によれば、組織は以下の活動を含むインシデント対応プロセスを確立し、維持しなければならない。
a) インシデント対応の計画と準備（役割と責任の定義、コミュニケーションチャネルの確立、トレーニングと意識向上の提供を含む）。b) 情報セキュリティイベントと脆弱性の検出と報告。c) 情報セキュリティインシデントの評価と決定。d) 事前定義された手順に従って情報セキュリティインシデントに対応。e) 情報セキュリティインシデントから学ぶ（根本原因の特定、是正措置の実施、インシデント対応プロセスの改善を含む）。f) 該当する場合、証拠を収集。
本規格では、インシデント対応プロセスを内部で行うべきか外部で行うべきかについては規定していません。組織が、プロセスが効果的であり、情報セキュリティの目標を満たしていることを保証すれば問題ありません。したがって、組織は、外部コンサルタントが組織のポリシーと手順を遵守し、関連情報の機密性、完全性、可用性を保護する限り、フォレンジック調査に外部コンサルタントを利用することを決定できます。
参照：ISO/IEC 27001:2022、8.2.3項；PECB ISO/IEC 27001 リードインプリメンター学習ガイド、8.2.3項。

質問: **96**
ある組織は、全従業員を対象に情報セキュリティに関する意識向上研修を毎月実施することを決定した。しかし、これらの研修に参加した従業員のうち、試験に合格できたのはわずか45%だった。
そのパーセンテージは何を表していますか？
A. 測定対象
B. 属性

C. パフォーマンス指標
正解: **C** (コメントを発表する)
ISO/IEC 27001:2022規格によれば、パフォーマンス指標とは 活動、プロセス、システム、または組織の有効性または効率性に関する情報を提供する指標」です 3.35項)。パフォーマンス指標は、測定可能、関連性、達成可能性、現実性、期限 SMART)を備えている必要があります。この場合、試験に合格した従業員の割合は、情報セキュリティ意識向上およびトレーニングセッションの有効性を測定するパフォーマンス指標です。これは、セッションが意図した学習成果をどの程度達成したか、また従業員が情報セキュリティの概念と実践をどの程度理解したかを示します。
参考文献：
* ISO/IEC 27001:2022、情報セキュリティ、サイバーセキュリティおよびプライバシー保護 - 情報セキュリティマネジメントシステム - 要求事項1
* ISO/IEC 27001 リードインプリメンター情報キット
* ISO 27001 ISMSの主要業績評価指標2

質問: **97**
ある金融機関のIT部門は、潜在的なセキュリティ侵害を回避するために予防的な対策を実施することを決定しました。そのため、開発、テスト、運用機器を分離し、オフィスを安全に管理し、暗号鍵を使用しました。しかし、セキュリティを強化し、セキュリティ侵害のリスクを最小限に抑えるためのさらなる対策を模索しています。以下のどの対策が、IT部門がこの目的を達成するのに役立つでしょうか？
A. 熱、煙、火災、水に関連する危険を検知する警報装置
B. すべてのシステムのパスワードをすべて変更する
C. 機密ファイルへのアクセスを制限するアクセス制御ソフトウェア
正解: **C** (コメントを発表する)
アクセス制御ソフトウェアは、ユーザーの身元、役割、または権限レベルに基づいて機密ファイルや情報へのアクセスを制限するように設計された予防的制御の一種です。アクセス制御ソフトウェアは、権限のないユーザーによる情報の閲覧、変更、削除を防止することで、情報の機密性、完全性、可用性を保護します。また、アクセス制御ソフトウェアは、誰がいつどの情報にアクセスしたかを記録する監査証跡を作成するのにも役立ち、これは説明責任やコンプライアンスの目的で有用です。
ある金融機関のIT部門は、潜在的なセキュリティ侵害を回避するために予防的な対策を実施することを決定しました。そのため、開発、テスト、運用機器を分離し、オフィスを厳重に管理し、暗号鍵を使用しました。しかし、セキュリティをさらに強化し、セキュリティ侵害のリスクを最小限に抑えるための追加措置を模索しています。アクセス制御ソフトウェアを導入することで、機密ファイルや情報に保護層を追加し、権限のある担当者のみがアクセスできるようにすることで、IT部門はこの目標を達成できるでしょう。
参照：
ISO/IEC 27001:2022 リードインプリメンターコースガイド1

ISO/IEC 27001:2022 リードインプリメンター情報キット2
ISO/IEC 27001:2022 情報セキュリティマネジメントシステム - 要求事項3 ISO/IEC 27002:2022 情報セキュリティ管理策の実施規範4 情報セキュリティ管理策とは？ - SecurityScorecard4 情報セキュリティ管理策の種類とは？ - RiskOptics2 完全性とは、情報と処理方法の正確性と完全性を保護する特性です。情報が不正または意図しない方法で変更または破壊された場合、完全性の侵害が発生します。このケースでは、ダイアナが誤って顧客の許可なく注文の詳細を変更したため、顧客は間違った製品を受け取りました。これは、顧客の注文に関する情報が正確または完全ではなかったことを意味し、したがって、完全性の原則が侵害されました。可用性と機密性は、他の2つの情報セキュリティ原則ですが、このケースでは侵害されていません。可用性とは、権限のあるエンティティが要求に応じてアクセスおよび使用できる特性であり、機密性とは、権限のない個人またはシステムへの情報の開示を防止する特性です。

質問: **98**
シナリオ 1: HealthGenic は、ウェブベースの医療ソフトウェアを使用して乳幼児から成人初期までの個人の健康と成長をモニタリングする小児科クリニックです。このソフトウェアは、予約のスケジュール設定、カスタマイズされた医療レポートの作成、患者のデータと病歴の保存、および両親、他の医師、医療検査スタッフを含むすべての関係者とのコミュニケーションにも使用されます。
先月、HealthGenicはソフトウェアにアクセスするユーザー数の増加により、何度かサービスの中断に見舞われた。同社がソフトウェアを使用する際に直面したもう一つの問題は、複雑なユーザーインターフェースであり、訓練を受けていない従業員にとっては使いこなすのが難しいと感じられた。
HealthGenicの経営陣は、この問題について直ちにソフトウェア開発会社に報告した。ソフトウェア会社は問題を修正したが、その過程でHealthGenicの患者に関する機密情報を含む一部のファイルを改変してしまった。その結果、医療報告書が不完全かつ不正確になり、さらに重要なことに、患者のプライバシーが侵害された。
シナリオ1に基づくと、HealthGenicの情報整合性が失われた場合、どのような影響が生じる可能性がありますか？
A. 業務の中断およびパフォーマンスの低下
B. 不完全または不正確な医療報告書
C. サービスの中断と複雑なユーザーインターフェース
正解: **(正解を表示します)**

質問: **99**
シナリオ10 :NetworkFuse社は、ネットワークハードウェアの開発、製造、販売を行っています。同社は、ISO/IEC 27001の要件に基づく運用情報セキュリティ管理システム（ISMS）と、ISO 9001に基づく品質管理システム（QMS）を約2年間運用してきました。最近、ISO/IEC 27001とISO 9001の両方の認証を取得するために、統合認証監査を申請しました。

認証機関を選定した後、NetworkFuseは従業員を監査に向けて準備させた。経営陣の判断により、監査前に自己評価を実施する必要はないと判断されたため、同社は自己評価を行わないことを決定した。さらに、内部監査報告書や経営陣によるレビュー、導入済みの技術、ISMSおよびQMSの一般的な運用状況など、文書化された情報が利用可能であることを確認した。
しかし、同社は認証機関に対し、文書を社外に持ち出すことはできないと要請した。しかし、NetworkFuseが割り当てられた監査チームリーダーを拒否し、その交代を要請したため、監査は予定された日数内には実施されなかった。同社は、同じ監査チームリーダーが主要な競合他社に認証の勧告を出しており、これは同社の経営陣にとって潜在的な利益相反であると主張した。認証機関はこの要請を受け入れなかった。シナリオ10によると、NetworkFuseは認証機関に対し、すべての文書をオンサイトでのみレビューするよう要請した。これは許容できるだろうか？
A. はい、被監査者は文書レビューを現地で行うよう要求することができます。
B. はい、監査チームが正式に機密保持契約に署名した場合に限ります。
C. いいえ、認証機関が文書審査をオンサイトで行うかオフサイトで行うかを決定します。
正解: **A** (コメントを発表する)
ISO/IEC 27001:2022規格によれば、認証機関は、文書化された情報のレビューを含め、監査の計画と実施に責任を負います。認証機関は、監査の目的、範囲、基準、およびリスクに応じて、文書のレビューをオンサイトまたはオフサイトで実施するかどうかを決定することができます。
被監査者は、機密保持またはセキュリティ上の正当な理由がない限り、文書へのアクセスに制限を課してはならない。ただし、そのような制限は監査前に合意されるべきであり、監査の有効性および公平性を損なうものであってはならない。

質問: **100**
シナリオ5 :Operazeは、世界中の様々な企業向けにアプリケーションを開発する小規模なソフトウェア開発会社です。最近、同社はデジタル環境での事業運営から生じる可能性のある情報セキュリティリスクを評価するため、リスクアセスメントを実施しました。侵入テスト、レスティングテスト、コードレビューなど、様々なテスト手法を用いて、同社はICTシステムにおけるいくつかの問題点を特定しました。これには、不適切なユーザー権限、セキュリティ設定の誤り、安全でないネットワーク構成などが含まれます。これらの問題を解決し、情報セキュリティを強化するため、OperazeはISO/IEC 27001に基づいた情報セキュリティマネジメントシステム（ISMS）を導入することを決定しました。
Operazeは小規模企業であるため、ITチーム全体がISMS導入プロジェクトに関与しました。まず、同社は業務要件と内部および外部環境を分析し、主要なプロセスと活動を特定し、関係者を特定して分析しました。さらに、Operazeの経営陣は、同社のほとんどの部門をISMSの対象範囲に含めることを決定しました。
定義された範囲には、組織的境界と物理的境界が含まれていました。ITチームは情報セキュリティポリシーを作成し、関係するすべての利害関係者に周知しました。さらに、セキュリ

ティ問題の詳細を定めるためのその他の具体的なポリシーが策定され、すべての利害関係者に役割と責任が割り当てられました。
その後、人事部長はISMSによって作成される書類はISMSの価値に見合わないため、ISMSの導入を中止すべきだと主張した。しかし、経営陣はこの主張は妥当ではないと判断し、ISMSの利点を関係者全員に説明するための啓発セッションを開催した。
Operaze は、自社の物理サーバーをサードパーティのインフラストラクチャ上の仮想サーバーに移行することを決定しました。新しいクラウド コンピューティング ソリューションは、会社にさらなる変化をもたらしました。一方、Operaze の経営陣は、効果的な ISMS を導入するだけでなく、ISMS 運用のスムーズな実行も確保することを目指しました。この状況で、Operaze の経営陣は、情報セキュリティ戦略を実行するために外部の専門家のサービスが必要であると結論付けました。一方、IT チームは、ISMS の範囲の変更を開始し、会社のプロセスに必要な変更を実施することを決定しました。
OperazeのISMS導入チームは、情報セキュリティポリシーの策定後、次にどのようなステップを踏むべきでしょうか？シナリオ5を参照してください。
A. 情報セキュリティポリシーを実施する
B. 情報セキュリティポリシーについて経営陣の承認を得る
C. 情報セキュリティポリシーを全従業員に周知徹底する
正解: **(**正解を表示します**)**
ISO/IEC 27001:2022の主たる実施者によると、情報セキュリティポリシーは、組織の情報セキュリティに関する目標、原則、およびコミットメントを定義する高レベルの文書です。このポリシーは、組織の戦略的方向性および状況に合致している必要があり、情報セキュリティ目標の設定とISMSの確立のための枠組みを提供するものでなければなりません。また、このポリシーは、ISMSとそのパフォーマンスに最終的な責任を負う経営陣によって承認される必要があります。
したがって、情報セキュリティポリシーの草案作成後、OperazeのISMS導入チームが次に取るべきステップは、経営陣の承認を得ることです。これにより、ポリシーが組織のビジョンと価値観に合致していること、そして導入と維持に必要なサポートとリソースが確保されることが保証されます。
ISO/IEC 27001 : 2022 リードインプリメンター学習ガイドおよび文書、セクション 5.2 ポリシー ISO/IEC 27001 : 2022 リードインプリメンター情報キット、12 ページ、情報セキュリティポリシー

質問: **101**
ある組織は、社内の機密エリアや施設への安全なアクセスを確保するために、新しい認証方法を採用しました。この方法では、すべての従業員に二要素認証（パスワードとQRコード）の使用を義務付けています。この管理方法は文書化され、標準化され、すべての従業員に周知されていますが、その使用は 個人の判断に委ねられており、不備が検出される可能性が高い」状況です。この管理方法は、どのレベルの成熟度に該当するでしょうか？
A. 最適化済み

B. 定義済み
C. 定量的に管理
正解**: (**正解を表示します**)**
説明
ISO/IEC 27001:2022 リード実装者の目的と内容によれば、情報セキュリティ管理策の成熟度レベルは、プロセス能力の 5 つのレベル (不完全、実行済み、管理済み、確立済み、最適化済み) を定義する ISO/IEC 15504 規格に基づいています。各レベルには、そのレベルのプロセスの特性を記述する一連の属性があります。定義済みレベルは、プロセスのパフォーマンスという属性に対応しており、プロセスが期待される結果を達成していることを意味します 2。この場合、2 要素認証の管理策は文書化、標準化、および伝達されており、明確な目的と期待される結果があることを意味します。しかし、管理策は一貫して実行、監視、または測定されていないため、管理済み、確立済み、または最適化済みという上位レベルの属性を満たしていません。したがって、管理策は定義済みレベルにあり、これは成熟度の 2 番目のレベルです。
参考文献：
1 :ISO/IEC 27001:2022 リードインプリメンターコースパンフレット、5ページ
2 :ISO/IEC 27001:2022 リードインプリメンターコースプレゼンテーション、スライド25

質問**: 102**
シナリオ 5: Bytes は、ハードウェアとソフトウェアの設計、製造、流通を専門とするダイナミックで革新的な企業であり、包括的なネットワークとサポートサービスの提供に重点を置いています。ナイジェリアの活気あるテクノロジーハブであるラゴスに本社を置いています。800 名を超える従業員を擁する多様で献身的なチームがあり、顧客に最先端のソリューションを提供することに情熱を注いでいます。事業の性質上、Bytes は社内および顧客やパートナーとのコラボレーション時に機密データを頻繁に扱います。
顧客、パートナー、そして自社の内部業務において、データを安全に共有する際に生じる課題を認識し、Bytesは強固な情報セキュリティ対策を実施しています。同社は、潜在的な脅威や情報セキュリティリスクを評価し対処するための明確なリスク評価プロセスを採用しています。このプロセスは、Bytesの業務において重要な側面であるISO/EC 27001の要件への準拠を保証します。
当初、Bytes は、その目的と関連があり、意図した情報セキュリティ管理システムの成果を達成する能力に影響を与える外部および内部の問題を特定しました。会社の制御範囲外の外部の問題には、社会的および文化的ダイナミクス、政治的、法的、規範的、規制環境、財務およびマクロ経済状況、技術開発、自然要因、競争圧力などの要因が含まれます。組織が制御できる内部の問題には、会社の文化、ポリシー、目標、戦略、ガバナンス構造などの側面が含まれます。
役割と責任: 採用された標準とガイドライン。ISMS の範囲内のプロセスに影響を与える契約関係: プロセスと手順 リソースと知識能力。物理インフラストラクチャ情報システム。情報フロー。意思決定プロセス。以前の監査とリスク評価の結果。Bytes はまた、ISMS に関連

する利害関係者を特定し、その要件を理解し、それらの要件のうちどれが ISMS で対処されるかを決定することにも重点を置きました。安全なデジタル環境を追求するにあたり、Bytes は最新のテクノロジーを活用し、自動脆弱性スキャンツールを使用して ICT システム内の既知の脆弱なサービスを特定しています。この積極的なアプローチにより、潜在的な弱点に迅速に対処し、全体的な情報セキュリティ体制を強化しています。Bytes は情報セキュリティに対する包括的なアプローチで、さまざまなリスクを特定し評価しました。このプロセス中に、セキュリティ制御を実装したにもかかわらず、Bytes の専門家チームは許容できない残存リスクを特定し、現在、特定された許容できない残存リスクに対処するための具体的なオプションについて不確実性に直面しています。
シナリオ5によると、Bytes社は自社のICTシステムのセキュリティを評価する際に、どのような点を考慮すべきでしょうか？
A. ICTシステムのセキュリティ評価に使用したツールのコスト
B. 環境コンテキストが不足しているため、彼らが使用したツールは偽陽性を生み出す可能性があります
C. ICTシステムの評価を担当するITチームのスキルと専門知識
正解: **(**正解を表示します**)**

質問: **103**
シナリオ 8: SunDee は、米国カリフォルニア州に本社を置くアメリカのバイオ医薬品会社です。同社は、心血管疾患、腫瘍、骨の健康、炎症に重点を置いた新しいヒト治療薬の開発を専門としています。同社は、過去 2 年間、SO/IEC 27001 に基づく情報セキュリティ管理システム (ISMS) を導入してきました。しかし、ISMS のパフォーマンスと有効性を監視または測定しておらず、定期的な管理レビューも実施していませんでした。再認証監査の直前に、同社は内部監査を実施することにしました。また、ほとんどの従業員に、過去 2 年間の各部門の書面による個人レポートをまとめるよう依頼しました。これにより、生産部門の人員が最適人数を下回り、会社の在庫が減少しました。
テッサはサンディーの内部監査員でした。50人の異なる従業員によって複数のレポートが作成されたため、内部監査プロセスは計画よりもはるかに時間がかかり、非常に一貫性がなく、定性的な尺度は全くありませんでした。テッサは、サンディーがISMSのパフォーマンスを適切に評価する必要があると結論付けました。彼女は、サンディーのISMSパフォーマンス評価の怠慢を重大な不適合と定義し、不適合の説明、監査結果、および推奨事項を含む不適合レポートを作成しました。さらに、テッサはサンディーがこれらの問題を解決できるようにする新しい計画を作成し、それを経営陣に提示しました。サンディーの怠慢はISMS認証にどのように影響しますか？シナリオ8を参照してください。
A. SunDeeはISMSの有効性を評価するための内部監査を実施したため、ISMS認証を更新します。
B. SunDeeは計画された間隔で経営レビューを実施していないため、ISMS認証を更新できない可能性がある。

C. 内部監査が予定より長引いたため、SunDeeはISMS認証を更新できない可能性があります。
正解: **(**正解を表示します**)**
説明
ISO/IEC 27001:2013の9.3項によれば、組織の経営陣は、ISMSの継続的な適合性、妥当性、および有効性を確保するために、計画された間隔でISMSをレビューしなければなりません。経営陣によるレビューでは、前回の経営陣によるレビューで実施された措置の状況、外部および内部の問題の変化、ISMSのパフォーマンスと有効性、利害関係者からのフィードバック、リスク評価と対策の結果、および継続的改善の機会を考慮する必要があります。経営陣によるレビューは、ISMSの方針と目標、リソース、リスクと機会、および改善に関連する決定と行動につながるものでなければなりません。経営陣によるレビューは、経営陣のISMSへのコミットメントと関与、および組織の戦略的方向性との整合性を示す重要なプロセスです。経営陣によるレビューは、内部監査および認証監査への情報提供にもなります。SunDeeは定期的なマネジメントレビューを実施しておらず、条項9.3の要件を満たしていません。これはISMS認証の更新を危うくする重大な不適合です。認証機関は、SunDeeがマネジメントレビューを実施したかどうか、また、そのレビューが効果的かつ文書化されているかどうかを確認します。SunDeeがマネジメントレビューの証拠を提示できない場合、認証を更新する前に是正措置を講じ、フォローアップ監査を受ける必要があります。あるいは、SunDeeが指定された期間内に不適合に対処しない場合、認証機関は認証を一時停止または取り消す可能性があります。
参考文献：
ISO/IEC 27001:2013、情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステム - 要求事項、9.3項 PECB、ISO/IEC 27001 リードインプリメンターコース、モジュール9 :ISO/IEC 27001に基づくISMSのパフォーマンス評価、測定、および監視 PECB、ISO/IEC 27001 リードインプリメンター試験準備ガイド、セクション9 :ISO/IEC 27001に基づくISMSのパフォーマンス評価、測定、および監視

質問**: 104**
シナリオ1：
HealthGenicは、カナダのトロントで患者に包括的な医療サービスを提供する大手総合医療機関です。同社は、患者の健康状態のモニタリング、予約のスケジュール設定、カスタマイズされた医療レポートの作成、患者データの安全な保管、そして患者、医師、臨床検査技師などの様々な関係者間の円滑なコミュニケーションを促進するために、ウェブベースの医療ソフトウェアプラットフォームを多用しています。
組織のサービス拡大と需要増加に伴い、頻繁かつ長期にわたるサービス中断が頻繁に発生するようになり、患者ケアや事務処理に重大な支障をきたすようになった。そこで、HealthGenicは直面するリスクの深刻度を評価するため、包括的なリスク分析を開始した。

リスク分析の結果をリスク基準と比較し、リスクとその重大性が許容範囲内か、あるいは許容できる範囲かを判断しようとした際、HealthGenicはキャパシティプランニングとインフラストラクチャの回復力に重大な欠陥があることに気づきました。この問題の緊急性を認識したHealthGenicは、自社プラットフォームを担当するソフトウェア開発会社に連絡を取りました。ソフトウェア開発会社は、医療技術、データ管理、およびコンプライアンス規制に関する専門知識を活用し、サービスの中断を無事解決しました。
しかしながら、HealthGenicはユーザーアクセス制御への不正な変更も発見しました。その結果、一部の医療報告書が改ざんされ、医療記録が不完全かつ不正確になっていました。同社はユーザーアクセス制御への意図しない変更を速やかに認め、修正しました。これらの変更の根本原因を分析した結果、HealthGenicはIT部門内の職務分掌に関する脆弱性を特定しました。この脆弱性により、システム管理権限を持つ担当者がユーザーアクセス制御も管理できてしまっていたのです。
そのため、HealthGenicは、職務分掌、ジョブローテーション、職務記述書、承認プロセスなど、組織構造に関連する管理を優先的に行うことを決定した。
サービス中断の影響に対応するため、ソフトウェア開発会社はクラウドプラットフォーム上でホストされるスケーラブルなアーキテクチャを採用することでインフラストラクチャを刷新し、需要に基づいた動的なリソース割り当てを可能にした。厳密な負荷テストとパフォーマンス最適化を実施し、潜在的なボトルネックを特定して対処することで、システムがユーザー負荷の増加に円滑に対応できるようにした。
さらに、同社は不正アクセスとデータ改ざんについて速やかに評価を行った。
インターンを含む全従業員がデータセキュリティの重要性と患者情報の適切な取り扱いを認識できるよう、HealthGenicは従業員研修、管理職によるレビュー、内部監査に特化した管理策を導入しました。さらに、患者データの機密性を考慮し、HealthGenicは多要素認証などの強力な認証方法を含む厳格な機密保持対策を実施しました。
HealthGenicは、直面する課題に対応するため、安全なクラウドコンピューティング環境を確保することの重要性を認識しました。そして、クラウドインフラストラクチャと運用方法のセキュリティを評価 強化するために特別に設計された、包括的な自己評価を開始しました。
シナリオ1に基づき、HealthGenicはどのような種類の対策を優先することに決定しましたか？
A. 技術管理
B. 管理統制
C. 経営管理
正解: **(**正解を表示します**)**

質問: **105**
シナリオ2 :Beautyは、最近従来の小売販売からeコマースモデルに移行した化粧品会社です。経営陣は、自社で独自のプラットフォームを構築し、オンライン送金に対応したオンラ

イン決済システムを運営する外部プロバイダーに決済処理を委託することを決定しました。
このビジネスモデルの変革に伴い、重要な資産に関連する脅威や脆弱性を特定し、それに基づいて多数のセキュリティ対策が実施されました。顧客情報を保護するため、ビューティー社の従業員は機密保持契約に署名する必要がありました。さらに、同社はすべてのユーザーアクセス権限を見直し、権限のある担当者のみが機密ファイルにアクセスできるようにし、新たな職務分掌図を作成しました。
しかし、この移行はITチームにとって困難なものでした。eコマースモデルへの移行後まもなく、セキュリティインシデントが発生したのです。インシデントを調査した結果、チームは、マルウェア対策ソフトウェアが旧式であったために、攻撃者がファイルへのアクセス権を不正に取得し、顧客の名前や住所などの顧客情報を漏洩させたという結論に至りました。
ITチームは、旧型のマルウェア対策ソフトウェアの使用を中止し、同様の事態が発生した場合に悪意のあるコードを自動的に削除する新しいソフトウェアを導入することを決定しました。新しいソフトウェアは、社内のすべてのワークステーションにインストールされました。インストール後、チームは最新のマルウェア定義でソフトウェアを更新し、常に最新の状態を保つために自動更新機能を有効にしました。さらに、機密情報へのアクセス時にユーザーIDとパスワードを要求する認証プロセスを確立しました。
さらに、ビューティー社は、システムおよびネットワークセキュリティの重要性に対する意識を高めるため、ITチームや機密情報にアクセスするその他の従業員を対象に、情報セキュリティに関する啓発セッションを複数回実施した。
以下の記述のうち、Beauty社がインシデントの発生を回避するのに役立つ管理統制を実施していることを示唆しているのはどれですか？シナリオ2を参照してください。
A. ビューティー社の従業員は機密保持契約書に署名しました
B. ビューティーは、ITチームや機密情報にアクセスできる他の従業員向けに、情報セキュリティに関する意識向上セッションを複数回実施した。
C. ビューティーが職務分担表を更新しました
正解: **B** (コメントを発表する)
管理統制とは、人間の行動に影響を与えることでセキュリティインシデントの発生を防止または軽減することを目的とした管理上の措置です。これには、ポリシー、手順、ガイドライン、基準、トレーニング、および啓発プログラムが含まれます。シナリオ2では、Beauty社はITチームおよび機密情報にアクセスできるその他の従業員向けに情報セキュリティ啓発セッションを実施することで、管理統制を実施しています。これらのセッションは、システムおよびネットワークセキュリティの重要性、潜在的な脅威と脆弱性、およびインシデントの発生を回避するために従うべきベストプラクティスについて従業員を教育することを目的としています。従業員の意識と知識レベルを高めることで、Beauty社は情報資産のセキュリティを損なう可能性のある人的ミスや過失を減らすことができます。

質問: **106**

SABSAモデルのどの層が、セキュリティアーキテクチャをビジネス要件や推進要因に整合させることに重点を置いていますか？
A. コンテクスチュアル ･アーキテクチャ
B. コンポーネントアーキテクチャ
C. 論理アーキテクチャ
正解: **(**正解を表示します**)**
SABSA（Sherwood Applied Business Security Architecture）モデルは、リスク主導型のエンタープライズ情報セキュリティアーキテクチャを開発するための広く受け入れられているフレームワークです。このモデルは6つのレイヤーで構成されています。
コンテキスト、概念、論理、物理、コンポーネント、運用。これらのうち、コンテキストアーキテクチャは最上位層であり、セキュリティアーキテクチャをビジネスの目標、推進要因、要件に合致させるように特別に設計されています。
具体的には、コンテキストアーキテクチャ層は次のような質問に答えます。
* その企業はどのような成果を達成しようとしているのか？
* 利害関係者は誰ですか？
* 重要なビジネス資産とは何ですか？
* リスク許容度とリスク耐性レベルはどのくらいですか？このレイヤーは、後続のすべてのレイヤーの基盤を確立し、セキュリティ戦略がビジネス目標と戦略的方向性を直接サポートすることを保証します。
したがって、オプションA :コンテキストアーキテクチャが正解となります。これは、セキュリティアーキテクチャをビジネス要件と推進要因に整合させることに重点を置いているからです。
ISO/IEC 27001:2022との関連性SABSAモデルはISO/IEC 27001:2022に明示的に含まれているわけではありませんが、特にビジネス戦略に沿った効果的な情報セキュリティマネジメントシステム（ISMS）の設計と実装をサポートするという点で、ISO規格を補完するものです。
ISO/IEC 27001:2022では、以下の条項がセキュリティアーキテクチャとビジネス要件との整合性をサポートしています。
* 条項 4.1 - 「組織とその状況の理解」：組織は、その目的に関連し、ISMS の意図する結果を達成する能力に影響を与える外部および内部の問題を特定しなければならない。」
* 条項 4.2 - 「利害関係者のニーズと期待の理解」：組織は、ISMS に関連する利害関係者と、これらの利害関係者の要求事項を決定しなければならない。」これらの条項は、より広範なビジネス環境、利害関係者の期待、および戦略的なビジネス推進要因を理解することの重要性を強調しています。これはまさに、SABSA のコンテキスト レイヤーが対処するように設計されているものです。
要約すると、SABSAのコンテキストアーキテクチャ層は、ISOの意図と構造に直接合致している。
/IEC 27001:2022 第4項に準拠しているため、この質問に対する正しい検証済みの選択肢となります。

質問: **107**
シナリオ10に基づくと、無効な電気部門は監査学習リーダーの交代を要求する正当な理由を提供しましたか？
A. いいえ、被監査企業は、監査人が被監査企業で勤務したことがある場合にのみ、監査人の交代を要求できるからです。
B. はい、なぜなら被監査企業は、主要な競合他社で勤務経験のある監査人を交代させるよう要求できるからです。
C. いいえ、主要な競合他社に認証勧告を発行することは利益相反には当たらないためです。
正解: **(**正解を表示します**)**

質問: **108**
ある会社が新しいビルに移転した。移転から数週間後、取締役のオフィスに予告なしに訪問者が現れた。調査の結果、訪問者用パスは社員用パスと同じアクセス権限を持つことが判明した。どのようなセキュリティ対策を講じていれば、このような事態を防げただろうか？
A. 物理的なセキュリティ対策
B. 組織的なセキュリティ対策
C. 技術的なセキュリティ対策
正解: **(**正解を表示します**)**

質問: **109**
あるテクノロジー企業は、ここ数年で事業を急速に拡大してきました。サーバー、データベース、通信ツールなどで構成される情報システムは、日々の業務において不可欠な部分となっています。しかし、急速な成長とデータ量の増加により、同社は情報システムの飽和状態に直面しています。この飽和状態は、応答時間の遅延、ダウンタイムの増加、そして膨大なデータ量の管理困難といった問題を引き起こしています。この脅威は、どのカテゴリーに分類されるでしょうか？
A. インフラ障害

B. 技術的な不具合
C. 機能の妥協
正解: **B** (コメントを発表する)
データフローの増加と急速な拡張による応答時間の遅延、ダウンタイム、システム飽和などは、技術的な障害に分類されます。これらの問題は、ITシステム（ハードウェア、ソフトウェア、通信インフラ）の限界や不具合に直接関係しています。
ISO/IEC 27005:2022では、このような事象を技術的障害として分類しています。
「技術的障害：情報システムの可用性とパフォーマンスに影響を与える、過負荷、飽和、または故障を含む、ITシステム、ソフトウェア、またはインフラストラクチャの障害。」
- ISO/IEC 27005:2022、8.2.2

質問: **110**
シナリオ 8: SunDee は、米国カリフォルニア州に本社を置くアメリカのバイオ医薬品会社です。同社は、心血管疾患、腫瘍、骨の健康、炎症に重点を置いた新しいヒト治療薬の開発を専門としています。同社は、過去 2 年間、SO/IEC 27001 に基づく情報セキュリティ管理システム (ISMS) を導入してきました。しかし、ISMS のパフォーマンスと有効性を監視または測定しておらず、定期的な管理レビューも実施していませんでした。再認証監査の直前に、同社は内部監査を実施することにしました。また、ほとんどの従業員に、過去 2 年間の各部門の書面による個人レポートをまとめるよう依頼しました。これにより、生産部門の人員が最適人数を下回り、会社の在庫が減少しました。
テッサはサンディーの内部監査員でした。50人の異なる従業員によって複数のレポートが作成されたため、内部監査プロセスは計画よりもはるかに時間がかかり、非常に一貫性がなく、定性的な測定がまったくありませんでした。テッサは、サンディーがISMSのパフォーマンスを適切に評価する必要があると結論付けました。彼女は、サンディーのISMSパフォーマンス評価の怠慢を重大な不適合と定義し、不適合の説明、監査結果、および推奨事項を含む不適合レポートを作成しました。さらに、テッサは、サンディーがこれらの問題を解決できるようにする新しい計画を作成し、それを経営陣に提示しました。シナリオ8に基づいて、サンディーは監視および測定プロセスに関してISO/IEC 27001の要求事項に準拠していますか?
A. はい。なぜなら、規格では監視および測定フェーズをいつ実施すべきかが規定されていないからです。
B. はい、なぜなら基準では監視・測定段階を2年ごとに実施することが求められているからです。
C. いいえ、規格ではそのようなプロセスをいつ実施すべきかは規定されていませんが、企業は監視および測定プロセスを導入する必要があります。
正解: (正解を表示します)
説明
ISO/IEC 27001:2022の9.1項によれば、組織は以下を決定しなければならない。

監視および測定する必要があるもの（情報セキュリティプロセスおよび管理、情報セキュリティパフォーマンス、ISMSの有効性など）、有効かつ信頼できる結果を確保するための監視、測定、分析および評価の方法、監視および測定を実施する時期、監視および測定を行う者、監視および測定結果を分析および評価する者、結果を伝達し、意思決定および改善に活用する方法。
組織は、監視および測定結果の証拠として、文書化された情報を保管しなければならない。
この規格は、監視および測定の具体的な頻度や方法を規定していませんが、組織が自らの状況、目的、リスク、機会に適した、明確に定義され文書化されたプロセスを持つことを求めています。また、組織は、監視および測定の結果を分析・評価し、ISMSのパフォーマンスと有効性を判断するとともに、不適合、ギャップ、改善の機会を特定する必要があります。
このシナリオでは、SunDee社は監視・測定プロセスを導入しておらず、ISMSのパフォーマンスと有効性を定期的に監視・測定していなかったため、これらの要件を満たしていませんでした。また、有効かつ信頼できる方法を使用しておらず、結果を共有して改善に活用することもしていませんでした。
したがって、サンディー社によるISMSパフォーマンス評価の怠慢は、テッサが正しく指摘したように、重大な不適合であった。
参照: ISO/IEC 27001:2022、情報セキュリティ、サイバーセキュリティおよびプライバシー保護 - 情報セキュリティマネジメントシステム - 要求事項、9.1項。PECB ISO/IEC 27001 リードインプリメンターコース、モジュール9: モニタリング、測定、分析および評価。

質問**: 111**
シナリオ5 :Operazeは、世界中の様々な企業向けにアプリケーションを開発する小規模なソフトウェア開発会社です。最近、同社はデジタル環境での事業運営から生じる可能性のある情報セキュリティリスクを評価するため、リスクアセスメントを実施しました。侵入テスト、レスティングテスト、コードレビューなど、様々なテスト手法を用いて、同社はICTシステムにおけるいくつかの問題点を特定しました。これには、不適切なユーザー権限、セキュリティ設定の誤り、安全でないネットワーク構成などが含まれます。これらの問題を解決し、情報セキュリティを強化するため、OperazeはISO/IEC 27001に基づいた情報セキュリティマネジメントシステム（ISMS）を導入することを決定しました。
Operazeは小規模企業であるため、ITチーム全体がISMS導入プロジェクトに関与しました。まず、同社は業務要件と内部および外部環境を分析し、主要なプロセスと活動を特定し、関係者を特定して分析しました。さらに、Operazeの経営陣は、ISMSの範囲に会社のほとんどの部門を含めることを決定しました。定義された範囲には、組織的および物理的な境界が含まれます。ITチームは情報セキュリティポリシーを作成し、すべての関係者に伝達しました。さらに、セキュリティ問題の詳細を定めるための他の具体的なポリシーが開発され、すべての関係者に役割と責任が割り当てられました。
その後、人事部長はISMSによって作成される書類はISMSの価値に見合わないため、ISMSの導入を中止すべきだと主張した。しかし、経営陣はこの主張は妥当ではないと判断し、ISMSの利点を関係者全員に説明するための啓発セッションを開催した。

Operaze は、自社の物理サーバーをサードパーティのインフラストラクチャ上の仮想サーバーに移行することを決定しました。新しいクラウド コンピューティング ソリューションは、会社にさらなる変化をもたらしました。一方、Operaze の経営陣は、効果的な ISMS を導入するだけでなく、ISMS 運用のスムーズな実行も確保することを目指しました。この状況で、Operaze の経営陣は、情報セキュリティ戦略を実行するために外部の専門家のサービスが必要であると結論付けました。一方、IT チームは、ISMS の範囲の変更を開始し、会社のプロセスに必要な変更を実施することを決定しました。
シナリオ5に基づき、OperazeはISMSの円滑な運用を確保するために、どの委員会を設置すべきでしょうか？
A. 情報セキュリティ委員会
B. 運営委員会
C. 運営委員会
正解: **(**正解を表示します**)**
説明
ISO/IEC 27001:2022の5.1項によれば、組織の最高経営陣はISMSのリーダーシップとコミットメントを確保する責任を負います。ただし、最高経営陣は、ISMSを監督し、その導入と運用に関するガイダンスとサポートを提供する情報セキュリティ委員会に、その責任の一部を委任することができます。情報セキュリティ委員会には、組織のさまざまな部門、機能、または階層の代表者、および外部の専門家やコンサルタントが含まれる場合があります。情報セキュリティ委員会は、次のようなさまざまな役割と責任を担う可能性があります。
情報セキュリティポリシーと目標の設定
リスク評価およびリスク処理の方法論と基準の承認 リスク評価およびリスク処理の結果と計画のレビューと承認 ISMS のパフォーマンスと有効性の監視と評価 内部および外部監査計画とレポートのレビューと承認 是正措置と予防措置の開始と承認 すべての関係者への ISMS の伝達と促進 ISMS が組織の戦略的方向性と目標に合致していることの確保 ISMS に必要なリソースと能力の確保 ISMS の継続的な改善の確保 したがって、シナリオ 5 では、Operaze は ISMS の円滑な運用を確保するために情報セキュリティ委員会を作成する必要があります。この委員会は、ISMS の実装と運用に必要なリーダーシップ、ガイダンス、およびサポートを提供します。
参考文献 :ISO/IEC 27001:2022、5.1項 ;PECB ISO/IEC 27001 リードインプリメンター コース、モジュール4、スライド9。

質問**: 112**
質問 :
経営陣による評価に関する記述のうち、正しいものはどれですか？
A. 経営レビューは組織内のさまざまなレベルで実施されます
B. 経営レビューは毎月実施しなければならない
C. 経営陣は、経営評価プロセスの最終的な責任を組織で働く個人に委任することができる。

正解: (正解を表示します)
ISO/IEC 27001:2022 条項 9.3 - マネジメントレビュー:
経営陣は、組織のISMSが継続的に適切、妥当、かつ有効であることを確認するため、計画された間隔でISMSをレビューしなければならない。」最終的な責任は経営陣にあるものの、より広範な可視性と整合性を確保するために、複数の組織レベルでレビューを実施することができる。ISO/IEC 27004は、戦術レベルおよび運用レベルでのレビューもサポートしている。
月次レビューの義務はありません。選択肢Cは誤りです。なぜなら、管理職は最終的な責任を完全に委任することはできず、サポート的な役割のみを委任できるからです。

質問: **113**
NeuroTrustMedは、韓国ソウルに本社を置く大手医療技術企業です。同社は、神経疾患の早期診断と治療計画に使用されるAI支援型神経画像ソリューションの開発を専門としています。機密性の高い患者の健康記録や医療研究データを扱うデータ集約型企業として、NeuroTrustMedはサイバーセキュリティと規制遵守を非常に重視しています。同社は過去3年間、ISO/IEC 27001認証を取得したISMSを維持しています。新たな脅威への対応、医療診断におけるイノベーションの支援、ステークホルダーの信頼維持のため、ISMSを継続的に見直し、改善しています。継続的改善への取り組みの一環として、NeuroTrustMedは潜在的な不適合を積極的に追跡し、根本原因分析を実施し、是正措置と予防措置を実施し、すべての変更が文書化され、同社の戦略目標と整合していることを確認しています。地域をまたいだデータ処理に影響を与える新たなデータ保護規制が施行された際、情報セキュリティチームは現行のポリシーと新規制とのギャップ評価を実施しました。その後、コンプライアンスを満たすために関連文書とプロセスを更新しました。これらの改訂を受けて、NeuroTrustMedはISMS文書を更新し、改善登録簿に新しいエントリを追加しました。構造化されたスプレッドシート形式で管理されている登録簿には、固有の変更番号、更新の説明、法的コンプライアンスによる優先度の高い分類、開始日と完了日、および情報セキュリティマネージャーによる承認が含まれていました。ほぼ同時期に、定期的な管理レビュー中に、情報セキュリティチームはオンボーディングエラーのパターンも特定しました。これらのエラーはデータ漏洩には至っていませんでしたが、不正アクセスのリスクがありました。これに対応して、オンボーディング手順が改訂され、アクセスを許可する前に正確性を確保するための自動検証ステップが追加されました。根本原因を理解するために、チームはプロビジョニングプロセスに関するデータを収集しました。プロセスログを分析し、オンボーディングスタッフにインタビューを行い、アクセスエラーをHRからITへの引き継ぎワークフローにおける設定ミスのあるステップまで追跡しました。チームは変更を実装する前に、テストケースを通じてこの発見を検証しました。確認後、情報セキュリティチームはISMSログに不適合を記録しました。文書には、問題の説明、影響を受けたシステム、影響を受けたユーザー、およびアクセス管理に関連する潜在的な影響に関する簡単なリスク評価が含まれていました。上記のシナリオに基づいて、次の質問に答えてください。
シナリオ10を参照して、認証決定委員会の構成は適切でしょうか？

A. はい、認証の決定を下す人と監査を実施した人は異なるからです。
B. いいえ、委員会は監査チームのメンバーのみで構成され、監査に関わっていない他の専門家は含めるべきではありませんでした。
C. いいえ、委員会には監査チームのメンバー1名と、認証機関に勤務するその他の個人を含める必要があります。
正解: **A** (コメントを発表する)
ISO/IEC 27001の認証制度においては、認証決定は監査自体に参加していない者によって行われることが基本要件となっている。この分離によって、認証決定の客観性、独立性、および信頼性が確保される。
ISO/IEC 27001はISMSの要求事項を定義しているが、認証決定のガバナンスについてはISO/IEC 17021-1で規定されており、以下のことが求められている。
監査チームは認証の決定を下しません
決定は、監査とは無関係の有能な担当者によって行われる。
シナリオ10では、認証決定委員会が監査チームとは別の個人で構成されていたことが示されており、これはこの要件を満たしている。
選択肢Bは誤りです。意思決定委員会は監査チームのメンバーだけで構成されるべきではありません。
選択肢Cは誤りです。監査チームのメンバーを意思決定機関に含めると、独立性が損なわれるからです。
この構造は、ISMS（情報セキュリティマネジメントシステム）の監査を行う認証機関を規定し、公平な認証決定の必要性を強調するISO/IEC 27006にも合致している。

質問: **114**
文書の分類を変更する権限を持つのは誰ですか？
A. 文書の所有者
B. 文書の所有者の管理者
C. 文書の管理者
D. 文書の著者
正解: (正解を表示します)

質問: **115**
シナリオ7 :サイテックシールド
アイルランドのダブリンに拠点を置くCyTekShieldは、デジタルリスク管理とエンタープライズセキュリティソリューションを専門とするサイバーセキュリティコンサルティングプロバイダーです。複数のセキュリティインシデントに直面した後、CyberTekShieldは、SadieとNiamhをチームに迎え入れ、情報セキュリティチームを拡張しました。このチームは、インシデント対応、セキュリティアーキテクチャ、フォレンジックの3つの主要部門で構成されています。Sadieは、スクリーニングサブネットネットワークアーキテクチャの実装の一環として、非武装地帯をCyTekShieldのプライベートネットワークとパブリックアクセス可能なリソースから分離します。さらに、Sadieは、予期せぬインシデント

を包括的に評価し、その原因を分析し、潜在的な影響を評価します。的な影響を評価します。彼女はまた、セキュリティ戦略とポリシーを策定しました。一方、フォレンジック調査の専門家であるNiamhは、証拠目的でさまざまなデータの記録を作成する責任を負います。これを効果的に行うために、彼女はまず、作成する記録の種類、その保管場所、特定の記録タイプに必要な形式と内容を概説する会社の情報セキュリティインシデント管理ポリシーを確認しました。
情報セキュリティインシデントに関連する証拠の取り扱いプロセスを支援するため、CyTekShieldは社内手順を確立しました。これらの手順により、証拠が社内で適切に識別、収集、および保存されることが保証されます。CyTekShieldの手順では、さまざまなストレージメディアに保存された記録の取り扱い方法が規定されており、デバイスの電源がオンかオフかにかかわらず、すべての証拠が元の状態で保護されることが保証されます。
CyTekShieldの情報セキュリティ対策強化イニシアチブの一環として、Niamhは重大な変更が提案された場合にのみ情報セキュリティリスク評価を実施し、これらのリスク評価の結果を文書化します。リスク評価プロセスの完了後、Niamhは情報セキュリティリスクに対処するための計画を策定および実施し、リスク対処の結果を文書化する責任を負います。
さらに、情報セキュリティのコミュニケーション計画を実行する際、CyTekShield の経営陣は新製品開発のロードマップを作成する責任を負っていました。このアプローチにより、同社はセキュリティ対策を製品開発の取り組みと整合させることができ、セキュリティを事業運営のあらゆる側面に統合するというコミットメントを示すことができます。CyTekShield は、Web またはアプリケーション プログラミング インターフェイス (API) を介してアクセスされるクラウド ベースのアプリを含むクラウド サービス モデルを使用しています。すべてのクラウド サービスはクラウド サービス プロバイダーによって提供され、データは CyTekShield によって管理されます。これにより、独自のセキュリティ上の考慮事項が生じ、この環境でデータとシステムが保護されていることを確認することが情報セキュリティ チームの主要な焦点となります。CyTekShield は、Web またはアプリケーション プログラミング インターフェイス (API) を介してアクセスされるクラウド ベースのアプリを含むクラウド サービス モデルを使用しています。すべてのクラウド サービスはクラウド サービス プロバイダーによって提供され、データは CyTekShield によって管理されます。これにより、独自のセキュリティ上の考慮事項が生じ、この環境でデータとシステムが保護されていることを確認することが情報セキュリティ チームの主要な焦点となります。
質問：
CyTekShieldは、情報セキュリティ関連の事象に関する証拠の取り扱いについて、適切に対応してきたか？
A. いいえ - 証拠品の取り扱いに関わる職員に対する適切な研修が含まれていないためです。
B. はい、証拠の取り扱いについて適切に対処しています。
C. いいえ。証拠収集のプロセスが十分に詳細に説明されていないためです。
正解: **(**正解を表示します**)**

ISO/IEC 27037:2012およびISO/IEC 27002:2022の8.16項 監視活動」および6.8項 情報セキュリティイベントの報告」では、以下の点が強調されています。
証拠は、捜査において信頼性と証拠能力を維持するために、適切に特定、収集、保存、保護されなければならない。」CyTekShieldのアプローチは、電源オン/オフ状態のデバイスの保護、コンテンツのフォーマット/場所の定義、承認された基準への準拠など、主要な証拠取り扱い方法すべてを網羅しています。

質問: **116**
シナリオ2 :Beautyは、最近従来の小売販売からeコマースモデルに移行した化粧品会社です。経営陣は、自社で独自のプラットフォームを構築し、オンライン送金に対応したオンライン決済システムを運営する外部プロバイダーに決済処理を委託することを決定しました。
このビジネスモデルの変革に伴い、重要な資産に関連する特定された脅威と脆弱性に基づいて、多数のセキュリティ対策が実施されました。これは、顧客の情報を保護するためです。
ビューティー社の従業員は機密保持契約書に署名しなければならなかった。さらに、同社はすべてのユーザーアクセス権限を見直し、許可された担当者のみが機密ファイルにアクセスできるようにし、新たな職務分掌図を作成した。
しかし、この移行はITチームにとって困難なものでした。eコマースモデルへの移行後まもなく、セキュリティインシデントが発生したのです。インシデントを調査した結果、チームは、マルウェア対策ソフトウェアが旧式であったために、攻撃者がファイルへのアクセス権を不正に取得し、顧客の名前や住所などの顧客情報を漏洩させたという結論に至りました。
ITチームは、旧型のマルウェア対策ソフトウェアの使用を中止し、同様の事態が発生した場合に悪意のあるコードを自動的に削除する新しいソフトウェアを導入することを決定しました。新しいソフトウェアは、社内のすべてのワークステーションにインストールされました。インストール後、チームは最新のマルウェア定義でソフトウェアを更新し、常に最新の状態を保つために自動更新機能を有効にしました。さらに、機密情報へのアクセス時にユーザーIDとパスワードを要求する認証プロセスを確立しました。
さらに、ビューティー社は、システムおよびネットワークセキュリティの重要性に対する意識を高めるため、ITチームや機密情報にアクセスするその他の従業員を対象に、情報セキュリティに関する啓発セッションを複数回実施した。
上記のシナリオに基づいて、次の質問に答えてください。
シナリオ2に基づくと、この攻撃によって侵害されなかった情報セキュリティの原則はどれですか？
A. 完全性
B. 入手可能性
C. 機密保持
正解: **A** (コメントを発表する)

質問: **117**
リスク保持の例となる記述はどれですか？
A. ある組織は、軽微なバグがまだ修正されていないにもかかわらず、ソフトウェアをリリースすることを決定しました。
B. ある組織がデータ損失防止ソフトウェアを導入しました
C. 激しい嵐のため、建設現場での作業を中止する組織
正解: **(**正解を表示します**)**
ISO/IEC 27001:2022 リードインプリメンターによると、リスク保持は、組織が許容できないリスクに対処するために選択できる 4 つのリスク処理オプションの 1 つです。リスク保持とは、組織がリスクの発生確率や影響を軽減するための措置を講じることなく、リスクを受け入れることを意味します。これは、対処するにはコストがかかりすぎる、または非現実的なリスク、あるいは発生確率や影響が低いリスクに適用されます。したがって、リスク保持の例としては、軽微なバグがまだ修正されていないにもかかわらず、組織がソフトウェアをリリースすることを決定する場合が挙げられます。これは、組織がバグのあるソフトウェアをリリースするリスクを評価し、バグが重大ではないか、バグを修正するコストがメリットを上回るため、それが許容できると判断したことを意味します。

質問: **118**
情報セキュリティ手順の策定、見直し、検証には、とりわけ誰が関与すべきでしょうか？
A. 外部の専門家
B. 情報セキュリティ委員会
C. ISMS運用を担当する従業員
正解: **(**正解を表示します**)**
ISO/IEC 27001:2022の7.5.1項によれば、組織は、ISMSおよびこの文書で要求される文書化された情報が、必要な場所とタイミングで利用可能かつ使用に適しており、かつ適切に保護されていることを保証するために管理されなければならない。これには、文書化された情報が適切かつ十分であるかどうかのレビューと承認を受けることが含まれる。情報セキュリティ手順は、ISMSプロセスの運用と情報セキュリティ管理策の実装をサポートする文書化された情報の一部である。したがって、情報セキュリティ手順は、ISMSを監督し、組織の目標と戦略との整合性を確保する責任を負うグループである情報セキュリティ委員会によって作成、レビュー、および検証されなければならない。情報セキュリティ委員会には、組織のさまざまな機能と階層の代表者、および必要に応じて外部の専門家を含めるべきである。情報セキュリティ委員会はまた、情報セキュリティ手順が関係する従業員およびその他の利害関係者に伝達され、必要に応じて定期的にレビューおよび更新されることを保証しなければならない。
参照：
ISO/IEC 27001:2022、情報セキュリティ、サイバーセキュリティおよびプライバシー保護 - 情報セキュリティマネジメントシステム - 要求事項、条項5.3、7.5.1、および9.3 ISO/IEC 27001:2022 リードインプリメンターの目的と内容、4および5

質問: **119**
シナリオ 4: L.JXfUI デザイン、QA およびソフトウェア テスト、モバイル アプリケーション開発を専門とする UX Software 社は、情報セキュリティ対策を改善する必要性を認識し、ISO/IEC 27001 に基づく ISMS を導入しました。この戦略的な取り組みは、業界標準およびベスト プラクティスに準拠し、社内外で共有される情報の機密性、可用性、および完全性を強化することを目的としていました。
ISMSをUX Softwareの既存プロセスに統合し、これらのプロセスがISMSのフレームワークに準拠するように調整されたことは、組織の情報セキュリティへの取り組みを強調する重要な節目となりました。UX Softwareは、ISMSフレームワークに沿うようこれらの手順を綿密に調整し、状況や文化に即した適切なものとなるよう配慮するとともに、不整合を回避しました。この積極的な姿勢は、従業員に安心感を与え、顧客からの信頼を高め、業務全体を通して機密データの保護を確実なものにしました。
UX Softwareの経営陣は、この取り組みを推進するため、ISMSの適用範囲をISO 1EC 27003に準拠させるべく行動を起こしました。UX Softwareの経営陣の主要メンバーであるSvenは、プロジェクトスポンサーの役割を担いました。これは、適切なリソースでISMSの実装を確実に実行するという重要な役割です。Svenのリーダーシップは、プロジェクトをISO 1EC 27003への準拠へと導く上で極めて重要な役割を果たしました。
UX Softwareは、情報セキュリティへの取り組みと並行して、セキュリティ管理策の技術仕様を適用性声明の正当化セクションに組み込みました。このアプローチは、ISO/IEC 27001の要求事項を満たすという同社のコミットメントを示し、セキュリティ管理策の徹底的な文書化と正当化を保証し、組織全体のセキュリティフレームワークを強化しました。さらに、UX Softwareは、是正措置の有効性を確保し、ISMS文書化情報を管理し、不適合に対処しながらISMSを継続的に改善する責任を負う委員会を設立しました。
ISO/IEC 27001に基づくISMSを導入することで、UX Softwareは情報セキュリティを向上させ、信頼できるパートナーとしての地位を強化しました。この情報セキュリティへの取り組みは、UX Softwareが社内関係者と大切な顧客の利益を守りながら、高品質なソフトウェアソリューションを提供することへの強い決意の証です。
シナリオ4によると、UXソフトウェアにおけるスヴェンの役割は何ですか？
A. ISMSプロジェクトマネージャー
B. ISMSプロジェクトチャンピオン
C. プロジェクトチームのメンバー
正解: **B** (コメントを発表する)
スヴェンは「UX Softwareのトップマネジメントチームの主要メンバーであり、ISMS導入を適切なリソースで確実に実行する責任を担う重要なポジションであるプロジェクトスポンサーの役割を引き受けた」と評されている。プロジェクトスポンサー、あるいはプロジェクトチャンピオンとは、リーダーシップを発揮し、リソースを確保し、ISMSイニシアチブを推進する経営幹部のことである。

経営陣は、ISMSプロジェクトにおける役割と責任を割り当てなければならない。これには、適切なリソースと組織的支援を確保するプロジェクトスポンサーまたは推進役の任命も含まれる。」
- ISO/IEC 27003:2017、5.3項 ;ISO/IEC 27001:2022、5.3項